INSTITUTO DE ESTUDOS SUPERIORES MILITARES

(CURSO DE PROMOÇÃO A OFICIAL GENERAL)

2010/2011

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

DOCUMENTO DE TRABALHO

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IESM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DA MARINHA PORTUGUESA / DO EXÉRCITO PORTUGUÊS / DA FORÇA AÉREA PORTUGUESA.

A CIBERGUERRA.
ESTRUTURA NACIONAL PARA ENFRENTAR AS VULNERABILIDADES – UMA CAPACIDADE MILITAR AUTÓNOMA OU PARTILHADA.

Pedro Jorge Pereira de Melo

Coronel de Transmissões

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

A CIBERGUERRA. ESTRUTURA NACIONAL PARA ENFRENTAR AS VULNERABILIDADES – UMA CAPACIDADE MILITAR AUTÓNOMA OU PARTILHADA.

Pedro Jorge Pereira de Melo

Coronel de Transmissões

Trabalho de Investigação Individual do CPOG 2010/11

Lisboa, IESM, 21 de Junho de 2011

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

A CIBERGUERRA. ESTRUTURA NACIONAL PARA ENFRENTAR AS VULNERABILIDADES – UMA CAPACIDADE MILITAR AUTÓNOMA OU PARTILHADA.

Pedro Jorge Pereira de Melo

Coronel de Transmissões

Trabalho de Investigação Individual do CPOG 2010/11

Orientador:

Coronel PILAV Nuno Manuel de Andrade Maia Gonçalves

Lisboa, IESM, 21 de Junho de 2011

AGRADECIMENTOS

Nunca pensei que a simples execução de um Trabalho de Investigação despertasse tal onda de solidariedade e vontade de ajudar. A começar pela minha mulher Lisa e filho Daniel, que desde cedo se prontificaram a colaborar na pesquisa de informação, passando por todos os camaradas do CPOG 2010/2011 que me forneceram pistas e elementos para investigação, e terminando em todos os que de maneira directa ou indirecta contribuíram para que este trabalho chegasse a bom porto.

Um agradecimento especial ao Cor Teixeira e Cor Fonseca e Sousa pelas longas horas de discussão, que tornaram curtas as viagens semanais entre Porto e Lisboa, e que também se reflectiram no desenvolvimento deste trabalho.

A todos os que se dignarem a ler este trabalho, e que achando que seja útil, façam com que tenha valido a pena a dedicação e o empenho com que abracei este Trabalho de Investigação.

ÍNDICE

Índice de Anexos

Índice de Figuras

Índice de Tabelas

RESUMO

O Trabalho estuda a Ciberguerra e o modo como as Forças Armadas se podem estruturar para melhor enfrentar as ameaças que a enformam. A massificação da Internet mudou o mundo e é consensual que nada alguma vez o mudou tão rapidamente, quanto a Internet o tem feito, trazendo desafios novos, para os quais ainda se procuram as respostas e faz com que a guerra no Ciberespaço seja considerada uma preocupação prioritária e se encontre no topo da agenda dos decisores políticos mundiais e das organizações mandatadas para zelar pela segurança dos Estados.

Num domínio em que o próprio termo Ciberguerra é ainda desconhecido, o trabalho procura fazer luz sobre esta parte da ciência militar, conceptualizando e distinguindo a Ciberguerra daquilo que ela não é, ao mesmo tempo que tenta despertar as consciências para uma ameaça que existindo num mundo virtual formado pelos computadores e pelas redes de computadores, cruzou, cruza e vai continuar a cruzar a barreira do virtual, provocando efeitos físicos e afectando os sistemas vitais de um país como sendo os sistemas de energia, transportes, financeiros e económicos entre outros.

Não pretendendo ser mais um acelerador na corrida, que já começou, às armas no Ciberespaço, o trabalho não deixa de ser uma ferramenta para evidenciar que o Ciberespaço representa um novo ambiente para a projecção de poder que se transforma num novo desafio para as Forças Armadas Portuguesas e ao mesmo tempo numa oportunidade. Se a faceta defensiva da Ciberguerra é mais ou menos pacífica no enquadramento legal da actuação pelos Estados, as componentes ofensiva e exploratória levantam problemas acrescidos que este trabalho não ignora mas aprofunda.

Igualmente aborda as capacidades de Ciberguerra, em todas as suas vertentes, que a Marinha, o Exército e a Força Aérea têm implementado, situando esta percepção no contexto dos Países nossos aliados e da NATO, e parte desse patamar para a visualização do que pode ser feito para melhor enfrentar as ameaças da Ciberguerra, não esquecendo que a universalidade de um Ciberespaço partilhado implica uma resposta global envolvendo tanto organizações nacionais como internacionais, sejam civis sejam militares, com responsabilidades na segurança e defesa dos Estados.

ABSTRACT

The paper studies cyberwar and how the Portuguese Armed Forces can be better structured to deal with the threats it carries. Widespread use of the Internet has changed the world and it is common sense that nothing ever changed it so quickly as Internet, bringing new challenges for which we are still seeking answers and makes war in cyberspace to be considered a priority concern and to be on top of the agenda of politics and organizations mandated to ensure the Countries defenses.

Focusing in one area where the very term cyberwar is almost unknown, the paper tries to shed light on this part of military science, conceptualizing and distinguishing cyberwar from what it is not and at the same time trying to raise awareness of a threat that exists in the virtual world, formed by computers and computer networks that already crossed ,is crossing and will go on crossing the barrier from the virtual, causing physical effects and affecting vital systems of a country such as energy, transportation, financial and economic systems, among others.

Not wishing to be one more accelerator in the race to the arms in Cyberspace, which has already begun, this work is a tool to demonstrate that Cyberspace represents a new environment for power projection, becoming a new challenge and at the same time an opportunity to Portuguese Armed Forces. If defensive aspect of cyberwar is more or less regulated by the Countries legal framework, the offensive and exploratory components pose additional problems that this work does not ignore but deepens.

It also discusses cyberwar capabilities, in all aspects that Navy, Army and Air Force have implemented, placing this perception in the context of the NATO and allied countries, and starts from that level for the visualization of what can be done to better cope with cyber threats, not forgetting that the universality of a shared cyberspace requires a global response involving both national and international organizations, whether civilian or military, with responsibilities on Countries security and defence.

PALAVRAS-CHAVE

Ciberguerra; Ciberespaço; Redes de Computadores;
Cyberwar; Cyberspace; Computer Network;

LISTA DE ACRÓNIMOS E ABREVIATURAS

AM - Academia Militar

CBS - *Columbia Broadcasting System*

CCD COE - *Cooperative Cyber Defence Centre of Excellence*

CDMA - *Cyber-Defence Management Authority*

CEME - Chefe do Estado Maior do Exército

CERT - *Computer Emergency Response Team*

CIRC - *Computer Incident Response Capability*

CM - Correio da Manhã

CNA - *Computer Network Attack*

CND - *Computer Network Defense*

CNE - *Computer Network Expoitation*

CNO - *Computer Network Operations*

COP - *Commom Operational Picture*

CPOG - Curso de Promoção a Oficial General

CRISI - Capacidade de Resposta a Incidentes de Segurança Informáticos

CYBERCOM – *US Cyber Command*

CWID - *Coalition Warrior Interoperability Demonstration*

DICSI - Divisão de Comunicações e Sistemas de Informação

EMGFA - Estado-Maior-General das Forças Armadas

ENISA - *European Network and Information Security Agency*

EUA - Estados Unidos da América

FCCN - Fundação para a Computação Científica Nacional

FFAA - Forças Armadas

GE - Guerra Electrónica

GAO - *United States Government Accountability Office*

HIP - Hipótese

I&D - Investigação e Desenvolvimento

IO - *Information Operations*

IP - Internet Protocol

ISP - *Internet Service Providers*

ITU - *International Telecommunication Union*

IWS - *Internet World Stats*

JFCC - *Joint Functional Component Command*

JP - *Joint Publication*

LAN - *Local Area Network*

LDN - Lei da Defesa Nacional

LOBOFA - Lei Orgânica de Bases da Organização das Forças Armadas

NATO - *North Atlantic Treaty Organisation*

NCIRC - *NATO Computer Incident Response Capability*

ONU - Organização das Nações Unidas

P E - Porto Editora

QC - Questão Central

QD - Questão Derivada

RCM - Rede de Comunicações da Marinha

RDE - Rede de Dados do Exército

RTm - Regimento de Transmissões

SCADA - *Supervisory Control and Data Acquisition Systems*

SI - Sistemas de Informação

SICOM - Sistema Integrado de Comunicações Militares

SIBA - Sistema de Informação das Bases Aéreas

SIGAP - Sistema de Informação de Gestão da Área de Pessoal

SIGMA - Sistema de Informação e Gestão de Manutenção e Abastecimento

SIGOP - Sistema de Informação e Gestão Operacional

STRATCOM – *US Strategic Command*

TII - Trabalho de Investigação Individual

USB - *Universal Serial Bus*

UE - União Europeia

WAN - *Wide Area Network*

Introdução:

– Justificação do tema

O termo *"Ciberguerra"* ainda não faz parte de alguns dicionários de referência da Língua Portuguesa. Mas consta o termo "*Ciberespaço*", definido como sendo "*Espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações*" (Editora, 2010:1). É formada pelas palavras (*ciber+guerra*), sendo que a primeira é oriunda do grego, cibernética, ("*kybernetiké*, a arte de governar). Actualmente existe um desvio do significado original da palavra grega, e podemos inferir que a ciberguerra é a guerra no ciberespaço.

"*A guerra no ciberespaço é preocupação prioritária das estratégias de defesa*" escreve o General Loureiro dos Santos ex-Chefe do Estado Maior do Exército (CEME) (CM, 2010:1). "*The cyber threat is one of the most serious economic and national security challenges we face as a nation*"[1], diz Barack Obama, presidente dos Estados Unidos da América (CBS, 2009:145). Declarações informadas como estas, colocaram no topo da agenda dos decisores políticos mundiais as preocupações com esta temática. Acções envolvendo a utilização de computadores e a *Internet* como arma, eram há cerca de uma década estudados como meros cenários possíveis. Hoje não só é possível como já aconteceu. É consensual, que nada mudou alguma vez o mundo tão rapidamente, quanto a *Internet* o tem feito. Esta velocidade na mudança, cria dificuldades acrescidas às organizações mandatadas para zelar pela segurança dos Estados, na protecção dos mesmos, quando este novo ambiente é utilizado para atingir interesses nacionais vitais.

Em Portugal, é inequívoca a vontade expressa na Lei, da protecção dos interesses nacionais, e às Forças Armadas (FFAA) incumbe a sua defesa militar. *"A República Portuguesa defende os interesses nacionais por todos os meios legítimos, dentro e fora do seu território, das zonas marítimas sob soberania ou jurisdição nacional e do espaço aéreo sob sua responsabilidade*", manda a Lei da Defesa Nacional (LDN) (AR, 2009:2). "*As Forças Armadas Portuguesas, são um pilar essencial da Defesa Nacional e constituem a estrutura do Estado que tem como missão fundamental garantir a defesa militar da República*" manda a Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA) (AR, 2009a:1),

É pois importante compreender o que significa a Ciberguerra, que conceitos

[1] "*A ameaça da Ciberguerra é um dos maiores desafios á economia e segurança nacional, que enfrentamos, como Nação*".

engloba, que ameaça representa para os Estados, e no caso concreto de Portugal como as suas FFAA se poderão estruturar para uma resposta eficaz. Nas operações tácticas convencionais, há operações ofensivas e defensivas. Será que a ameaça da Ciberguerra obrigará a equacionar a execução de operações ofensivas? Será que as operações no Ciberespaço, não estarão já cobertas pelas operações de Guerra Electrónica? Estas são o tipo de questões a que procuramos responder, neste trabalho de investigação.

Apenas uma correcta identificação e caracterização da ameaça permite definir a resposta adequada. Para isso é fundamental que os conceitos sejam perfeitamente conhecidos e interpretados da mesma maneira por todos os actores no processo da decisão. Como vimos, até o simples facto da palavra "Ciberguerra" não constar do dicionário de Português, prova que ainda não existe uma sistematização conceptual estabilizada a nível nacional, sendo quase certo que cada um dos intervenientes classifica o mesmo facto de forma diferente, uns falando de "Guerra da Informação", outros de "Operações de Informações", "Operações Centradas na Rede" ou ainda "Guerra do Comando e Controlo", conceitos que foram aparecendo ao longo do tempo para caracterizar a evolução das operações militares, mas que retratam situações diversas.

A precisão militar exige uma definição precisa da realidade, daí a importância deste trabalho também como um contributo na clarificação da ameaça e da sua terminologia.

- **Enunciado, contexto e base conceptual**

O tema proposto para este trabalho tem o seguinte enunciado: "**A Ciberguerra. Estrutura Nacional para Enfrentar as Vulnerabilidades – uma Capacidade Autónoma ou Partilhada"**.

Centrando-se na Ciberguerra, assume relevante importância pelas seguintes razões:

- As ameaças vindas do "Ciberespaço", são uma ameaça real, que poderão afectar em grande amplitude os interesses económicos, políticos, sociais e de segurança do País. A crescente utilização da *Internet*, com o seu ritmo elevado de expansão, a procura intensiva de comunicações móveis com acesso à *Internet*, a imensa quantidade de serviços do Estado e das empresas que se passaram a realizar através da "Rede", e a quantidade de sistemas ou máquinas monitorizados remotamente, aumentam continuamente os riscos de uma acção maliciosa deliberada. Este risco potencial tem pois tendência para aumentar e certamente atingirá níveis críticos semelhantes aos existentes nos Estados

Unidos da América (EUA) onde a digitalização está mais avançada. A North Atlantic Treaty Organization (NATO) reconhece essa ameaça, nas recomendações de peritos para o seu novo conceito estratégico: "*The most probable threats to Allies in the coming decade are unconventional. Three in particular stand out: 1) an attack by ballistic missile (whether or not nuclear-armed); 2) strikes by international terrorist groups; and 3) cyber assaults of varying degrees of severity"*[2]*(NATO, 2010:17)*;

- Cabendo às FFAA a defesa militar da República, estas têm que se estruturar para fazer frente a todo o tipo de ameaças aos interesses nacionais quando para isso solicitadas. Dessa estrutura resultará a preparação de forças para uma resposta atempada das FFAA para conter a ameaça;
- A análise da Ciberguerra tem também importância acrescida, na medida em que desta análise sairão com certeza contributos para uma disciplina já bastante conseguida nas FFAA, que é a da Segurança das Comunicações e Informações, cujo domínio de actuação se toca com o da Ciberguerra;
- Este é um tema actual, sobre o qual pouca doutrina existe.

Este tema foi escolhido pela vontade pessoal de adquirir sapiência nesta área, sabendo que muitos anos da vida do autor foram dedicados a trabalhar na área oposta mas complementar: a Investigação e Desenvolvimento (I&D), na área dos Sistemas de Informação (SI) para o Comando e Controlo, e também na Simulação e Jogos de Guerra, sempre com recurso a computadores e redes de computadores.

- **Objecto do estudo e sua delimitação**

Neste Trabalho de Investigação Individual (TII) estudamos a Ciberguerra e o conceito e estrutura, a nível militar, que devem estar presentes para enfrentar esta ameaça.

Dada a abrangência do tema, procuramos delimitar o estudo, assumindo que a base conceptual seguida explora o termo Ciberguerra em todas as suas vertentes: ofensiva, defensiva e exploratória. Embora o título mencione a estrutura nacional, este trabalho centra-se no nível militar, pois tal é o requerido na descrição detalhada do tema. Como estudo comparado em termos de conceitos e estrutura organizacional, utilizamos a doutrina americana, quando existente, sem prejuízo da sua articulação com a realidade nacional, e

[2] As ameaças mais prováveis para os Aliados na década que se aproxima são não convencionais. Três em particular sobressaem: 1) um ataque com misseis balísticos (com ou sem ogivas nucleares); 2) Ataques por grupos terroristas internacionais; e 3) assaltos no Ciberespaço com variados graus de severidade.

tendo sempre presente a NATO, União Europeia (UE), Organização das Nações Unidas (ONU) e outras organizações transnacionais com relevância nesta temática.

A Segurança da Informação e das Comunicações, é uma responsabilidade há longos anos implementada nas FFAA, bem estruturada e a responder correctamente ao tratamento de informação classificada. Não é esta uma área que o tema aprofunda ou tenta alterar. A atenção é mais geral e parte do princípio de que a Ciberguerra explora as falhas de segurança, qualquer que esta seja, sendo aí que é necessária a intervenção, como resposta.

Na sua vertente ofensiva, a Ciberguerra levanta problemas específicos a nível legal, em vários países. Neste trabalho assumimos que as FFAA não se devem autolimitar nas suas capacidades para fazer frente a ameaças de Ciberguerra, sempre dentro dos limites legais, que exploramos.

- **Objectivo da investigação**

O objectivo geral desta investigação é verificar se a actual estrutura das FFAA permite responder cabalmente às ameaças da Ciberguerra. Para isso, procuramos atingir os seguintes objectivos específicos:

- Mostrar, descrever e analisar os conceitos subjacentes à Ciberguerra;
- Esclarecer a existência de uma capacidade militar, nas suas vertentes defensiva, ofensiva e exploratória, no domínio da Ciberguerra;
- Mostrar uma estrutura que permita a nível das FFAA implementar uma capacidade militar no domínio da Ciberguerra.

- **Questão Central e Questões Derivadas**

Definimos a seguinte questão central (QC) a que pretendemos dar uma resposta e que orienta toda a nossa investigação:

*"***De que forma se devem estruturar as Forças Armadas para enfrentar a ameaça da Ciberguerra?***"*

Como orientação para o estudo e para melhor resposta à questão central, levantamos as seguintes Questões Derivadas (QD):

QD 1: Sendo travada num espaço virtual, que factores transformam a ciberguerra numa ameaça ao mundo real?

QD 2: Que desafios se colocam à existência de uma capacidade militar na área da Ciberguerra?

QD 3: Devem as FFAA manter uma capacidade autónoma nas operações de Ciberguerra ou partilhar as responsabilidades com outras organizações?

Para responder a estas questões derivadas formulamos as seguintes Hipóteses (HIP) que procuraremos validar:

HIP 1: Os ataques pelo ciberespaço podem paralisar infra-estruturas fundamentais e afectar serviços vitais ao funcionamento do Estado.

HIP 2: As FFAA dispõem de uma capacidade limitada na defesa contra operações de Ciberguerra.

HIP 3: As FFAA não dispõem de uma capacidade ofensiva e exploratória no Ciberespaço.

HIP 4: Num quadro de universalidade de um Ciberespaço partilhado, o sucesso em operações de Ciberguerra, deve ser alicerçado na cooperação com outras organizações**.**

- **Metodologia da investigação, percurso e instrumentos**

Na execução deste trabalho seguimos o método hipotético-dedutivo, como metodologia de investigação, de acordo com a NEP nº 218, do IESM, de 14 de Outubro de 2010.

Começamos a investigação com uma pesquisa bibliográfica e documental, sobre artigos e autores de reconhecido mérito científico que investigaram sobre o assunto e através de uma pesquisa global pela Internet, para sentir o "estado da arte", no que respeita à ameaça da Ciberguerra.

Recolhemos documentação escrita e multimédia, produzida por autores nacionais e estrangeiros. Em seguida realizamos entrevistas exploratórias ao nível da Divisão de Comunicações e Sistemas de Informação (DICSI) do Estado Maior General das Forças Armadas (EMGFA) e da Academia Militar (AM). Consultamos a legislação nacional relativa à Defesa nomeadamente LDN e LOBOFA para situar as responsabilidades das FFAA.

Na posse de informação suficiente, delimitamos o tema, formulamos a Questão Central, estabelecemos as Questões Derivadas e elaboramos as Hipóteses orientadoras da pesquisa.

- **Organização e conteúdo**

Este trabalho está organizado em seis partes. Nesta introdução enunciamos o tema,

justificamos o seu interesse, descrevemos o objecto e objectivos da investigação, fazemos a sua delimitação e abordamos a metodologia seguida.

No capítulo segundo, analisamos a Ciberguerra, mostramos o porquê de ser considerada uma ameaça real, caracterizamos e aprofundamos o conceito, e definimos a problemática do seu tratamento pela ciência militar.

No capítulo terceiro abordamos os desafios que se colocam às FFAA para obterem uma capacidade militar efectiva no Ciberespaço na sua vertente defensiva.

No capítulo quarto abordamos a problemática das operações ofensivas e exploratórias do Ciberespaço.

No capítulo quinto debruçamo-nos sobre a forma como as FFAA se devem estruturar para assegurar o sucesso nas operações de Ciberguerra. Além de mostrar o caminho que deve seguir a evolução da estrutura implementada, analisamos a cooperação com outras organizações.

Finalmente apresentamos as conclusões da investigação e as recomendações resultantes e sustentadas pelo trabalho no sentido do seu aproveitamento pelas FFAA.

"O ciberataque de há três anos à rede de serviços
da Estónia não foi ficção científica, foi real"
Rasmussen, Secretário-geral da NATO
(Expresso, 2010:34)

1. A Ciberguerra como ameaça real

Neste capítulo caracterizamos a Ciberguerra. A nível militar esclarecemos conceitos e mostramos o que a Ciberguerra não é. Assinalamos algumas ocorrências a nível mundial associadas à utilização do Ciberespaço por Estados ou organizações desconhecidas. Procuramos mostrar que a Ciberguerra apesar de ser uma guerra travada no Ciberespaço é uma ameaça real e não virtual.

a. A caracterização da ameaça

O Ciberespaço como infra-estrutura de comunicação e informação digital globalmente interligada, tem o seu apogeu com a massificação da *Internet.* Fisicamente é baseado em computadores, dispositivos de encaminhamento e comutação chamados *Router*, interligados por fibra óptica, cabos de cobre ou mesmo sem fios (através do espaço electromagnético). Actualmente, dispositivos como telemóveis e televisões, são autênticos computadores em miniatura e encontram-se ligados à *Internet*.

A *Internet* é uma rede descentralizada de redes de computadores, sem uma entidade única responsável pelo seu governo ou segurança. Os computadores a ela ligados estão sujeitos às leis e políticas do país onde estão fisicamente ligados, embora os utilizadores de outros países possam aceder ou colocar informação nesses computadores. Em 2010 havia mais de 1.9 mil milhões de utilizadores da *Internet* (IWS, 2010:1) e mais de 4.6 mil milhões de telemóveis (ITU, 2010:1).

Num Ciberespaço tão densamente povoado, é difícil classificar os utilizadores em amigos e inimigos. Quando alguém se liga à *Internet*, entra num domínio que pode ser utilizado para fins lícitos e produtivos, mas que pode também ser utilizado para fins criminosos ou hostis. Não há aí nenhum local ou santuário onde os inocentes se sintam protegidos. A ameaça à segurança da utilização dos sistemas é variada e pode provir de fontes diversas, como podemos observar na Tabela Nº1, elaborada com base num relatório apresentado ao Congresso dos EUA pelo *Government Accountability Office*(GAO).

Tabela 1: Principais fontes de ameaças no Ciberespaço (GAO,2010:4)

Ameaça	Descrição
Controladores	Utilizam a "Rede" para controlar remotamente os sistemas comprometidos e coordenar outras

de "*Bot-nework*"	acções como roubo de dados pessoais, bancários e outros, enviar "lixo electrónico" ou instalar *software* malicioso. Muitos desses serviços são posteriormente negociados no submundo.
Grupos Criminosos	Procuram atacar os sistemas com objectivo de ganhar dinheiro. Privilegiam a utilização de *software* para roubo de identidade e fraude internacional.
Hackers	Programadores avançados que quebram as defesas de um sistema pelo desafio que isso representa, vingança, ou ganho monetário
Alguém de dentro da Organização	É a principal fonte de crime por computador. Não necessitam de grande conhecimentos de intrusão, pois têm acesso fácil privilegiado, podendo danificar os sistemas ou roubar dados. Inclui também empresas contratadas e empregados que sem intenção introduzem software malicioso no sistema.
Estados	Utilizam ferramentas informáticas como parte da sua pesquiza de informação e espionagem. Alguns estados estão a trabalhar agressivamente em desenvolver doutrina sobre guerra da informação, programas e capacidades.
Terroristas	Procuram destruir, incapacitar ou explodir infra-estruturas críticas visando ameaçar a segurança nacional, causar vitimas em larga escala e afectar a moral e a confiança das populações.

Iremos ver que a natureza da fonte responsável pela iniciação de um incidente, é tema de discussão para a classificação do incidente como crime ou fraude, roubo ou extorsão, ataque ou agressão externa, servindo ainda de ponto de partida para a discussão se é um ataque classificado como guerra ou não guerra, principalmente se a fonte for um Estado. Mas veremos isso a seu tempo, no nosso trabalho.

Mas concretamente, de que tipo de ameaças estamos a falar, quando o meio é o Ciberespaço? Na Tabela Nº 2 resumimos a principal forma que pode assumir a materialização daquilo a que chamamos uma ameaça à segurança no Ciberespaço.

Tabela 2: Tipologia das ameaças existentes no Ciberespaço (GAO, 2010:5)

Tipo	Descrição
Negação de Serviço	Um método de ataque que nega o acesso a utilizadores legítimos, pela sobrecarga de mensagens enviadas para o computador alvo. Na prática o sistema fica bloqueado. Pode ser feito a partir de apenas uma fonte ou a partir de de vários computadores, numa acção coordenada.
Phishing	A criação ou uso de Correio Electrónico ou Páginas da Internet, desenhadas para parecerem iguais a páginas legítimas de bancos, e organizações governamentais, tendo em vista obter os dados pessoais e senhas de acesso a contas bancárias.
Trojan Cavalo de Tróia	Um programa de computador que esconde código malicioso. Normalmente está camuflado dentro de programas comuns, legítimos.
Vírus	Um programa que infecta ficheiros de computador, inserindo uma cópia de si mesmo noutros ficheiros. Difere dos "*Worms*" , no sentido de que depende da intervenção humana para se propagar.
Worm: Verme	Um programa autónomo que se reproduz copiando-se de um sistema para outro através da "Rede". Não necessita de intervenção humana.
*Sniffer: i*nterceptador de pacotes	Um programa que intercepta e examina os pacotes de dados que circulam na Internet, na procura de informação específica, como senhas transmitidas em texto não cifrado.

b. Exemplos de ataques através do ciberespaço, comprovados

Diariamente existem milhares de acções criminosas realizadas através do ciberespaço, efectuadas por indivíduos ou organizações criminosas. Embora importantes do ponto de vista económico e da segurança individual e podendo ser uma ameaça à segurança colectiva, não é este o tipo de criminalidade mais preocupante. O que preocupa os decisores políticos e os responsáveis pela segurança colectiva são as acções desencadeadas por outros estados ou por grupos terroristas: São exemplos as seguintes situações reportadas recentemente:

- Em Maio de 2007 a Estónia anunciou ter sido alvo de um ataque do tipo "Negação de Serviço", com consequências a nível nacional. O ataque coordenado colocou fora de serviço parte dos sítios governamentais e comerciais tendo a análise do tráfego malicioso revelado que *hackers* russos podem ter estado envolvidos no ataque, mas também revelou que foram utilizados computadores situados nos Estados Unidos, Canadá, Brasil, Vietname e outros (Computerworld, 2007:1);
- Em 11 de Agosto de 2008, a embaixada Georgiana em Londres acusou as forças armadas da Rússia de terem lançado um ataque coordenado de Ciberguerra contra sítios georgianos na *Internet*, coincidentes com operações militares na província georgiana da Ossétia do Sul. O sítio do governo central, e as páginas dos ministérios da Defesa, e dos Negócios Estrangeiros permaneceram inacessíveis, tal como outros sítios comerciais, incluindo serviços noticiosos (Telegraph, 2008:1);
- Em 26 de Setembro de 2010 o *worm* denominado *Stuxnet* infectou milhares de computadores em todo o mundo, com especial incidência no Irão (30 000), infectando alguns computadores na primeira central nuclear do Irão. A principal característica deste *worm*, é a sofisticação, e estar concebido para tomar o controlo e não apenas a provocar danos, de algumas grandes infra-estruturas industriais explorando uma vulnerabilidade de sistemas de controlo fabricados pela companhia alemã Siemens. Não se sabe o criador, mas especula-se que pode ser a primeira aparição de um *worm* criado por uma agência governamental, dada a complexidade e sofisticação, que obrigatoriamente terão envolvido alargado investimento (CBSNEWS, 2010:1).

Hunker, face à capacidade de disrupção que os ataques pelo Ciberespaço podem

provocar, mesmo sendo perpetrados por terroristas, não os classifica como uma "*weapon of terror*", mas sim como sendo uma "*weapon of mass annoyance*" (Hunker, 2010:12). O autor defende que não visiona a utilização de ataques pelo ciberespaço, a não ser numa escala limitada, nos antecedentes de um início das hostilidades, ou por acidente. Que os ataques pelo ciberespaço só têm significado se seguidos por acções de guerra cinética, convencional, com danos físicos alargados. Que a efectividade de um ataque pelo Ciberespaço, embora eficaz num primeiro instante, tende a diluir-se com o tempo, à medida que são implementadas alternativas aos sistemas afectados, ou estes são devidamente protegidos e tornados menos vulneráveis (Hunker, 2010:12). O autor parece ignorar a ameaça maior dos ataques pelo Ciberespaço, quando se materializam provocando efeito cinéticos, que se poderão comparar em efeito ao de potentes armas convencionais. Acresce também que, citando Loureiro dos Santos, "*A Internet e as múltiplas intranets que permitem aceder ao Ciberespaço podem servir também para accionar os sistemas de armas mais complexos e potentes, desde os rockets guiados aos mísseis intercontinentais*" (Santos, 2009:302).

Os factos parecem confirmar estes receios com a descoberta de um novo actor. O "*Stuxnet*" parece ser o primeiro exemplo conhecido de um novo tipo de ameaça que eleva a dimensão do patamar dos potenciais perigos vindos através do Ciberespaço.

c. O "Stuxnet" a primeira "*ciberarma*"?

O "Stuxnet", pode vir a ser considerado o protótipo da primeira arma no ciberespaço criada para cruzar a fronteira da realidade virtual para o mundo físico especificamente desenhada para destruir alguma coisa. Na prática, segundo Fisher, é um "cibermissil" de estatuto militar, lançado em 2009, para procurar e destruir um alvo real de elevada importância cuja identidade ainda é desconhecida (Fisher, 2010:1). Tem a habilidade de ao infiltrar-se num computador determinar se este é a máquina industrial específica de que está à procura para destruir. Se não for, abandona o computador industrial sem deixar rasto, não sem antes se ter propagado a pelo menos mais dois computadores. É este comportamento que distingue o "Stuxnet" de um *software* de espionagem e o classifica como s*oftware* de ataque preparado para destruir um alvo específico. O alvo principal são os sistemas Siemens de Supervisão, Controlo e Aquisição de Dados (SCADA), muito utilizados em instalações industriais. Este *worm*, reprograma estes sistemas, tomando o controlo das instalações.

d. A Ciberguerra na ciência militar

Sendo uma ciência relativamente recente, estes assuntos referentes à Ciberguerra têm vindo paulatinamente a entrar na terminologia militar e a conquistar o seu espaço. As actividades que se desenvolvem através dos meios de comunicação electrónicos vão sofrendo diversas classificações e atribuição de responsabilidade, sendo por vezes difícil distinguir o que as separa. Uma forma de compreender o que é a Ciberguerra, também passa por dizer aquilo que ela não é.

A inclusão destes conceitos no corpo do nosso trabalho, é intencional, pois consideramos que um dos problemas que existe quando se fala da Ciberguerra, é conceptual e definimos como um dos nossos objectivos, contribuir para diminuir este défice, clarificando a terminologia. Assim são conceitos relevantes:

- **Guerra Electrónica (GE)**: Acção militar envolvendo a utilização de energia electromagnética e energia dirigida para controlar o espectro electromagnético ou para atacar o inimigo (JP, 1_02, 2010:152). Desde cedo as unidades de GE receberam como missão efectuar acções de Pesquisa, Intercepção e Identificação de emissões rádio para Comunicações ou Não-Comunicações (radares), incluindo também a sua Radiolocalização. Uma capacidade ofensiva de Empastelamento e Decepção são também missões típicas das unidades de GE. Este conceito está estabilizado e foi assimilado pelas forças armadas do mundo ocidental. Algumas correntes de pensamento, todavia, advogam que as actividades de Ciberguerra se podem enquadrar nas operações de GE, aumentando-lhe o âmbito;
- **Guerra da Informação:** Pode ser entendida como a utilização e o tratamento da informação na procura de uma vantagem competitiva sobre um oponente. Trata do conjunto de acções destinadas a perseverar os nossos sistemas de informação da exploração, corrupção ou destruição, enquanto simultaneamente se explora, corrompe ou destrói os sistemas de informação adversários, procurando diminuir a qualidade da sua informação. Este conceito desapareceu da terminologia americana (*Information warfare*), não aparecendo no JP_3_13;
- **Guerra Centrada na Rede:** Mais do que acções de guerra, esta designação caracteriza uma doutrina de emprego das forças geograficamente dispersas, em que plataformas de armas, sensores e centros de comando e controlo estão interligados através de redes de comunicações de alta velocidade. Segundo

Alberts, embora o nome tenha a palavra guerra, esta doutrina visa principalmente uma forma de apoiar as nossas forças num cenário de guerra aumentando o seu poder de combate (Alberts, 1999:6) e não propriamente explorar ou atacar os sistemas adversários;

- **Guerra do Comando e Controlo:** Conceito e terminologia já obsoleta (JP 3_13, 2010:GL-5). Foi um dos primeiros conceitos a aparecer, quando os primeiros sistemas de informação começaram a utilizar computadores, e advogava a possibilidade de explorar e defender os nossos sistemas de comando e controlo e tentar romper, corromper ou destruir os sistemas de comando e controlo do adversário.

A doutrina de referência americana englobou todas as operações que têm a ver com a informação, o meio em que circula e os computadores que a processam sob a designação de **"*Information Operations*"** (IO) que é então definido como sendo:

- O emprego integrado das capacidades principais da Guerra Electrónica, "*Computer Network Operations*" (CNO), Operações Psicológicas, Decepção Militar e Segurança das Operações, concertado com capacidades de apoio e relacionadas, para influenciar, romper ou corromper o processo de decisão adversário humano ou automatizado, ao mesmo tempo que protege o sistema próprio (JP 1_02, 2010:224).

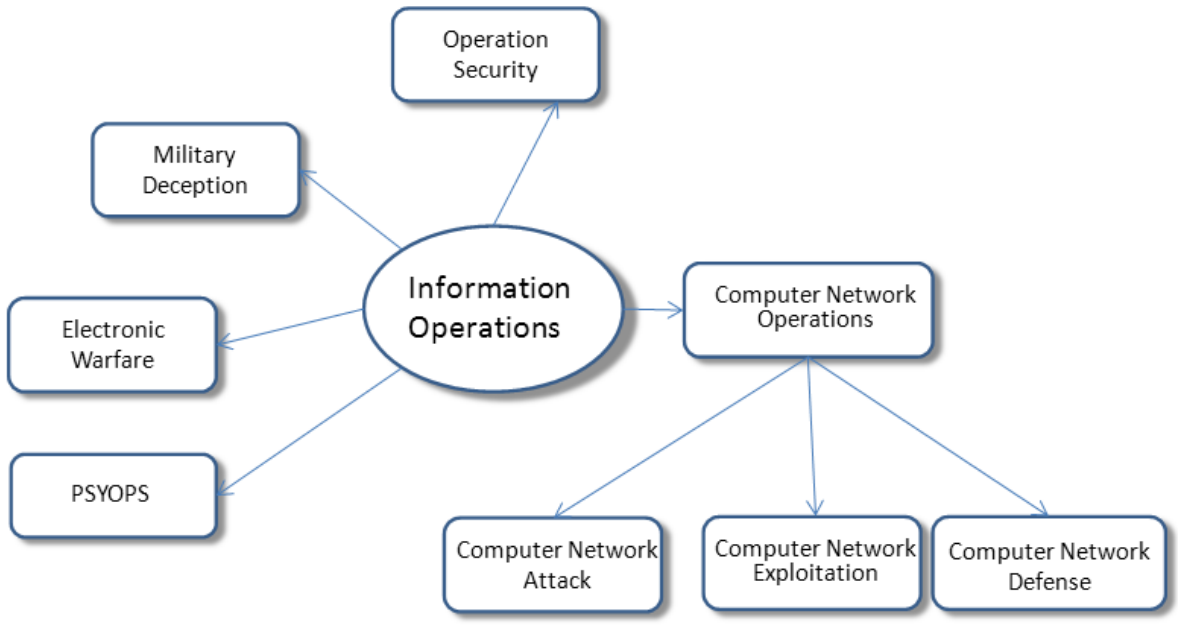


Figura 1: A Ciberguerra na doutrina americana

Fica implícito que todas as actividades a que nos referimos como Ciberguerra, na doutrina americana são designadas "*Computer Network Operations*"[3], e compõem-se de três áreas, subdividindo-se em operações ofensivas, defensivas e exploratórias (JP 3_13, 2010:I-6):

- ***Computer Network Attack*** (CNA): Acções executados com a utilização de redes de computadores para romper, negar, degradar, ou destruir a informação residente nos computadores e redes de computadores, ou o próprio computador e as redes;
- ***Computer Network Defense*** (CND): Acções executadas para proteger, monitorizar, analisar, detectar e reagir a actividade não autorizada dentro dos sistemas de informação e redes de computadores;
- ***Computer Network Exploitation*** *(CNE*): A capacidade de executar operações de recolha de informações conduzidas através da utilização da rede de computadores para reunir dados do alvo ou dos sistemas de informação adversários automatizados ou das redes de computadores.

Neste trabalho, quando referimos operações defensivas, ofensivas e exploratórias do Ciberespaço estamos a falar respectivamente de operações de CND,CNA e CNE. Fica também claro, na terminologia americana, o cuidado em retirar a palavra "*war*" das definições, pela carga simbólica que a palavra "guerra" representa, e as susceptibilidades que provoca nos cidadãos, sendo substituída por "Operações". Daí que tratar a "Ciberguerra", por "Operações no Ciberespaço", torna mais fácil o tratamento do tema nas opiniões públicas, e afasta a carga negativa que a palavra "guerra" alimenta. E também ajuda a não depreciar o forte conteúdo que a palavra "guerra" incorpora. De referir que esta afirmação representa apenas a visão do autor, que não conseguimos confirmar por outra fonte.

e. A corrida às armas no Ciberespaço

Vários países encetaram planos, para obterem capacidades exploratórias e ofensivas no domínio da ciberguerra. Recolhemos alguns dados sobre essas capacidades, mas cumpre-nos dizer que estes dados valem o que valem, pois estamos a falar de uma área em que a dissuasão tem pouco impacto pelo que anunciar que se tem uma grande capacidade nesta área não tem o mesmo peso do que dizer que se tem uma capacidade nuclear, daí que os números indicados, devem ser lidos apenas de uma forma informativa pois os Países

[3] Operações na Rede de Computadores

não colhem grandes benefícios ao anunciar as suas capacidades neste domínio.

A tabela Nº 3 mostra um extracto de uma lista de Países classificada de 1 (baixo), a 5 (alto), quanto à capacidade implementada.

Tabela 3: Quadro das capacidades em Ciberguerra dos Estados (TECNOLYTICS, 20010:13)

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

O Ciberespaço representa um novo ambiente para a projecção de poder, e assume-se como um desafio e uma oportunidade para os países com ambições hegemónicas. A crescente consciencialização da importância do Ciberespaço só agora começa a despertar e a revelar as fragilidades e as vulnerabilidades da generalidade dos Países, pelo que se prevê um aumento dos investimentos também nesta área.

f. Síntese Conclusiva

Da análise efectuada às operações no Ciberespaço numa tentativa de verificar até que ponto a Ciberguerra, apesar de ser travada num espaço virtual constitui uma ameaça real, concluímos:

- As fontes de ameaças são diversas podendo ser praticadas tanto por indivíduos, por grupos criminosos, terroristas, ou mesmo estados;
- A forma da ameaça pode variar entre vários tipos de código malicioso utilizado, para controlar, danificar, roubar, ou negar o acesso aos sistemas de informação;
- Existem relatos reais de ocorrências que afectaram os interesses vitais de alguns Estados, especulando-se que os atacantes poderão ter sido outros Estados;
- A nível militar, classificamos as operações no Ciberespaço em operações ofensivas, defensivas e exploratórias seguindo a doutrina americana;
- Vimos também que muitos países já dispõem de uma capacidade em Ciberguerra.

Os factos apresentados respondem à QD 1 e validam a HIP 1.

Mas se é certo que operações no Ciberespaço representam uma ameaça que não é virtual, significa também que as organizações responsáveis pela segurança dos Estados têm que se preparar para lidar com essa ameaça. Têm que desenvolver uma doutrina clara da utilização do Ciberespaço, esclarecer questões com a utilização ofensiva, defesa, resposta a ataques e dissuasão.

No próximo capítulo analisamos a Ciberguerra sob a perspectiva da defesa.

"Aquele que defende tudo, não defende nada"

Frederico o Grande

2. A capacidade defensiva nas operações de Ciberguerra

No capítulo anterior fizemos uma caracterização da Ciberguerra e notámos que na doutrina militar americana são tratadas como *Computer Network Operations* , sendo uma disciplina de um tronco comum: as "*Information Operations*". Neste capítulo tratamos de um modo especial as operações defensivas nas redes de computadores, as CND. Proteger, monitorizar, analisar, detectar e reagir a actividades não autorizadas nos sistemas de informação e redes de computadores, caracterizam a capacidade defensiva no Ciberespaço.

a. Generalidades

Sendo lugar-comum dizer que a melhor defesa é o ataque, e sem querermos discutir a substância de tal afirmação, na área do Ciberespaço o defensor dificilmente ganhará o combate se o oponente o encontrar totalmente desprotegido. Possivelmente ao primeiro ataque que sofrer, o defensor perde qualquer hipótese de resposta eficaz, pois os seus sistemas ficarão de tal forma afectados e comprometidos que nem sequer saberá quem o atacou, ou de onde partiu o ataque, ou mesmo se era um ataque. Sem protecção alguma, como por exemplo a proporcionada pelos sistemas antivírus, qualquer estudante com alguns conhecimentos de informática pode, pura e simplesmente, fazer desligar a maioria dos computadores e sistemas computorizados interligados em rede, como acontece com o *worm "Blaster"*. Sendo este o resultado desastroso de um único código malicioso, imagine o leitor o resultado obtido com um "*cocktail*" de códigos do mesmo tipo.

Uma capacidade defensiva, não é pois uma opção, mas sim uma necessidade para quem pretenda utilizar o Ciberespaço mesmo que apenas no apoio das operações militares clássicas que decorram nos domínios da terra, mar e ar.

b. Princípios basilares na defesa

Os sistemas de informação são constituídos por três partes: *software*[4], *hardware*[5] e comunicações. A segurança da informação e destes sistemas está alicerçada nos princípios fundamentais de assegurar:

- **Integridade**: protecção contra a modificação não autorizada ou a destruição da informação;

[4] Software: programa de computador
[5] Hardware: parte física de um computador e de outros equipamentos electrónicos

- **Confidencialidade**: garantia de que a informação não é divulgada a indivíduos não autorizados;
- **Disponibilidade**: acesso oportuno e seguro a dados e serviços de informação por utilizadores autorizados.

Podendo ser complementada pelos princípios da (CWID, 2006:1):

- **Autenticação**: um meio de confirmar a autorização que um individuo tem para receber categorias específicas de informação;
- **Não repúdio**: garantia de que o emissor da informação recebe uma prova de que o receptor a recebeu, e que o receptor recebeu uma prova da identidade do emissor, para que nenhum deles possa mais tarde negar ter processado a informação.

Uma questão torna-se pertinente na análise dos três primeiros princípios, pois parecem contraditórios e concorrerem entre si. Na verdade, no campo de batalha, um comandante pode sentir que é mais importante ter a informação disponível, do que manter a confidencialidade da mesma. Num outro cenário, um decisor pode sentir que o mais importante é a integridade da informação. Num outro, por exemplo se tratar informação classificada, é dado mais relevo à confidencialidade (CWID, 2006:1).

Uma ameaça a qualquer um destes princípios pode colocar em risco todo o sistema. Normalmente os mecanismos de protecção dos sistemas desenvolvem-se em várias camadas ao nível físico, pessoal ou organizacional e envolve a implementação de políticas e procedimentos que educam os utilizadores e administradores num modo de utilização que garanta a segurança da informação. A encriptação dos dados ajuda a manter a confidencialidade dos dados, mas qualquer sistema de encriptação, pode ser violado, sendo uma questão de tempo, perseverança e probabilidades.

A utilização de *software* e *hardware* de protecção, como antivírus e *firewalls*[6], permite automatizar a grande maioria das tarefas defensivas contra ataques maliciosos e a existência de "s*enhas de acesso*", permite restringir o acesso da informação apenas aos utilizadores autorizados. Os ataques no Ciberespaço, destinam-se exactamente a contornar ou iludir estes mecanismos de defesa, quer roubando ou adivinhando as senhas de acesso, quer infiltrando programas que uma vez dentro podem abrir, as portas, ou o acesso ao atacante.

[6] Firewall: programa de software ou hardware que filtra o acesso a um sistema

c. Não há sistemas seguros no Ciberespaço

Apesar da terminologia militar apontar para a existência de sistemas chamados seguros, tal pode induzir ao erro de pensar que tais sistemas estão imunes a ataques no Ciberespaço. Não há sistemas imunes no Ciberespaço. Mesmo desligado da *Internet*, um sistema pode ser, ou ter sido comprometido, quer na instalação de aplicações, quer por ter sido adquirido já com *software* maligno juntamente com o sistema operativo. Podemos com segurança afirmar que são menos inseguros que os sistemas totalmente abertos ou não classificados, mas não mais do que isso.

Os sistemas antivírus normalmente, possuem enormes bases de dados, com a assinatura digital dos milhares de programas maliciosos que vão sendo conhecidos, bem como da sua cura, ou vacina, e também o procedimento para o eliminar ou tornar inactivo. E funcionam bem nesse papel. Um sistema dito seguro, na sua comunicação com outras redes abertas, não deixa que um vírus conhecido entre no seu perímetro de segurança. Todavia, esta sensação de segurança é ilusória. Porquê? Esse sistema não pára um ataque efectuado por um código malicioso do tipo "*zero-day attack*" ou ataque do dia zero, ou seja um ataque que explora uma vulnerabilidade do sistema até aí desconhecida e antes de a vulnerabilidade ser corrigida pelo autor do programa. Como os sistemas de protecção desconhecem aquele tipo de ataque, não o detectam.

Os sistemas de protecção que as organizações utilizam nos computadores que tratam informação classificada, ditos seguros, baseiam-se na criação de uma protecção similar a uma barreira semelhante a um castelo medieval com as suas muralhas, e portas de entrada bem defendidas. Parecendo inexpugnável, sabemos o que a história nos conta sobre os castelos tomados. Desde traidores a abrirem as portas ao inimigo, cavalos de Tróia a serem oferecidos, até assalto usando novas técnicas de transposição, ou túneis desconhecidos. O problema deste tipo de defesa, é que depois de entrar o atacante tem acesso a tudo podendo inclusive controlar o castelo. Isso mesmo foi referido pelo MGen Webber da Força Aérea Americana que traduzimos: "*A nossa abordagem na segurança do Ciberespaço, no passado, foi construir paredes em redor da rede cada vez mais altas e espessas. Isto coloca toda a protecção nas nossas fronteiras, e protege tudo o que está dentro com a mesma protecção. Esta estratégia de defesa periférica é similar à estratégia da Linha Maginot, aplicada durante a II Guerra Mundial. Uma defesa do Ciberespaço no perímetro, provou ser igualmente ineficaz: uma vez que o adversário quebre as barreiras*

defensivas, eles têm o controlo das nossas redes e temos dificuldade em rastreá-los e em expulsá-los" (Webber, 2010:6).

Segundo Webber, este modelo de protecção começa a estar esgotado, pois a realidade provou que não se consegue proteger tudo. Na verdade, dificilmente alguém poderá pensar que existe um perímetro no ciberespaço. Em alternativa advoga um modelo de protecção consistindo numa defesa em profundidade, com camadas de protecção diferenciadas consoante o valor dos sistemas a proteger. Desse modo o atacante terá que quebrar as sucessivas barreiras que cercam os sistemas mais valiosos, que neste caso já poderão estar mais protegidos, com os recursos poupados na diminuição da protecção de sistemas menos valiosos (Webber, 2010:7).

Uma pequena amostra das vulnerabilidades existentes em Portugal, é a revelada por um estudo quadrimestral da Universidade de Coimbra que concluiu que dos 9715 servidores nacionais ligados à *internet* testados, mais de 7000 têm um esquema de criptografia de tal modo vulnerável, que permite aos atacantes informáticos acesso a toda a informação. Desses servidores 1251 pertencem ao Estado (Expresso, 2011:1)

d. A estratégia da NATO na defesa no Ciberespaço

O relatório da sessão anual de 2009 do "*Sub_Committe on Future Security and Defence Capabilities"* refere que os ataques no Ciberespaço, são agora uma das mais sérias ameaças assimétricas que a Aliança enfrenta, a par do terrorismo e da proliferação nuclear e que a natureza aberta da *Internet* torna a prevenção destes ataques difícil, sendo necessária uma efectiva cooperação internacional, cabendo à NATO a responsabilidade de tomar as medidas adequadas para protecção própria e potencialmente manter um papel importante na contribuição para a defesa dos seus Membros contra ataques no Ciberespaço (NATO, 2009:67).

Neste sentido emitiu algumas recomendações, realçando que as iniciativas para a segurança no Ciberespaço são semelhantes às iniciativas tomadas contra o avanço da proliferação nuclear, cabendo aos parlamentos nacionais desempenhar um papel importante na resposta a ataques no Ciberespaço, desenhando e votando leis nacionais, ratificando acordos internacionais e assegurando que as leis e outras medidas são correctamente aplicadas. Assim entre muitas recomendações aos governos destacam-se (NATO, 2009:63):

A nível interno:

Se ainda não existir, apoiar o desenvolvimento de uma Estratégia Nacional de

Segurança no Ciberespaço, incluindo os seguintes passos:

- Definir e classificar os riscos e ameaças na área da defesa no Ciberespaço, e garantir que são implementadas medidas práticas para tratar os potenciais incidentes. Estas medidas devem incluir a efectivação de "*Computer Emergency Response Teams*[7]" e a designação de uma autoridade constituída para dirigir e coordenar os esforços nacionais de defesa do ciberespaço;
- Escrutinar o enquadramento legal interno, e assegurar que são implementadas leis coerentes para resolver a ameaça crescente vinda do Ciberespaço;
- Estabelecer fortes parcerias entre governos e empresas privadas na área dos computadores, para assegurar a segurança das redes governamentais e melhorar a troca de conhecimentos e informação no caso de uma quebra de segurança.

A nível internacional:

- Apoiar o "Cooperative *Cyber Defence Centre of Excellence*" (CCD COE), com recursos humanos, materiais e financeiros, e enviar pessoal para receber formação e treino;
- Apoiar esforços no sentido de desenvolver uma efectiva regulação internacional, no modo como os "*Internet Service Providers*[8]" (ISP) tratam o código malicioso, e na adopção de um mínimo de protocolos de segurança para os computadores autorizados a utilizar os serviços dos ISP.

As preocupações na NATO, já passaram da teoria à prática, e um passo importante foi dado com a criação do CCD COE em Tallinn na Estónia, em Maio de 2008, com o objectivo de melhorar as capacidades defensivas da NATO no Ciberespaço. É um esforço internacional visando a educação e treino, investigação e desenvolvimento, e a cooperação e troca de informação entre as Nações NATO, incluindo outros países parceiros (CCDCOE, 2010:1).

Em 2008 foi criada a "Autoridade NATO para a Gestão da Defesa no Ciberespaço (CDMA)", com a missão de estabelecer ligações com as organizações nacionais que tratam da segurança no Ciberespaço.

Foi também decidido implementar uma Capacidade para Responder a Incidentes de Computador, " *NATO Computer Incident Response Capability*" (NCIRC), composta por vários níveis, para permitir gerir os eventos no Ciberpaço, e dispondo de ligações directas

[7] Equipas de resposta a situações de emergência com computadores
[8] Fornecedores do serviço de *Internet*

com as organizações equivalentes das Nações membro. Esta capacidade está em evolução, e novos serviços vão sendo adicionados como a capacidade de enviar uma equipa em apoio de um País membro ou parceiro (Signalonline, 2009:1).

Na Cimeira de Lisboa, em 19 de Novembro de 2010, a NATO aprovou o seu novo Conceito Estratégico. No seu ponto 19 sobre a defesa e dissuasão, estabelece que a NATO garantirá as capacidades necessárias para desenvolver ainda mais a sua capacidade para prevenir, detectar, defender e recuperar de ataques pelo Ciberespaço, incluindo a utilização do processo de planeamento NATO para reforçar e coordenar as capacidades nacionais de defesa do Ciberespaço, colocando todos os organismos NATO sob "*cyber protection*" centralizada, e integrando melhor a visão NATO do Ciberespaço, "*NATO cyber awareness*", e o sistema de alerta e resposta com os Países membros (NATO, 2010b:11).

e. As FFAA e a defensiva no Ciberespaço

As FFAA, para planear, dirigir, coordenar e controlar as operações militares, apoiam-se em equipamentos de comunicações e sistemas de informação, que juntamente com a adopção de procedimentos, constituem o seu sistema de comando e controlo. A evolução nesta área, tem levado à crescente digitalização das redes de comunicações, e a utilização de computadores é já imprescindível a qualquer actividade nas FFAA. Em termos de digitalização, os próprios rádios, que até há alguns anos, utilizavam uma tecnologia puramente analógica, começam a ser autênticos computadores, dispondo de um endereço IP, e comportando-se como mais um elemento na Rede.

Neste campo, a organização das FFAA não difere da orientação seguida por outros Países, como por exemplo os EUA. Como podemos ver no Anexo G, existem redes tácticas, redes fixas constituindo uma malha cobrindo o território, e redes locais específicas de apoio a alguns órgãos. Lá como cá cada Ramo possui redes próprias que administra. Estas redes tanto podem suportar aplicações de gestão, como de comando e controlo, ou mesmo de apoio a sistemas de armas e plataformas. A ligação destas redes tácticas, com a infra-estrutura fixa, é executada com a criação de "*gateways*[9]" que fazem a ligação entre sistemas diferentes, convertendo protocolos, e controlando o acesso. Muitas destas redes tácticas utilizam comunicações sem fios.

Sobre a mesma infra-estrutura física de comunicações, são estabelecidas redes com graus de confidencialidade diversa, havendo redes praticamente abertas a todos os

[9] G*ateway*: porta de entrada

utilizadores e outras de acesso restrito. Normalmente as redes abertas, têm acesso à *Internet*, sendo que esse acesso é controlado e filtrado por *hardware* e *software* de segurança. Mesmo nas redes mais seguras há comunicação com as redes abertas, embora sujeita a filtros mais apertados. Se assim não fosse a informação não fluía para as redes seguras, já que normalmente os produtores de informação, são as unidades tácticas, que operam em cenários que fazem que a prioridade nas redes em que operam seja a disponibilidade e não a confidencialidade, e não é possível manter os critérios exigidos pela manutenção de uma classificação de segurança elevado. Mas para dar ordens ou ter uma COP actualizada nos escalões elevados, a laborarem em redes mais seguras, a informação tem que cruzar essas redes com menor segurança. A tendência, para tirar todo o proveito de uma abordagem das operações centradas na rede, é a de utilizar a infra-estrutura de comunicações da *Internet* para apoio das operações militares, sem prejuízo de uma utilização segura desse ambiente.

Nas FFAA Portuguesas existem assim redes próprias da Marinha, Exército e Força Aérea e também redes do EMGFA. As redes tácticas são construídas de acordo com as necessidades das operações, e são interconectadas com essas redes, mesmo que as operações decorram no exterior do País, sendo normalmente a interligação feita por satélite. O EMGFA dispõe de uma rede segura, e administra o Sistema Integrado de Comunicações Militares (SICOM). As redes não seguras dos Ramos têm uma interligação com a *Internet.*

Notamos pois, que não existem grandes diferenças no modo como as diversas unidades e órgãos dos Ramos implementaram as suas redes de computadores. Todas têm em comum aplicarem sistemas de segurança que asseguram uma protecção mínima contra ataques pelo Ciberespaço, sendo certo que o objectivo primordial é manter os sistemas a funcionar.

O Exército mantém uma organização que está já orientada para as operações defensivas no Ciberespaço com a implementação do módulo *Computer Incident Response Capability* (CIRC).

Vejamos em pormenor algumas das características particulares destas redes.

(1) O Exército

A rede de dados do Exército é gerida pelo Regimento de Transmissões, da Direcção de Comunicações e Sistemas de Informação do Comando das Forças Terrestres, que mantém um controle centralizado sobre a adição de utilizadores e respectivos privilégios

de acesso. Instala e gere também "*software"* de segurança como antivírus e "*gateways"* para acesso à *Internet* usando a "*firewall IXBOX"*. Especificamente, na área defensiva do Ciberespaço, CND, tem as principais missões exigidas, como sejam deter, prevenir, detectar e recuperar de qualquer tipo de incidente ou ataque contra os sistemas de informação. Organicamente, dispõe de um núcleo CIRC com a capacidade de resposta a incidentes de computador e partilha informação com os elementos CIRC nacionais (RTm, 2010:1). O módulo táctico CIRC está implementado, tem mobilidade táctica e foi demonstrado no Exercício ORION 2009.

(2) A Marinha

A Marinha tem uma rede de comunicações conhecida por Rede de Comunicações da Marinha (RCM). As unidades dentro da Base Naval de Lisboa e na área de Lisboa estão ligadas por fibra óptica com uma largura de banda elevada. A comunicação com as unidades mais distantes é feita utilizando a rede de transmissão militar administrada pelo EMGFA, o SICOM. Os utilizadores e os recursos de rede estão registados num domínio especificado por "marinha.pt" através do qual são aplicadas políticas de segurança. Há mais de 7200 computadores, contando com mais de 10200 contas de correio electrónico individuais e quase 2600 institucionais (Correia, 2010:26). Sobre a RCM correm também serviços protegidos de comando e controlo, destacando-se o correio electrónico militar. A Marinha concentra e controla a ligação à *Internet* através de uma ligação de 26 Megabits por segundo.

(3) A Força Aérea

A Força Aérea tem redes de comunicações de área local em todas as suas bases e unidades, que se interligam através da rede militar SICOM. Estas têm pólos de gestão local, sendo as políticas de gestão e segurança administradas centralmente pela Direcção de Comunicações e Sistemas de Informação. Estas redes têm interligação com a *Internet*.

Sobre estas redes correm os vários sistemas quer de apoio operacional quer de apoio administrativo e logístico, como o Sistema de Informação e Gestão Operacional (SIGOP), o Sistema de Informação de Bases Aéreas (SIBA), o Sistema de Informação e Gestão de Manutenção e Abastecimento (SIGMA) e o Sistema de Informação de Gestão da Área de Pessoal (SIGAP) entre outros.

f. Síntese conclusiva

Dos factos estudados neste capítulo, verificamos que uma capacidade defensiva no

Ciberespaço, não é uma opção mas sim uma necessidade. Essa necessidade traduz-se na protecção dos valores da *Integridade*, *Confidencialidade* e *Disponibilidade* da informação da constante ameaça dos ataques vindos pelo Ciberespaço, que tentam contornar ou iludir os mecanismos de defesa implementados.

Não há sistemas completamente seguros, e as estratégias de defesa tendem a evoluir para uma defesa em profundidade, com várias camadas que não protegendo tudo, permitem proteger melhor os recursos mais valiosos.

A NATO encara a sério a defesa no Ciberespaço, criando o CCC COE, uma capacidade NCIRC, e a Autoridade NATO para a Gestão do Ciberespaço.

Em Portugal, os Ramos têm múltiplas redes de computadores, com uma gestão própria, e implementação de protocolos orientados prioritariamente à gestão, com o objectivo de manter operacional a infra-estrutura e os serviços disponíveis, e não propriamente deter um ataque organizado, mantendo apenas uma capacidade mínima de defesa contra ataques externos.

Estes factos permitem responder à QD 2 e validam a HIP 2.

Mas além da importante parte defensiva do Ciberespaço, outras operações militares podem ser desenvolvidas. São as operações ofensivas e exploratórias, que aprofundamos no próximo capítulo.

"Assistimos ao surgimento de um novo paradoxo da conflitualidade, assente no facto de podermos estar em guerra sem saber contra quem"

General Pinto Ramalho (AM, 2004:103)

3. A capacidade ofensiva e exploratória nas operações de Ciberguerra

Depois de abordarmos as operações defensivas no ciberespaço no capítulo anterior, estudamos agora, as operações, quiçá mais problemáticas em termos jurídicos e sobre a qual os Estados tendem a não manifestar publicamente as suas intenções. Falamos das capacidades ofensivas e exploratórias na utilização do ciberespaço.

a. Generalidades

Muitos países trabalham hoje para implementar capacidades ofensivas em matéria de Ciberguerra. Normalmente um dos primeiros desafios com que se deparam é encontrar um quadro de emprego compatível com o direito internacional. O recurso à Carta das Nações Unidas ou à Convenção de Genebra são tema obrigatório quando se pretende enquadrar o emprego de uma capacidade ofensiva.

b. "Jus in Bello" no Ciberespaço

O "*direito na guerra"*, por vezes referido como direito humanitário, resulta da adesão de muitos Estados a tratados internacionais sobre os conflitos armados, permitindo a existência de algumas regras que é necessário cumprir, para que uma acção militar possa ser considerada legal, à luz do direito internacional consuetudinário, nomeadamente as convenções de Haia e Genebra. Entre outros, distinguem-se os princípios:

- **Distinção e Discriminação**: as partes de um conflito armado têm que distinguir entre a população civil e combatentes e entre objectos civis e objectivos militares. Qualquer alvo que se pretenda atingir, terá que ser um alvo militar;
- **Proporcionalidade**: são proibidos ataques se causarem mortes acidentais de civis, provocarem ferimentos em civis, ou danificarem objectos civis em excesso à vantagem militar concreta e prevista do ataque.

De acordo com Tissier, no Ciberespaço há muitas vezes uma utilização dual das infra-estruturas, que são utilizadas quer para fins civis quer para utilização militar. Dá como exemplos as redes de comunicações filares e de fibra óptica intercontinentais e nacionais e os satélites civis, que também são utilizados pelos Estados, para apoiar operações militares, fora do seu território. Tissier conclui que no caso da utilização dual, a lei não oferece dúvidas pois permite que o objecto civil se transforme num objectivo militar, tornando legal a sua destruição ou inutilização (Tissier, 2009:102).

São proibidas operações no Ciberespaço, que visem uma infra-estrutura puramente civil, como por exemplo tornar inactivo um satélite de comunicações, quando esta acção não produz *vantagem militar significativa*. Recai então nos comandantes, ou nos dirigentes políticos dos Estados, a responsabilidade de determinar o patamar dessa vantagem militar significativa, de modo a tornar legal essa acção. Acresce ainda, para ser legal, uma operação ofensiva no Ciberespaço, o atacante tem que avaliar em permanência os potenciais danos colaterais nos alvos civis.

Neste contexto, não existe diferença entre o que acontece nos domínios da terra, ar, mar, utilizando armas cinéticas com que acontece no domínio do Ciberespaço.

c. "Jus ad Bellum" no Ciberespaço.

O "*direito a fazer a guerra"* também se encontra regulamentado, neste caso pela Carta das Nações Unidas. Vejamos até que ponto uma acção ofensiva no Ciberespaço se assemelha ou não com uma outra qualquer acção militar clássica.

Na utilização do ciberespaço, a grande maioria das actividades ilícitas como a contrafacção, intrusão, alteração e roubo de dados, a propagação de vírus, a fraude e a usurpação de identidade caem dentro do conceito de criminalidade. Os seus autores, estão sujeitos às leis do país onde praticaram a acção.

De acordo com Ventre, se em vez de simples cidadãos, ou organizações criminosas, for um estado a executar estes actos, mesmo utilizando os mesmos métodos, as mesmas regras, as mesmas técnicas e os mesmos actores, parece difícil aceitar que se possa falar de criminalidade. A agressão de um Estado por outro tem uma dimensão política, estratégica e de segurança, que ultrapassa a dimensão da acção criminal de um delinquente (Ventre, 2008:121). A questão que tentamos responder é determinar quando é que é internacionalmente aceitável ou legal reagir a uma acção executada através do ciberespaço, recorrendo á força armada como resposta.

O artigo 2º da Carta das Nações Unidas, que Portugal assinou em 1955, interdita os seus membros a recorrer à ameaça ou ao uso da força quer seja contra a integridade territorial e a independência política de um Estado, quer seja de qualquer outro modo incompatível com os objectivos das Nações Unidas (ONU, 1955:1). A mesma Carta define as excepções à regra atrás enunciada. Sob o mandato do Conselho de Segurança, o uso da força armada pode ser utilizado, diz o artigo 42. Por sua vez o artigo 51 reconhece o direito inerente de legítima defesa individual ou colectiva no caso de ocorrer um ataque armado contra um país membro. Pelo artigo 39, apenas o Conselho de Segurança poderá qualificar

um evento de ameaça à paz, ruptura de paz ou acto de agressão, ou seja qualificar um acto como ataque armado.

Ventre desafia-nos com várias questões. Uma operação ofensiva no Ciberespaço poderá ser qualificada como ataque armado? Se é um acto de agressão, quais são as armas? Que critérios consideramos para o qualificar de ataque armado ou utilização da força? Os meios utilizados, o nível de danos provocados, os alvos atingidos, o número de vítimas ou o estatuto dos autores do acto? (Ventre, 2008:122).

Não existindo consenso internacional numa definição precisa do uso da força, dentro ou fora do Ciberespaço, cada Estado pode afirmar como certas diferentes definições, e pode aplicar diferentes patamares para o que considera ser o uso da força. Então quer seja no Ciberespaço, quer seja noutro domínio, há sempre um potencial desacordo entre os Estados sobre a intensidade que pode ser considerada uma ameaça ou uso da força, afirma o LTGen. Keith Alexander, na audição para a sua nomeação para Comandante do "*United States Cyber Command*" em Março de 2010 (Alexander, 2010:1).

Podemos pois considerar que as actuais leis da guerra se podem aplicar igualmente às operações militares no ciberespaço, não esquecendo porém que estas operações apresentam certas especificidades que exigem reflexão, pois dificultam o exercício do direito a fazer a guerra pelos ameaçados. Falamos da noção de território, da atribuição da culpa e até da invasão (sobrevoo, passagem, utilização) de um território neutral.

d. A Atribuição da Culpa

A identificação dos culpados por uma acção no Ciberespaço é muito difícil, se não impossível, bem expressa pela expressão "*os electrões não utilizam uniformes*". As actividades executadas na rede de computadores são inerentemente anónimas, e são o resultado do próprio desenho da *Internet,* e dos protocolos de comunicação que a suportam, que assumia que a confiança entre os seus utilizadores era um facto adquirido, coisa que não acontece actualmente.

Goodman aborda esta temática e confirma que quando um sistema sofre remotamente um ataque, o atacado normalmente desconhece o atacante. E se um ataque acontece e provoca danos, não se consegue que um anónimo seja penalizado e sofra as consequências dos actos praticados. E se todos os utilizadores de um sistema forem anónimos, nem sequer há a possibilidade de distinguir, entre acções autorizadas ou não autorizadas, o que ainda dificulta mais a tarefa, pois o atacado pode nem saber que está sob ataque. Segundo ele a atribuição, representa a capacidade de associar um actor com uma

acção (Goodman, 2007:113). O actor é caracterizado por alguns atributos, como sejam o nome, um número de série da máquina na rede, ou outra qualquer propriedade única. Para uma correcta atribuição algumas características são importantes como a precisão, que procura um atributo que inequivocamente distinga um actor de outro; a exactidão, relaciona-se com a precisão e mede a qualidade da atribuição, ou seja a probabilidade de esta estar correcta.

Mesmo que consiga estabelecer o ponto de origem, localização geográfica, de um ataque, isso não significa que o dono desse computador seja efectivamente o atacante, pois também pode ter sido uma vítima, que o atacante utilizou como ponto intermédio para lançar o ataque e melhor esconder a identidade, ou então implicar esta vítima, colocando evidências que lhe atribuam a autoria.

A dificuldade na atribuição também de certo modo está relacionada com a falta de uma estratégia de dissuasão que é utilizada em outras áreas. A análise forense para identificar um atacante pode demorar semanas, meses ou até anos ou nunca se conseguir. Segundo Lynn, *Deputy Defense Secretary dos EUA*, esta situação quebra o tradicional conceito estratégico de dissuasão que foi utilizado durante a Guerra Fria. Citando e traduzindo Lynn: "*Se não soubermos a quem atribuir um ataque, não podemos retaliar contra esse ataque, logo não podemos dissuadir através da ameaça de punição*" (Lynn, 2010:1).

Mas será que o Ciberespaço, que dissemos ser densamente povoado, por si só, pode hipoteticamente ser considerado um Estado?

e. As fronteiras do ciberespaço

Se consideramos um Estado como uma *Nação organizada politicamente*, sendo uma Nação, o *conjunto de indivíduos que constituem uma sociedade política autónoma, fixada num determinado território, regida por leis próprias e submetida a um poder central* (Infopedia, 2010:1), não podemos concluir que existe um Ciber-Estado. Em termos de população mais de 1,6 mil milhões de indivíduos utilizam a *Internet* mas não mantêm verdadeiramente a noção de uma identidade digital própria. O endereço *Internet Protocol* (IP) do seu computador pode mudar constantemente, e mesmo o de Correio Electrónico não constitui identidade, pois também pode ser regularmente alterado. É pois difícil definir qual a comunidade de internautas que está submetida a um Cyber- Estado.

Relativamente ao território, o Ciberespaço, conhece fronteiras naturais, que são os pontos de entrada da *Internet* no País e como nas fronteiras do mundo real, estas fronteiras

podem ser violadas ou evitadas, utilizando redes de satélite, redes privadas, troca de dados utilizando discos rígidos ou memórias Universal Serial Bus (USB). Se os postos fronteiriços são patrulhados ou controlados pelos Estados, não é o caso com as entradas da *Internet*, embora tal seja possível, como está demonstrado pela China que instalou uma capacidade de censurar a informação (Maupeau, 2009:59).

Por outro lado, existem grandes empresas como a Google e a Cisco, que poderão ser considerados como verdadeiros Ciber–Estados, pois coleccionam milhões de informações dos indivíduos, e disponibilizam imensos serviços aos seus utilizadores, comportando-se como um verdadeiro Estado.

f. A NATO e o artigo V

Durante os ataques pelo Ciberespaço sofridos pela Estónia em 2007, esta apelou à intervenção da Aliança, alegando que estava a ser atacada. A questão ao ser colocada, obrigou a responder se ataques pelo Ciberespaço são ou não ameaças que caem sob a alçada do artigo V da Aliança, que considera que um **ataque armado** contra um dos Membros é considerado um ataque contra todos os Membros (NATO, 1949:1). Na altura não houve uma resposta efectiva da Aliança, tendo os ataques terminado. Mas uma possível resposta para esta questão pode ser encontrada no relatório Nº51 do "*Council on Foreign Relations*", organização independente, em Fevereiro de 2010: "Por definição, os ataques no Ciberespaço, não são **ataques armados**, mas para a Aliança significar algo, a NATO tem que se unir em face de assaltos que ameaçam um Estado membro". Nestas situações, não-militares, a NATO pode invocar o artigo IV que diz: " *as Partes consultar-se-ão sempre que, na opinião de qualquer deles, a integridade territorial, a independência política ou a segurança de qualquer uma das Partes estiver ameaçada*". E continua reafirmando que o ponto importante não é se uma ameaça pode ser melhor considerada sob o artigo IV ou V; o importante é o compromisso da Aliança de que uma ameaça a um dos Membros será tratada colectivamente. No seu Conceito Estratégico os Membros da NATO deveriam afirmar que: "*qualquer acção iniciada por um Estado externo ou um actor não-Estado, que ameace a segurança política ou económica ou a integridade territorial de um Membro da NATO, irá despoletar uma resposta colectiva"* (Goldgeir, 2010:7).

A proposta apresentada pelo Grupo de Peritos para o Novo Conceito Estratégico, NATO 2020, parece incluir a ideia atrás expressa: "*Ataques no Ciberespaço, contra sistemas NATO ocorrem frequentemente, mas a maior parte das vezes abaixo do patamar*

que cause preocupação política. Contudo o risco de um ataque em larga escala nos sistemas de comando e controlo da NATO, ou redes de energia, pode facilmente mandatar consultas ao abrigo do artigo IV e pode, possivelmente, conduzir a medidas colectivas de defesa sob o artigo V" (NATO, 2010:58).

O Conceito Estratégico da NATO, aprovado na Cimeira de Lisboa, confirma estes dados ao explicitamente estabelecer no seu ponto "*4.a Collective defence*" que "*NATO members will always assist each other against attack, in accordance with Article 5 of the Washington Treaty. That commitment remains firm and binding. NATO will deter and defend against any threat of aggression, and against emerging security challenges where they threaten the fundamental security of individual Allies or the Alliance as a whole*." (NATO, 2010b:2). Note-se a referência aos desafios de segurança emergentes, onde facilmente se podem colocar os ataques pelo Ciberespaço. No seu ponto 12 explicita que estes ataques podem ser executados quer por forças militares ou de espionagem estrangeiros, organizações criminosas, terroristas e/ou grupos extremistas.

g. O exemplo americano nas operações ofensivas no Ciberespaço

O "*US Strategic Command*" (STRATCOM) desempenha um papel chave nas operações no Ciberespaço. É formado por sete componentes funcionais, incluindo cinco Comandos de Componentes Funcionais Conjuntos (JFCC). Um destes componentes é o "*US Cyber Command*" (CYBERCOM), com a missão de "*planear, coordenar, integrar, sincronizar e conduzir actividades para: conduzir as operações e a defesa de redes de informação específicas do Departamento de Defesa e preparar-se para, quando ordenado, conduzir operações militares no Ciberespaço, em todo o espectro, de modo a permitir acções em todos os domínios, assegurar a liberdade de acção no Ciberespaço aos EUA e Aliados e negar o mesmo aos adversários*" (STRATCOM, 2010:1). A capacidade operacional inicial foi atingida em Maio de 2010. O CYBERCOM, centraliza o comando das operações no Ciberespaço, e dispõe de quatro comandos subordinados, dos vários Ramos: *Army Forces Cyber Command, 24th USAF, Fleet Cyber Command e Marine Forces Cyber Command.* A quantidade de militares destacados para servir nestes Comandos começa a mostrar a verdadeira dimensão da aposta que os EUA depositam no valor que atribuem às operações no Ciberespaço. Para o *Army Forces Cyber Command* , o Exército destacou cerca de 21 000 militares e civis, principalmente vindos das unidades de Transmissões e Informações. A Marinha afectou 40 000 militares e civis, embora também

cubram as áreas da meteorologia e oceanografia e a Força Aérea cerca de 8 500 homens (REUTERS, 2010:5).

h. A capacidade exploratória no Ciberespaço

Mais do que as capacidades defensivas ou ofensivas existentes na utilização do ciberespaço, existe um potencial elevado que pode ser utilizado em proveito e em suporte das outras operações militares, mesmo mantendo um estatuto neutral na sua utilização. Explorar as redes de computadores e sistemas de informação do inimigo, é por si só um método muito eficiente de obter uma vantagem, que no contexto de uma operação militar clássica, pode conduzir a uma superioridade no campo de batalha.

Não existe grande diferença entre o conhecimento, técnicas e recursos que são necessários para as CNA e as CNE. Segundo Owens, fundamentalmente o que as distingue é a natureza da recompensa. Enquanto num ataque, o atacante pode querer destruir os ficheiros em determinado computador, numa acção exploratória, o explorador quererá copiar os ficheiros, comprometer a confidencialidade da informação, e tirar proveito do seu conteúdo. Um agente desenvolvido para exploração pode também conter as funcionalidades necessárias para ser utilizado, noutra altura, para acções ofensivas. Esta ambiguidade nestes dois tipos de operações, que não existe nas operações com armas cinéticas, nucleares, biológicas ou químicas, tem algumas consequências (Owens, 2009:150):

- A parte atacada pode não saber distinguir entre uma actividade no Ciberespaço exploratória, de uma actividade ofensiva no Ciberespaço;
- As autoridades legais, e o enquadramento jurídico, podem ser bastante diferentes para cada uma destas operações;
- Do ponto de vista do treino, o desenvolvimento de aptidões para atacar, também desenvolve aptidões para conduzir exploração no Ciberespaço, e vice-versa.

i. As Forças Armadas e a capacidade ofensiva e exploratória no Ciberespaço

A natureza das operações ofensivas e exploratórias no Ciberespaço, não difere tacticamente dos procedimentos utilizados pela Guerra Electrónica, nas suas actividades de intercepção, escuta, análise, empastelamento e decepção, já há longos anos implementadas nas FFAA. O que difere é o meio em que se desenvolve esta actividade. Como acontece na GE, os constrangimentos de ordem legal relativos à escuta ou exploração, ou ao empastelamento, em tempo de paz e de alvos não militares, são uma condicionante

importante que limita os graus de liberdade existentes para o treino e preparação destas capacidades. O próprio conhecimento de que existe uma tal capacidade, por vezes inquieta as opiniões públicas, temerosas de uma aplicação interna e ilegal de tais capacidades e receosas de alguma invasão da privacidade. Por outro lado, na eventualidade de um conflito, estas são capacidades que não se conseguem adquirir de um momento para o outro. Além de exigirem recursos humanos altamente qualificados, obrigam a uma estrutura permanentemente activa e em evolução contínua. No nosso entender tais receios são infundados, já que o mesmo raciocínio poderia colocar-se em qualquer outra área das FFAA se os seus meios ou capacidades fossem utilizados de forma indevida e ilegal. Ou o mesmo se pode dizer de qualquer outra actividade do Estado se os seus agentes utilizarem ilegalmente os seus poderes e competências.

Possivelmente, por esta ser uma área operacional muito recente, não é muito fácil às Forças Armadas dos diversos países adquirirem capacidades nesta área. Ao contrário do que acontece actualmente com os meios de GE, em que os fabricantes de equipamentos apresentam soluções que cobrem todo o espectro das operações militares no ambiente electromagnético, o mesmo ainda não acontece com o Ciberespaço, não só pela natureza do meio, mas também pela volatilidade das soluções, pois o facto de normalmente as operações no Ciberespaço explorarem vulnerabilidades dos sistemas, se estas foram conhecidas, e teriam de o ser para o fabricante propor o equipamento, quando o equipamento fosse adquirido, já as vulnerabilidades haviam sido corrigidas tornando inútil o equipamento. Daqui resulta uma das grandes especificidades que caracteriza esta área das operações militares e da dificuldade de adquirir competências e capacidades neste domínio.

As FFAA apenas estão a iniciar os primeiros passos neste campo, seguindo aliás o mesmo caminho da NATO, tentando desenvolver competências nesta área, fundamentalmente vocacionadas para o treino das próprias defesas a ataques vindos do Ciberespaço. O único Ramo que manifesta organicamente uma estrutura com capacidades ofensivas neste domínio é o Exército.

(1) Exército

Na área das CNA, o Exército tem na sua estrutura orgânica o módulo táctico CIRC, com a missão de apoiar a vertente ofensiva no Ciberespaço, nomeadamente efectuar intrusões tendo em vista afectar os princípios básicos de segurança (confidencialidade, integridade e disponibilidade) nos sistemas de informação e comunicações opositores

(RTm, 2010:1). Este módulo, como vimos, está sedeado no RTm e em termos operacionais articula-se sob o Comando do Batalhão de Tm, sedeado na EPT. Operacionalmente tem sido utilizado em exercícios para detectar vulnerabilidades nos sistemas de informação tácticos do Exército e ajudar a desenvolver procedimentos e mecanismos para os corrigir.

j. Síntese conclusiva

As operações ofensivas no Ciberespaço, obrigam ao estudo do direito de resposta a um ataque sob o ângulo do quadro legal internacional, não havendo para já razões para não aplicar a lei vigente que rege os conflitos armados, sem prejuízo de clarificações que uniformizem uma mesma leitura universal. Os problemas principais que se colocam são, a identificação do atacante, dada a natureza anónima do Ciberespaço, e a inexistência de fronteiras físicas definidas. A NATO caminha para uma posição que suporta que ataques no Ciberespaço a um dos membros podem conduzir a medidas colectivas de defesa ao abrigo do artigo V.

Os EUA implementam uma capacidade militar no Ciberespaço que inclui operações em todo o espectro, ou seja operações ofensivas, defensivas e exploratórias, apostando claramente na obtenção da supremacia neste novo domínio, recrutando milhares de homens.

A capacidade exploratória do Ciberespaço, configura a existência do mesmo conhecimento, técnicas e recursos necessários para as operações ofensivas.

AS FFAA não têm implementadas capacidades ofensivas ou exploratórias do Ciberespaço efectivas, embora o Exército disponha na sua estrutura do módulo CIRC que tem na missão implementar operações nessa área e tenha adquirido competências orientadas para o aumento da segurança das suas redes, permitindo detectar e antecipar vulnerabilidades e sempre orientado para o emprego em campanha.

Os factos apresentados completam a resposta à QD 2 e validam a HIP 3.

Depois de esclarecidas as capacidades militares no Ciberespaço, e a situação das FFAA a esse respeito, no capítulo seguinte vamos mostrar de que modo pode melhorar a capacidade militar existente nesta área.

"O homem sábio, em tempo de paz, prepara-se para a guerra"

Horácio

4. Uma responsabilidade partilhada na procura do sucesso na guerra do Ciberespaço

A defesa de um Ciberespaço universalmente partilhado não é tarefa simples. Como não existe uma autoridade única que superintenda esse domínio, existem dificuldades que ultrapassam as capacidades de uma só organização. Mesmo nas FFAA, que executam operações no domínio aéreo, marítimo e terrestre e necessitam do apoio centrado na utilização do Ciberespaço, poderá haver responsabilidades repartidas. Com o aprofundamento desta questão podemos estar em condições de mostrar uma estrutura que permita preparar as FFAA para responder eficazmente à ameaça da Ciberguerra.

a. A necessidade de uma Percepção da Situação ("*Situation awareness*") partilhada

Há a tendência, quando se fala de Ciberguerra, de concentrar os esforços principalmente na tecnologia. Todavia há um conjunto de processos, procedimentos e regras da utilização que não envolvem forçosamente nova tecnologia, como por exemplo a integração dos sensores existentes nas diferentes redes, ou a definição dos processos para a partilha de informação.

Como nas outras áreas militares, apenas uma boa percepção da situação, conseguida através de mapas de situação permanentemente actualizadas permite uma resposta adequada. Segundo Keys, é necessário que alguém compreenda o que está a acontecer, o que está prestes a acontecer e o que já aconteceu. Uma tal percepção da situação, inclui a compreensão do campo de batalha, a identificação das possíveis ameaças, e os riscos que colocam. Inclui ainda uma priorização da ameaça, o conhecimento das capacidades amigas, as suas vulnerabilidades e o estado operacional actual. Acresce que no Ciberespaço, não existe actualmente uma Entidade que tenha a capacidade ou autoridade para manter o nível de detalhe necessário na percepção da situação, garantindo um acesso ininterrupto ao Ciberespaço. A percepção da situação, depende da troca de informação entre um vasto leque de entidades, desde parceiros internacionais, agências governamentais, indústria, meios académicos, e mesmo utilizadores individuais. (Keys, 2009:12).

Ainda segundo o Gen Keys, uma visão comum deste novo campo de batalha, ou

Common Operational Picture (COP) ilustrando todas as actividades do ciberespaço, quer do ponto de vista das nossas forças, quer do ponto de vista das forças opositoras, é uma necessidade sem a qual não é possível suportar os esforços da resposta a incidentes do ciberespaço, sejam eles associados com desastres naturais, acidentais, ou devidos a uma falha intrínseca ou a ameaças derivadas de ataques terroristas, militares ou criminosos. Esta COP terá que ser integrada, dinâmica, agregada e partilhada, para permitir prever acções no Ciberespaço, desenvolver modalidades de acção, executar e monitorizar as acções de resposta, e possibilitar análise posterior. Deve permitir a obtenção das seguintes capacidades:

- Capacidade para compreender os acontecimentos correntes no Ciberespaço;
- Capacidade para antecipar ataques e eventos no Ciberespaço;
- Capacidade para reconhecer eventos não planeados na rede;
- Capacidade para iniciar precocemente a análise de acções alternativas;
- Capacidade para monitorizar a compatibilidade na rede;
- Capacidade para escolher respostas defensivas, mais completas e efectivas ou reconfigurações da rede.

As capacidades elencadas por Keys como sendo as necessárias para uma boa percepção, embora fáceis de listar, envolvem em si mesmas uma panóplia de tecnologias, procedimentos e recursos humanos que não são de desprezar e a obtenção de todas elas em conjunto, obriga a um planeamento cuidado e a uma política de investimentos na infra-estrutura de comunicações e sistemas de informação que facilite a gestão a monitorização e o controle de uma forma automática, única forma de responder defensivamente de forma eficaz a ataques vindos do Ciberespaço.

É pois necessário haver uma COP do Ciberespaço, tal como existe actualmente para os outros domínios da actividade militar, Terra, Mar e Ar com as "imagens" terrestre, marítima e aérea, fornecida pelos diversos sistemas de comando e controlo, que além de permitirem o seguimento em tempo real das operações, são um importante apoio à tomada de decisão, nos postos de comando.

Apenas tendo a percepção do que está a acontecer se podem efectivamente tomar decisões que minorem ou evitem os danos que um incidente possa provocar. É também esta percepção do estado da rede, dos computadores que formam a rede e dos programas que neles correm, que contribuirá para o aumento da confiança e segurança, na utilização do Ciberespaço no apoio às operações militares executadas pelos Ramos. Como nos

sistemas de comando e controle, esta COP do Ciberespaço, poderá suportar vários patamares de agregação, como forma óbvia de reduzir o consumo de largura de banda e tráfego com a informação de gestão e controle da própria rede. Estes patamares podem situar-se ao nível dos Ramos e ser centralizados num patamar superior com sede no EMGFA. Colocamos este cenário, já numa perspectiva de aplicação às FFAA. Mas ao mesmo tempo que falamos na necessidade de uma COP que pode ser gerada pelos Ramos e depois de agregada, partilhada com o EMGFA, não podemos ignorar um primeiro aspecto que importa esclarecer. A quem nas FFAA deverá ser atribuída a defesa e a exploração do Ciberespaço?

b. Uma missão para um Ramo ou para os Ramos

Ao longo dos tempos as FFAA foram alterando a sua estrutura de modo a optimizarem a sua capacidade militar, tendendo à especialização. Na situação actual existem três Ramos, Exército, Marinha e Força Aérea, sendo que a Força Aérea apenas existe como Ramo desde 1 de Julho de 1952, data em que se tornou independente, integrando as aviações incorporadas na Marinha e no Exército. Quarenta anos antes tinha nascido a aviação militar portuguesa no Exército. Um domínio, o ar, que até então não tinha valor militar, nem se apresentava como uma ameaça, ganha repentinamente um valor imensurável, graças ao avanço tecnológico que foi a invenção do avião. As operações no domínio aéreo ganharam tal relevância, que as operações nos outros domínios, terra e mar, apenas têm hipóteses de sucesso, se estiver garantida a supremacia aérea.

O relevo ganho pelo Ciberespaço, ilustrado na Figura Nº2, ao constituir-se num novo domínio em que que é necessário supremacia para poder ser utilizado em proveito das operações militares nos outros domínios colocou a questão de qual o Ramo a que deve ser atribuída a missão quer de defender, quer de explorar o Ciberespaço. Relativamente a esta questão nas Forças Armadas Americanas, referia o Gen Keith B. Alexander, Comandante do *USA Cyber Command*, que traduzimos: "*O Ciberespaço é de alguma maneira parecido com o domínio aéreo, na medida em que não tinha relevância no planeamento militar até que de repente uma nova tecnologia lhe ofereceu acesso. Um século atrás os militares de todo o mundo, tiveram que aprender rapidamente a lutar no Ar, e tiveram que fazê-lo, todos ao mesmo tempo, no meio de uma guerra mundial. Reconhecemos que nenhum Ramo pode possuir o domínio aéreo por completo ou reclamar o seu exclusivo uso; todos os Ramos requerem acesso, todos requerem capacidades aéreas*

e todos contribuem para a batalha conjunta. O paralelo com o Ciberespaço parece óbvio: liberdade de acção no Ciberespaço, tal como a liberdade de manobra no Ar, é crucial para o emprego de uma força em todos os domínios"(Alexander, 2010b:5). Esta declaração clarifica a política que foi seguida nos EUA relativamente às operações no Ciberespaço. Na verdade como vimos, tanto a Marinha como o Exército, a Força Aérea e os Marines, dispõem de "*Cyber Commands*", centralizados pelo CYBERCOM.

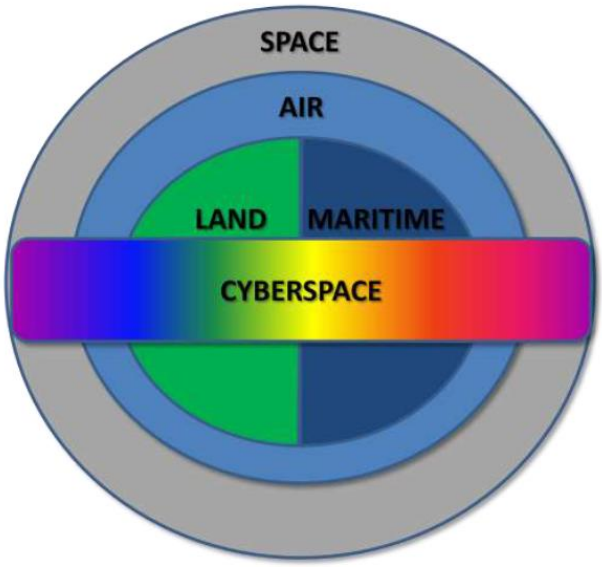


Figura 2: Relações entre os domínios operacionais[10]

Uma abordagem deste género aplicada às FFAA, facilita desde logo a implementação, pois para combater nas redes de computadores do Ciberespaço, são precisas redes de computadores, e estas já existem e estão distribuídas pelos vários Ramos. São os Ramos que conhecem as suas redes e as suas necessidades específicas em termos de serviços de rede. Além de que, a utilização do Ciberespaço é essencial para a conduta de operações nos outros domínios, pelo que cada Ramo tem que ter algum controle sob uma parte do Ciberespaço para o apoio e execução das suas operações militares. Tal como nos EUA, pensamos que os Ramos devem ter liberdade de acção no Ciberespaço, podendo dispor de todas as capacidades de que necessitem sem prejuízo da coordenação superior ditada pela natureza das operações militares que sejam atribuídas às FFAA. A própria existência de três ou quatro núcleos com capacidades no domínio do Ciberespaço, e consequente aumento de recursos humanos, significa a valoração e a seriedade que deve

[10] Fonte: United States Air Force Doctrine Document 3-12 (USAF, 2009:20)

ser atribuída a este assunto.

A coordenação superior, centralizada ao nível das FFAA é também fundamental, principalmente para as estratégias de defesa, pois as vulnerabilidades detectadas num dos Ramos só serão efectivamente úteis na defesa dos outros Ramos, se rapidamente ou automaticamente, políticas comuns de segurança e defesa forem aplicadas a todas as redes tornadas vulneráveis e expostas.

O facto da principal rede física militar de transporte das comunicações, o SICOM, já ser administrado centralmente pelo EMGFA, facilita a introdução de equipamentos de gestão e segurança, que não se podem apenas limitar á malha principal da rede, mas devem abranger também as próprias redes locais das unidades e órgãos, mesmo que a parte de administração e gestão local, continue a ser executada, como até aqui, pelas equipas existentes nos Ramos, normalmente com os recursos existentes nas unidades em coordenação com a entidade gestora dos sistemas de comunicação e informação de cada Ramo. No fundo a instalação, gestão e manutenção da infra-estrutura física de transporte e equipamentos de rede será totalmente da responsabilidade do EMGFA, enquanto a sua exploração será feita, pelos Ramos. Uma harmonização centralizada da infra-estrutura, facilita a coerência de todo o sistema, e é um factor relevante não só para uma maior resistência a acções ofensivas vindas do Ciberespaço, mas também para uma maior resiliência, dada uma melhor facilidade de programar automaticamente caminhos alternativos criando redundâncias.

c. Uma Responsabilidade autónoma ou partilhada?

Mas será que a criação de uma estrutura nos Ramos, apoiada e coordenada por um núcleo centralizado no EMGFA, garante que as FFAA ficam estruturalmente preparadas para as operações que utilizem o Ciberespaço?

Centrando-nos apenas nas operações defensivas, podemos com segurança responder que não. Num espaço, como atrás foi referido, tão densamente povoado, a melhor segurança é uma segurança cooperativa. O Ciberespaço será tanto mais seguro, quanto mais forem as organizações que efectivamente se preocupem com a sua segurança. Os núcleos CIRC dos Ramos e do EMGFA, depois de criados, têm de partilhar informações sobre vulnerabilidades detectadas com outros núcleos CIRC existentes, quer a nível nacional, com outros organismos governamentais, quer a nível internacional, no quadro das organizações militares em que se insere, nomeadamente a NATO.

Exemplo deste caminho, são os passos que o EMGFA já trilhou e que apontam no sentido descrito. O EMGFA, considerando a crescente importância que as questões da segurança das redes e da informação vêm assumindo, procurou melhorar a sua protecção, estabelecendo protocolos de colaboração com entidades nacionais, que se preocupam também com a segurança, das redes de computadores, ligadas à internet, no sentido de manter uma **C**apacidade de **R**esposta a **I**ncidentes de **S**egurança **I**nformáticos (CRISI). O protocolo estabelecido com a Fundação para a Computação Científica Nacional (FCCN), permite a troca de informação e conhecimento visando a implementação de mecanismos, procedimentos e gestão de segurança, por forma a prevenir, detectar e deter os incidentes de segurança que possam afectar a confidencialidade, integridade e disponibilidade dos Sistemas de Informação e Comunicação nas FFAA. Sendo a FCCN a responsável nacional pelo serviço do "*Computer Emergency Response Team*-CERT.PT, garante também a ligação com entidades europeias congéneres, incluindo a Agência Europeia para a Segurança da Informação e Redes (ENISA).

Esta responsabilidade pela segurança, apresenta pois vários patamares de responsabilidade partilhada. Um primeiro patamar entre os Ramos e o EMGFA, um segundo entre o EMGFA e as organizações nacionais, e um terceiro entre o EMGFA e as organizações militares internacionais a que Portugal pertence, com natural destaque para a NATO. Lembramos a este respeito, que no seu Conceito Estratégico, como referimos anteriormente, a NATO pretende melhorar a integração da sua COP sobre o Ciberespaço, assim como o sistema de alerta e resposta com os Países membros.

O facto de o nosso trabalho ter sido delimitado para estudar apenas as FFAA, nos seus desafios para enfrentar a ameaça da Ciberguerra, não nos impede, antes pelo contrário, obriga-nos a entender as implicações que existem ao nível da sociedade civil, quando falamos das ameaças vindas do Ciberespaço, e da melhor forma de as combater.

(1) A partilha com as entidades privadas e organismos do Estado

Na verdade, quando atrás, caracterizámos a Ciberguerra como uma ameaça real, vimos que um dos alvos mais prováveis de ataques pelo Ciberespaço, serão as infra-estruturas vitais que suportam o actual modo de vida das nossas sociedades. São exemplo destes possíveis alvos, a rede eléctrica formada pelas centrais eléctricas, quer hidráulicas, baseadas nas várias barragens, quer térmicas, quer eólicas, e todo o subsistema de distribuição e interligação. Relembramos que todos estes sistemas são actualmente controlados por sistemas computorizados, muitos deles por controlo remoto. Outro

exemplo são as infra-estruturas de transportes, seja o ferroviário, seja o aéreo, ambos fortemente dependentes do Ciberespaço. Na área financeira e económica a dependência do Ciberespaço é avassaladora.

Mesmo antes de tentarmos equacionar a articulação das FFAA com qualquer outras entidades, deveremos questionar, em termos legais, a quem cabe defender as infra-estruturas vitais do Estado face a um ataque vindo do Ciberespaço. Será às FFAA? Às Forças de Segurança e Polícias? Às entidades gestoras dessas infra-estruturas? Estas questões, que se colocam sobre a Ciberguerra, são idênticas às que se colocam sobre outros tipo de ameaças, como sejam ataques terroristas que utilizam técnicas e métodos cinéticos, nomeadamente explosivos ou projécteis, tendo sido amplamente estudado pelo Coronel Isidro Pereira no seu trabalho sobre o emprego das FFAA nas operações de combate ao terrorismo internacional. Segundo o autor, existem lacunas, imprecisões e vazios legislativos que podem conduzir a situações dúbias e a processos de decisão demorados (Pereira, 2009:31). E continua referindo que muita da legislação, mesmo recente, ao apontar os novos conjuntos de missões para as FFAA continuam a não definir as situações concretas do emprego, remetendo para as habituais expressões "nos termos da Constituição e da lei", " a definir na lei",etc., E conclui, afirmando que a legislação referente às FFAA transportam do texto constitucional a tradicional separação entre defesa nacional e segurança interna.

Na verdade o texto constitucional, pelo seu Art. 273, Nº2 associa a defesa nacional, à defesa "…*contra qualquer agressão ou ameaça externas*". Pelo Art. 275, "*Às FFAA incumbe a defesa militar da República*" sendo também estabelecido no seu ponto 7, "*As leis que regulam o estado de sítio e o estado de emergência fixam as condições do emprego das Forças Armadas quando se verifiquem essas situações"* (Constituição,2005:55). O primeiro grande problema começa aqui, com a classificação de "*externa*" a uma ameaça ou agressão, e da dificuldade que resulta para um decisor, seja ele político ou militar, classificar um ataque efectuado pelo Ciberespaço. Como referimos, no nosso trabalho, é muito difícil, se não impossível, identificar de onde vem um ataque, e muito menos quem nos está a atacar, e esse facto não devia ser inibidor de haver uma resposta imediata e eficaz. Se a utilização das FFAA fica dependente de uma classificação que nunca irá ocorrer, ninguém conseguirá dar a ordem que permitiria mitigar os danos. Alguns autores advogam que o critério para a actuação das FFAA deveria incluir um critério de "*dimensão e intensidade da ameaça*" em vez da dimensão *externa*.

Não é inócuo o facto de haver alguma ambiguidade e mesmo omissão de quem é a responsabilidade sobre a defesa a ataques vindos pelo Ciberespaço. É que para defender é necessário preparar a defesa. Para prevenir é necessário que se treine a defesa. Para treinar a defesa é necessário ter os meios e definir os procedimentos. É ainda necessário haver formação para que tudo isto aconteça. Não se pode estar à espera que aconteça o ataque, para depois vermos como é que se vai defender. Infelizmente não é assim que funciona a realidade. Se para defender as redes das FFAA, suas infra-estruturas e sistemas, não há ambiguidade, pois tal responsabilidade cabe às próprias FFAA, quando se trata de defender as outras infra-estruturas vitais do Estado, geridas por organizações governamentais, ou por organizações civis, numa primeira análise tal defesa cumpre às próprias entidades, sem prejuízo de um complemento com capacidades residentes nas FFAA.

Daqui resulta, que para haver uma defesa eficaz contra ameaças de segurança, vindas do Ciberespaço, as infra-estruturas consideradas vitais para o funcionamento do Estado e da sociedade, devem possuir também sistemas de protecção e segurança das suas redes, terem os seus próprios CERT se necessário e para uma resposta integrada devem partilhar informação com um CERT nacional de topo, que deverá ter a autoridade respectiva para coordenação, ao qual também se liga o CIRC do EMGFA. Claro que para tudo isto ser possível, terá que haver alguma legislação adicional, que além de criar os CERT e CIRC, facilite a articulação operacional, e no mínimo estabeleça estruturas e procedimentos comuns que garantam a interoperabilidade de equipamentos e dos sistemas de segurança e protecção.

d. O que é necessário fazer?

Tendo analisado a problemática da segurança no Ciberespaço, fomos levados a concluir, como Quémener, que a defesa da rede, a fim de evitar uma Ciberguerra não pode ser concebida que de um modo global e o conjunto de actores devem estar imbuídos de uma dinâmica comum (Quémener, 2009:95). E colocámo-nos na posição de perguntar o que é que é necessário fazer, para enfrentar este desafio. Podemos enunciar alguns princípios básicos a seguir na implementação dos sistemas de protecção e segurança das redes de computadores, que sendo válidos para as FFAA são de aplicação universal, podendo ser aplicados a outras organizações. Assim devemos entre outras:

- Ter uma arquitectura que aceite indicações e forneça avisos ou alertas;
- Implementar capacidades de gestão das redes e ferramentas básicas de protecção da informação, incluindo *firewalls*, antivírus e detecção de intrusão;

- Manter uma gestão hierarquizada da rede;
- Criar um centro de operações para as redes do Ciberespaço, que mantenha actualizada a COP, para fornecer atempada detecção, prever e responder a ataques às infra-estruturas das redes. Aliás esta "*situation awareness picture*" deve ser um atributo de qualquer dos núcleos CIRC;
- Elaborar um programa de gestão de todo o processo que garanta a segurança, integridade e confidencialidade da informação incluindo a definição das políticas de segurança, a avaliação, acreditação, a certificação dos sistemas e o treino dos utilizadores;
- Definir um programa de exercícios, para obter treino e experiência em remediar, recuperar e fazer planos de contingência alternativos;
- Definir as áreas prioritárias de investimento, enumerando as infra-estruturas críticas a proteger;
- Definir o quadro legal que permita a atribuição de responsabilidades aos diversos intervenientes.

e. Síntese conclusiva

Vemos neste capítulo que a defesa das redes de computadores, a fim de evitar uma Ciberguerra não pode ser concebida, senão de um modo global. A defesa do Ciberespaço só será efectiva se houver uma cooperação e partilha de responsabilidades entre os vários actores, nomeadamente as FFAA, as entidades governamentais, entidades gestoras de infra-estruturas publicas e privadas, englobando ainda as principais organizações internacionais, de protecção e segurança na área do Ciberespaço, civis e militares, nomeadamente a NATO.

Dentro das FFAA, os Ramos também devem ter responsabilidades na defesa e protecção da parte do Ciberespaço de que necessitam para apoio das operações militares específicas do respectivo Ramo, devendo para o efeito manter um CIRC com ligação subordinada ao CIRC do EMGFA que manterá a ligação nacional e internacional na área das FFAA aos outros CERT´s.

Mostramos que manter uma COP do Ciberespaço, é um passo fundamental na detecção e prevenção, antecipação de ataques, bem como no apoio à tomada de decisão.

Concluímos também que a legislação não é clara quanto ao emprego ou atribuição de missões ou responsabilidades às FFAA, na resolução de ataques pelo Ciberespaço.

Os factos apresentados permitem responder à QD 3 e validam a HIP 4.

Conclusões

Para a abordagem do presente trabalho estudando a forma como as FFAA se devem estruturar para enfrentar a ameaça da Ciberguerra optámos por o dividir em quatro capítulos, tentando validar outras tantas hipóteses de resposta que formulámos para responder às três Questões Derivadas que nos orientaram.

Assim no primeiro capítulo caracterizamos a Ciberguerra, esclarecendo conceptualmente o que é que deve ser entendido como tal. Mostramos que a Ciberguerra apesar de ser tratada no Ciberespaço, é uma ameaça real e não virtual. Para chegar a essa conclusão, tipificamos as principais ameaças e descrevemos as principais fontes ou possíveis autores. Mostramos que as fontes de ameaças são diversas podendo ser praticadas quer por indivíduos, grupos criminosos, terroristas ou mesmo estados e a forma pode variar entre vários tipos de código malicioso, utilizado para controlar, danificar, roubar ou negar o acesso aos sistemas de informação.

Ilustramos a ameaça, realçando uma realidade que veio para ficar e à qual os decisores políticos e os responsáveis pela segurança e defesa dos Estados não poderão ficar indiferentes, relembrando os exemplos mais recentes e relevantes de ataques característicos de Ciberguerra e enquadramos a Ciberguerra na ciência militar utilizando a doutrina de referência americana partindo para a sua classificação em operações defensivas, ofensivas e exploratórias do Ciberespaço.

Notamos ainda que muitos são os países que já dispõem de capacidades em Ciberguerra.

No segundo capítulo analisamos a Ciberguerra sob o ponto de vista meramente defensivo, e verificamos que manter uma capacidade defensiva não é uma opção, mas sim uma necessidade, para podermos garantir a utilização, com segurança, do Ciberespaço no apoio das operações militares. Indicamos que essa necessidade se traduz na protecção dos valores da *Integridade*, *Confidencialidade* e *Disponibilidade* da informação, da constante ameaça dos ataques vindos do Ciberespaço, que tentam contornar ou iludir os mecanismos de defesa implementados. Realçamos que não há sistemas completamente seguros, e que se devem rever as estratégias de defesa, seleccionando os recursos mais valiosos, e elegendo-os para uma mais profunda protecção.

Mostramos que a NATO encara a sério a defesa do Ciberespaço e criou o CCC COE, uma capacidade NCIRC e a autoridade NATO para a gestão do Ciberespaço e que nas FFAA, os Ramos têm múltiplas redes de computadores, com uma gestão própria

mantendo uma capacidade mínima de defesa contra ataques externos.

No terceiro capítulo debruçamo-nos sobre as operações ofensivas e exploratórias do Ciberespaço, quiçá as operações que mais reservas e preocupações levantam aos Estados quanto ao enquadramento legal da sua posse e utilização. Estas operações obrigam ao estudo do direito de resposta a um ataque sob o ângulo do quadro legal internacional, não havendo razões para não aplicar a lei vigente que rege os conflitos armados, não obstante o principal problema que se coloca e que tem a ver com a dificuldade da identificação do atacante.

Clarificamos que a NATO caminha para uma posição que suporta que ataques no Ciberespaço a um dos seus membros podem conduzir a medidas colectivas de defesa ao abrigo do artigo V e mostramos que a capacidade exploratória do Ciberespaço configura a existência do mesmo conhecimento, técnicas e recursos necessários para as operações ofensivas.

Notamos que os EUA implementam uma capacidade militar no Ciberespaço que inclui operações em todo o espectro, e apostam claramente na intenção de obter a supremacia neste novo domínio da guerra, indiciando que, mais do que combater no Ciberespaço, os EUA estão a preparar os combatentes do futuro, antecipando a guerra do futuro, que será travada com *joysticks*. Ao mesmo tempo esclarecemos que as FFAA não têm implementadas capacidades ofensivas ou exploratórias efectivas, embora o Exército disponha na sua estrutura do módulo CIRC que tem a missão de implementar operações nessa área.

No último capítulo apresentamos a forma de melhorar as capacidades existentes nesta área da ciência militar, no que respeita às FFAA e concluímos que a defesa não pode ser concebida senão de um modo global. A partilha de responsabilidades é multifacetada, ocorrendo não só entre os próprios Ramos e o EMGFA, que devem possuir os seus próprios CIRC, mas também uma responsabilidade partilhada com os organismos governamentais e empresas gestoras das infra-estruturas vitais do país, e ainda com as organizações internacionais congéneres civis e militares, com especial destaque neste último caso para a NATO.

Mostramos a necessidade de elaborar e manter uma COP do Ciberespaço, como passo fundamental na detecção, prevenção e antecipação de ataques bem como no apoio à decisão e evidenciamos também, que a legislação que regula o emprego ou atribuição de missões ou responsabilidades às FFAA na resolução de ataques pelo Ciberespaço, não é

clara, sendo por vezes ambígua, e por isso um problema sério que necessita de ser corrigido, tendo alguma analogia com o tratamento a dar à defesa contra ataques terroristas de dimensão e intensidade elevados, e o empenhamento das FFAA nessas operações.

Por fim indicamos alguns dos passos que as organizações podem implementar para estabelecer uma capacidade de defesa na área da Ciberguerra, pois também nos outros sectores do Estado não são visíveis grandes preocupações com as ameaças vindas do ciberespaço e reafirmamos que para uma defesa eficaz, as infra-estruturas consideradas vitais para o funcionamento do Estado e da sociedade, devem possuir também sistemas de protecção e segurança das suas redes.

Concluímos assim, que o Ciberespaço não conhece fronteiras físicas, mas tem de ser protegido do mesmo modo que são protegidos o espaço aéreo, o espaço terrestre e o espaço marítimo, lembrando que para combater redes de computadores, são precisas redes de computadores, e que os Ramos já possuem as suas redes, e necessitam do controle de uma parte do Ciberespaço para apoio das suas operações específicas militares. Por isso defendemos que os Ramos devem possuir núcleos com as capacidades necessárias para efectuar operações de Ciberguerra, sempre com interligação e coordenação com o EMGFA que estenderá a defesa cooperativa às organizações militares de que Portugal faz parte nomeadamente a NATO, e às organizações civis relevantes.

Com a validação das quatro hipóteses apresentadas neste trabalho, estamos em condições de responder à Questão Central por nós formulada, apresentando os caminhos que as FFAA devem percorrer para melhor enfrentarem as ameaças da Ciberguerra, caminhos esses que passam pela ajustamento da estrutura, clarificação do quadro legal de emprego, cooperação com entidades nacionais e internacionais com interesses comuns na área da Ciberguerra, complementando com a necessidade de obter formação e treino.

BIBLIOGRAFIA

- AMARAL, Paulo (2008), *Top Secret. Como Proteger os Segredos da sua Empresa e Vigiar os Seus Concorrentes*. Alfragide: Academia do Livro, 2008, ISBN: 9789898194022.
- ALEXANDER, Keith (2010), *Advanced questions for Lieutenant General Keith Alexander, USA Nominee for Commander,United States Cyber Command* [Em linha]. Washington, 15 de Abril de 2010. [Referência de 18 de Outubro de 2010]. Disponível em: http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf
- ALEXANDER, Keith (2010b), *Statement of General Keith Alexander, Commander United States Cyber Command before The House Committee on Armed Services* [Em linha]. Washington, 23 de Setembro de 2010. [Referência de 4 de Novembro de 2010]. Disponível em: http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf
- ALBERTS, David S., GARSTKA,John J., STEIN,Frederick P.(1999),*Network Centric Warfare*, Washington: *Library of Congress*, 1999.
- AM (2004), *Seminário Final*. Pós-Graduação Guerra de Informação Competitive Inteligence. Lisboa: Academia Militar, 20 de Fevereiro de 2004 p. 103.
- AR (2009), *Lei nº 31-A/2009 - Lei de Defesa Nacional*. Diário da República Electrónico,1ª série Nº129 de 7 de Julho de 2009. Art 2º,2 [Em linha]. Lisboa: Imprensa Nacional Casa da Moeda, 7 de Julho de 2009. [Referência de 12 de Outubro de 2010]. Disponível em: http://www.mdn.gov.pt/mdn/pt/Defesa/Legislacao/
- AR (2009a), *Lei nº 1-A/2009 - Lei Orgânica de Bases da Organização das Forças Armadas.* Diário da República Electrónico, 1ª série Nº129 de 7 de Julho de 2009, Cap. I, Art. 1º,1. [Em linha]. Lisboa: Imprensa Nacional Casa da Moeda, 7 de Julho de 2009. [Referência de 12 de Outubro de 2010]. Disponível em: http://www.mdn.gov.pt/mdn/pt/Defesa/Legislacao/
- CBS (2009), *Cyber war: Sabotaging the system. 60 minutes* [Em linha]. Washington: Columbia Broadcasting System, 9 de Novembro 2009 aos 2mn e 25s. [Referência de 7 de Outubro de 2010]. Disponível em: http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml

−CBSNEWS (2010), *Computer Worm Attacks Iran Nuclear Plant* [Em linha]. New York: Columbia Broadcasting System,26 de Setembro 2010. [Referência de 14 de Outubro de 2010]. Disponível em: http://www.cbsnews.com/video/watch/?id=6903168n

−CCDCOE (2010), *Cooperative Cyber Defence Centre o Excellence Tallinn, Estonia*[Em linha]. [Referência de 29 de Outubro de 2010]. Disponível em: http://ccdcoe.org/

−CM (2010), *A visão do general - Ciberguerra* [Em linha]. Lisboa: Correio da Manhã, 5 de Setembro 2010. [Referência de 7 de Outubro de 2010]. Disponível em: http://www.cmjornal.xl.pt/detalhe/noticias/opiniao/loureiro-dos-santos/ciberguerra

−COMPUTERWORLD (2007), *Estonia recovers from massive denial-of-service attack* [Em linha]. Framingham:COMPUTERWORLD,17 de Maio de 2007. [Referência de 14 de Outubro de 2010]. Disponível em: http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

−CONSTITUIÇÃO, da República Portuguesa(2005) [Em linha]. Lisboa: Assembleia da República 2005. [Referência de 30 de Janeiro de 2011]. Disponível em: http://www.cne.pt/dl/crp_pt_2005_integral.pdf

−CORREIA, CFR Dias (2010), artigo na 2ª Conferência: *As comunicações na Marinha*. Lisboa: Revista da Armada Nº444, Agosto de 2010.

−CWID(2006), *Information Assurance (IA) Results* [Em linha],Coalition Warrior Interoperability Demonstration 2006 Final Report.[Referência de 27 de Outubro de 2010]. Disponível em: http://www.cwid.js.mil/public/CWID06FR/htmlfiles/134ia.html

−DINIS, Cor José (2009), *A guerra da Informação: Perspectivas de Segurança e Competitividade*. Lisboa: Revista Militar, artigo publicado em 18 de Junho de 2009.

−EDITORA,Porto (2010),*Dicionário da Lingua Portuguesa* [Em linha]. Lisboa: Porto Editora 2010.[Referência de 22 de Outubro de 2010]. Disponível em: http://www.infopedia.pt/lingua-portuguesa/

−EXPRESSO (2010), *Ciberataques e pirataria são novas preocupações da NATO*. Lisboa: Jornal Expresso 23 de Outubro de 2010, p 34.

−EXPRESSO (2011), *Sistema Vigilis detecta 75 mil vulnerabilidades em Portugal.*. [Em linha]. Lisboa, 4 de Janeiro de 2011.[Referência de 4 de Janeiro de 2011]. Disponível em http://aeiou.expresso.pt/ataques-informaticos-sistema-vigilis-deteta-75-mil-vulnerabilidades-em-portugal=f624021

−FISHER,Max (2010), *Military-Grade Malware Spurs Theories on New Cyberwar Threat.*

[Em linha]. Washington,24 de Setembro de 2010. [Referência de 15 de Outubro de 2010]. Disponível em: http://www.theatlanticwire.com/opinions/view/opinion/Military-Grade-Malware-Spurs-Theories-on-New-Cyberwar-Threat-5158

- FREIRE, Cor Fernando José Vicente Freire (2010), Conferência, *As Forças Armadas em rede: ameaças e vantagens competitivas*. Évora, 2 de Junho de 2010, I Congresso Nacional de Segurança e Defesa.
- GAO (2010), *Cyberspace – Report to Congressional requesters* [Em linha]. Washington: United States Government Accountability Office,12 de Julho de 2010. [Referência de 12 de Outubro de 2010]. Disponível em: http://www.gao.gov/new.items/d10606.pdf .
- GOLDGEIER, James M.(2010), *The Future of NATO*, Council Special Report Nº51 [Em linha]. Washington: COUCIL on FOREIGN RELATIONS, Fevereiro de 2010. [Referência de 30 de Outubro de 2010]. Disponível em: www.cfr.org/content/publications/attachments/**NATO_CSR51**.pdf
- GOODMAN, Seymour E. LIN, Helber S. (2007). *Toward a Safer and More Secure Cyberspace.* Washington: The National Academies Press, 2007.
- GUEDES, Prof Armando Marques (2010), Artigo: *The new geopolitical coordinates of cyberspace*. Lisboa: Revista Militar, Agosto/Setembro de 2010, Pag 823-846
- HERNANDEZ, MGen US Army Rhett (2010), *Statement before the House Armed Services Committee, as incoming Commanding General of US Army Forces Cyber Command.*[Em linha]. Washington 23 de Setembro de 2010. [Referência de 6 de Fevereiro de 2011]. Disponível em: http://cryptome.org/dodi/army-cyber.pdf
- HILÁRIO, Cor Francisco Manuel de Sampaio (2008), *O sistema de informação do Minitério da Defesa Nacional. Sua relevância na administração da Força Aérea*. Lisboa: IESM 2008, TII
- HUNKER, Jeffrey (2010) , *Cyber war and cyber power, issues for Nato doctrine* [Em linha]. Roma: NATO Defense Colledge, Research Paper Nº62, Novembro 2010. [Referência de 23 de Janeiro de 2011]. Disponível em: http://www.ndc.nato.int/research/series.php?icode=1
- INFOPEDIA (2010), *Enciclopédia e Dicionários Porto Editora.* [Em linha]. Porto 2010. [Referência de 17 de Outubro de 2010]. Disponível em: http://www.infopedia.pt/lingua-portuguesa

- ITU (2010), *Press release: 4.6 billion mobile subscriptions by the end of 2009* [Em linha]. .Genève: International Telecomunication Union, 6 de Outubro de 2009. [Referência de 13 de Outubro de 2010]. Disponível em: http://www.itu.int/newsroom/press_releases/2009/39.html
- IWS (2010), *Usage and Population Statistics* [Em linha]. 30 de Junho de 2010. Internet World Stats.[Referência de 13 de Outubro de 2010]. Disponível em: http://www.internetworldstats.com/stats.htm.
- JENKINS, Lt Col USAF James M.(2003), *Computer Network Defense: DoD and the National Responsev*[Em linha]. Alabama: Air War Colledge, 2 de Dezembro de 2002. [Referência de 30 de Outubro de 2010]. Disponível em: http://www.au.af.mil/au/awc/awcgate/awc/jenkins.pdf
- JP 1_02 (2010), *Dictionary of Military and Associated Terms* [Em linha]. Washington: Joint Publication 1-02, 31 de Julho de 2010. [Referência de 15 de Outubro de 2010]. Disponível em: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
- JP 3_13 (2010), *Information Operations* [Em linha].Washington: Joint Publication 3_13, 13 de Fevereiro de 2006. [Referência de 15 de Outubro de 2010]. Disponível em: http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm.
- JP 6_0 (2010), *Joint Communications System*. Washington: Joint Publication 6_0, 10 de Junho de 2010.
- KEYS, Ron General (ret), McKEY, Larry (2009), *Concept for Possible Cyberspace Shared situational Awareness*. Washington: *Joint Concept Technology Demonstration*, 22 de Setembro de 2009.
- LYNN,William (2010), US deputy Defense Secretary, *Cyberwarfare Extends Scope of Conflit* [Em linha]. Washington: *American Forces Press Service*. [Referência de 1 de Novembro de 2010]. Disponível em: http://www.defense.gov/news/newsarticle.aspx?id=61107
- Marques, CALM Gameiro (2010, *"A Engenharia na Marinha"*. Apresentação na Ordem dos Engenheiros. [Em linha]. Lisboa, 16 de Março de 2010. [Referência de 11 de Fevereiro de 20111]. Disponível em: http://www.ordemengenheiros.pt/fotos/dossier_artigo/7055920d969179ed6620ed49bf277a7c.pdf
- MAUPEAU, Stanislas de (2009), Internet, nouvelle infrastructure vitale!. Paris: Defense nationale et sécurité collective – Maio de 2009.

- NATO (1949), *The North Atlantic Treaty* [Em linha]. Washington D.C. 4 de Abril de 1949. [Referência de 30 de Outubro de 2010]. Disponível em: http://www.nato.int/cps/en/natolive/official_texts_17120.htm
- NATO (2009), *Nato and Cyber Defence*, 173 DSFC 09 E bis . p 67[Em linha]. [Referência de 28 de Outubro de 2010]. Disponível em: http://www.nato-pa.int/default.asp?SHORTCUT=1782
- NATO (2010), *NATO 2020 – Analysis and Recommendations of the Group of Experts on a new strategic Concept for NATO* [Em linha]. Brussels,17 de Maio de 2010. [Referência de 12 de Outubro de 2010]. Disponível em: http://www.nato.int/strategic-concept/expertsreport.pdf.
- NATO (2010b), *Strategic Concept For the Defense and Security of the Members of the North Atlantic Treaty Organization.* [Em Linha]. Lisboa, 19 de Novembro de 2010. [Referência de 28 de Janeiro de 2011]. Disponível em: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf
- NUNES, Paulo Fernandes Viegas Nunes, *Ciberterrorismo: Aspectos de Segurança*. Lisboa: Revista Militar, 25 de Junho de 2009.
- ONU (1955), *Carta das Nações Unidas* [Em linha]. Nova Iorque: ONU,14 de Dezembro de 1955. [Referência de 16 de Outubro de 2010]. Disponível em: http://www.fd.uc.pt/CI/CEE/pm/Tratados/carta-onu.htm
- OWENS, William A.,DAM Kenneth W., LIN, Herbert S. (2009). *Tecnology, Policy,Law, and Ethics Regarding U.S. Acquisition and Use of cyberattack capabilities*. Washington: The National Academies Press, 2009.
- PEREIRA, Cor Inf Isidro (2009), *As Forças Armadas nas Operações de combate ao terrorismo internacional,narcotráfico e imigração ilegal, numa perspectiva de emprego conjunto*. Lisboa: IESM , TII CPOG 08/09.
- QUÉMÉNER,Myriam, FERRY,Joel (2009), *La Guerre du cyberspace aura bien lieu.* Paris: Defense nationale et sécurité collective. Março de 2009.
- RAMOS, João(2011), *Primeiro Vírus Informático Criado há 40 Anos.* [Em linha]. Artigo na revista Exame Expresso de 19 de Março de 2011. [Referência de 19 de Março de 2011]. Disponível em : http://aeiou.expresso.pt/primeiro-virus-informatico-criado-ha-40-anos=f638343
- REED, John (2010), *USAF Stands up Cyber Unit* [Em linha]. Artigo de 25 de Janeiro de 2010.[Referência de 6 de Fevereiro de 2011]. Disponível em:

http://www.defensenews.com/story.php?i=4469657

−REUTERS (2010), Special Report:*The Pentagon´s new cyber warriors* [Em linha]. Washington 5 de Outubro de 2010. [Referência de 28 de Janeiro de 2010]. Disponível em: http://www.reuters.com/article/2010/10/05/us-usa-cyberwar-idUSTRE69433120101005?pageNumber=5

−RTm (2010), *Possibilidades Resultantes da missão Restabelecida* [Em linha]. Lisboa: Portal do Exército. [Referência de 31 de Outubro de 2010]. Disponível em: http://www.exercito.pt/sites/RT/Paginas/Visao_e_Missao.aspx

−SANTO, Gen Espírito (2010). *Novo Ano,Novos Desafios: Ciberataques e Ciberdefesa*.[Em linha]. Lisboa: Revista Militar, editorial de Julho de 2010. [Referência de 1 de Novembro de 2010]. Disponível em: http://www.revistamilitar.pt/modules/articles/article.php?id=533

−SANTOS,Gen José Alberto Loureiro dos (2009),*As Guerras Que Já Aí Estão e as Que Nos Esperam Se os Políticos não Mudarem*.Lisboa: Publicações Europa-América, Dezembro de 2009.

−SIGNALONLINE (2009), *Nato Confronts Cyberthreats* [Em linha]. FAIRFAX:AFCEA SIGNAL ONLINE, 8 de Setembro de 2009. [Referência de 30 de Outubro de 2010]. Disponível em: http://afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2052&zoneid=47

−STRATCOM (2010), *US Cyber Command* [Em linha]. United States Strategic Command, 2010. [Referência de 1 de Novembro de 2010]. Disponível em: http://www.stratcom.mil/factsheets/cc/

−TECNOLYTICS (2010), *Cyber Commander´s Handbook.* Washington: Technolytics, Janeiro de 2010.

−TELEGRAPH (2008), *Georgia: Russia conducting cyber* war [Em linha]. Londres: Telegraph.co.uk, 11 de Agosto 2008. [Referência de 16 de Outubro de 2010]. Disponível em: http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html

−TISSIER,Guillaume (2009), *Lutte informatique et droit international*. Defense nationale et sécurité collective. Paris, Março de 2009.

−USAF, United States Air Force (2009), *Air Force Doctrine Document 3-12* [Em linha].

Washington, 15 de Julho de 2010. [Referência de 28 de Janeiro de 2011]. Disponível em: http://www.airforce-magazine.com/SiteCollectionDocuments/TheDocumentFile/Strategy%20and%20Concepts/AFDD3-12.pdf

- VENTRE, Daniel (2008), *Cybercriminalité, recours à la force,attaque armée*, Defense nationale et sécurité collective. Paris, Maio de 2008.
- WEBBER, MGen *Richard* E.(2010), *Presentation to the House Armed Services Committee, subject on Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations* [Em linha]. Washington, 23 de Setembro de 2010. [Referência de 28 de Janeiro de 2011]. Disponível em: http://democrats.armedservices.house.gov/index.cfm/files/serve?File_id=8b28f10f-e164-481f-93cc-0c0734195fb1

ENTREVISTAS

- COIMBRA, MGen Dias, 2ºCmdt da Academia Militar, e Presidente da Associação para a *Competitive Intelligence & Information Association Warfare – Club*, 20 de Outubro de 2010.

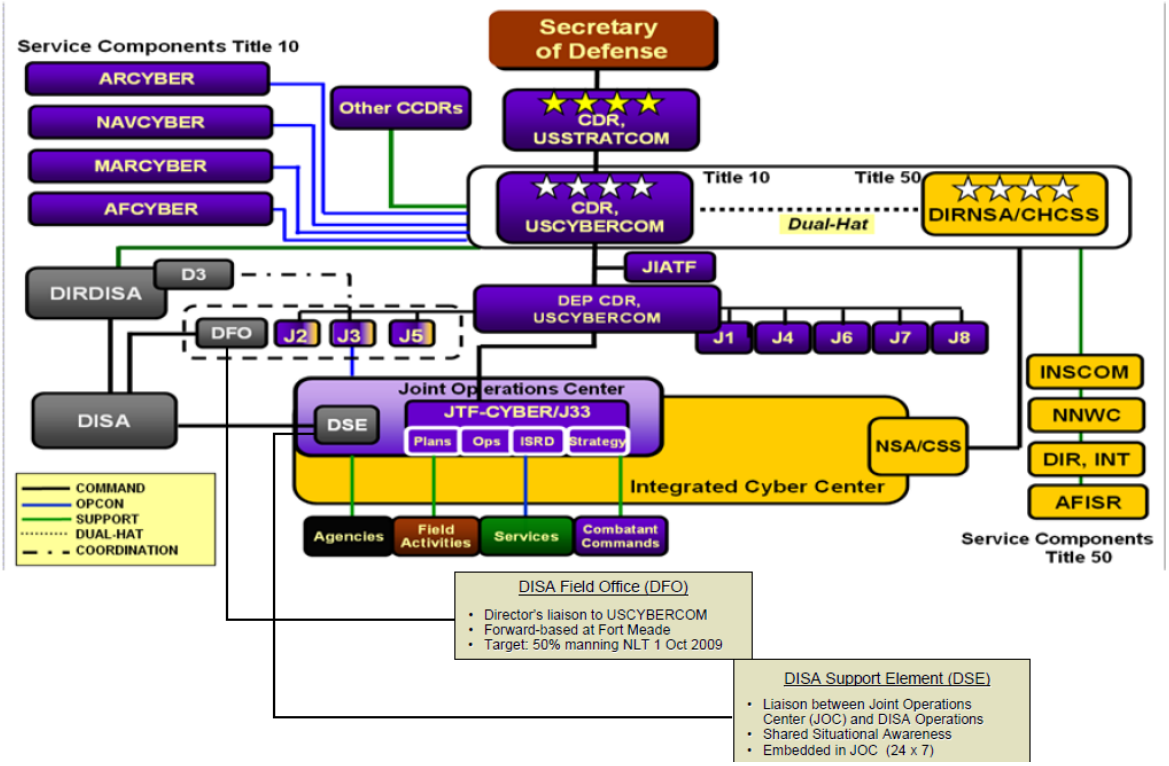
- PEREIRA, CMG SOUSA, Divisão de Comunicações e Sistemas de Informação do Estado-Maior-General das Forças Armadas, 19 de Outubro de 2010.

ANEXOS

Anexo A – USA Cyber Command[11]

U.S. Cyber Command - Fort Meade, MD
Plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

USCYBERCOM Organization



USCYBERCOM is a sub-unified command subordinate to U. S. Strategic Command (USSTRATCOM). Service Elements include Army Forces Cyber Command (ARFORCYBER); 24th USAF; Fleet Cyber Command (FLTCYBERCOM); and Marine Forces Cyber Command (MARFORCYBER).

[11] Fonte.: http://www.stratcom.mil/files/2011-01-28_printable.pdf

Anexo B – US Fleet Cyber Command[12]

The mission of Fleet Cyber Command is to direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; to organize and direct Navy cryptologic operations worldwide and support information operations and space planning and operations, as directed; to direct, operate, maintain, secure and defend the Navy' portion of the Global Information Grid; to deliver integrated cyber, information operations cryptologic and space capabilities; and to deliver global Navy cyber network common cyber operational requirements.

The mission of Tenth fleet is to serve as the Number Fleet for Fleet Cyber Command and exercise operational control of assigned Naval forces; to coordinate with other naval, coalition and Joint Task Forces to execute the full spectrum of cyber, electronic warfare, information operations and signal intelligence capabilities and missions across the cyber, electromagnetic and space domains.

[12] Fonte: http://www.fcc.navy.mil/

Anexo C – Army Forces Cyber Command

"Army Forces Cyber Command (ARFORCYBER) is the Army's service component in support of U.S. Cyber Command (USCYBERCOM), a sub-unified command under U.S. Strategic Command (USSTRATCOM). Our mission is to plan, coordinate, integrate, synchronize, direct, and conduct network operations in defense of all Army networks and mission objectives. We stand ready, when directed, to conduct those cyberspace operations necessary to ensure U.S. and allied freedom of action in cyberspace.

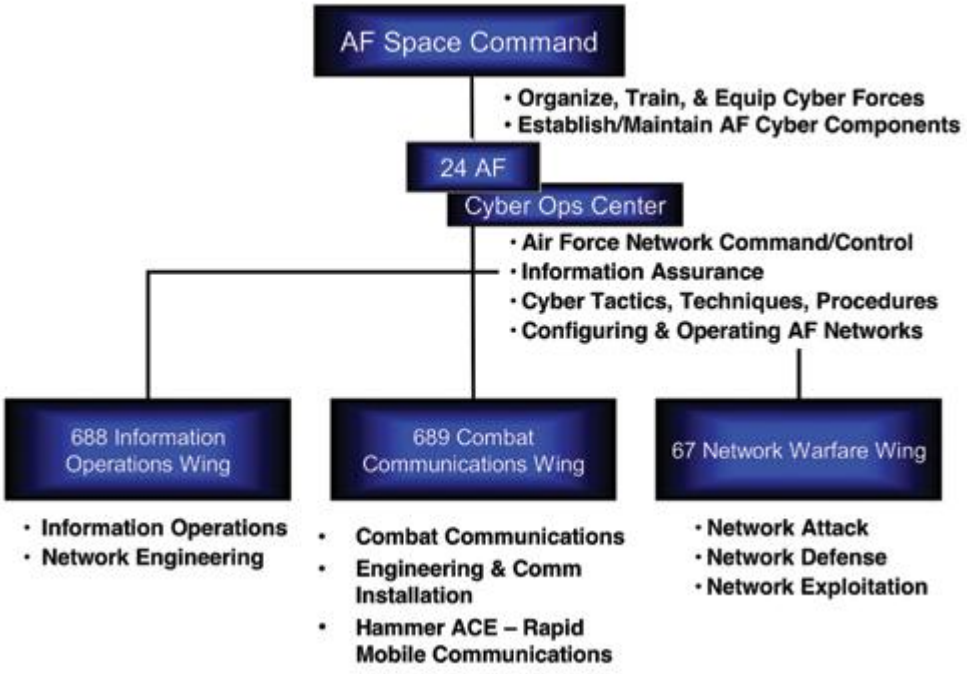
As the Army's service component, my headquarters will coordinate with USCYBERCOM to organize, train, and equip effective cyberspace forces to support all USCYBERCOM Lines of Operation. We will also support USCYBERCOM with prioritization, coordination, and validation of Army mission requirements and force capabilities. This synchronized relationship will enhance situational awareness and achieve more effective coordination across the spectrum of cyberspace operations. Further, when USCYBERCOM directs, we will support establishment of Joint Task.

ARFORCYBER will provide shared situational awareness of the Army's portion of Department of Defense (DoD) information networks to support cyberspace operations so the Commander, USCYBERCOM, can effectively command and control operations using a common Joint operational cyber picture"(Hernandez, 2010:2).

Subordinate Units

- .Army Network Enterprise Technology Command / 9th Army Signal Command (NETCOM/9thSC(A))
- 1st Information Operations Command (Land) (1st IO CMD (L))
- Army Intelligence and Security Command (INSCOM) will be under the operational control of ARCYBER for cyber-related actions

Anexo D – The US 24th Air Force



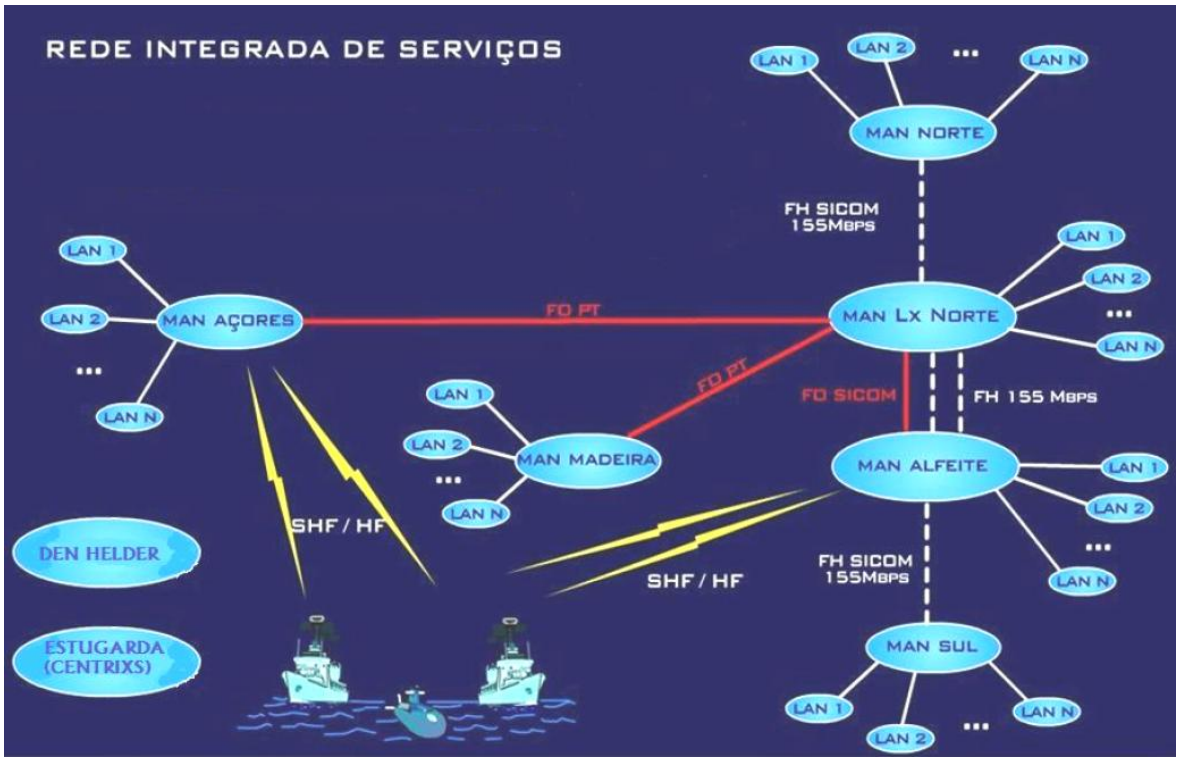
The 24th Air Force's IOC is the culmination of years of sometimes controversial work by the service to establish an effective cyber fighting command. In 2007, the service announced that it was aiming to establish a full major command dedicated to cyberwarfare, even releasing television ads depicting the service as the country's only line of defense from cyber attack. Many saw this move as a turf grab by the air service and its former leaders, Air Force Secretary Michael Wynne and Chief of Staff Gen. T. Michael Moseley.

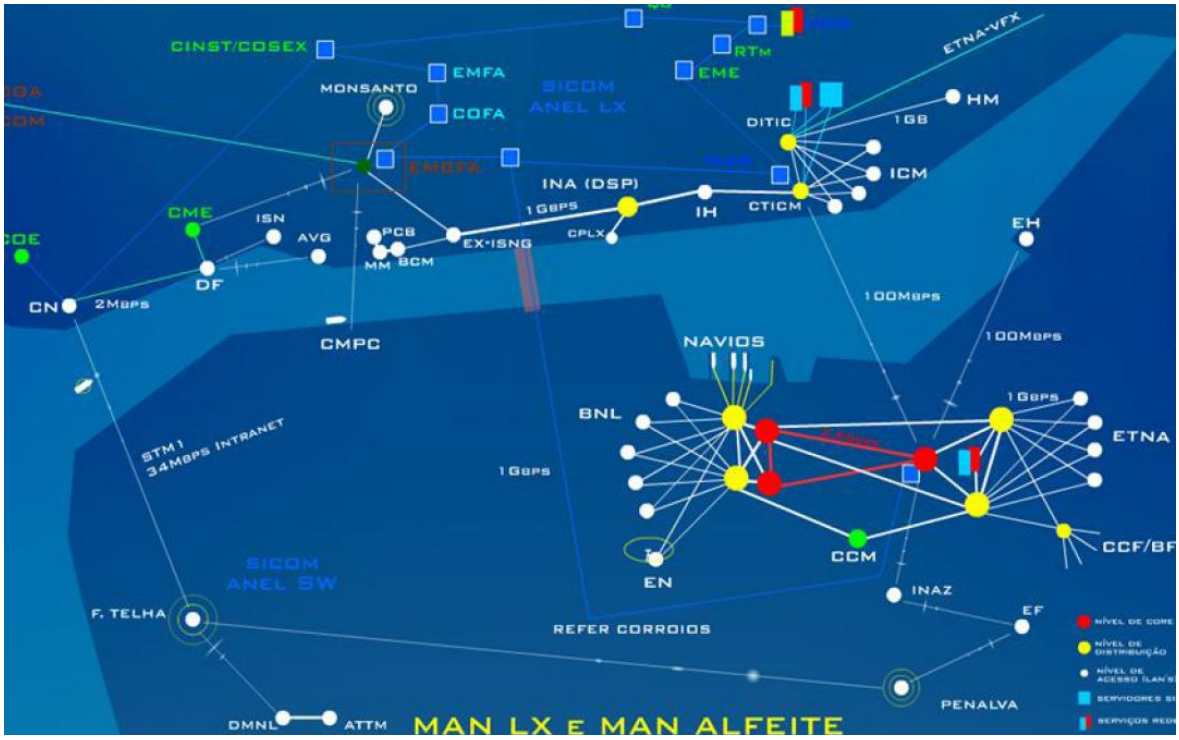
However, soon after Wynne and Moseley were fired by Defense Secretary Robert Gates in the summer of 2008, new Air Force Chief of Staff Gen. Norton Schwartz announced that the service was suspending its pursuit of establishing a cyber MAJCOM. That fall, Schwartz announced that the Air Force would instead establish a numbered air force reporting to Air Force Space Command that would focus on cyber warfare. In August 2009, the service stood up 24th Air Force.

Service leaders say that the numbered air force will serve as the air service's contribution to U.S. Cyber Command when that organization is stood up. For now, however, 24th Air Force reports to AFSPACE.

Although Air Force officials have long *acknowledged* that 24th Air Force's mission will be to operate and defend Air Force computer networks, they remain cryptic about the unit's offensive mission, saying only that it will "provide full spectrum capabilities for the joint war fighter" (Reed, 2010:1).

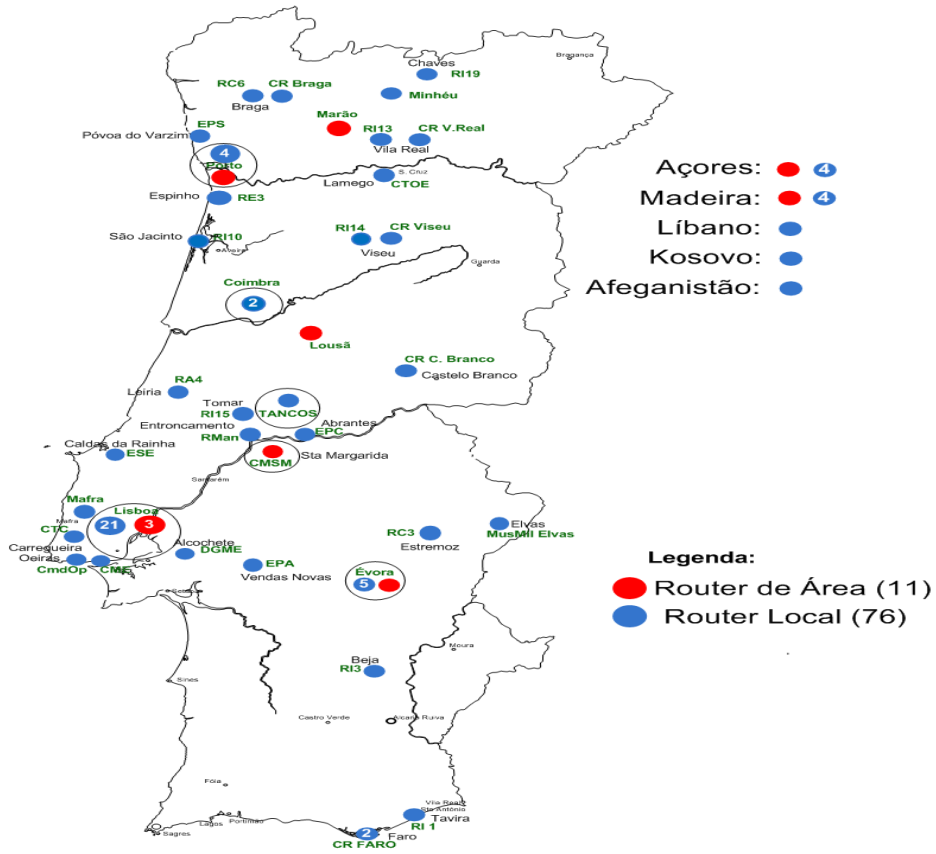
Anexo E – Rede de Comunicações da Marinha[13]





[13] Fonte: Apresentação na Ordem de Engenheiros "*A Engenharia na Marinha*" pelo CALM Gameiro Marques, 16 de Março 2010

Anexo F – Rede de Dados do Exército[14]

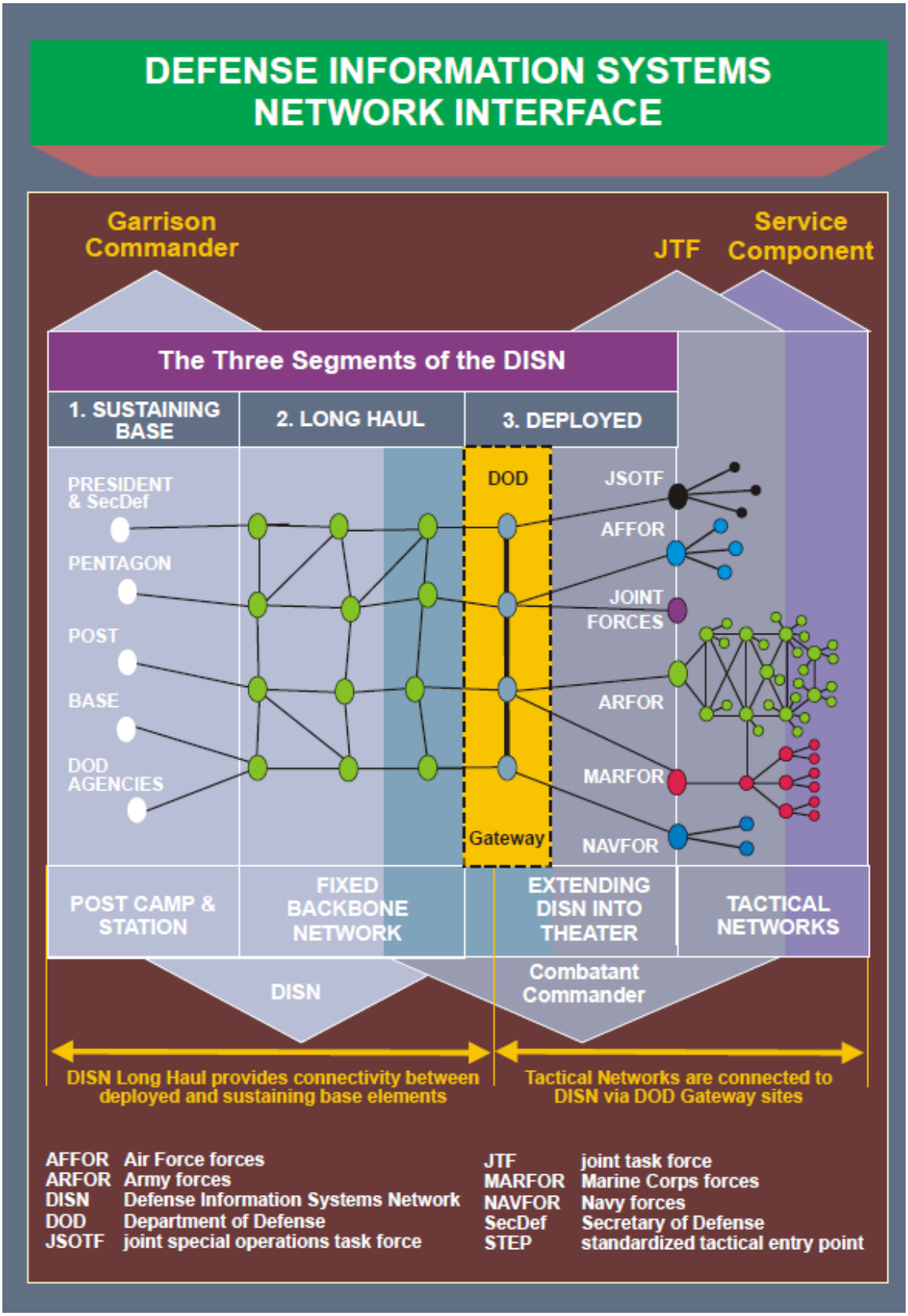


A Rede de Dados do Exército (RDE) assenta na utilização do protocolo Internet Protocol (IP). O encaminhamento (*routing*) da informação é assegurado por uma *Wide Area Network* (WAN), constituída por um conjunto de equipamentos activos designados por *routers*, que formam uma malha nacional constituída por 10 *routers* de área, que formam o Segmento Core da RDE, e 72 *routers* locais para apoio das Unidades, Estabelecimentos e Órgãos (Segmento Acesso).

As Redes Locais de Dados (*Local Area Network* – LANs) das Unidades Estabelecimentos e Órgãos são fundamentalmente constituídas por duas componentes – activa e passiva. A componente activa é genericamente constituída por um conjunto de equipamentos activos de rede (*switch*) e equipamentos de suporte de energia, que garantem aos utilizadores o acesso à RDE e consequentemente acesso aos serviços disponibilizados pela rede (serviços de rede, dados, voz e vídeo). A componente passiva é genericamente constituída por infra-estruturas de subsolo, cablagem estruturada de fibra óptica e cablagem estruturada de cobre.

[14] Fonte: Revista "A Almenara Nº1 2ºSemestre de 2009, RTm"

Anexo G – Defense Information Systems Network Interface[15]



[15] Fonte.: Joint Publication 6.0 (JP, 2010:156)

Anexo H – Global Information Grid, Reporting Flow[16]

[16] Fonte: Joint Publication 6.0 (JP, 2010:101)