INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR

2011/2012

TII

O IMPACTO DO CIBERESPAÇO COMO NOVA DIMENSÃO NOS CONFLITOS

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

JOÃO MANUEL DIAS MOREIRA

CAPITÃO JURISTA

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

O IMPACTO DO CIBERESPAÇO COMO NOVA DIMENSÃO NOS CONFLITOS

Cap Jur João Manuel Dias Moreira

Trabalho de Investigação Individual do Curso de Promoção a Oficial Superior 2011/2012

Lisboa – 2012

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

O IMPACTO DO CIBERESPAÇO COMO NOVA DIMENSÃO NOS CONFLITOS

Cap Jur João Manuel Dias Moreira

Trabalho de Investigação Individual do Curso de Promoção a Oficial Superior 2011/2012

Orientador: TCor Pilav Rui Romão

Lisboa – 2012

Agradecimentos

O meu profundo agradecimento à Senhora Professora Doutora Maria Luísa Duarte pelo seu douto contributo para o presente trabalho e pronta disponibilidade face ao pedido de entrevista que lhe efetuei.

À Senhora Professora Doutora Maria Francisca Saraiva pela disponibilidade e colaboração prestada.

Ao meu orientador Senhor Tenente Coronel Piloto Aviador Rui Romão pela sua constante disponibilidade e clareza das suas orientações e conselhos.

Aos meus Pais.

À minha mulher, Elsa, e às minhas filhas Leonor e Madalena pelo tempo que ficaram privadas da minha companhia durante o período de elaboração do presente trabalho de investigação.

A todos quantos se interessarem pela leitura do mesmo.

Índice

Índice de tabelas

Resumo

O tema do presente trabalho de investigação é o impacto do ciberespaço como nova dimensão nos conflitos. Para a execução do mesmo foi seguido o procedimento metodológico de investigação aprovado pela NEP n.º 218, do IESM, de 15 de setembro de 2011, que corresponde à metodologia proposta por Raymond Quivy e Luc Van Campenhoudt na obra Manual de Investigação em Ciências Sociais.

Dada a vastidão do tema a tratar e às limitações em termos de dimensão do trabalho houve necessidade de restringir a análise a efetuar. Desse modo, o objetivo geral desta investigação é saber em que circunstâncias poderá Portugal, sendo alvo de um ciberataque, exercer o seu direito à legítima defesa à luz do direito internacional. Começou-se por definir ciberespaço e as suas principais caraterísticas. Sendo essencial a compreensão dos ciberataques e das infraestruturas críticas de um Estado, densificaram-se estes conceitos e procedeu-se à sua caracterização. Exigindo o Regime jurídico internacional do uso da força, concretamente o artigo 51.º da CNU a existência de um ataque armado para se poder reagir em sede de legítima defesa, definiu-se ataque armado e conclui-se que em determinadas situações um ciberataque pode ser qualificado como um ataque armado para aplicação daquela disposição legal. Porém, não basta a existência de um ataque armado. Torna-se também necessário imputar a responsabilidade do ciberataque a um Estado, pelo que se procurou confirmar se essa imputação é atualmente possível. Após análise de vários indicadores conclui-se que é perfeitamente possível efetuar essa imputação de responsabilidade, embora a esmagadora maioria dos autores trate o tema em sede de responsabilidade objetiva. Concluiu-se então que em determinadas circunstâncias precisas Portugal poderá face a um ciberataque às suas infraestruturas críticas, imputada a responsabilidade do mesmo a um Estado, exercer o seu direito à legítima defesa ao abrigo do artigo 51.º da CNU.

Abstract

The theme of this research work is the impact of cyberspace as a new dimension in conflicts. To implement was followed methodological research approved by the NEP n.º 218, of IESM, of September 15, 2011, which corresponds to the methodology proposed by Raymond Quivy and Luc Van Campenhoudt work in Manual for Research in Social Sciences.

Given the vastness of the topic to be discussed and the limitations in size of the work was necessary to restrict the analysis to perform. Thus, the overall goal of this research is to know in what circumstances can Portugal, the target of a cyberattack, exercise their right to self-defense in light of international law. It began by defining cyberspace and its main features. Is essential to understand the cyber-attacks and critical infrastructure of a state, we defined these concepts and proceeded to his characterization. The international legal regime of use of force, specifically Article 51.º. of CNU requires the existence of an armed attack in order to react in self-defense, and set up armed attack we concluded that in certain situations a cyber attack can be qualified as an armed attack for the application of that statutory provision. However, it´s not enough the existence of an armed attack. It is also necessary to allocate the responsibility of the State to a cyberattack, and it is sought to confirm that this allocation is currently possible. After analysis of several indicators concludes that it is perfectly possible to make this attribution of responsibility, but the overwhelming majority of authors treat the subject in place of objective liability. It was concluded then that in certain prescribed circumstances Portugal may face a cyber attack of its critical infrastructures, attributed responsibility to a State to exercise its right to self defense under Article 51.º of CNU.

Palavras-Chave

Ciberespaço; Ciberataque; Infraestruturas Críticas; Ataque Armado; Responsabilidade dos Estados.

Lista de abreviaturas, siglas e acrónimos

AA - Ataque Armado
AG - Assembleia Geral
CDI - Comissão de Direito Internacional
CNA - *Computer Network Attack*
CNE - *Computer Network Exploitation*
CNO - *Computer Network Operations*
CNU - Carta das Nações Unidas
DARS - *Draft Articles on Responsability of States for International Wrongful Acts*
DoS - *Denial of Service*
DRE - Diário da República Electrónico
EUA - Estados Unidos da América
GAO - *Government Accountability Office*
HIP - Hipótese
IC - Infraestrutura crítica
IESM - Instituto de Estudos Superiores Militares
JP - *Joint Publication*
LG - Legítima defesa
NEP - Norma de Execução Permanente
ONU - Organização das Nações Unidas
PP - Pergunta de partida
PD - Pergunta derivada
RFA - Regulamento da Força Aérea
TII - Trabalho de Investigação Individual
TIJ - Tribunal Internacional de Justiça

Introdução

O tema consiste no impacto do ciberespaço como nova dimensão nos conflitos. Esta dimensão, com ênfase para a internet, seu maior ambiente, revolucionou o mundo em que vivemos. Nas sociedades desenvolvidas é cada vez maior a dependência dos sistemas de informação e comunicação por parte de pessoas, empresas ou dos próprios Estados. Existem atividades e setores vitais para a qualidade de vida e segurança das pessoas e dos Estados, por exemplo o transporte de bens e pessoas, as comunicações, a banca e finanças, o fornecimento e distribuição de eletricidade, água e gás, que são geridos no âmbito dos sistemas de informação e comunicação, logo no ciberespaço. Tratam-se de infraestruturas críticas porquanto essenciais para a sociedade.

Estas infraestruturas críticas por terem funções essenciais, face à sua dependência do ciberespaço e características deste ambiente, encontram-se vulneráveis a ataques e manipulações internas e externas. Se atacadas podem causar efeitos profundos de consequências extremas. Daí que se pretende analisar, à luz do direito internacional, a utilização do ciberespaço enquanto veículo de agressão a um Estado, mormente através de ciberataques às suas infraestruturas críticas. Pretende-se averiguar em que condições um ciberataque é qualificado um ataque armado (AA), e em que circunstâncias uma ação ofensiva via ciberespaço pode ser imputada a um Estado.

Assim, analisaremos a ameaça que representam os ciberataques a infraestruturas críticas de um Estado, de modo a responder à questão atrás referida. Conceitos como ciberespaço, ciberataques, infraestruturas críticas, ataque armado e responsabilidade dos Estados serão densificados.

O objetivo geral desta investigação é saber em que circunstâncias poderá Portugal, sendo alvo de um ciberataque, exercer o seu direito à legítima defesa à luz do direito internacional. Consequentemente, elencámos os seguintes objetivos específicos: saber se um ciberataque pode ser considerado um AA e descortinar se essa ação pode ser imputada a um Estado.

Na execução deste trabalho seguimos o procedimento metodológico de investigação aprovado pela Norma de Execução Permanente (NEP) n.º 218, do Instituto de Estudos Superiores Militares (IESM), de 15 de setembro de 2011.

Ele comporta três fases e pressupõe o cumprimento de sete etapas. As fases do procedimento são constituídas pela rutura, construção e verificação. Pretende-se numa fase inicial romper com ideias pré concebidas e falsas evidências relativamente ao tema a investigar, para depois na fase de construção, criar uma matriz conceptual organizada e

lógica, que coincide com a fase da identificação da problemática e da construção do modelo de análise, culminando o procedimento com a fase da verificação na qual as proposições são ou não verificadas. Relativamente às sete etapas do procedimento e atendendo à vastidão do tema a tratar, na etapa um, após leitura perfunctória de artigos e trabalhos sobre o mesmo, foi apresentada a seguinte Pergunta de Partida (PP) de forma a orientar a investigação:

"Em que circunstâncias poderá Portugal, sendo alvo de um ciberataque, exercer o seu direito à legítima defesa à luz do direito internacional?".

Prosseguiu-se para a segunda etapa continuando-se com a recolha de informação sobre o assunto, nomeadamente artigos e estudos maioritariamente estrangeiros. Foram nesta fase realizadas algumas entrevistas exploratórias de forma a colher a sensibilidade dos entrevistados sobre o assunto. Passou-se à fase da problemática, etapa dois, na qual se constatou que para responder à PP era necessário efetuar e responder às seguintes Perguntas Derivadas (PD):

-PD1: Em que circunstâncias pode um ciberataque ser considerado um ataque armado;

-PD2: Em que circunstâncias pode a responsabilidade por um ciberataque ser imputada a um Estado.

Tratam-se de questões de resposta complexa uma vez que nem na prática ocorreram factos que tenham causado tais interrogações, embora tenha sucedido algo semelhante na Estónia e na Geórgia, nem o regime jurídico internacional foi edificado prevendo situações destas.

Seguiu-se a etapa da construção do modelo de análise (Anexo A), com a PP, duas PD e respetivas Hipóteses (HIP) bem como o corpo de conceitos a definir e explicitar (Anexo B). As hipóteses a verificar são:

-HIP1: As infraestruturas críticas portuguesas estão a ser alvo de um ciberataque coordenado e de grande intensidade tipo DoS, que já originou dezenas de vítimas mortais e avultados danos materiais, com efeitos ao nível político, militar e civil;

-HIP2: Atualmente os ciberataques não podem ser imputados a Estados.

Nas etapas de observação e análise da informação, quinta e sexta etapa do procedimento, concebeu-se o modelo de observação, aplicou-se o mesmo, e trataram-se e analisaram-se os dados obtidos, que resultaram da apreciação crítica das teorias, pareceres e outros indicadores. Dessa forma, e com os resultados obtidos, foram apreciadas as HIP

possibilitando o surgimento de respostas juridicamente fundamentadas para as PD efetuadas, e finalmente para a PP.

Esta investigação está organizada em quatro capítulos. O primeiro trata da noção e caracterização do Ciberespaço, do conceito de ciberataque, suas tipologias e autores. Remata-se com a noção e importância das infraestruturas críticas, classificando-as como vulnerabilidades face a ciberataques. O capítulo seguinte aborda o regime jurídico internacional do uso da força pelos Estados, nomeadamente a Carta das Nações Unidas (CNU), especialmente no que concerne à legítima defesa e seus pressupostos. Nele se averiguará em que circunstâncias um ciberataque pode ser qualificado como um ataque armado. No terceiro procede-se à análise do regime de imputação de ciberataques aos Estados, recorrendo-se aos indicadores fornecidos pelo *Draft Articles on Responsability of States for International Wrongful Acts*. No quarto capítulo efetua-se uma síntese conclusiva global finalizando-se com o tratamento das HIP, PD e PP.

1. O Ciberespaço

a. Noção e Características.

Não existe consenso no que a uma definição uniforme e universal de ciberespaço concerne. Há contudo na generalidade acordo acerca do facto de ter sido o escritor William Gibson, em 1984, no seu livro de ficção científica *Neuromancer* um dos primeiros a conceptualizar e a utilizar o termo ciberespaço. Este escritor, no seu romance descreve-o como uma rede de computadores contendo um ambiente composto por uma enorme quantidade de informação no qual os utilizadores poderiam vivenciar ambientes ficcionados com efeitos no mundo físico (Gibson, 1984).

O Regulamento da Força Aérea (RFA) 390-6, que aprovou a Política de Ciberdefesa da Força Aérea, define ciberespaço como "*Domínio digital gerado por computadores e redes de computadores, no qual os indivíduos e os computadores coexistem e que inclui todos os aspectos das actividades on-line"* (Força Aérea Portuguesa, 2011, p. 1-3).

O termo é também definido por dois dicionários de referência como "*espaço onde se estabelece comunicação electrónica*", "*realidade virtual*" (Academia das Ciências de Lisboa, 2001: p. 809) e, "*espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações*" (Porto Editora, 2012).

Para o Departamento de Defesa Norte Americano ciberespaço é um domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de tecnologia de informação incluindo a internet, redes de telecomunicações, sistemas de computadores e os inerentes processadores e controladores (JP 1-02, p. 83).

Desta definição de ciberespaço uma conclusão lateral se retira. O ciberespaço não se confunde com a *Internet,* apesar desta ser o seu principal e mais relevante ambiente. Neste sentido, conforme mencionado no RFA 390-6, o ciberespaço "… *consiste não só na Internet e nos computadores a ela ligados mas também nos sistemas e equipamentos eletrónicos ligados a outros equipamentos ou sistemas ou que partilham a mesma estrutura de energia ou o mesmo espaço de emissão electromagnética. São exemplos comuns a máquinas ATM, os sistemas de controlo de produção energética ou industrial, os telefones e as redes de telecomunicações abrangendo, portanto, todos os domínios de actividade humana*" (Força Aérea Portuguesa, 2011, p. 1-1).

Daqui resulta que podemos falar em ciberespaço tanto numa aceção ampla como numa aceçao restrita. Nesta estará em causa apenas a sua dimensão virtual constituída pela informação contida e armazenada nesse ambiente não físico e não palpável. Naquela, além

da dimensão virtual, o ciberespaço aglutinará também a sua dimensão física e material abrangendo todo o complexo de equipamentos e de sistemas materiais que o integram, nomeadamente computadores, servidores e equipamentos controlados.

Mas, quando falamos em ciberespaço de imediato algumas ideias ganham relevo. Desde logo a perda da ideia de presencialidade, do mundo físico, pois tudo se passa maioritariamente no domínio ou ambiente virtual, em quase anonimato. A noção de desmaterialização está imediatamente constatada porquanto no ciberespaço, na sua dimensão virtual, não há matéria, não existe nada de físico, tudo circula, flui e se armazena no ambiente virtual citado. Também a perspetiva de territorialidade é alterada uma vez que não existem fronteiras para a comunicação, para a transmissão de dados pois eles circulam no mundo virtual sem qualquer necessidade de visto de entrada ou saída (Gouveia, 2012). Trata-se igualmente de um espaço transnacional, de nenhures, sem dono e lugar. Por último, a certeza de que é um mundo transversal, capaz de atuar e influenciar em todos os domínios, quer sejam políticos, económicos, sociais, e mesmo militares.

Benedikt caracterizou o ciberespaço da seguinte forma. Trata-se de um novo e paralelo universo criado e mantido pelos computadores e linhas de comunicação, onde circulam conhecimentos, segredos e indicadores; É uma realidade virtual, presente ao mesmo tempo em qualquer lugar e em lugar algum; É também um espaço por natureza ilimitado, sem restrições de tempo e lugar, bastando para nele aceder possuir um computador seja em que parte do globo for; Consiste num mundo que depende da eletricidade para o explorar-mos; E é sobretudo informacional pois nele sobressai a ilimitada quantidade de informação e dados disponíveis que se caracterizam pela sua intemporalidade (1991, pp. 1-3).

b. Os Ciberataques

As potencialidades e características atrás mencionadas têm permitido melhorar direta ou indiretamente a qualidade de vida dos cidadãos e contribuído decisivamente para o desenvolvimento da sociedade tal como a conhecemos hoje. Atualmente, nas sociedades tecnologicamente desenvolvidas, os sistemas de satisfação de necessidades básicas da população utilizam e dependem do ciberespaço para prosseguirem tal desiderato, desde sistemas de gestão e abastecimento de eletricidade e água potável a sistemas financeiros, de transportes e telecomunicações. E esta dependência deriva do facto destes sistemas, na sua esmagadora maioria pertencentes ao setor privado, serem atualmente geridos por computadores ou sistemas atuando em rede.

Por outro lado, o ciberespaço tem desempenhado um papel determinante para a rápida difusão de informação. Recorde-se o que sucedeu com a denominada primavera árabe, em que a informação veiculada através do ciberespaço foi decisiva para que a comunidade internacional pudesse entender as aspirações dos povos em questão. Relembre-se igualmente a manifestação convocada e organizada através do ciberespaço denominada geração à rasca ocorrida em Portugal em março de 2011 e que juntou milhares de jovens em protesto.

No entanto, este ambiente virtual e ilimitado tem também sido utilizado para a prática de atos ilícitos por determinados atores, mais ou menos relevantes, organizados ou não, prosseguindo os mais variados objetivos e possuindo as mais diversas motivações.

E neste aspeto o ciberespaço serve para estes atores tanto como instrumento ou canal para a prática de tais atos, como alvo ou objeto da ação (Gouveia, 2012). Se o objetivo é por exemplo negar a distribuição de eletricidade, então o ciberespaço é um instrumento para o conseguir. Se o objetivo é danificar um determinado computador ou sistema, então o ciberespaço, na sua dimensão física, é ele próprio o objeto do ato ilícito.

À prática destes atos ilícitos através ou contra o ciberespaço dá-se geralmente o nome de ciberataques, realidades a que o RFA 390-6, se refere como tendo por finalidade provocar danos na capacidade dos sistemas, embora não nos dê uma noção de ciberataque (Força Aérea Portuguesa, 2011, p. 1-3). Podemos então definir ciberataque como um ataque lançado geralmente a partir de um computador recorrendo ao método de intrusão e que tem como finalidade adquirir, explorar, perturbar, romper, negar, degradar ou destruir informação constante em computadores ou em redes de computadores, em sistemas e equipamentos eletrónicos ligados a outros equipamentos ou sistemas ou que partilham a mesma estrutura de energia ou o mesmo espaço de emissão eletromagnética, bem como os próprios computadores, redes de computadores, sistemas e equipamentos. A densificação do conceito desta forma abrangente permite englobar no seu conteúdo o que na doutrina Norte Americana, no âmbito das denominadas *Computer Network Operations*, se designa como *Computer Network Attack* (CNA) e *Computer Network Exploitation* (CNE). Os CNA são ações executadas 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, enquanto que a CNE é 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 (JP 3-13, 2006,II-5)**.**

Debruçando-nos sobre a identificação dos principais autores ou ameaças destes ciberataques e sua descrição, utilizamos a tabela utilizada por Melo tendo por base os dados apresentados pelo *Government Accountability Office* (GAO) em relatório apresentado ao Congresso dos Estados Unidos da América (EUA).

Tabela 1- Principais fontes de ameaça no ciberespaço

Ameaça	Descrição
Controladores de "*Bot-Network*"	Utilizam a "rede" para controlar remotamente os sistemas comprometidos e coordenar outras ações como roubo de dados pessoais, bancários e outros, enviar "lixo eletrónico" ou instalar *software* malicioso
Grupos Criminosos	Procuram atacar os sistemas com o 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, por vingança ou ganho monetário
Insiders	É a principal fonte de crime por computador. Não necessitam de grandes conhecimento de intrusão, pois têm acesso fácil e privilegiado, podendo danificar os sistemas ou danificar dados. Inclui também empresas contratadas e empregados que sem intenção introduzem *software* malicioso no computador.
Estados	Utilizam ferramentas informáticas como parte da sua pesquisa 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 infraestruturas criticas visando ameaçar a segurança nacional, causar vitimas em larga escala e afectar a moral e a confiança das populações.

Fonte : (GAO, 2010, 4 cit. por Melo, 2010, pp. 7-8).

Da análise da tabela verificamos que os autores dos ciberataques podem ir desde os simples *hackers*, que o fazem pelo desafio que isso representa, vingança ou simplesmente para obtenção ilícita de recursos financeiros, até aos terroristas e Estados que podem ter como objetivo lesar a segurança nacional de um Estado, causando vítimas, afetando a moral e a confiança das populações. De facto, existem Estados que têm já capacidades ofensivas e defensivas no ciberespaço (Anexo C), pelo que se avistam futuros ciber conflitos entre Estados, passando a ser o ciberespaço mais uma dimensão nos conflitos, tal como o mar, a terra, o ar e o espaço (Durán, 2010, p. 233).

A título de exemplo, os Estados Unidos da América implementaram o *United States Cyber Command* (USCYBERCOM), com a missão de planear, coordenar, integrar, sincronizar e conduzir atividades 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 espetro, de modo a permitir ações em todos os domínios, assegurar a liberdade de ação no ciberespaço aos EUA e Aliados e negar o mesmo aos adversários (STRATCOM, 2010, p.1, cit. por Melo, 2010, p. 30).

Relativamente às potencialidades e capacidades dos ciberataques elas dependem da sua intensidade, da natureza dos alvos e do tipo de ciberataques utilizados. E nesta sede, de tipologia de ciberataques, Melo identificou-os e descreveu-os numa tabela tendo igualmente por fonte o atrás citado relatório do GAO.

Tabela 2 - Tipologia das ameaças existentes no ciberespaço

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 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 um código malicioso. Normalmente está camuflado dentro de programas comuns, legítimos.
Virús	Um programa que infecta ficheiros de computador, inserindo uma cópia de si mesmo noutros ficheiros. Difere dos "*Worms*", no sentido de que depende de 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 Interceptador de pacotes	Um programa que intercepta e examina os pacotes de dados que circulam na internet, na procura de informação especifica, como senhas transmitidas em texto não cifrado.

Fonte :(GAO, 2010, p.5 cit. por Melo, 2010, p.8).

Da sua análise resulta que, em grande parte, a capacidade do ataque depende do tipo de ciberataque utilizado pelos agressores. Uma negação de serviço será potencialmente mais gravosa que um ciberataque *Pishing*. Contudo, os efeitos do ciberataque também serão mais ou menos gravosos consoante a natureza dos alvos. Se estes possuírem a natureza de infraestruturas críticas (IC) de um Estado, os seus efeitos terão maiores repercussões do que se se tratarem de infraestruturas sem essas características. Por esse facto se diz que um ciberataque em grande amplitude e escala a essas IC poderá ter consequências ao nível político, militar e civil, podendo considerar-se como tendo potencialmente efeitos estratégicos.

c. As infraestruturas críticas como vulnerabilidades.

Por esse facto, o General Bispo, citado por Balsinhas, define IC como aquela cuja rutura pode produzir efeitos de âmbito nacional, ou regional, de tal forma que afete o regular funcionamento dos serviços da sociedade civil e das instituições nacionais, criando um problema de segurança nacional (2003, p.16).

Conforme já referido, desta densificação do conceito resulta que um ciberataque a IC pode ter repercussões ao nível político, da sociedade civil e até no âmbito militar, pois a defesa militar de um Estado depende em muito do ciberespaço, na sua aceção ampla. Por este facto, esta dependência pode ser considerada como um requisito crítico gerando causalmente a existência de uma vulnerabilidade, conceito que Monteiro refere tratar-se de uma caraterística da conceção, implementação ou operação de um elemento de uma IC que o torna suscetível a destruir-se ou ficar incapacitado perante uma ameaça (2007, p. 12). Nunca é demais frisar que as IC têm influência ao nível político, militar, económico, social, de infraestruturas e informacional. Têm caráter transversal.

Reconhecendo a importância deste tipo de infraestruturas, a nível europeu o Conselho emanou a Diretiva n.º 2008/114//CE, de 8 de dezembro, que estabelece um procedimento para a identificação e designação de IC a nível europeu.

Portugal, cumpriu a obrigação de transposição através do Decreto-Lei n.º 62/2011, de 9 de maio, pretendendo com este diploma estabelecer procedimentos para a identificação das diversas infraestruturas com funções essenciais para a sociedade, e cuja perturbação ou destruição teria um impacto significativo, porque implicaria que deixasse de poder assegurar essas funções (Ministério da Defesa Nacional, 2011).

Neste contexto, o diploma densifica o conceito de IC como "…*a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções*".

O diploma legal tem o seu âmbito de aplicação inicialmente limitado aos setores da energia e transportes mas abre a possibilidade de iniciar o procedimento de designação e identificação de IC noutros setores.

É essencial portanto face à importância deste tipo de infraestruturas compreender e assumir as suas vulnerabilidades, de modo a protegê-las especialmente de ciberataques, no caso concreto. Se pensarmos no impacto de um ataque de grande amplitude e escala a estas IC e nos efeitos daí decorrentes não se poderá encarar esta realidade doutra forma.

2. O Regime Jurídico Internacional do Uso da Força

a. A Carta das Nações Unidas e a Legítima Defesa

O regime jurídico do uso da força em Direito Internacional reside, de forma universal, na Carta das Nações Unidas (CNU), aprovada em 1945 e que instituiu a organização internacional conhecida por Organização das Nações Unidas (ONU), atualmente com 193 membros. A CNU foi publicada no Diário da República através do Aviso n.º 66/91, de 18 de março (Ministério dos Negócios Estrangeiros, 1991).

A CNU estabeleceu como objetivos para a ONU, manter a paz e a segurança internacionais, desenvolver relações de amizade entre as nações e realizar a cooperação internacional. Para manter a paz e segurança internacionais a organização deve tomar medidas eficazes para prevenir e afastar ameaças à paz e reprimir os atos de agressão ou qualquer outra rutura de paz e chegar, por meios pacíficos, a uma solução das controvérsias.

Os objetivos supra referidos devem ser alcançados pela organização e seus membros seguindo os princípios da igualdade soberana dos Estados, da boa fé, da resolução pacifica dos conflitos, da proibição do uso da força, da legítima defesa, da integridade territorial e independência política, e por último do princípio do domínio reservado dos Estados.

Podemos afirmar que é a ONU que detém o monopólio do uso legítimo da força em Direito Internacional (Machado, 2004, p. 566). Como já acima indiciado, não é licito aos Estados recorrer à ameaça ou ao uso da força, quer seja contra a integridade territorial ou independência politica de um Estado, ou de qualquer modo incompatível com os objetivos da ONU, o que consubstancia o princípio da proibição do uso da força por parte dos Estados, como grande regra geral.

É a esta organização que compete prevenir e afastar ameaças à paz e reprimir os atos de agressão através do Conselho de Segurança que determinará, bem ou mal, no caso concreto, a existência dessas ameaças e atos de agressão, adotando as medidas necessárias para lhes colocar termo inclusivamente determinando o uso da força conforme disposto no artigo 42 da CNU.

No entanto, como todas as regras comportam exceções, existe uma muito particular à regra da proibição do uso da força por parte dos Estados. Trata-se do uso da força a título individual por parte de um Estado enquadrado no direito à legítima defesa (LD), que mais não é do que uma cláusula de exclusão da ilicitude do facto em virtude do exercício de um direito, o direito à LD.

Assim, consagra o artigo 51.º da CNU que " *Nada na presente carta prejudicará o direito inerente de legítima defesa individual ou colectiva, no caso de ocorrer um ataque armado contra um membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer momento, a acção que julgar necessária à manutenção ou restabelecimento da paz e da segurança internacionais"* (Ministério dos Negócios Estrangeiros, 1991).

Trata-se do exercício de um direito que está sujeito a limitações. Deve ser exercido em obediência aos Princípios da subsidiariedade, provisoriedade e proporcionalidade. O Princípio da subsidiariedade impõe que o uso da força em LD apenas ocorra se não houver outro meio para afastar o ataque armado (AA). Esse uso da força além de apenas ter a duração necessária para afastar o ataque só se manterá até ser encontrada outra solução, o que corresponde ao Princípio da provisoriedade. Por outro lado, o uso da força em LD deverá ser proporcional ao ataque e à ameaça, o que configura o Princípio da proporcionalidade.

Esta norma tem sido alvo de muita discussão e objeto de várias interpretações quer pela doutrina, quer pelo Tribunal Internacional de Justiça (TIJ), nomeadamente devido ao conceito de AA e ao estudo da figura da LD preventiva.

b. O Ataque Armado como pressuposto do direito de Legítima Defesa

Da análise do artigo 51.º da CNU verificamos que um dos pressupostos para o uso da força por um Estado ao abrigo do seu inerente direito à LD é que tenha ocorrido um AA, conceito que é há muito controvertido na doutrina e jurisprudência internacional quanto à sua definição e alcance.

Trata-se efetivamente de um conceito aberto que difere do conceito de agressão, este com maior amplitude, e densificado pela resolução 3314, de 14 de dezembro de 1974, da Assembleia Geral (AG) da ONU, embora tal densificação não tenha sido isenta de críticas ao longo dos tempos (Seara, 1991, p. 89).

Esta resolução, começando por dizer de uma forma ampla e geral que agressão é o uso da força armada por um Estado contra a soberania, a integridade territorial e a independência politica de outro Estado, posteriormente quando lista, de forma não

exaustiva, atos de agressão, refere que além dos AA nela mencionados, como bombardeamentos por forças armadas contra o território de outro Estado por exemplo, é qualificado como ato de agressão o bloqueio de portos ou da costa de um Estado pelas forças de outro Estado. Infere-se assim que o conceito de agressão é mais amplo que o de AA.

De facto, mesmo recorrendo ao teor da resolução referida tem sido difícil densificar e distinguir todos os conceitos em jogo neste tabuleiro internacional. Como refere Baptista a noção de AA é mais restrita (pressupondo o uso mais grave da força) do que a de agressão, e a noção de agressão é mais restrita do que a de uso ilícito da força, sendo esta a utilização da força em desrespeito do artigo segundo número quatro da CNU (2003, p. 116). Pelo que, quando falamos em uso da força por um Estado, consoante a gravidade podemos qualificar esse uso como um AA, ato de agressão, ou mero uso ilícito da força, sendo este o menos grave e intenso.

O próprio TIJ efetua esta distinção quando refere "*it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms*" e "*Alongside certain descriptions which may refer to agression, this text includes others which refer only to less grave forms of the use of force*" (Tribunal Internacional de Justiça, 1986, p. 101).

Perante este enquadramento, Baptista refere que a definição de agressão da Assembleia Geral contém referência a meros usos ilícitos da força, a agressões e AA, mas numa diferenciação confusa, não ficando clara a fronteira entre essas realidades distintas (Baptista, 2003, p. 117). Daí que para este autor, à semelhança da jurisprudência do TIJ que avança que um AA deve ser de "*significant scale*" (Tribunal Internacional de Justiça, 1986, p. 104), a noção de AA compreende apenas ações bélicas em grande escala, como invasões do território de um Estado ou ações de gravidade paralela e não meros incidentes (Baptista, 2003, p. 120).

Neste sentido, os acidentes de fronteira, ou mesmo as incursões de irregulares por um período curto, não são normalmente classificados como AA o que, significa que as noções de "amplitude" e "gravidade" têm grande importância na triagem dos factos, pese embora variarem no tempo e no modo e de serem impulsionadas pelos progressos da tecnologia militar, orientações doutrinais e teorias estratégicas (Saraiva, 2007: p. 79).

No entanto, até agora apenas concluímos que AA não é sinónimo de agressão, nem esta é sinónimo de uso ilícito da força. Por outro lado, verificámos que para qualificar um ataque como AA para efeitos do artigo 51.º da CNU têm de estar também reunidas

determinadas condições como a amplitude, gravidade e escala consideráveis do ataque. Falta-nos portanto saber, concretamente, o que considerar um AA atendendo a que a CNU não nos dá uma noção.

Assim, ataque é definido como ato de violência contra o adversário pelo artigo 49.º do I Protocolo Adicional às Convenções de Genebra de 1949 (Presidência da República, 1992). No entanto, como alerta Schmitt o termo violência é explicativo, pois a violência reporta-se mais às consequências do ato do que ao próprio ato (2002, p. 377).

Por outro lado, o ataque será armado quando empregar uma arma. Arma é qualquer instrumento ou dispositivo fabricado pelo homem para se defender ou atacar (Verbo, 2001: p. 337). Porém, existem instrumentos que não foram fabricados com essa finalidade mas que podem ser usados como armas. Por isso, Zemanek nota que não é a designação do dispositivo, nem o seu uso normal que o qualifica como arma, mas a intenção com que é usado, bem como pelos efeitos produzidos. Para este autor o uso de qualquer dispositivo que resulte na perda de vidas e em extensa destruição de propriedade preenche as condições para ser considerado um AA (Zemanek, 2010. cit. por Roscini, 2010, p.114).

Tudo exposto, podemos definir AA como ato , com grande amplitude, gravidade e escala, praticado utilizando quaisquer instrumentos ou dispositivos que tenha consequências e provoque efeitos violentos no adversário, ainda que os instrumentos ou dispositivos usados não tenham normalmente essa finalidade.

Densificado o conceito de AA, resta saber, se em tese um ciberataque pode ser qualificado como AA assumindo as características de amplitude e gravidade para o Estado alvo beneficiar da causa de exclusão da ilicitude do uso da força, caso opte por essa via a título individual.[1]

E sobre este aspeto, entrevistada para o efeito, Duarte referiu que "*A legítima defesa constitui uma excepção ao princípio geral da proibição do uso da força, concretamente uma causa de exclusão da ilicitude do recurso à força. Por conseguinte, a interpretação do artigo 51 da CNU não pode ser extensiva e flexível, sob pena da excepção consumir a regra*". Acrescenta ainda que "*Um ataque perpetrado pelo recurso aos meios tecnológicos, com o objectivo de neutralizar a rede de informação e de estruturas básicas de funcionamento de um Estado constitui, decerto, um perigo e uma ameaça graves, constituindo eventualmente um acto de agressão ou ameaça à paz. Não justificará, contudo, o recurso à força, no exercício da legítima defesa individual, mas*

[1] Essas decisões competem às autoridades nacionais do Estado vítima (Tikk, 2011, p.110).

justificará o recurso ao Conselho de Segurança, nos termos do artigo 39 da CNU e para fundamentar uma acção da ONU ou em seu nome" (2012).

Contudo, não podemos concordar com este entendimento que no fundo conclui que um ciberataque não pode ser considerado um AA, afastando desde logo a aplicação do artigo 51.º da CNU. Recorrendo à densificação do conceito de AA acima efetuada, numa dimensão literal, podemos afirmar que um ciberataque pode em determinados casos ser considerado um AA. Um vírus informático é passível de ser considerado uma arma, e por conseguinte consideramos que um ataque intencional utilizando *software* malicioso que tenha consequências e efeitos violentos no Estado vítima, pode ser qualificado como um AA. Basta partirmos do pressuposto que um ciberataque coordenado e em grande escala, pode ter efeitos a nível político, militar, civil, económico e financeiro, causando vítimas mortais e elevada destruição física, o que atribuirá a amplitude e gravidade necessária ao ataque. Tanto mais assim será se considerarmos os objetivos da CNU. Para os mais céticos, poderão estar em causa ciberataques com capacidades para interromper fornecimento de água, gás, eletricidade às populações, de negar comunicações, de interferir em sistemas de transporte, e sistemas de comando e controlo, com grande possibilidade de ocorrerem vítimas mortais, de negar a correta gestão de tráfego aéreo, provocando enorme destruição física. Tratam-se de ciberataques a infraestruturas críticas de um Estado. Não se trata de um cenário de ficção, mas de capacidades reconhecidas a um ciberataque bem coordenado, de grande amplitude e intensidade, necessariamente apenas na disponibilidade de Estados e com vista à destruição de um Estado ou à obtenção de uma vantagem militar por parte do atacante.

A conclusão semelhante parece chegar Gouveia, para quem um ciberataque embora não sendo considerado pela resolução interpretativa 3314 como um tipo de AA, face à evolução quer do conceito quer das técnicas militares, deve-se reconhecer que essa realidade se for de certas proporções e com certas características tem de ser evidentemente considerado um AA e essa qualificação deve ser suscetível de permitir ações no âmbito do direito à LD. Acrescenta ainda que importante e decisivo é a intensidade do ciberataque, reforçando que deve ser um ciberataque com certas proporções, finalidades e realizado por certas entidades (2012).

Sharp considera igualmente a possibilidade de ciberataques armados, ataques de grande magnitude, intensidade e duração suficientemente graves para admitirem a legítima defesa (1999, p. 119, cit. por Saraiva, 2009, p. 427).

No entanto, reconhece-se que não é isento de dificuldades, considerar-se que um ciberataque é um AA, pois não é em si um ataque físico, razão pela qual existem autores que preferem abordagens diferentes. Concretamente, autores que consideram que um ciberataque pode não ser considerado um AA, mas pode ter efeitos idênticos, ou ainda, que pode chegar a um nível de AA. Tratam-se de linhas de argumentação que resolvem o dilema com enfoque nos efeitos que um ciberataque pode provocar no Estado alvo, o que se resume no essencial a uma abordagem ou dimensão causal do ciberataque. Não interessará aqui o meio pelo qual se perpetram os ataques mas sim os efeitos dele decorrentes.

Parece-nos que é a argumentação de Wingfield quando diz que um AA pode ocorrer quando o uso da força ou uma ação normalmente não qualificada como AA, é exercido de tal forma que causa efeitos equivalentes. E para o efeito, sugere que se apreciem três fatores para se concluir se existem efeitos equivalentes. São eles, o objetivo do ataque, a sua duração e intensidade (2000, cit. no *Operational Law Handbook*, 2008: p.147).

É também, de facto, uma abordagem defensável. Se entendemos que o que é verdadeiramente relevante para questão de saber se um ciberataque pode cair na previsão do artigo 51.º da CNU, tem sobretudo a ver com os efeitos do ciberataque, sendo certo que este pode originar o mesmo género de devastação que os AA utilizando armamento convencional e físico, então esta pode ser a saída para resolver esta querela. E de facto, para esta corrente, este é o fator essencial a ponderar. Não são os meios utilizados que são relevantes e decisivos. Será indiferente para a qualificação do ataque saber se uma refinaria ou central nuclear explodiu em virtude de um míssil ou em consequência de um *software* malicioso. Assim, se os efeitos de um ciberataque forem de dimensão semelhante aos provocados por um ataque qualificado como AA, então merece e tem dignidade para receber o mesmo tratamento conferido pela lei internacional.

Acresce que, sempre se dirá, numa última *ratio*, que uma interpretação restritiva nesta matéria, seria esquecer que o artigo 51.º da CNU não pode limitar o exercício do direito à legítima defesa para além do que é considerado razoável, pois "…*o direito inerente de legítima defesa individual*…", conforme consta no artigo 51.º da CNU, existia muito antes de 1945.

É que, como em relação ao ciberataque ocorrido na Estónia, Ene Ergma, porta voz do parlamento, doutorada em física nuclear, referiu, quando olha para uma explosão nuclear e para o que sucedeu na Estónia vê a mesma coisa. Como a radiação duma

explosão nuclear, um ciberataque pode destruir um Estado moderno, ainda que sem derramar sangue (2007, cit. por Shackelford, 2009, p.194).

3. A responsabilidade dos Estados por Ciberataques

a. A Inexistência de Direito Internacional Convencional

Recorrendo aos ciberataques de que foi alvo a Estónia (Anexo D), um dos problemas que surgiu para as autoridades Estonianas foi o da atribuição a um Estado daquelas ações (Shackelford, 2009, p.229). A Estónia acusou Moscovo de estar relacionada com os ciberataques às suas infraestruturas críticas, quer governamentais, quer civis. E este problema coloca-se, pondo de parte as questões de natureza prática decorrentes das características do ciberespaço dificultarem a análise forense no sentido de se detetar a origem, porque os ciberataques podem ser conduzidos por simples *hackers*, organizações criminosas, terroristas ou por Estados, pelo que se torna difícil averiguar a sua autoria.

Não é indiferente saber quem é o autor de um ciberataque uma vez que é também a partir da natureza deste que se retiram importantes ilações no sentido de saber se nos encontramos no âmbito da cibercriminalidade, do ciberterrorismo ou, com maior relevância para o presente trabalho, perante um ciberataque a qualificar como AA ou com efeitos equivalentes a este, com as inerentes consequências daí decorrentes.

A cibercriminalidade e o ciberterrorismo (este último se não for conetado com um Estado) terão obviamente um tratamento diferente, essencialmente ao nível do direito interno, mormente o direito criminal do Estado alvo, sendo que neste caso é obviamente necessário recorrer aos instrumentos particulares da criminalidade transnacional como a estreita cooperação judiciária entre os Estados envolvidos em matéria de investigação e recolha de prova.

A este aspeto, não é alheia a Lei do Cibercrime que estabelece as disposições penais materiais e processuais para este tipo de criminalidade e as correspondentes normas relativas à cooperação internacional concretamente no que respeita à recolha de prova. De destacar o artigo 20.º que determina que as autoridades nacionais cooperam com as autoridades estrangeiras competentes para efeitos de investigação criminal neste âmbito e recolha de prova dos crimes. (Assembleia da República, 2009).

Mas, o que é relevante para o presente trabalho é saber se é possível imputar a responsabilidade por ciberataques a Estados. Daí que seja essencial averiguar se um ciberataque pode ser imputado a um Estado.

As questões relacionadas com a imputação ou atribuição destes atos aos principais sujeitos de direito internacional tocam na temática da responsabilidade internacional dos Estados. O reconhecimento da responsabilidade internacional destes assenta na mesma

razão de ser pelas quais no direito interno dos Estados, tem existência a responsabilidade individual, e nesse aspeto existe largo acordo no sentido de que os Estados devem ser responsabilizados pelas suas condutas ilícitas.

Mas, um dos problemas é o facto do regime da responsabilidade internacional dos Estados não estar codificado, recorrendo-se sobretudo ao direito consuetudinário e à jurisprudência dos Tribunais para o especificar. Contudo, a Comissão de Direito Internacional (CDI) da ONU, aprovou em 2001, na sua 53.º sessão, um projeto de regime jurídico sobre responsabilidade dos Estados por atos ilícitos internacionais denominado de "*Draft Articles on Responsability of States for International Wrongful Acts*" (DARS), e que foi colocado para apreciação em AG da ONU (Assembleia Geral das Nações Unidas: 2001).

Trata-se efetivamente de um projeto, não sendo ainda direito convencional, mas que contém indicadores seguros acerca do que se pretende para este regime e quais as suas principais orientações (Machado, 2004, p. 502).

b. A imputação dos ciberataques aos Estados

Um dos aspetos em que a DARS fornece indicadores está relacionado precisamente com a imputação de atos ilícitos aos Estados. Mas antes de avançar, uma questão prévia relevante. É que a prática dos Estados e a jurisprudência do TIJ, e também o DARS (não se fala em culpa neste projeto), têm seguido a teoria da responsabilidade objetiva como princípio geral, ou seja sem necessidade de averiguar da intenção (dolo) ou negligência (culpa), embora tal averiguação possa ser relevante em casos especiais, pois apesar da culpa (em sentido lato) não ser condição geral de responsabilidade pode desempenhar um papel importante em certos contextos (Brownlie, 1996, p. 462-464). Obviamente que provando-se a intenção tanto melhor, mormente através de indícios credíveis relevantes.

Efetuada esta consideração prévia, o artigo segundo do DARS começa por dizer que a conduta de um Estado, quer por ação (comissiva) quer por omissão (omissiva), é ilícita do ponto de vista internacional, quando além de lhe ser imputada, constituir uma violação das suas obrigações internacionais. Duas questões se levantam.

A primeira questão é a de saber quando é que um ato é imputável a um Estado. E quanto a esse aspeto, dispõe o artigo quarto do DARS sob a epígrafe de "*Conduct of organs of a State*" que a conduta de qualquer órgão do Estado será a este imputado, independentemente de se tratar de um órgão legislativo, executivo, judicial ou com quaisquer outras funções, sendo que órgão será qualquer pessoa ou entidade que tenha esse

estatuto nos termos da lei interna desse Estado. É também nesta direção que aponta o grupo de peritos que se encontra a elaborar o manual de direito internacional aplicável à ciberguerra quando nele se estabelece a seguinte presunção " *if a cyberoperation has been launched or otherwise originated from governmental cyber infrastructure there is a rebuttable presumption that the state in question is associated with the operation*" (Tikk, 2011, p. 104).

Por outro lado, nos termos do artigo oitavo sob a epígrafe "*Conduct directed or controlled by a State*", as condutas de uma pessoa ou grupo de pessoas (que não, órgãos do Estado) serão consideradas como atos do Estado, se estiverem sob instruções, direção ou controlo desse Estado para levarem a cabo essas ações. Definitivamente, parecem incluir-se aqui os casos de grupos direta ou indiretamente patrocinados por Estados, quer em termos materiais quer em termos financeiros, para aquelas finalidades concretas.

No entanto, Shackelford chama a atenção para o facto da jurisprudência internacional não ser pacífica quanto ao controlo necessário para que o ato praticado por terceiros seja atribuído a um Estado. O TIJ no "*Nicarágua case*" entendeu necessário o controlo efetivo, ou seja, as pessoas ou grupo de pessoas que praticaram o ato ilícito têm de estar sobre completa dependência do Estado, ao passo que no caso do Tribunal Internacional Criminal para os crimes cometidos na ex Jugoslávia "*Tadic case*", se decidiu que se o Estado tem um papel na coordenação e organização do grupo, além de fornecer apoio, então existe controlo operacional, o que significa que os atos praticados por esse grupo são imputáveis ao Estado (2009, p.234). Quanto a nós entendemos que basta o controlo operacional. Mais, entendemos que face a uma ameaça desta natureza basta que Estado tenha conhecimento das atividades desenvolvidas no seu território por esses grupos e nada faça para as deter. Há aqui, claramente, uma imputação em resultado de uma omissão quando se estava obrigado a uma conduta ativa em respeito pelos objetivos da ONU.

Quanto à segunda questão, a de saber quando é que o ato é ilícito. O artigo segundo do DARS responde a esta questão quando dispõe que a conduta de um Estado é ilícita do ponto de vista internacional, quando constituir uma violação ou não conformidade com as suas obrigações internacionais. Obviamente que uma das principais obrigações dos Estados é não recorrer à ameaça ou ao uso da força, quer seja contra a integridade territorial ou independência politica de um Estado, ou de qualquer modo incompatível com os objetivos da ONU.

4. Síntese Conclusiva Global

Neste capítulo procuraremos retirar as conclusões principais das matérias constantes nos capítulos anteriores para depois nos debruçarmos sobre as HIP, PD e PP. No capítulo referente ao ciberespaço, clarificámos e caracterizamos este conceito. Densificámos o conceito de ciberataque e de IC. Concluímos, que os ciberataques podem ter atores diversos e diferentes motivações, e que os efeitos dos ciberataques serão mais ou menos gravosos consoante a natureza dos alvos. Se possuírem a natureza de IC, sendo ciberataques de grande amplitude e escala, poderão ter consequências ao nível político, militar e civil, podendo considerar-se como tendo potencialmente efeitos estratégicos. Logo, as IC são consideradas vulnerabilidades pois influenciam os domínios político, militar, económico, social, de infraestruturas e informacional de um Estado. No segundo capítulo, dedicou-se especial atenção à LD em direito internacional e ao conceito de AA seu pressuposto. Foi então definido AA como ato com grande amplitude, gravidade e escala, praticado utilizando quaisquer instrumentos ou dispositivos que tenha consequências e provoque efeitos violentos no adversário, ainda que os instrumentos ou dispositivos usados não tenham normalmente essa finalidade. No terceiro capítulo verificou-se os casos em que com base nos indicadores do DARS é possível imputar um ciberataque a um Estado.

Assim, quanto à HIP 1 em que "as infraestruturas críticas portuguesas estão a ser alvo de um ciberataque coordenado e de grande intensidade tipo DoS, que já originou dezenas de vítimas mortais e avultados danos materiais, com efeitos ao nível político, militar e civil", verifica-se que é uma das circunstâncias em que um ciberataque é considerado um AA. Enquadra-se perfeitamente na densificação do conceito acima efetuado pelo que se encontra respondida a PD1. Recorrendo à dimensão causal de AA, relativa apenas aos efeitos, o resultado seria o mesmo. Relativamente à HIP 2 em que "atualmente os ciberataques não podem ser imputados a Estados", verifica-se precisamente o contrário. Aos Estados podem ser imputados ciberataques conforme indicia de forma segura o DARS. Aliás, no âmbito do manual de direito internacional aplicável à ciberguerra estabelece-se a presunção de que um ciberataque oriundo de uma ciber infraestrutura governamental presume-se ato do Estado. Portanto, há imputação de responsabilidade por um ciberataque a um Estado se as autoridades do Estado titular das infraestruturas críticas violentadas, através da investigação e análise forense comprovarem que o ataque foi perpetrado por órgãos daquele, ou por pessoas ou grupo de pessoas que não sendo órgãos, são por este controladas. Responde-se desta forma à PD2.

Face a tudo exposto, se as IC portuguesas estão a ser alvo de um ciberataque coordenado e de grande intensidade tipo DoS, que já originou dezenas de vítimas mortais, avultados danos materiais, com efeitos ao nível político, militar e civil e as autoridades concluírem que foi perpetrado por órgãos de um determinado Estado, ou por pessoas ou grupo de pessoas que não sendo órgãos, são por este controladas, podem decidir invocar o artigo 51.º da CNU para atuarem em LD.

Consequentemente, à Pergunta de partida "poderá Portugal, face a um ciberataque, exercer o seu direito à legítima defesa à luz do direito internacional", responde-se afirmativamente nos termos e condições acima descritas.

Conclusões

No presente trabalho de investigação foi seguido o procedimento metodológico de investigação seguido pelo IESM, que corresponde à metodologia proposta por Raymond Quivy e Luc Van Campenhoudt na obra Manual de Investigação em Ciências Sociais, adotada na NEP n.º 218, do IESM, de 15 de setembro de 2011.

Este procedimento metodológico comporta várias fases e etapas. As fases são constituídas pela rutura, construção e verificação. Pretende-se numa fase inicial romper com falsas evidências relativamente ao tema, para na fase de construção, criar uma matriz conceptual organizada e lógica, que coincide com a fase da identificação da problemática e da construção do modelo de análise, culminando com verificação, na qual as proposições são ou não verificadas. Relativamente às sete etapas do procedimento foram ultrapassadas as primeiras, sendo que o presente capítulo corresponde à sétima. Recebido o tema a tratar " O impacto do ciberespaço como nova dimensão nos conflitos", na etapa um, dada a vastidão do tema foi efetuada a seguinte Pergunta de Partida: "Em que circunstâncias poderá Portugal, sendo alvo de um ciberataque, exercer o seu direito à legítima defesa à luz do direito internacional". Dessa forma direcionou-se e restringiu-se o tema. Prosseguiu-se para a segunda etapa continuando-se a recolha de informação, nomeadamente artigos e estudos. Foi nesta fase que se realizaram entrevistas exploratórias de forma a colher a sensibilidade dos entrevistados. Na fase da problemática, constatou-se que para responder à Pergunta de Partida era necessário averiguar se face ao regime jurídico internacional, um ciberataque poderia ser considerado um AA e se era possível imputar a responsabilidade por esse ato a um Estado. Questões de resposta complexa pois na prática nunca ocorreram factos que tenham causado tais interrogações, embora tenha sucedido algo parecido na Estónia e na Geórgia. Seguiu-se a etapa da construção do modelo de análise, com a Pergunta de Partida, já referida, e duas Perguntas Derivadas e respetivas Hipóteses bem como o corpo de conceitos a definir e explicitar. Nas etapas de observação e análise da informação, respetivamente, quinta e sexta etapa do procedimento metodológico, concebeu-se o modelo de observação, aplicou-se o mesmo, e trataram-se e analisaram-se os dados obtidos, que resultaram da apreciação crítica das teorias, pareceres e outros indicadores. Dessa forma, e com os resultados obtidos, foram apreciadas as hipóteses possibilitando o surgimento de respostas fundamentadas para as Perguntas Derivadas.

Para a abordagem do presente trabalho optámos por o dividir em quatro capítulos com a finalidade de melhor verificar as hipóteses formuladas e responder às perguntas derivadas que nortearam a investigação.

No primeiro capítulo, sobre a noção de ciberespaço, verificámos que não existe uma definição consensual para esta realidade e discorrermos sobre as características deste novo ambiente. Concluímos que se trata de um novo universo, ao mesmo tempo virtual e físico, a que são associadas inúmeras características. Densificámos o conceito de ciberataque, a sua tipologia, bem como os seus principais autores e motivações. Os seus principais autores vão desde simples *hackers*, passando por terroristas e por último os Estados, estes com verdadeiras capacidades para atacar as vulnerabilidades que constituem as infraestruturas críticas de um Estado e assim produzirem efeitos ao nível politico, militar e civil. Adotámos o conceito de infraestruturas críticas especificado pelo General Bispo referindo também que existem infraestruturas críticas em Portugal em domínios tão relevantes como o político, militar, económico, social, físico (infraestruturas) e informacional. Concluímos, em síntese, que as infraestruturas críticas nacionais constituem vulnerabilidades face a um ciberataque coordenado e de grande intensidade.

No segundo capítulo, versando sobre o regime jurídico internacional do uso da força, desenvolveu-se com a profundidade suficiente o regime da CNU no que concerne ao princípio da proibição do uso da força por parte dos Estados. Abordou-se a temática da legítima defesa individual e coletiva como exceção a esse princípio norteador da CNU. Verificou-se após análise ao artigo 51.º da CNU que um dos pressupostos para a invocação por um Estado do seu direito inerente de legítima defesa era ter sofrido um AA, pelo que se procedeu à densificação do conceito. Averiguou-se se era possível enquadrar um ciberataque no conceito de AA. Concluiu-se que embora haja uma corrente de opinião que defende que um ciberataque não pode ser considerado um AA para os efeitos previstos no artigo 51.º da CNU, é juridicamente viável, segundo outros autores, operar aquela disposição face a um ciberataque com determinadas características a infraestruturas críticas de um Estado, quer considerando-o um verdadeiro AA, ou ainda que não o considerando um AA, como uma ação com efeitos ou consequências equivalentes. Foi o que se concluiu em síntese. Dessa forma considerou-se que no caso referido na Hipótese 1 estamos perante um AA, respondendo à Pergunta Derivada 1 no sentido de que aquela hipótese é um caso em que um ciberataque é considerado um AA.

No capítulo terceiro, relativo à atribuição da responsabilidade a um Estado de ciberataques, não existe direito internacional convencional em relação a essa matéria, sendo as questões de responsabilidade dos Estados resolvidas recorrendo ao direito consuetudinário e à jurisprudência dos tribunais internacionais. No entanto, em 2001 surgiu o projeto da CDI da ONU a que foi dado o nome de "*Draft Articles on*

Responsability of States for International Wrongful Acts" que embora não constitua ainda direito convencional, nos fornece algumas indicações sobre as soluções encontradas e o caminho que se pretende seguir. Conforme nele disposto a conduta de um Estado, quer por ação (comissiva) quer por omissão (omissiva), é ilícita do ponto de vista internacional, quando além de lhe ser imputada, constituir uma violação ou não conformidade com as suas obrigações internacionais. Após a constatação de que um ciberataque é um ato ilícito por violação do Princípio da proibição do uso da força por parte dos Estados, tal levou-nos a indagar quais os casos em que se podem imputar atos aos Estados. Conclui-se que a conduta de qualquer órgão do Estado será a este imputado, independentemente de se tratar de um órgão legislativo, executivo, judicial ou com quaisquer outras funções, sendo que órgão será qualquer pessoa ou entidade que tenha esse estatuto nos termos da lei interna desse Estado. Deu-se também notícia de que no âmbito do *Cooperative Cyber Defense Centre of Excellence,* na Estónia, o grupo de peritos que se encontra a elaborar o manual de direito internacional aplicável à ciberguerra estabeleceu a seguinte presunção " *if a cyberoperation has been launched or otherwise originated from governmental cyber infrastructure there is a rebuttable presumption that the state in question is associated with the operation*". Explicitado o regime, procurou-se saber se era possível imputar um ciberataque a um Estado, verificando-se que é perfeitamente viável isso suceder. Face ao que se verificou a Hipótese 2 como não confirmada e respondeu-se à Pergunta Derivada 2 no sentido de que os ciberataques podem ser imputados a um Estado se se provar que o ataque foi perpetrado por órgãos daquele, ou por pessoas ou grupo de pessoas que não sendo órgãos, são por este controladas.

Assim sendo, confirma-se que um ciberataque pode operar a invocação do artigo 51.º da CNU por parte do Estado cujas infraestruturas críticas foram atacadas. Dentro de determinados parâmetros um ciberataque pode ser considerado um AA, ou para quem não lhe reconhece essa possibilidade, uma ação com efeitos equivalentes a AA. Mas para tal suceder o ciberataque tem que ter tido como alvo infraestruturas críticas do Estado e produzido efeitos ao nível político, militar e civil, o que sucede se existirem vítimas mortais e destruição física, ao ponto de colocar em causa a segurança nacional desse Estado. Esta factualidade dará as características de escala, intensidade e gravidade, exigidas pela Jurisprudência do TIJ e pela doutrina internacional, a qualquer ataque para que tenha aplicação aquela disposição da CNU, incluindo um ciberataque. Essa invocação deve ser efetuada pelas autoridades nacionais do Estado. Por outro lado, há que atribuí-lo ou imputá-lo a um Estado, responsabilizando-o conforme a teoria da Responsabilidade

apresentada. Vimos as situações em que é viável imputar a responsabilidade por ciberataques a um Estado. Por último, torna-se necessário o preenchimento dos restantes pressupostos da legítima defesa, concretamente a subsidiariedade, a proporcionalidade e a provisoriedade da defesa, pois apenas assim ela será legítima. Contudo, este último aspeto é lateral ao presente trabalho.

O presente trabalho constitui uma abordagem realista à perigosidade dos ciberataques, dissertando, sobre a opção dos Estados vítimas face ao direito internacional particularmente no que ao direito de legítima defesa concerne.

Assim, como contributos concretos para o conhecimento podemos afirmar que construímos uma *ratio* que determina as condições que um ciberataque deve possuir para que seja considerado um AA nos termos e para os efeitos consignados no artigo 51.º da CNU. Complementarmente, considerámos que essa é uma análise e decisão que compete às autoridades do Estado lesado.

Concretizámos, com base nos indicadores fornecidos pelo DARS quais as situações em que se pode imputar a responsabilidade por ciberataques a um Estado. Verificámos que, de facto, as infraestruturas críticas de um Estado têm vulnerabilidades face a ciberataques, sendo urgente medidas de proteção, pois como referido, a sua rutura pode produzir efeitos de âmbito nacional, ou regional, de tal forma que afeta o regular funcionamento dos serviços da sociedade civil e das instituições nacionais, criando um problema de segurança nacional.

Constatámos ainda que, face ao facto da legislação sobre proteção de infraestruturas críticas apenas ter sido publicada recentemente (Decreto-Lei n.º 62/2011, de 9 de Maio) ainda é longo o caminho a percorrer, não sendo incorreto dizer, como Collins referiu no congresso Norte-Americano, que não ocorre outro domínio na segurança nacional de um Estado em que a ameaça seja tão grande e o que tenha sido feito até agora para a prevenir e combater tenha sido tão pouco face aos danos que potencialmente pode provocar (2012).

No que concerne a recomendações é imprescindível o acompanhamento do tratamento que tem sido dado a esta temática na doutrina e jurisprudência internacionais.

O acompanhamento da doutrina e postura da ONU e da NATO, bem como a frequência de cursos e seminários do *Cooperative Cyber Defense Centre of Excellence*, é também essencial. A adesão por parte de Portugal a este Centro também não era de rejeitar.

É também fulcral que se deixe de olhar para os ciberataques apenas na perspetiva da cibercriminalidade e do ciberterrorismo e apreender definitivamente que os Estados têm

novas ciberestruturas no âmbito militar, que atuando originarão potencialmente a regulação pelo *Jus ad bellum* e *Jus in bello*.

Por último, no seguimento do que se disse no anteriormente, recomenda-se a participação em exercícios NATO no âmbito do ciberespaço, mas em que se teste todo o espetro de incidentes. Portugal através dos Ramos têm participado no exercício NATO "Cyber Coalition", mas tem ficado de fora nos incidentes referentes à aplicação do direito dos conflitos armados.

Bibliografia

Academia das Ciências de Lisboa, *Dicionário da Língua Portuguesa Contemporânea*, I Volume, Editora Verbo, 2001.

Assembleia da República, 2009. *Aprova a Lei do Cibercrime* (Lei n.º 109/2009, de 15 de setembro), Lisboa, Diário da República.

Assembleia Geral das Nações Unidas, 2001. *Responsability of States for International Wrongful Acts* [Em linha] (Resolução n.º 56/2001, de 12 de Dezembro de 2001). Disponível em: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/477/97/PDF/N0147797.pdf?OpenElement. [Consult. 04 Jan. 2012].

Balsinhas, P., 2003., *Os riscos do Ciberespaço – Análise e Gestão dos Riscos nas Infraestruturas Críticas de Informação, Academia Militar*, 2003.

Baptista, EC, 2003. *O Poder público bélico em Direito Internacional: O uso da força pelas Nações Unidas em especial*, Colecção Teses, Doutoramento, Almedina, 2003.

Benedikt, M., 1991. *Introduction to Cyberspace: first steps*, MIT Press, 1991. [Em linha] Disponível em: http://services.exeter.ac.uk/cmit/media/texts/benedikt1991/introduction.pdf [Consult. 14 Dez. 2011].

Brownlie, I, 1996. *Princípios de Direito Internacional Público*, Fundação Calouste Gulbenkian, 1996.

Butrimas, V, 2011. *An Unsettling Trend: Attacks Show the Need for a Proactive Defense Strategy in Cyberspace, per* Concordiam, *Cyber Security, Jornal of European Security and Defense Issues*, volume 2, Issue 2, *George C. Marshall European Center for Security Studies*.

Center for Strategic and International Studies, 2012. *Significant Cyber incidents since 2006* [Em linha]. Disponível em http://csis.org/files/publication/120410_Significant_Cyber_Incidents_Since_2006.pdf [Consult. 10 fev. 2012].

Collins, S, 2012. *Stuxnet: Computer Worm opens new era of warfare* [Registo vídeo em linha]. 60 Minutes, CBSnewsonline. 2012. Disponível em: http://www.youtube.com/watch?v=6WmaZYJwJng [Consult. 14 abr. 2012]

Duarte, ML, 2012. *Ciberataques e ataques armados*. Entrevista efetuada pelo autor em 2 abr. 2012. Lisboa.

Durán, JD, 2010. *La Cibersuguridad en el Ámbito Militar* [Em linha], in Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, Cuadernos de Estratégia 149, Ministerio de Defensa. Dísponivel emhttp://www.portalcultura.mde.es/Galerias/publicaciones/fichero/CE_149.pdf: [Consult. 25 Abr. 2012].

Força Aérea Portuguesa, 2011. *Aprova a Política de Ciberdefesa da Força Aérea* (Regulamento da Força Aérea 390-6, de fevereiro de 2011), Alfragide, 2011.

Government Accountability Office, 2010. *Cyberspace. Report to Congressionals Requesters.* Estados Unidos da América [Em Linha]. Dísponivel em: http://gao.gov/assets/310/308401.pdf [Consult. 05 jan. 2012].

Gibson, W, 1984. *Neuromancer*, New York, Ace Books.

Gouveia, JB, 2012. *Ciberespaço: espaço virtual, mediático e global* [Registo vídeo em linha], Conferência realizada na Academia de Ciências de Lisboa. Disponível em: http://www.jorgebacelargouveia.com/2512012-direito-do-ciber-espaco-academia-de-ciencias-de-lisboa.html [Consult. 8 Mar.2012].

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 de novembro de 2010, revisto em 15 de Janeiro de 2012 [Em linha]. Disponível em http:// dtic.mil/ doctrine/new_pubs/jp1_02.pdf [Consult. 25 jan. 2012]

JP 3-11, *Information Operations*, 13 de fevereiro de 2006 [Em linha]. Disponível em: http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm [Consult. 27 jan. 2012]

Machado, JEM, 2004. *Direito Internacional: Do Paradigma Clássico ao Pós 11 de Setembro*. Coimbra Editora, 2004, 2.ª Ed..

Melo, P., 2010 *A Ciberguerra, Estrutura para enfrentar as vulnerabilidades: uma capacidade crítica autónoma ou partilhada*, Instituto de Estudos Superiores Militares, Trabalho de Investigação Individual do CPOG, 2010.

Ministério da Defesa Nacional, 2011. *Estabelece os procedimentos de identificação e protecção das infraestruturas essenciais* (Decreto-Lei n.º 62/2011, de 9 de Maio). Lisboa. Diário da República.

Ministério dos Negócios Estrangeiros, 1991. *Publica os textos em inglês e português da Carta das Nações Unidas e o Estatuto do Tribunal Internacional de Justiça* (Aviso n.º 66/91, de 18 de Março), Lisboa, Diário da República.

Monteiro, MH, 2007. *Infra-Estruturas Críticas e Vulnerabilidades Sociais: o paradigma do mundo mais desenvolvido*. Revista de Planeamento Civil de Emergência, n.º 19, 2007. Conselho Nacional de Planeamento Civil de Emergência.

Operational Law Handbook, 2008. International and Operational Law Department. The Judge Advocate General´s Legal Center&School, U.S. Army, Virginia.

Porto Editora, 2012. *Dicionário da Língua Portuguesa* [Em linha], Porto Editora 2012. Disponível em: http://www.infopedia.pt/lingua-portuguesa/ciberespa%C3%A7o [Consult. 15 jan. 2012).

Presidência da República, 1992. *Aprova o Protocolo Adicional I e II às Convenções de Genebra de 12 de Agosto de 1949* (Decreto do Presidente da República n.º 10/92, de 1 de Abril), Lisboa, Diário da República.

Roscini, M, 2010. *World Wide Warfare – Jus ad Bellum and the use of Cyberforce*, Max Planck Yearbook of United Nations Law, Volume 14, 2010 [Em linha]. Disponível em: http://www.mpil.de/shared/data/pdf/pdfmpunyb/03_roscini_14.pdf [Consult. 23 abr. 2012]

Shackelford, SJ, 2009. *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law* [Em linha]. Berkeley Journal of International Law, 2009, Vol. 7:1. Disponível em: http://www.boalt.org/bjil/docs/BJIL27.1_Shackelford.pdf. [Consult. 10 dez. 2011].

Saraiva, FM, 2007. *A definição de Agressão da Assembleia Geral das Nações Unidas: História de uma Negociação*, Cadernos Navais, N.º 23, 2007.

Saraiva, FM, 2009. *Poder Militar e Agressão Armada em Ambiente Pós-bipolar: Análise Jurídico-Estratégica das "Guerras High Tech" e das "Novas Guerras" nos discursos e práticas sobre Agressão e Legítima Defesa*, Tese de Doutoramento, Lisboa, ISCSP, 2009.

Schmitt, MN, 2002. *Wired warfare: Computer network attack and jus in bello*. International Review of the Red Cross, 2002, Vol. 84, n.º 846, International Committee of the Red Cross, 2002.

Seara, FR, et al., 1991, *Direito Internacional Público - Documentos fundamentais*. Universidade Lusíada, 1991.

Tikk, E, 2011. *Comprehensive Legal Approach to Cyber Security*, Tese de Doutoramento, Universidade de Tartou, Estónia [Em linha]. Dísponivel em: http://dspace.utlib.ee/dspace/bitstream/handle/10062/17914/tikk_eneken.pdf?sequence=1 [Consult. 12 Jan. 2012].

Tribunal Internacional de Justiça, 1986. *Military and Paramilitary Activities in and against Nicarágua (Nicaragua v. United States of America), Merits*, [Em linha]. Dísponivel em : http://www.icj-cij.org/docket/files/70/6503.pdf [Consult. 19 Jan. 2012].

Anexo A - Corpo de conceitos

Ciberespaço - Domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de tecnologia de informação incluindo a internet, redes de telecomunicações, sistemas de computadores e os inerentes processadores e controladores.

Ciberataque - Ataque lançado geralmente a partir de um computador recorrendo ao método de intrusão e que tem como finalidade adquirir, explorar, perturbar, romper, negar, degradar ou destruir informação constante em computadores ou em redes de computadores, em sistemas e equipamentos eletrónicos ligados a outros equipamentos ou sistemas ou que partilham a mesma estrutura de energia ou o mesmo espaço de emissão eletromagnética, bem como os próprios computadores, redes de computadores, sistemas e equipamentos.

Infraestruturas críticas - Aquelas cuja rutura pode produzir efeitos de âmbito nacional, ou regional, de tal forma que afete o regular funcionamento dos serviços da sociedade civil e das instituições nacionais, criando um problema de segurança nacional.

Ataque Armado - Ato , com grande amplitude, gravidade e escala, praticado utilizando quaisquer instrumentos ou dispositivos, que tenha consequências e provoque efeitos violentos no adversário, ainda que os instrumentos ou dispositivos usados não tenham normalmente essa finalidade.

Responsabilidade dos Estados - Imputação da responsabilidade de um ciberataque a um Estado.

Anexo B - Mapa conceptual

PD1: Em que circunstâncias pode um ciberataque ser considerado um ataque armado.

PD2: Em que circunstâncias pode a responsabilidade por um ciberataque ser imputada a um Estado.

Hipótese 1	**Conceitos**	**Dimensões**	**Indicadores**
As infraestruturas críticas portuguesas estão a ser alvo de um ciberataque coordenado e de grande intensidade tipo DoS, que já originou dezenas de vítimas mortais e avultados danos materiais, com efeitos ao nível político, militar e civil.	Ciberespaço	Virtual e física	Carta das Nações Unidas Jurisprudência Artigos e Estudos Exemplos da Estónia e Geórgia *Responsability of States for International Wrongful Acts* CCDCOE Trabalhos do IESM DIVOPS e DEPJUR/FAP Entrevistas
	Ciberataque	Política, militar e civil	
	Infraestruturas críticas	Política, militar, económica, social, infraestruturas e informacional	
	Ataque Armado	Literal e causal Política, militar, civil	
Hipótese 2			
Atualmente os ciberataques não podem ser imputados a Estados	Responsabilidade dos Estados	Comissiva Omissiva	

Anexo C - Quadro de capacidades

Quadro demonstrativo das capacidades no âmbito do ciberespaço implementadas nos Estados nele identificados. A classificação vai de 1 (baixo) a 5 (alto) quanto à capacidade implementada.

Quadro de capacidades

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

Fonte : (Tecnolytics, 2010, p. 13, cit. por Melo, 2010, p.14)

De salientar, além do USCYBERCOM, que a China reportou a criação de Batalhões e Regimentos para o Ciberespaço. Israel tem pessoal especializado na *Internet Warfare* e a Alemanha possui uma ciber unidade (Roscini, 2010, p. 98).

Anexo D - Casos significativos de ciberataques

- maio de 2007. A Estónia sofreu ciberataques tipo *Denial of Service* (DoS) às suas infraestruturas críticas com consequências a nível nacional. O ataque coordenado colocou fora de serviço parte dos sítios governamentais e comerciais (Computerworld, 2007:1 cit. por Melo, 2010: p. 9).

- agosto de 2008. Foi a vez da Geórgia ser alvo de ciberataques às suas infraestruturas críticas de comunicações e informações, quer governamentais quer civis, só que desta vez tal ação precedeu a execução de uma operação militar convencional por parte da Rússia naquele território. Desta forma, a capacidade da Geórgia para coordenar e organizar a sua defesa nacional face à invasão Russa foi severamente comprometida (Butrimas, 2011: p. 13).

- outubro de 2010. W*orm* denominado *Stuxnet* que neutralizou centrifugadoras de uma central nuclear Iraniana. Este *worm* demonstrou que um ciberataque pode não só neutralizar o alvo mas destruí-lo, motivo pelo qual existem estudos que sugerem que face à potencialidade apresentada, apenas se encontra na disponibilidade e nos domínios de um Estado (Butrimas, 2011: p. 13). Foram afetados milhares de computadores em todo o mundo, com especial incidência no Irão infetando computadores na primeira central nuclear do Irão (CBSNEWS, 2010:1, cit. por Melo, 2010: p. 9).

- setembro de 2011. Um vírus de origem desconhecida foi introduzido nos sistemas de controlo de UAVs na Creech Air Force Base no Nevada, nos EUA. As autoridades referiram que não perderam o controlo de nenhum aparelho, mas adiantaram que apenas decorridas várias tentativas é que conseguiram remover o vírus (Center for Strategic and International Studies, 2012).

-março de 2012**.** O Ministro das Comunicações e Tecnologias da Informação da India referiu no parlamento que 112 sítios governamentais foram comprometidos de dezembro de 2011 a fevereiro de 2012. Muitos ataques aparentam ter tido origem no Paquistão (Center for Strategic and International Studies, 2012).

.