FACULDADE DE CIÊNCIAS SOCIAIS E HUMANAS
UNIVERSIDADE NOVA DE LISBOA

Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional

Octávio Pimenta Militão

Mestrado em Ciência Política e Relações Internacionais, especialização em Relações Internacionais

Abril 2014

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Ciência Política e Relações Internacionais na Área de Especialização em Relações Internacionais, realizada sob a orientação científica de

Professora Doutora Teresa Maria Ferreira Rodrigues

e

Tenente-Coronel de Transmissões (Doutor) Paulo Fernando Viegas Nunes

À Patrícia, à Rita, ao Ivo

e

à memória do Abel

AGRADECIMENTOS

A realização desta investigação não se extingue na minha concretização individual; trata-se do culminar do contributo de todos aqueles que, no seu momento e ao longo do meu percurso - académico e/ou profissional, souberam cativar-me, apoiar-me e fazer-me apaixonar; a todas elas a minha gratidão será uma constante intemporal.

À minha família nuclear pelos valores recebidos, pela paciência, incentivo e motivação.

Aos meus orientadores, Professora Doutora Teresa Maria Ferreira Rodrigues e Tenente-Coronel de Transmissões (Doutor) Paulo Fernando Viegas Nunes pela disponibilidade e facilidade na comunicação; e pela extrema compreensão do facto de a minha ocupação profissional me drenar as horas e os dias.

Por fim, um especial agradecimento para os amigos e familiares que pela sua existência e insistência, cada um, à sua forma me ajudaram e contribuíram para alcançar mais uma *stepstone* no meu caminho e sem os quais teria sido muito mais difícil. Obrigado a todos!

Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional

Octávio Pimenta Militão

O Ciberespaço alterou o paradigma da segurança e defesa internacional, obrigou à adoção de novas estratégias, metodologias de ação e capacidade tecnológica. A sua transversalidade aos diversos outros meios dotam-no simultaneamente de características e capacidades próprias que extrapolam o que se poderia imaginar à vinte anos atrás. Desta forma surgiu a necessidade de uma cooperação internacional mais intensa e eficaz, que promovesse uma ação multi ou transnacional conjunta, que fizesse face ao crescendo de ameaças no ciberespaço. No presente trabalho iremos abordar este tema, elaborando também de que forma este novo meio influenciou a balança de poderes internacional e qual a premência de estabelecimento de fronteiras que garantam delimitações físicas e legais idênticas às existentes fora o ciberespaço.

Cyberspace changed the entire international safety and security scale. It compulsory obligated the introduction of new methodologies, strategic actions and technologic capability due to its transnational and transversal identity, as well as, because of its inherent characteristics. The need of an international cooperation more intense, accurate and effective emerged from the increasing of cyberspace treats. In the present work we will elaborate more on this subject as well as the way it influenced the international scale of powers. Moreover we will address the importance of establishing borders in cyberspace that maintain an equivalent to the legal and physical system already existing.

PALAVRAS-CHAVE: Ciberespaço, ciberdefesa, cibersegurança, fronteiras, cooperação

KEYWORDS: Cyberspace, cyberdefense, cybersecurity, borders, cooperation

Índice

LISTA DE ABREVIATURAS

IDN – Instituto da Defesa Nacional

CERT – Computer Emergency Response Team

CNC – Centro Nacional de Cibersegurança

EC3 – European Cybercrime Centre

ENISA – European Network Security Agency

CSDP – Política Comum de segurança e Defesa

CEPOL – European Police College

Introdução

Com o surgimento das novas tecnologias de informação o mundo alterou por completo a visão sobre os parâmetros da acessibilidade, disponibilidade e distância. À medida que se estudam e se procuram enquadrar dinâmicas internacionais, rapidamente se recai neste tema tão premente e difundido pelos próprios meios que o compõe. Estas estruturas tendencialmente influenciam a opinião pública, sendo que estão à disponibilidade de todos e na maioria das vezes, até contra vontade dos utilizadores. Sendo um agente, cada vez mais influenciador no que concerne ao apoio à decisão política, acaba por chegar a variâncias que dificultam a governança e podem inclusive gerar acérrimos debates sobre a sua utilização.

Estamos perante o ciberespaço. Confrontados com todas as suas capacidades, é-nos permitido vislumbrar tanto aspetos positivos como negativos que advêm da sua utilização. Não se poderá imaginar hoje um mundo sem recurso aos meios que este novo 'meio' dotou a atualidade. Desta forma, surgem interesses como em qualquer outro meio, sendo que este é mais que um mero meio. Em última instância, acaba por ser fonte e meio de replicação da realidade através do recurso às novas tecnologias, devido a inúmeros fatores, sendo os principais a velocidade de propagação e dispersão e ainda a possibilidade de multiplicação e multiplicidade de funções simultâneas em diferentes pontos. Apresenta-se assim de extrema urgência o surgimento de organismos de controlo, a cibersegurança e a ciberdefesa.

A elas são acometidas diversas funções e são explorados diversos paradigmas e modos de atuação. A sua necessidade é hoje talvez mais importante que uma defesa

bélica tradicional cem por cento apta e eficaz, denotando a importância que a mesma tem para a compreensão da transformação que ocorre da comunidade internacional.

Desta forma, é necessário avaliar muitíssimo bem a proporcionalidade entre os desafios das condições promovidas pelo meio e a capacidade de resposta.

Este é um tema que recolhe cada vez maior atenção no cenário tanto nacional como internacional, mas cujo conhecimento sobre o seu real funcionamento, bem como as suas vulnerabilidades e sujeições, nunca ou dificilmente serão na sua plenitude mapeadas. Desta forma, poder-se-á afirmar que existe - e existirá - continuamente uma carência de estudos amplos e cuja delimitação seja holística ao meio.

As questões de partida da presente dissertação assenta sobre de fazer coincidir as fronteiras legais fora do ciberespaço com a criação de fronteiras idênticas no seio deste? Se esta será uma forma mais eficaz de garantir e aplicar uma ciberdefesa e cibersegurança mais eficazes? E finalmente de que forma esta criação de fronteiras no ciberespaço pode alterar positiva ou negativamente o equilibro do sistema internacional. Não se verificando serem questões de resposta fácil, estabelecemos uma série de questões derivativas estruturantes para o presente trabalho de investigação que passamos a apresentar.

Assim, definimos três questões de partida derivadas que assumiremos como vetores de análise para responder às questões anteriores: (1) qual a profundidade de cooperação internacional necessária para um combate ativo e eficaz às novas ameaças do ciberespaço, (2) de que forma a evolução do ciberespaço influenciou as redes de poder no cenário internacional e qual a sua premência para a criação de um plano de ciberdefesa eficiente, finalmente (3) qual seria a eficácia de um Centro Nacional de Cibersegurança unificado que agrupasse as áreas civil e militar.

Deste modo, e para responder a estas questões temos que o objeto de estudo desta dissertação será a cibersegurança e a ciberdefesa, sob que aspetos esta é uma ativa modificadora da balança internacional de poderes. Procurar-se-á perceber-se de que forma a cibersegurança e a ciberdefesa moldam os seus vetores em virtude da multiplicidade de papéis que necessitam desempenhar para um efeito preventivo e

eficiente. Na prossecução deste objetivo será feito um enquadramento da segurança e defesa nacional, bem como das suas reais capacidades e afeções, para que nos seja possível desenhar um enquadramento, tanto teórico-metodológico como de necessidades práticas e reais, que nos são remetidas pela emergência do meio em que nos vamos focar.

Assim sendo, sentimos a necessidade de definir o papel da identidade para compreender a real dimensão do que nos é acometido pelo e no ciberespaço. A identidade dos indivíduos é transportada para o ciberespaço e isso pode afetar a aplicação de uma ciberdefesa e a garantia de uma cibersegurança eficazes dada a volatilidade de recriação de uma identidade. Por isso mesmo, serão desenvolvidas estas problemáticas para compreender como esta renegociação delimita e estrutura o padrão de funcionamento, passível de influência humana, do ciberespaço. A necessidade de abordar temas como o cibercrime e a vulnerabilidade das infraestruturas críticas nacionais, surge como consequência da avaliação identitária conjugada com a temática da segurança e defesa nacional sendo que é a primeira, a identidade, que em muito define as metas necessárias para uma ação eficaz da segunda.

Em virtude da crescente mobilidade das populações observou-se, uma cada vez mais acentuada, permeabilidade de fronteiras. Por oposição evolucionária, o ciberespaço era pautado pela inexistência de fronteiras que dotavam os seus utilizadores de uma capacidade extrema de dispersão, sendo agora observável que algumas fronteiras começam agora a ser estabelecidas e impostas. As fronteiras políticas reais foram estabelecidas a sangue e a uma luta extensa tanto no tempo como como no espaço. As suas implicações legais podem ser fortemente verificadas ou como verificável na União Europeia podem ser permeáveis e por isso mais ligeiras. A questão é que as fronteiras existem para distinguir o 'eu' e desta forma deveriam ser transportadas para o ciberespaço em moldes similares aos existentes no do espaço terrestre. Inicialmente as suas implicações e as dificuldades podem ser consideráveis, porém, a médio-longo prazo deverá verificar-se de mais fácil controlo e cujas implicações legais são mais transparentes e adequadas a cada estado soberano.

No seguimento desta linha de pensamento, propomo-nos a avaliar os novos desafios impostos ao sistema internacional em virtude deste novo meio, definir quais as vulnerabilidades estratégicas do ciberespaço, efetuar uma avaliação ao risco em questões de ataque, a abordar o porquê de se apelidarem as armas deste meio como de dirupção massiva e ainda de que forma as relações de cooperação internacional são moldadas às especificidades do meio.

I. CONCEPTUALIZAÇÃO

I.1.I. Metodologia

A investigação em ciências sociais ultrapassa a necessidade da descoberta. Procura descrever, compreender e tentar explicar como decorrem certos fenómenos e acontecimentos sociais[1]. Na maioria dos processos de investigação, o procedimento metodológico é dedutivo, através do qual se confirmam premissas iniciais, das quais partiu a investigação, com recurso a determinadas regras de inferência. Ou seja, a metodologia de investigação a que comummente se recorre em relações internacionais é aquela que permite uma envolvência lógica de raciocínio em torno da questão ou questões iniciais a que se pretende responder.

Os métodos de aplicação podem ser diversos, porém existe uma preferência por parte dos cientistas sociais ligados às Relações Internacionais.

Como primeira etapa, observa-se maioritariamente uma pesquisa por meios de disseminação de informação escrita, leiam-se constituições, leis e livros, monografias, dicionários históricos e ainda paper's académicos de reconhecidos autores científicos. Estas são em ciências sociais as fontes primárias e secundárias de informação, respectivamente.

Como fonte terciária de informação em ciências sociais podem ainda ser utilizadas entrevistas e - menos comum - pode ainda recorrer-se a questionários. Cada um destes dois últimos métodos possui uma metodologia de aplicação própria que varia consoante o intuito da investigação a que são propostas, pelo que a sua explicação carece de uma atenção que nos parece excessiva para o que nos propomos no presente trabalho.

[1] Silva, A. S., & Pinto, J. M. (Eds.). (1999). *Metodologia das Ciências Sociais*. Porto, Edições Afrontamento

Ultrapassada a metodologia de investigação, iniciamos o processo de análise dos resultados. Para tal, em ciências sociais inicia-se a metodologia analítica com recurso a uma análise histórica que permita um enquadramento histórico-político envolvente de toda a temática que se pretende abordar. Em seguida procurar-se-á enquadrar o tema de investigação e análise em todas as esferas, sobre as quais recairá a análise metodológica.

I.1.II. Aplicação Metodológica

O ciberespaço e toda a sua envolvência carecem de um estudo amplo e cientificamente compreensível. Desta forma, na presente dissertação procuramos compreender e analisar as questões e objectivos já definidos, de forma a pudermos responder ao que nos propusemos no início da elaboração do presente trabalho de investigação.

Inicialmente para dar início a uma investigação completa e envolvente à temática escolhida, procedeu-se à definição de uma série de conceitos considerados essenciais para compreender a dimensão das esferas que iremos abordar. Em seguida procedeu-se a uma análise conceptual que enquadra-se o tema, quanto à sua aplicabilidade, enriquecendo-a com uma análise histórico política que o enquadrassem e explicassem a sua pertinência para o panorama internacional.

Recorreu-se à análise de diversas leis nacionais e internacionais, bem como a livros de autores de renome nas diversas áreas abordadas, bem como a alguns artigos científicos e paper's académicos que se consideraram enriquecedores para uma melhor explanação do tema.

Assistiram-se a diferentes palestras de assuntos periclitantes relacionados com o tema em análise que se procuraram inserir enquanto informação escrita que soma-se algo mais no discorrer desta dissertação.

A metodologia utilizada careceu de adaptações ao estrito das ciências sociais pois verificou-se necessária uma investigação e análise prática das ciências exatas dada a pertinência da matéria escolhida.

I.2. Mapa de Conceitos

O estudo o ciberespaço e do que ele envolve é complexo e carece de uma exploração por diferentes termos, que os definam, para que possa ser possível enquadrar teoricamente o tema a que nos referimos. O nosso estudo assenta sobre dois pilares, o da segurança e da defesa nacional pelo que temos:

Segurança Nacional – "condição da Nação que se traduz pela permanente garantia da sua sobrevivência em paz e liberdade; assegurando a soberania, independência e unidade, a integridade do território, a salvaguarda colectiva de pessoas e bens e dos valores espirituais, o desenvolvimento normal das tarefas do Estado, a liberdade de ação política dos órgãos de soberania e o pleno funcionamento das instituições democráticas[2]."

Defesa Nacional – "Conjunto de medidas e ações adequadamente integradas e coordenadas, que, globalmente ou sectorialmente, permitem fortalecer a capacidade

[2] Carvalho, Jorge Silva (2009) "Segurança Nacional, Serviços de Informações e as Forças Armadas", Palestra proferida na Faculdade de Letras de Lisboa a 28 de Maio de 2009

da Nação, com vista a alcançar a segurança nacional, procurando criar as melhores condições para a prevenção e combate de quaisquer ameaças que, direta ou indiretamente, se oponham à consecução dos objectivos nacionais[3].”

Partindo da definição destes dois conceitos à que compreender o que o tema escolhido comporta, nomeadamente, o que é o ciberespaço:

Ciberespaço – “é o ambiente artificial criado por meios informáticos no qual se agrupam e relacionam utilizadores, linhas de comunicação, sites, fóruns, serviços de internet e outras redes[4].”

Será portanto neste meio que iremos desenvolver o nosso processo de investigação. Iremos trabalhar circularmente em torno da cibersegurança e da ciberdefesa, da guerra da informação, ciberguerra, ciberespionagem e cibercrime. Iremos ainda relacionar este último, o cibercrime, com o terrorismo e explicar qual a importância das infraestruturas críticas para o equilíbrio funcional de uma sociedade bem como do sistema político internacional.

Cibersegurança – é a garantia de fiscalização e ‘policiamento’ do ciberespaço de forma a garantir uma eficaz reação à prática criminosa no mesmo[5].

Ciberdefesa – tem a função de garantir a realização de missões de segurança e defesa nacional, ou seja de garantir uma soberania do estado no ciberespaço global[6].

[3] Definição do Instituto da Defesa Nacional

4 Definição do Dicionário da Real Academia Espanhola, citada em (2013) Estratégia da informação e Segurança no Ciberespaço,IDN

5 Nunes, Paulo Viegas (2013) “Cibersegurança e Estratégia Nacional de Informação: Estruturas de Coordenação Nacional no Ciberespaço”, Conferência, Beja, IV SimSIC

6 Nunes, Paulo Viegas (2012) “A Definição de uma Estratégia Nacional de Cibersegurança”, Cibersegurança, N.º133, IDN

Guerra da Informação – "pode ser definida como qualquer ação de negação, exploração, corrupção, ou destruição das estruturas e funções de informação do adversário, ao mesmo tempo adoptando condutas para contrariar essas ações quando provenientes do adversário, e potenciando as próprias capacidades de gestão de informação."[7]

Ciberguerra – "é a materialização de ação de defesa ou de ataque contra todo o género de estruturas da informação e redes de computador, em que o campo de batalha é conduzido numa dimensão digital."[8]

Ciberespionagem – é uma variante da espionagem tradicional. É perpetrada por estados que procuram adquirir conhecimento e recolher informações, que lhe podem conceder uma vantagem estratégica sobre terceiros[9].

Cibercrime – é toda e qualquer prática criminosa que tenha associada à sua realização, ou como meio um aspecto *cyber* ou o recurso à utilização de computadores. Existem diversas tipologias e métodos de praticar o cibercrime, sendo um sistema o meio do ataque ou o alvo do mesmo[10].

Ciberterrorismo – "é um novo tipo de atividade criminal, (...) que materializa a convergência do ciberespaço com o terrorismo[11]." E "constitui um ataque político

[7] Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008) Cyberwar – O Fenómeno, as Tecnologias e os Atores, Lisboa, FCA

[8] idem.

[9] Pereira, Júlio (2012) "Cibersegurança – O Papel do Sistema de Informações da República Portuguesa", *Segurança e Defesa*, Maio-Agosto 2012, Lisboa, Diário de Bordo

[10] "What is Cybercrime?", Norton, Symantec. Disponível em: http://us.norton.com/cybercrime-definition

[11] Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008) *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, Lisboa, FCA

premeditado levado a cabo por terroristas que se socorrem de TI para efetuar ataques a sistemas e redes de computadores, dos quais resulta violência preferencialmente contra alvos não-combatentes[12]."

Terrorismo – é a prática de um mal e violência indiscriminados, que procurar minar, principalmente, governos aceites e reconhecidos para destruírem o modo de governação ou estrutura social de determinada sociedade. O terrorismo é um ato político e funciona como um meio para atingir diferentes fins.[13]

Infraestruturas críticas – são uma rede de estruturas críticas para o regular funcionamento da sociedade, "devem constituir uma preocupação central de um país perante as diversas ameaças que surgem do ciberespaço (...) são elementos estruturantes de todas as atividades que são estratégicas para um país pelo que em sequência disso, o número de pontos sensíveis cresce com a proliferação tecnológica.[14]"

Sistema Político Internacional – é "o conjunto constituído pelas unidades políticas que mantêm relações entre si e que são susceptíveis de entrar numa guerra geral"[15] e "Um conjunto de centros independentes de decisões políticas que interatuam com uma certa frequência e regularidade"[16]

[12] Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008) *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, Lisboa, FCA

[13] Lutz, James M. e Lutz, Brenda (2009) *Global Terrorism*, Londres, Routledge

[14] Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008) *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, Lisboa, FCA

[15] Aron, Raymond (1986) Paz e Guerra entre as Nações, Brasília, Universidade de Brasília

[16] Couto, Abel Cabral (1988) Elementos de Estratégia Vol. I, Lisboa, Instituto de Altos Estudos Militares

II. ATRAVESSAR FRONTEIRAS

"The first rule of unrestricted warfare is that there are no rules"

Qiao Liang[17]

O Estado é a entidade de organização política que carece de uma delimitação territorial relativamente à qual possa exercer o seu poder. Este estado a que nos referimos é aquele que surge como legítimo descendente da sedentarização[18] dos povos, tendo surgido da necessidade de resolver contendas na nova estrutura organizacional das sociedades[19]. Seguindo este princípio, as partes que compõem o Estado podem variar em composição, quantidade e finalidade no decorrer do tempo e de acordo com o espaço[20] que ocupam.

Ao Estado reconhece-se a capacidade última de proteger os seus cidadãos, pelo que a lealdade destes para com ele é teoricamente incontestável, conferindo-lhe uma autoridade total para o território ao qual está delimitado.

Este território é a tentativa do Estado em fazer coincidir as fronteiras culturais e ideológicas com as fronteiras territoriais que a ele estão sujeitas[21]. Surge assim o

[17] Liang, Qiao e Xiangsui, Wang (1999) *Unrestricted Warfare – China's Master Plan to destroy America*, China, People's Liberation Army

[18] A sedentarização foi um processo de alteração da vida em comunidade, quando à aproximadamente 6000 anos as comunidades agro-pastoris se fixaram em determinadas zonas geográficas que lhes eram benéficas para o cultivo e desenvolvimento de atividades pastoris. Foi a sedentarização que permitiu às pequenas comunidades desenvolverem estruturas de organização mais complexas dada a delimitação do espaço que podiam ocupar. Weber, Keith T. Horst, Shannon (2011) "Desertification and livestock grazing: The roles of sedentarization, mobility and rest", *Pastoralism*, Springer Journal. Disponível em: http://www.pastoralismjournal.com/content/1/1/19

[19] Rodrigues, Carlos Coutinho (2012) Contributo para uma "Estratégia abrangente" de gestão de crises, Lisboa, IDN Cadernos, Imprensa Nacional - Casa da Moeda

[20] Moreira, Adriano (2005) Teoria das Relações Internacionais, Coimbra, Edições Almedina

[21] Amante, Maria de Fátima (2007) Fronteira e Identidade - Construção e Representação Identitárias na Raia Luso-Espanhola, Lisboa, Instituto Superior de Ciências Sociais e Políticas

conceito de soberania como coluna vertebral do Estado, sendo ela, responsável pela instauração do poder incontestável do Estado e pela garantia da sua total independência em relação a outros Estados com pretensões políticas ou territoriais ao 'seu'. É a soberania política e territorial que define o que é interno do que é externo, sendo ela a grande âncora para a delimitação de fronteiras.

As fronteiras são necessárias, pois asseguram o que 'é de cá' e o que 'é de lá', ou seja são as fronteiras culturais e territoriais que distinguem a pertença dos indivíduos, quer pela sua associação ou dissociação ao termo de comparação.

Este princípio da soberania do Estado é o mecanismo de regulação da política interna e externa, configurando-se como uma grande fonte de atritos internacionais dada a heterogeneidade do Sistema Político Internacional, verificando-se assim, a necessidade de proteger este Estado, as suas fronteiras e as suas populações.

II.1. Segurança e Defesa

O termo segurança abrange múltiplas construções[22]. Em linhas gerais, pode-se afirmar que este conceito que significa um estado de despreocupação, derivado do latim *securitas*, refere-se à qualidade daquilo que é seguro, ou seja, àquilo que está ao abrigo de quaisquer perigos, danos ou riscos. Sugere ainda, pela sua etimologia[23], ocupação de si próprio (*se+cura*).

Algo é seguro quando o âmbito significa que é algo certo, firme ou estável e indubitável. A segurança é portanto uma certeza, uma necessidade. Em muitas ocasiões, a referência a segurança segue uma deturpação daquilo que é a Defesa

[22] Ribeiro, António Silva (2009) Teoria Geral da Estratégia: O Essencial ao Processo Estratégico, Coimbra, Edições Almedina

[23] Etimologia é a ciência que se dedica inteiramente ao estudo da origem de palavras.

Nacional[24]. Uma vez que estas são políticas que os Estados desenvolvem e aplicam para prevenir ou impedir ataques que possam ser levados a cabo por outros países.

O conceito foi gradualmente alargando, a partir do início da década de 90[25] e passou a abranger, para além do militar, os campos político, económico, social, ambiental e de direitos humanos. Assim, as medidas que visam a segurança são de largo espectro, envolvendo, também, a proteção civil, a segurança pública, as políticas económicas, de saúde, educativas, ambientais e as de garantia das instituições democráticas e da legalidade. Surge aqui a necessidade de fazer uma clara distinção sobre o que é a Segurança Interna e Segurança Externa, sendo esta última um tema virado para o conceito de Defesa Nacional que tende a estar vinculada às forças armadas e ao armamento, sendo estas o seu instrumento militar exclusivo.

Verifica-se deste modo necessário explanar e caracterizar as esferas, pública e privada, da segurança nacional de um estado.

II.1.1. Segurança Nacional

A Segurança refere-se mais ao sentimento[26], à sua própria sensação, enquanto a defesa é a realidade efetiva do ato de agir preventivamente, antecipando uma situação de quebra de segurança, ou de pós-ação onde se reestabelece o equilíbrio e a

[24] A Defesa Nacional é, segundo definição do IDN, um "Conjunto de medidas e ações adequadamente integradas e coordenadas, que, globalmente ou sectorialmente, permitem fortalecer a capacidade da Nação, com vista a alcançar a segurança nacional, procurando criar as melhores condições para a prevenção e combate de quaisquer ameaças que, direta ou indiretamente, se oponham à consecução dos objectivos nacionais".

[25] O Conceito de Defesa Nacional sofreu alterações devido ao paradoxo que surgiu entre segurança e defesa na era pós Guerra fria.

[26] Friedman, George (2012) *A Próxima Década - Onde temos estado... e para onde nos dirigimos*, Lisboa, D. Quixote

normalidade da vida quotidiana, trazendo à Nação (novamente) a sensação de segurança.

Nesta distinção, o estado de segurança não se consegue unicamente com a defesa mas também com a atividade de segurança interna. Para melhor analisarmos este tema convém ter em mente alguns conceitos que se aceitando, configurem o enquadramento da política de defesa e de segurança.

A Segurança Nacional é a condição da Nação que se exprime na permanente garantia da sua sobrevivência em paz e liberdade, assegurando a soberania, independência e unidade, a integridade do território, a salvaguarda coletiva da população e bens inerentes e dos valores espirituais, o desenvolvimento normal das tarefas do Estado, a liberdade de ação política dos órgãos de soberania e o pleno funcionamento das instituições democráticas. A Defesa Nacional está enquadrada e é definida[27] como o conjunto de medidas tanto de carácter militar como político, económico, social e cultural que, devidamente coordenadas, integradas e desenvolvidas tanto de uma perspetiva macro como sectorial, levam ao reforço direto das potencialidades de uma Nação. Minimizar as suas vulnerabilidades, com vista a torná-la apta a enfrentar todos os tipos de ameaça, direta ou indiretamente, que coloquem em causa a Segurança Nacional será o grande mote. Poderá ser entendida enquanto estrutura funcional que concorre para a consecução da segurança nacional como fim de Estado ou enquanto atividade instrumental de segurança externa da organização Estatal.

A Segurança Interna, nos termos legais[28], será a atividade desenvolvida pelo Estado que garanta a ordem, a segurança e a tranquilidade públicas, a proteção de pessoas e bens, a prevenção e repressão de criminalidade, assegurando o normal funcionamento das instituições democráticas, o regular exercício dos direitos,

[27] A Defesa Nacional está definida e consagrada na Resolução do Conselho de Ministros n.º 6/2003, contudo pode também ser observado o seu enquadramento em Rodrigues, Alexandre Reis (2013) *Enquadramento Conceptual e Legal da Segurança e Defesa Nacional* [disponível em: http://database.jornaldefesa.pt/politicas_de_defesa/portugal/JDRI%20031%20200113%20enquadramento%20segurança%20defesa.pdf]

[28] O enquadramento legal da Segurança Interna Nacional está consagrado pela Lei n.º 53/2008 de 29 de Agosto [disponível em: http://dre.pt/pdf1s%5C2008%5C08%5C16700%5C0613506141.pdf]

liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática. Verifica-se que a atividade de defesa nacional e a atividade de segurança interna visam, cumulativamente e simultaneamente, a obtenção de um estado de segurança nacional. A atividade de defesa nacional compete essencialmente às Forças Armadas e a atividade de segurança interna compete na sua essência às forças de segurança (polícias).

II.1.2. Segurança do Indivíduo

O conceito de Segurança Humana[29] é relativamente recente, bastante utilizado para descrever a proteção dos indivíduos perante uma vasta panóplia de ameaças, riscos e desafios, dos Estados falhados às catástrofes naturais, passando pela guerra civil, graves perturbações de ordem pública, subdesenvolvimento, epidemias, práticas de genocídio, fome, migrações em massa de populações e graves atentados contra os direitos humanos[30]. A sua conceção restrita centra-se na violência interna exercida pelos próprios governos ou grupos politicamente organizados sobre comunidades e indivíduos, enquanto a sua abordagem mais ampla considera que também se devem incluir a fome, as doenças e os desastres naturais. Embora os defensores e promotores da segurança humana apresentem divergências entre si acerca de que ameaças os indivíduos devem ser protegidos, o consenso em torno da noção de que o primeiro objetivo é a proteção dos indivíduos e a dignidade humana é suficiente para produzir alterações sensíveis, já que o quadro analítico tradicional que explica e procura evitar as guerras entre Estados ou promover a segurança dos e entre Estados é claramente

[29] Gasper, Des (2008) *The Idea of Human Security* [disponível em: http://www.unhistory.org/reviews/Garnet_HumanSecurity.pdf]

[30] Rodrigues, Teresa Ferreira (2010) "Dinâmicas Migratórias e Riscos de Segurança – A velha Europa", *Relações Internacionais,* n.º26, Lisboa, IPRI

insuficiente e irrelevante para explicar e prevenir os conflitos violentos dentro dos Estados e proteger os indivíduos de certos atentados ou tragédias.

Isto deve-se ao terrorismo e ao crime organizado[31] que abalaram fronteiras e tornaram totalmente permeável o interno e o externo, criando uma zona dúbia, à qual o Estado tem dificuldade em definir, em contínuo e na generalidade, uma instituição soberana entre a segurança e defesa (interna ou externa). O princípio da responsabilidade de proteção surge como norma internacional ou padrão de comportamento para a comunidade dos Estados. Esta noção é ainda demasiado ambígua para se perceber o verdadeiro sentido da sua evolução. Concretamente, sobre qual o agente que se pretende garantir proteção e como efetivar essa responsabilidade. Com efeito, um número importante de países teme que este princípio seja instrumentalizado arbitrariamente pelos Estados mais poderosos para impor a sua vontade e defender certos interesses, enquanto outros (a começar pelos Estados Unidos e alguns estados europeus) pretendem evitar que a responsabilidade de proteger se torne numa obrigação à intervenção internacional. Ainda assim, o relativo consenso em torno da necessidade de proteger indivíduos e comunidades de tragédias humanitárias foi suficiente para que este princípio fosse adotado na Cimeira Mundial da ONU, em Setembro de 2005[32].

II.1.3. Segurança Pública

A segurança pública não pode ser tratada apenas como medida de vigilância e ação repressiva, mas como um sistema integrado e otimizado envolvendo instrumentos de prevenção, coação, justiça, defesa dos direitos, saúde e social. O

[31] Jenkins, Brian M. (1974) International Terrorism: A New Kind of Warfare, California, The Rand Paper Series, The Rand Corporation.

[32] O Documento final da Cimeira Mundial 2005 da ONU está [disponível em: http://www.un.org/spanish/Depts/dpi/portugues/pdf/WorldSummitOutcome-ptREV.pdf]

processo de segurança pública inicia-se pela prevenção e termina no atento reparo do ato danoso, no tratamento das causas e na reinserção na sociedade dos agentes prevaricadores ao normal estado de vivência em comunidade. Assim, segurança pública é um processo, seja, uma sequência contínua de fatos ou operações que apresentam certa unidade ou que se reproduzem com carácter regular, que compartilham uma visão focada em componentes preventivas, repressivas, judiciais, de saúde e sociais. É um processo sistémico, pela necessidade da integração de um conjunto de conhecimentos e ferramentas estatais que devem interagir com a mesma visão, compromissos e objetivos. Devem ser também otimizados estes elementos, pois dependem de decisões rápidas e resultados imediatos. Sendo a ordem pública um estado de serenidade, apaziguamento e tranquilidade pública, em consonância com as leis, os preceitos e os costumes que regulam e ditam a convivência em sociedade, a preservação deste direito do cidadão só será plena se o conceito de segurança pública for aplicado.

As competências anteriormente definidas encontram-se estatutariamente distribuídas pelas polícias, tal como se pode verificar a seguir:

- Polícia Judiciária (PJ): polícia de investigação criminal especializada na repressão ao crime organizado, terrorismo, tráfico de estupefacientes, corrupção e criminalidade económica e financeira[33]. Este organismo está na dependência do Ministério da Justiça;
- Polícia de Segurança Pública (PSP): corpo civil de segurança pública, que atua fundamentalmente em grandes áreas urbanas e se encontra na dependência do Ministério da Administração Interna;
- Guarda Nacional Republicana (GNR): é uma força de segurança de natureza militar, constituída por militares organizados num corpo especial de tropas, atuando fundamentalmente em áreas rurais, estradas nacionais e zonas

[33] Como figura no n.º 2, art.º 7.º da LOIC – Lei n.º 49/2008, de 27 de Agosto [disponível em: http://www.policiajudiciaria.pt/PortalWeb/content?id={CBD3F401-5D03-492E-9FCF-9396ED545D27}]

costeiras. Esta força dependente conjuntamente dos Ministérios da Administração Interna e da Defesa Nacional[34];

- Corpo Nacional Prisional: é uma força de segurança uniformizada e armada que tem por missão garantir a segurança e tranquilidade da comunidade, nomeadamente, mantendo a ordem e segurança do sistema prisional. A sua estrutura é ligeiramente diferente da Guarda Nacional Republicana e depende do Ministério da Justiça através da Direcção-Geral de Reinserção e Serviços Prisionais[35];

- Serviço de Estrangeiros e Fronteiras (SEF)[36]: é o serviço policial responsável pela vigilância e controle das fronteiras e combate à imigração ilegal. Está dependente do Ministério da Administração Interna;

- Autoridade de Segurança Alimentar e Económica (ASAE): é uma polícia especializada no combate aos delitos económicos e contra a saúde pública, dependente do Ministério da Economia e da Inovação[37];

- Polícia Marítima (PM): órgão policial criminal da Autoridade Marítima Nacional, dependente do Ministério da Defesa Nacional, através do CEMA, patrulhando o mar, rios, e a costa nacional[38].

- Polícias do Exercito (PE), Aérea (PA) e Naval (PN): garantem a ordem e a disciplina nas Forças Armadas, bem como a segurança do seu pessoal e das instalações. Cada Polícia reporta ao Chefe do Estado-maior do ramo a que pertence, estando tuteladas pelo Ministério da Defesa Nacional;

---

[34] Como disposto nos art.º 2.º e 3.º da Lei n.º 63/2007, de 6 de Novembro [disponível em: http://gnr.pt/documentos/Legislacao/LEI_ORGANICA.pdf]

[35] Como figura nos art.º 2.º e 3.º do DL n.º 215/2012, de 28 de Setembro [disponível em: http://www.dgsp.mj.pt/backoffice/Documentos/DocumentosSite/Legislacao/LO_215-2012.pdf]

[36] Como presente no art.º 1 do DL n.º 252/2000, de 16 de Outubro [disponível em: http://dre.pt/pdf1s%5C2000%5C10%5C239A00%5C57495766.pdf]

[37] Como figura no DL n.º 274/2007, de 30 de Julho [disponível em: http://dre.pt/pdf1sdip/2007/07/14500/0487204876.PDF]

[38] Como figura no art.º 1.º do DL n.º 245/95, de 21 de Setembro [disponível em: http://www.dre.pt/pdf1s/1995/09/219A00/58905896.pdf]

- Polícia Judiciária Militar: é o órgão policial de investigação criminal no âmbito militar[39], a ela só cabe investigar eventuais infrações cometidas por militares. Dependente inteiramente do Ministério da Defesa Nacional.
- Polícias Municipais: São órgãos municipais de fiscalização do cumprimento dos regulamentos[40] das localidades onde realizam as suas ações.

II.1.4. Segurança Privada

Segundo a Lei Orgânica do Ministério da Administração Interna, aprovada pelo DL n.º 203/2006, de 27 de Outubro[41], integrou na PSP as atribuições da Secretaria-Geral do Ministério da Administração Interna em matéria de segurança privada.

A PSP tornou-se assim, a entidade de controlo da atividade de segurança privada em Portugal competindo-lhe, pelo estabelecido pela Lei n.º 53/2007[42], de 31 de Agosto o controlo, licenciamento e fiscalização de toda a atividade de segurança privada[43].

A atividade de segurança privada, complementar e subsidiária face às competências desempenhadas pelas forças e serviços de segurança pública, assume particular relevo quer na proteção de pessoas e bens quer na prevenção e dissuasão da prática de atos ilícitos, em virtude da complementaridade da sua ação.

---

[39] Como figura no DL n.º 200/2001, de 13 de Julho, alterado pela Lei n.º 100/2003, de 15 de Novembro [disponível em: http://www.emfa.pt/www/conteudos/informacaofap/legislacao/estatcondmilitar/justmilitar/LeiOrganicadaPoliciaJudiciariaMilitar.pdf]

[40] Como presente na Lei n.º 19/2004, de 20 de Maio [disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=227&tabela=leis]

[41] Lei Orgânica do Ministério da Administração Interna [disponível em: http://www.dre.pt/pdfgratis/2006/10/20800.pdf]

[42] Lei Orgânica da Polícia de Segurança Pública [disponível em: http://www.psp.pt/Legislacao/Lei_53-2007.pdf]

[43] A autorização ao governo de Portugal para alterar o regime jurídico do exercício da segurança privada está contemplada na Lei n.º 29/2003, de 22 de Agosto [disponível em: http://dre.pt/pdf1sdip/2003/08/193A00/53105312.pdf]

O Decreto-Lei n.º 35/2004[44], de 21 de Fevereiro com as alterações introduzidas pela Lei n.º 38/2008[45], de 8 de Agosto, regula o exercício da atividade de segurança privada e tipifica o âmbito e as condições em que esta pode ser desenvolvida. As atribuições acometidas à PSP são desta forma, exercidas pelo Departamento de Segurança Privada, e cujo Conselho é o órgão, de consulta do Ministro da Administração Interna, a quem compete elaborar um relatório anual sobre esta atividade.

A atividade de segurança privada é uma área com um potencial crescente no tempo, atendendo ao número de cidadãos-trabalhadores envolvidos e ao número significativo de empresas existentes. Esta é uma área sensível e que pode conflituar com Direitos, Liberdades e Garantias. Por isso, a atividade licenciadora e, em especial, fiscalizadora por parte da PSP pode contribuir para uma redução acentuada de eventuais intromissões ou abusos contra estes Direitos Constitucionalmente consagrados. A atividade nem sempre foi regulada e esta necessidade prendeu-se essencialmente com os abusos averiguados em contínuo por queixas remetidas à PSP[46].

II.1.5. A Relação Público-Privada

As atividades de segurança e defesa são acionadas por indivíduos especializados com conhecimentos quer práticos quer teóricos nas matérias em questão. Hoje em dia, muito em parte por razões essencialmente económicas, os Estados sentiram a necessidade de reduzir nos efetivos de segurança pública (forças

[44] Decreto-Lei n.º 35/2004 [disponível em: http://www.dre.pt/pdf1s/2004/02/044A00/09320941.pdf]

[45] Lei n.º 38/2008 [disponível em: http://dre.pt/pdf1s/2008/08/15300/0534505346.pdf]

[46] Mesquita, António Arnaldo (2010) "Triplicam as queixas de cidadãos por abuso de autoridade das forças de segurança", *Público,* [disponível em: http://www.publico.pt/portugal/jornal/triplicam-as-queixas-de-cidadaos-por-abuso-de-autoridade-das-forcas-de-seguranca-20615218]

armadas e forças de segurança) o que colocou aos próprios Estados num dilema securitário[47].

Este dilema tem base económica, ou seja, os 'cofres' públicos face às adversidades económicas surgidas uma época pós 11 de Setembro, não tinham, nem têm capacidade de abarcar grandes projetos[48] de envolvimento securitário e assim, é-lhes crucial a existência de instituições de segurança privada, algumas com fundos megalómanos, para que os seus projetos sejam exequíveis.

O financiamento do sector da defesa é, sem dúvida, uma grande fatia da disponibilidade económica de um Estado, sem ser a sua área mais dispendiosa, em especial quando as preocupações com a segurança[49] e a defesa extrapolaram o conhecimento clássico da noção de fronteiras, com isto reportando-nos ao terrorismo e ao crime internacional. Desta forma as instituições de segurança privada são muito importantes, pois colmatam a insuficiência do estado nesta matéria e são menos dispendiosas, um exemplo fulcral é o dos Estados Unidos da América e o controlo que as agências de segurança privada já possuem no seio do país. Outro exemplo importante será o do Brasil, pois ao contrário dos Estados Unidos da América, os indivíduos que trabalham em empresas privadas, não são ex-militares, ex-agentes das polícias ou das agências governamentais, são na realidade agentes e militares no ativo, que paralelamente atuam no sector de segurança privada, como forma de obter rendimentos extra.

---

[47] As alterações decididas pelo Governo de Portugal, bem como a conjuntura internacional, levaram a um decréscimo no número de efetivos na segurança pública e também na defesa. Estimam-se que os dados para os últimos três anos sejam ainda mais alarmantes. Espírito Santo, General Gabriel Augusto do (2009) "Os Efetivos nas Forças Armadas", *Revista Militar*, No. 2484 , [disponível em: http://www.revistamilitar. pt/artigo.php?art_id=363]

[48] Santos, Rui Teixeira (2012) "À procura dos culpados – A Grande Crise Financeira e Portugal", *Centro de Estudos de Gestão Pública do ISCAD,* [disponível em: http://cegep.iscad.pt/index.php/ noticias/93-a-procura-dos-culpados-a-grande-crise-financeira-e-portugal]

[49] A despesa do Estado no que concerne à defesa pouco tem alterado nos últimos 15 anos, tendo-se observado um aumento após os ataques de 11 de Setembro. Em contrapartida a despesa do Estado com a sua segurança interna tem aumentado significativamente, e de uma forma abrupta desde os finais da década de 90. (2013) *A Defesa Nacional no Contexto da Reforma das Funções de Soberania do Estado*, Lisboa, Instituto de Defesa Nacional, pp. 7-15 [disponível em: http://www.defesa.pt/Documents/20130307_IDN_reforma_do_estado_soberania_jan2013.pdf]

Uma realidade é a necessidade de escoltar bens ou pessoas, que ao Estado não se demonstram de interesse, em contrapartida às instituições que demonstram esse interesse. Esta visão denota a necessidade de contrapartidas e relações de entreajuda por vezes necessárias e benéficas entre o sector privado e públicos.

O sector de segurança pública, pode recorrer ao outsourcing de empresas privadas, quer por fatores de razão económica ou de competências técnicas pois é uma forma de rentabilizar custos, equipamentos e indivíduos nunca esquecendo que as entidades reguladoras destas agências de segurança privadas são as agências de segurança pública.

No caso português isto vem expresso no art.º 31.º da Lei n.º 38/2008 de 8 de Agosto[50] que estipula que,

> "A fiscalização da atividade de segurança privada e respetiva formação é assegurada pela Direção Nacional de Polícia de Segurança Pública, com a colaboração da Guarda Nacional Republicana, sem prejuízo das competências das forças e serviços de segurança e da Inspecção-Geral da Administração Interna"

As empresas de Segurança Privada fornecem também algo de muito importante, o chamado *inside intel* já que estão capacitadas a recolher dados que podem transmitir às agências de segurança pública no que concerne ao combate ao tráfico ilícito de droga e ao desmantelamento de cadeias de crime organizado, uma vez que são empresas 'privadas' sem vínculo aos Estados e por isso credíveis para os seus solicitadores como inócuas em questões de Segurança e Defesa Nacional e que utilizam essa *inside intel* na manutenção de relação contratual.

[50] Documento integral com as alterações [disponível em: http://dre.pt/pdf1sdip/2008/08/15300/0534505346.PDF]

Convém relembrar que na era em que nos encontramos estas empresas do sector privado não trabalham só em cenários de guerra, como aconteceu no Afeganistão[51], mas sim, dentro das fronteiras do Mundo Ocidental e mesmo no mundo virtual, que é uma crescente preocupação enquanto ameaça à segurança de um Estado.

Portugal não possui historial relevante em parcerias público-privadas no sector da segurança. Não obstante, a fiscalização de uma agência de segurança privada está à guarda de uma entidade do estado. Contudo, a relação efetiva, como a existente nos Estados Unidos da América, não é uma realidade à qual estejamos sujeitos.

A relação entre estes sectores de segurança em Portugal, carece ainda de muito trabalho e padece de várias patologias, sendo que a mais comum é a de quebra total de valores, já que os agentes de segurança privada se assumem como iguais e os agentes de segurança pública se destacam como assumidamente 'superiores' em virtude da sua capacidade de licenciar e fiscalizar as atividades do sector privado.

Ao invés desta situação, tanto sector privado como sector público deviam adotar um modelo semelhante ao dos Estados Unidos da América, onde os recursos são aproveitados e rentabilizados ao máximo.

[51] Na Guerra do Afeganistão (2001-) foram contratadas algumas empresas de segurança privada. A maioria delas pelos Estados Unidos da América. Quando em funções estas empresas funcionavam sob ordem militar, mas com uma hierarquia e orçamento próprios, o que facilitava algumas missões simultaneamente dificultando o controle por não serem pessoal militar, mas do sector privado. Auner, Eric (2013) "As U.S. Drawns down in Afghanistan, Role Continues for Private Security Firms", *World Politics Review,* [disponível em: http://www.worldpoliticsreview.com/trend-lines/13446/as-u-s-draws-down-in-afghanistan-role-continues-for-private-security-firms] e ainda Apps, Peter(2012) "As Iraq, Afghan wars end, private security firms adapt", *Reuters,* [disponível em: http://www.reuters.com/article/2012/10/21/us-usa-arms-contractors-idUSBRE89K02B20121021]

II.2. Defesa Nacional

A garantia da Defesa Nacional é algo muito importante para um estado, pois não só garante que os seus interesses são defendidos e salvaguardados, como garante uma manutenção das fronteiras politicamente estabelecidas[52]. Deste modo a defesa nacional procura garantir que a prática da segurança nacional possa ser livremente executada através da prossecução de uma estratégia integrada.

> "A localização geográfica não deve servir de base a uma compartimentação do conceito de segurança Nacional segundo as fronteiras do país, porque as ameaças são estruturalmente complexas, dispõem de grande mobilidade e possuem um carácter transnacional e difuso, que não respeita esses limites políticos. Nestas circunstâncias, não é possível descodificar verdadeiramente o que constitui hoje uma ameaça para a segurança interna, que não o seja, também, para a segurança externa, nem distinguir uma ameaça que deva ser combatida por forças policiais, que não possa requerer o contributo de forças militares e vice-versa."
>
> *Segurança e Defesa Nacional*[53]

Assegurar a segurança e a defesa das populações bem como garantir a integridade do território nacional e ainda a prossecução dos objetivos estratégicos são hoje ações mais difusas sobre as quais é difícil definir qual é uma ameaça externa e interna. Os estados procuram hoje rentabilizar os recursos que têm disponíveis interligando as ações de defesa e segurança. Desta forma é-nos possível afirmar que o

[52] Como figura na Lei de Defesa Nacional e das Forças Armadas, Lei n.º 29/82 de 11 de Dezembro [disponível em: http://ruadosbragas223.home.sapo.pt/DIREITO/Lei_29-82_Defesa_Nacional_e_Forcas_Armadas.pdf]

[53] Silva Ribeiro, António (2011) *Segurança e Defesa Nacional*, Academia de Ciências de Lisboa

conceito de defesa nacional evoluiu[54] e que à defesa estão cometidas ações perante ameaças, a par que à segurança reportam situações de risco para lá daquelas provocadas por indivíduos, como as catástrofes[55].

II.3. Cibersegurança e a Ciberdefesa, duas definições

Os conceitos de cibersegurança e ciberdefesa são consideravelmente diferentes e cada um deles comporta uma esfera específica de ação no ciberespaço. A cibersegurança contém a ação das forças policiais e ainda dos serviços informáticos a par que a ciberdefesa decorre exclusivamente das forças armadas.

Cibersegurança	Forças de Segurança	Cibercrime
		Hacktivismo
	Serviços Informáticos	Ciberespionagem
		Ciberterrorismo
Ciberdefesa	Forças Armadas	Ciberguerra

Tabela 1[56] - Cibersegurança e Ciberdefesa, adaptado de *Estruturas de Coordenação Nacional no Ciberespaço*

Os campos de preocupação da Cibersegurança e Ciberdefesa são possíveis de observar no quadro acima (tabela 1), porém iremos apenas referir-nos ao que se

[54] Correia, Pedro de Pezarat (2003) Manual de Geopolítica e Geoestratégia, Conceitos, Teorias e Doutrinas vol. I, Coimbra

[55] Correia, Pedro de Pezarat (2006) Políticas de Defesa e Segurança, Conferência no CCC e Silva Ribeiro, António (2011) Segurança e Defesa Nacional, Academia de Ciências de Lisboa

[56] Nunes, Paulo Viegas (2013) "Cibersegurança e Estratégia Nacional de Informação: Estruturas de Coordenação Nacional no Ciberespaço", Conferência, Beja, IV SimSIC

contém na cibersegurança pois a ciberguerra terá direito a um capítulo próprio mais à frente.

A Cibersegurança são o conjunto de medidas que procuram garantir o bem-estar e o regular funcionamento da ação de um estado e das suas populações no ciberespaço e fora dele, desde que derivado de ações diretamente a ele acometidas. Deste modo com o surgimento deste meio e com o objetivo de garantir a segurança dos que a ele recorrem ou dele dependem, definiram-se os seguintes pilares de ação no âmbito da cibersegurança:

- **Cibercrime** - Com o crescendo de utilização do ciberespaço, surgiu um aproveitamento ilícito das novas potencialidades por ele conferidas. A atividade criminosa no, ciberespaço pode surgir de diversas formas e nos mais variados contextos. Com o objetivo de se poder regular legislativamente estas práticas ilícitas, sentiu-se necessidade de estabelecer categorias nas quais se pudessem integrar as diferentes tipologias de ação criminosa neste espaço. O quadro seguinte (tabela 2) serve o propósito de resumidamente apresentar as diferentes categorias de cibercriminalidade definidas,

Crime	Tipologia
Relativos aos conteúdos	Pornografia Infantil
	Descriminação racial e/ ou religiosa
	Difamação e injúria
	Casinos: Jogos de Fortuna e Azar
Violação da Confidencialidade e dados Pessoais	Violação de correio eletrónico e fóruns de discussão
	Invasão da vida privada
	Crimes Informáticos

Burla informática e de telecomunicações		
Falsidade Informática		
Dano e Sabotagem		
Acesso Ilegítimo "Intrusão de sistemas"	Interceção ilegítima	
	Pirataria	
Autodeterminação	Cyberstalking	E-mail
		Internet
		Computador
	Cyberbullying	

Tabela 2[57] - Categorias de criminalidade, adaptado de *Cyberwar – O Fenómeno, as Tecnologias e os Atores*

- **Hacktivismo** – Inicialmente esta prática foi desenvolvida por especialistas que tentavam encontram falhas nos sistemas, seguida de uma fase em que o interesse era o de criar algo novo. Finalmente o Hacktivismo atingiu uma expressão de atividades de índole criminosa que vão desde a pirataria ao desenvolvimento e implantação de *malware*[58], existem assim 4 tipos de atividades desenvolvidas por *hackers*, que servem para as agrupar pelas suas características: Hackers, Phreakers, Crackers, Cypherpunks ou Criptoanarquistas.

[57] Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008) *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, Lisboa, FCA

[58] idem.

Hackers	Normalmente são intrusos de diversos sistemas informáticos que criam e libertam *malware* .
Phreakers	Praticam burlas e intrusões unicamente em redes de comunicações.
Crackers	A atividades destes hackers é removerem as proteções a determinados programas para que estes se tornem acessíveis por todos.
Cypherpunks ou Criptoanarquistas	Especialistas em criptografia que desenvolvem métodos de proteção de comunicações ou ações maliciosas no ciberespaço

Tabela 3[59] - Diferenciação entre atividade de Hackers, adaptado de *Cyberwar – O Fenómeno, as Tecnologias e os Atores*

- **Ciberespionagem** – esta metodologia de ação é peremptoriamente utilizada por Estados como forma de prevenirem ataques e potenciarem o seu crescimento económico, através da realização de ataques que procuram recolher informações que promovam um reconhecido poder estratégico[60]

- **Ciberterrorismo** – Como o próprio nome indica o ciberterrorismo surge da união entra a prática do terrorismo e o imenso 'espaço' do ciberespaço. O ciberterrorismo é uma prática ambicionada pois permite uma facilidade de

[59] Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008) *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, Lisboa, FCA

[60] Pereira, Júlio (2012) "Cibersegurança – O Papel do Sistema de Informações da República Portuguesa", *Segurança e Defesa*, Maio-Agosto 2012, Lisboa, Diário de Bordo

ação e dispersão só alcançáveis neste meio[61]. A estrutura da internet é semelhante à das novas redes de terrorismo[62], em rede e transnacional[63] na sua ação e metodologia de ataque.

Com a crescente dependência do ciberespaço[64] surgem equitativamente em franco crescimento um aumento de ameaças reais, bem como de ataques perpetrados contra as mais diversas estruturas e organismos, como é possível observar pela análise das figuras 1 e 2.

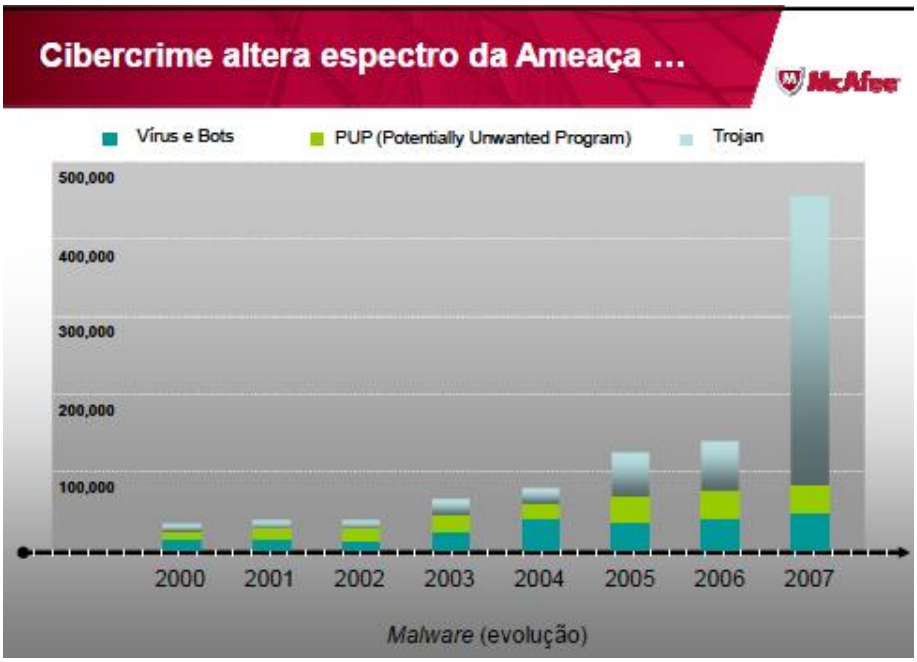


Figura 1[65] - Aumento de ataques *McAfee Labs*

[61] Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008) *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, Lisboa, FCA, pp. 85-98

[62] Novais, Rui Alexandre (2012) "Media e (Ciber)Terrorismo", *Cibersegurança n.º133*, Lisboa, Nação e Defesa – Instituto de Defesa Nacional

[63] Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008) *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, Lisboa, FCA, pp. 85-98

[64] idem.

[65] Nunes, Paulo Viegas (2013) "Cibersegurança e Estratégia Nacional de Informação: Estruturas de Coordenação Nacional no Ciberespaço", Conferência, Beja, IV SimSIC

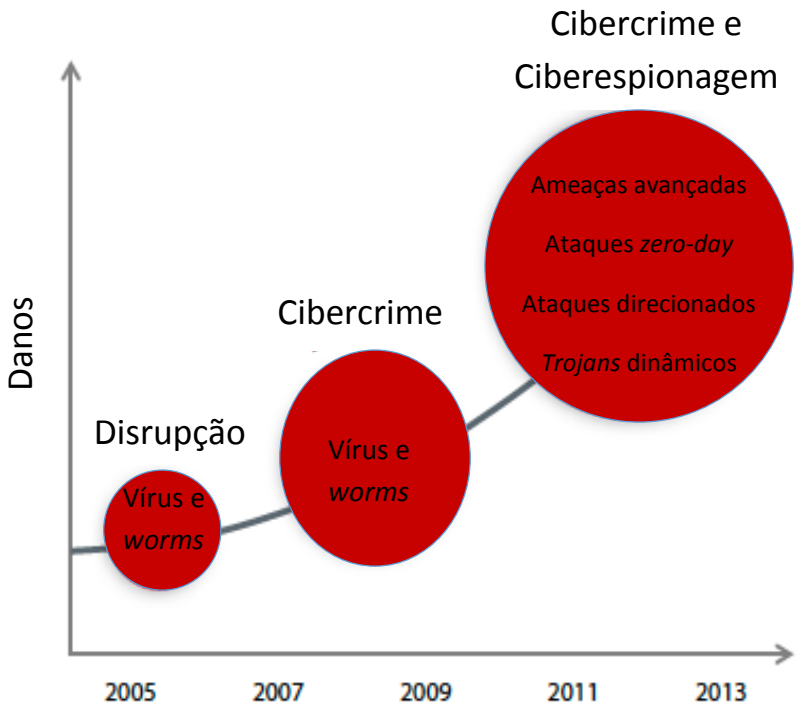


Figura 2[66] - Evolução da tipologia de ataques

A nova realidade provocou o surgimento de uma metodologia própria à ciberdefesa que comporta dois processos simultâneos, um a nível nacional e outro de dependência internacional. Estes processos estão respetivamente sob a dependência do Centro Nacional de Cibersegurança e do seu homólogo internacional, um CERT[67].

[66] Aziz, Ashar (2013) "The evolution of Cyber attacks and Next Generation Threat Protection", *RSA Conference 2013*, FireEye, Inc.

[67] Nunes, P.V. (2013) Cibersegurança e Estratégia Nacional de Informação: Estruturas de Coordenação Nacional no Ciberespaço, Conferência IV SIMSIC, Beja

II.3.1. Necessidade de uma Estratégia Nacional de Cibersegurança

O Objetivo final da criação de uma estratégia nacional de cibersegurança é a garantia de informação para que se possam ter todos os detalhes, aquando da criação de um meio seguro para utilização de todos os indivíduos em simultâneo com a garantia de segurança das redes críticas nacionais[68].

> " (…) considera-se que o principal desafio de Portugal se coloca essencialmente ao nível da Garantia da Informação (Information Assurance) garantindo a Confidencialidade, a Integridade e a Disponibilidade."
>
> Proposta de Estratégia Nacional de Cibersegurança[69]

Uma das principais preocupações de um estado no que concerne à segurança do 'seu' ciberespaço é o seu florescimento económico[70], sendo que tem havido uma preocupação crescente com a segurança em utilizar uma *cloud*[71](figura 3). Esta tem essencialmente duas benesses face aos anteriores métodos pois (1) diminui consideravelmente os custos destinados às TI e (2) promove uma mais rápida dispersão e disponibilidade de informação considerada pertinente.

---

[68] Nunes, P.V. (2013) Cibersegurança e Estratégia Nacional de Informação: Estruturas de Coordenação Nacional no Ciberespaço, Conferência IV SIMSIC, Beja

[69] *Proposta de Estratégia Nacional de Cibersegurança*, GNS [disponível em: http://www.gns.gov.pt/media/1247/PropostaEstratégiaNacionaldeCibersegurançaPortuguesa.pdf]

[70] Storch, Tyson (2012) *Cibersegurança: Pilar de uma sociedade ligada e segura*, Microsoft Trustworthy Computing

[71] Uma *cloud* é um sistema autônomo de armazenamento e processamento, que não distribuído quer lógica quer fisicamente. Erroneamente fala-se 'na *cloud*' porém a maior probabilidade é que quando dois ou mais indivíduos se referem à *cloud*, não estejam a referir-se à mesma.

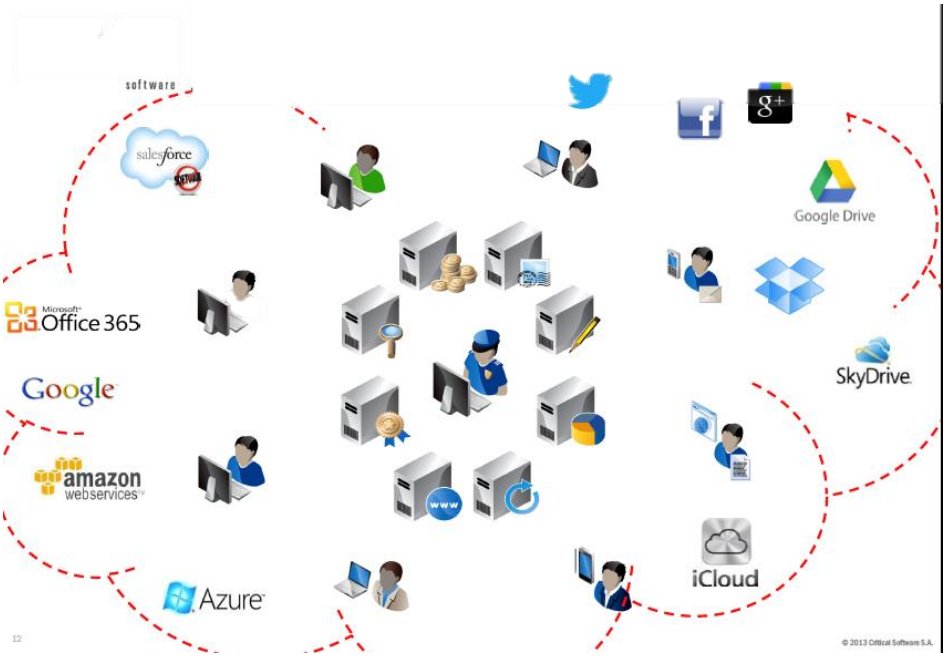


Figura 3[72] - Exemplo explicativo do funcionamento das diversas *clouds*

[72] Quadros, G. (2013) Internal Threat: Information Security and Competition, 7ºEIN Lisboa: Critical Software

III. O NOVO MUNDO

"Uma meia verdade é a pior das mentiras em informação"

José Manuel Barata-Feyo[73]

III.1. Renegociar Identidades

A identidade de um indivíduo advém de uma constante renegociação entre o que este perceciona de si próprio e como os outros o veem e se relacionam com ele[74]. Este fenómeno geralmente define que um indivíduo é a soma de todas as suas perceções, aceções e conceções[75].

> If we abandon the conception of a substantive soul endowed with the self of the individual at birth, then we may regard de development of the individual's self and of his self-consciousness within the field of his experience (...)
>
> *Mind, self, and society*[76]

[73] Barata-Feyo, J. M. Citado em Gonçalves, J. A.B.F.M. (2005) *Sociedade da Informação*, Faculdade de Economia da Universidade de Coimbra. Disponível em: http://www4.fe.uc.pt/fontes/trabalhos/2005003.pdf

[74] O ideal seria que a relação entre o indivíduo e o meio social em que este está inserido fosse reciproca e constante. Stryker S. (1980). *Symbolic interactionism: A social structural version*. Menlo Park, Benjamin Cummings.

[75] Mead, G. H. (1934). *Mind, self, and society*. Chicago, University of Chicago Press

[76] idem.

Uma grande parte da construção identitária de um individuo advém do conhecimento e da influência exercida sobre si, da sociedade em que está inserido. Por isso mesmo é possível, após um certo período longo de observação conhecer o individuo como prever quais os seus possíveis movimentos futuros. É esta capacidade que permite que analistas façam previsões sobre o comportamento de determinado grupo[77].

A capacidade que cada individuo possui para se identificar e para que cada grupo se identifique e reconheça como um grupo é a memória, neste caso a individual e a coletiva respetivamente. É através dela que cada um recorda as suas perceções tornando-a um bem de valor inestimável[78]. A memória coletiva, por sua vez é o que permite aos indivíduos reconhecerem um determinado grupo em virtude de se identificarem com as suas construções e por todos os membros possuírem um passado comum. Por si mesma, a construção de uma identidade é caracterizada pelo conflito, a nível individual ou coletivo, ou seja interno ou com influências exteriores. Maurice Hallbwachs (1992), defende esta identidade coletiva, porém reitera que esta só funciona porque a capacidade de memória, ou seja de recordar, é inerentemente individual[79].

No ciberespaço a identidade de cada um sofre profundas alterações e os grupos aos quais se pertence fora deste espaço podem não ser os mesmos aos quais se associam, os indivíduos, no ciberespaço. Não pretendemos fazer juízos de valor afirmando que os indivíduos aproveitam as potencialidades do ciberespaço para se tornarem numa outra pessoa, procuramos sim que seja compreensível, que mesmo um individuo procurando manter-se fiel a si próprio e aos seus princípios procurará projeta-los tanto num espaço como em outro, entenda-se fora ou dentro dos ciberespaço como os dois espaços em análise.

Porém mesmo que seja um objetivo projetar-se tanto no ciberespaço como fora dele de igual forma, a realidade é liminarmente diferente pois o ciberespaço

[77] Leary, Mark e Tangney, June (2005) *Handbook of Self and Identity*, Guilford Press

[78] Ricoeur, Paul (2006) *Memory, History, Forgetting*, Chicago, University of Chicago Press

[79] Halbwachs, Maurice (1992) *On Collective Memory* , Chicago, University of Chicago Press

confere aos indivíduos que a ele 'recorrem' características de relacionamento e de envolvimento muito diferentes das possíveis de observar fora do ciberespaço.

A liberdade de ação e a diminuição de constrangimentos promovem uma grande interação por parte dos que utilizam o ciberespaço, tanto para a sua vida pessoal, como para a vida profissional. Estas diferenças conferidas pelo meio, conjugadas com a liberdade de pensamento - característica da sociedade pós-moderna - criaram indivíduos cuja identidade possui um carácter fragmentado e profundamente mutável e moldável[80].

Uma consequência destas novas identidades é o meio através do qual os indivíduos se relacionam. Uma ação de relação no ciberespaço com outro indivíduo ou indivíduos é a terceira categoria de relacionamento definida por John Thompson[81]. Assim, uma interação no ciberespaço pode decorrer sob duas formas, (1) reativa e (2) mútua em que uma distingue uma relação com resultados obtidos expectáveis e outra os resultados que vão sendo estabelecidos temporalmente, respectivamente uma vez que se reportam a uma forma evolutiva de interagir[82].

Desta perspetiva evolucionista, poder-se-á afirmar que o ciberespaço moldou os indivíduos pois se numa fase inicial recorriam a ele como fonte de informação, hoje os indivíduos recorrem a este meio para disseminação e até mesmo produção da sua informação, ou seja o ciberespaço tornou o individuo um ser ativo na construção, manutenção e perpetuação do seu meio[83].

Na essência, a construção de uma identidade assenta sobre estes pressupostos, pelo que a alteração do paradigma no que toca à construção de identidades é a possibilidade infinita que o ciberespaço confere aos seus utilizadores de se transformarem continuamente sem as amarras da identidade associada a um corpo

[80] Hall, Stuart (2002) *A identidade cultural na pós-modernidade*, Rio de Janeiro, DP&A

[81] Thompson, John (1998) *A Mídia e a Modernidade - Uma teoria social da mídia*, Petrópolis, Vozes

[82] Primo, Alex (2007*) Interação mediada por computador: comunicação, cibercultura, cognição*. Porto Alegre, Sulina

[83] Chagas, Polyana Amorim (2011) "Entre o virtual e o real: o sujeito no ciberespaço", *Simsocial – Simpósio em tecnologias digitais e sociabilidade* através de Wertheim, Margareth (2001) *Uma história do espaço: de Dante à Internet,* Rio de Janeiro, Jorge Zahar

físico. A possibilidade de um indivíduo em se definir textualmente, confere-lhe o tempo necessário para que este se recrie numa imagem por si considerada e percepcionada de si próprio, podendo isto refletir-se na criação de um novo indivíduo, ou como Sherry Turkle[84] afirma, uma persona com características próprias diferentes da pessoa 'real'.

> The relative anonymity of life on the screen – one has the choice of being known only by one's chosen "handle" or online name – gives people the chance to express often unexplored aspects of the self. (...) Online services offer their users the opportunity to be known by several different names.
>
> "Cyberspace and Identity"[85]

As identidades são geradas por conflitos e o interno, aquele que cada um vive individualmente, é um dos mais analisados na sociedade pós-moderna devido às implicações que essa construção, significa para a vida em sociedade. A construção ou renegociação de uma identidade no ciberespaço potência a importância do ciberespaço, dadas as proporções políticas, sociais e económicas que se atingem. Bastava dizer, que este 'novo' meio é um território global, ainda não controlado e cujas reais delimitações não são, ainda conhecidas.

> "As identidades não são estanques e não só as pessoas podem assumir várias como também podem querer mudar para uma nova identidade, diferente daquela em que foi socializado, alienando-se"
>
> *Os Conflitos Étnicos e Interculturais*[86]

[84] Turkle, Sherry (1999) "Cyberspace and Identity", *Contemporary Sociology*, American Sociological Association vol.28, No 6, pp.643-648

[85] idem.

Ainda segundo Turkle, percebemos que a negociação de identidades devido ao ciberespaço foi apenas um facilitismo oferecido aos indivíduos, uma vez que a sua natureza já os encaminhava para uma identidade mutável, devido às exigências da sociedade moderna. Ou seja, é em parte graças à capacidade 'conflituosa' que cada um tem que conseguimos construir-nos individual e (por fim) colectivamente.

Desta forma, não de pode ignorar a capacidade que os indivíduos possuem, em assumirem variadas identidades em consonância com o contexto ou realidade em que se encontram.

III.2. Ciberdefesa

Com a ampla introdução da tecnologia na vida diária da sociedade conseguiu atingir-se um patamar em que a maioria da população mundial possui um acesso rápido e sem fios à internet[87]. Esta possibilidade poderá parecer uma situação óbvia, porém recuando pouco atrás no tempo possuir um livro era uma coisa rara e reservada aos grupos sociais mais elevados da população.

Desde a Revolução Industrial (meados do séc. XVIII) que o desenvolvimento tecnológico assumiu um papel preponderante no decorrer da vida, individualmente e em sociedade, na organização dos Estados e no poder que estes detêm uns sobre os outros no cenário internacional. Numa primeira instância, a corrida tecnológica centrou-se em coisas para o lar, como eletrodomésticos e automóveis, sendo que, com isto, surgiram conceitos e práticas, dentro os quais se destacam as linhas de

[86] Pignatelli, Marina (2010) *Os Conflitos Étnicos e Interculturais*, Lisboa, Instituto Superior de Ciências Sociais e Políticas

[87] Castells, Manuel (1999), *A Sociedade em rede*, 2ª ed., São Paulo, UNESP

montagem industrial e a produção em massa. Como todas as novas ciências, existe uma desapropriação quase infalível aquando do seu surgimento, pois muitas das suas vulnerabilidades e falhas são ainda desconhecidas. Ficou para a história o excesso de produção provocada pela produção de bens desenfreada, bem como a inundação e a destabilização que isso provocou nos mercados internacionais. A falha estava, não nas medidas tecnológicas, mas nas instituições políticas que delas se apropriavam e exploravam.

Desta forma, o desenvolvimento tecnológico continuou em larga escala, aumentando em conhecimento, em capacidades, em recursos e em produtos finais. O mundo, estava agora a abrir uma porta que nunca mais fecharia. A lei de Moore, diz que a cada 18 meses a capacidade de processamento de qualquer equipamento informático como que duplica. Seguindo esta lei, o ser humano é confrontado com as suas próprias capacidades quer técnicas, quer imaginativas, notando que da mesma forma que ao aumentar os aspetos positivos, aumenta em igual escala a possibilidade de ocorrerem aspetos negativos. É aqui que entra a temática da Segurança. O ser humano é um ser inerentemente sociável e desde que exista mais do que um individuo a segurança dos mesmos é posta em causa. Com o surgimento da tecnologia e mais especificamente dos sistemas informáticos, surgiram uma nova série de possibilidades e de ameaças à integridade do ser humano, das suas organizações estatais e direitos, culminando na necessidade de surgimento de uma nova esfera de análise.

"Tudo o que se passa numa sociedade é do interesse particular dos Serviços de Informação "

Mafalda Borges, SIS[88]

Com o surgimento do cidadão cibernético e da automatização dos processos de produção, surgiu um novo meio para preocupação, no qual fosse garantida a segurança e defesa dos indivíduos e dos processos em si. A velocidade de

[88] Palestra proferida no âmbito do Curso de Defesa para Jovens 2013, IDN

disseminação neste meio, bem como a multiplicidade de ações quase simultâneas conferem a este meio características indubitavelmente únicas no que concerne à sua importância enquanto meio gerador de uma fluente economia[89]. Desta forma qualquer ato que impeça uma regular fluência destas atividades, será não só considerado profundamente danoso, como na realidade um ato que prejudica o bem-estar da população ou populações afetadas[90].

III.3. Novos contornos de Guerra

Para além do cibercrime, outras atividades do género foram exportadas de fora do ciberespaço, para o seu interior. Nasce aqui um novo conceito a ter em consideração, o da Ciberguerra. Esta foi uma nova categoria criada para que se pudesse analiticamente analisar a metodologia de ação de uma guerra perpetrada num novo 'campo de batalha' o ciberespaço[91].

É de notar que a ciberguerra surgiu num mundo já dominado pela Guerra da Informação, em que o mais valioso não são as ligações mas a informação contida nessas ligações ou que é difundida através das mesmas. Desta forma criou-se uma divisão no conceito de Guerra da Informação para que o mesmo pudesse ser analisado, tal como se observa pela tabela seguinte,

[89] Fernandes, José Pedro Teixeira (2012) "Utopia, Liberdade e Soberania no Ciberespaço", *Cibersegurança n.º133*, Lisboa, Nação e Defesa – Instituto de Defesa Nacional

[90] Freire, Vicente (2012) "Cibersegurança e Ciberdefesa: a inevitabilidade de adoção de uma estratégia nacional", *Segurança e Defesa*, Maio-Agosto 2012

[91] Nunes, Paulo Viegas (2012) *Novos Desafios da Segurança e Defesa no Ciberespaço – Conferência PGEES*

Guerra da Informação	
Ofensiva	Obtenção de informação através da exploração não autorizada de sistemas.
Defensiva	Prevenção, através da monitorização e acesso a informação disponível de terceiros

Tabela 4[92] - Guerra da Informação, adaptado de "A estratégia de Informação Nacional"

A ciberguerra veio alterar o paradigma existente da Guerra, as suas pedras basilares foram os estrondosos avanços tecnológicos e as capacidades que advieram da utilização do amplo meio que é o ciberespaço[93]. Esta 'nova guerra' surge com características muito próprias que a dotam de um poder de destruição único.

É importante distanciar os conceitos de Ciberguerra e de Ciberterrorismo, pois enquanto o primeiro se refere a uma ação de amplo espectro e cuja dimensão objetiva é atingir a maior dispersão espacial e de danos, o segundo conceito é projetado, visando atingir fins políticos cujos alvos estão espacialmente e temporalmente confinados[94].

O grande perigo da ciberguerra é que as ações tomadas no ciberespaço, vão expandir-se e perpetuar-se para fora dele, onde as suas consequências tendem a ser consequentemente mais graves e desastrosas do que se perspetivaria[95].

É uma Guerra assimétrica[96] (Figura 4) que pode decorrer de forma irregular, ou seja os seus intervenientes adotam regularmente métodos de ação definidos como

[92] Hayes, Richard (2012)"A Estratégia de Informação Nacional", *5º Simpósio Internacional*, Exército Português

[93] Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008) *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, Lisboa, FCA

[94] Idem

[95] Idem

[96] Pignatelli, Marina (2010) *Os Conflitos Étnicos e Interculturais*, Lisboa, Instituto Superior de Ciências Sociais e Políticas; Pires, Nuno Lemos e Ferreira, Rui (2012) "Guerra Assimétrica" – Conferência

(referência continua na página seguinte)

atos extremos[97] e desproporcionais em relação aos outros. Com o fenómeno da globalização, a capacidade de provocar uma guerra assimétrica aumentou, devido à grande discrepância e sofisticação das ameaças, bem como o aumento dos fluxos migratórios e o ressurgir de ideologias extremas[98]. Para se compreender o que é na realidade uma guerra assimétrica propomos as seguintes definições,

<table>
<tr><td colspan="3">Guerra

“ação recíproca violenta entre dois grupos políticos organizados (governos ou não)”[99]</td></tr>
<tr><td rowspan="3">Guerra formal</td><td colspan="2">Guerra Total – quando o objetivo é a aniquilação de pelo menos um dos estados envolvidos.</td></tr>
<tr><td colspan="2">Guerra Geral – com objetivo igual à anterior tipologia, porém não se faz recurso de todos os meios disponíveis.</td></tr>
<tr><td colspan="2">Guerra Limitada – é confinada no tempo, no espaço e nos recursos humanos e de meios utilizados, ou seja à partida já existem limites.</td></tr>
<tr><td rowspan="3">Guerra revolucionária</td><td rowspan="3">É uma guerra que decorre a nível intranacional, com objetivo de fazer oposição ao Governo do Estado a que pertence.</td><td>Operações paramilitares</td></tr>
<tr><td>Guerra interna</td></tr>
<tr><td>Luta de guerrilhas</td></tr>
</table>

PGEES’11; Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008) Cyberwar – O Fenómeno, as Tecnologias e os Atores, Lisboa, FCA, pp-99 ;

[97] Pignatelli, Marina (2010) *Os Conflitos Étnicos e Interculturais*, Lisboa, Instituto Superior de Ciências Sociais e Políticas

[98] Nye, Joseph S. (2012) *O Futuro do Poder*, Lisboa, Circulo de Leitores

[99] Lara, António de Sousa (2011) *Ciência Política – Estudo da Ordem e da Subversão*, 6ª edição, Lisboa, Instituto Superior de Ciências Sociais e Políticas, pp. 315, fazendo referencia a Huntington, Samuel P. (1996) “A luta de guerrilhas”, *Antologia da Guerra Subversiva,* 1ª parte

		Guerra subversiva
		Guerra terrorista
		Atividades rebeldes
		Insurreição armada
		Resistência armada
		Luta partisan

Tabela 5[100] - Guerra, adaptado de *Ciência Política – Estudo da Ordem e da Subversão*

III.4. O Cibercrime como estrutura organizada de financiamento ao terrorismo.

Muitas esferas de ação da vida fora do ciberespaço foram extrapoladas para o seu interior, a prática criminosa não foi exceção. O novo meio que surgiu, o do ciberespaço, foi na realidade uma oportunidade única de expansão e solidificação de um mercado criminoso emergente.

[100] Lara, António de Sousa (2011) *Ciência Política – Estudo da Ordem e da Subversão*, 6ª edição, Lisboa, Instituto Superior de Ciências Sociais e Políticas

A atividade criminosa fora do ciberespaço, nomeadamente, as redes de crime organizado, há mais de uma década que servem como meio de propagação de bens, pessoas e fundos para a prática terrorista. As suas redes metódicas profundamente enraizadas na sociedade conferem-lhe características únicas, no que toca a fazer desaparecer e a movimentar pessoas e valores.

Ao passar a atuar no ciberespaço as redes de crime organizado deram origem a um novo tipo de crime que se verificou uma fonte muito rentável, que possui poucos riscos e que finalmente, é anónima[101]. É importante definir que o cibercrime é diferente do ciberterrorismo, pois o primeira serve como estrutura de movimentação e angariação de fundos, a par que o segundo extravasa esse sentido apenas mantendo em comum o meio de ação e o aproveitamento das regalias da mesmo.

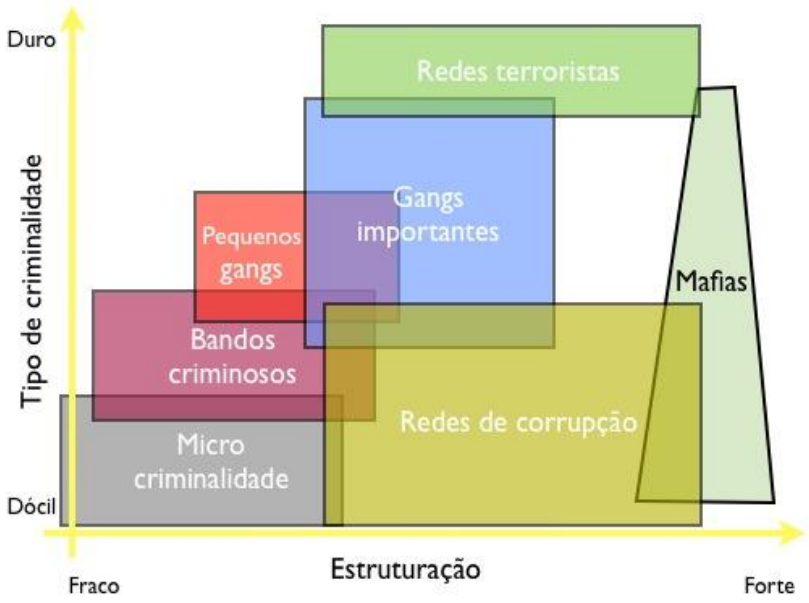


Figura 4[102] – Os Diferentes formatos da Guerra Assimétrica, adaptado de Baud, J. *La Guerre Asymétrique*

[101] McAfee (2012) *Cyber-security: The vexed question of global rules - An independent report on cyber-preparedness around the world* [disponível em: http://www.mcafee.com/au/resources/ reports/rp-sda-cyber-security.pdf]

[102] Baud, J. (2003) *La Guerre Asymétrique ou la Défaite du Vainquer*, L'Art de La Guerre, Éditions du Rocher

Este meio possui a capacidade de se modificar com o tempo, funcionando como uma espécie de organismo que se vai adaptando. Deste modo, com o passar do tempo, tornou-se possível a deteção e monitorização de redes terroristas através das suas ações no ciberespaço, como a transação de valores e as comunicações estabelecidas entre os diferentes membros pertencentes à rede como é possível ver na figura 5.

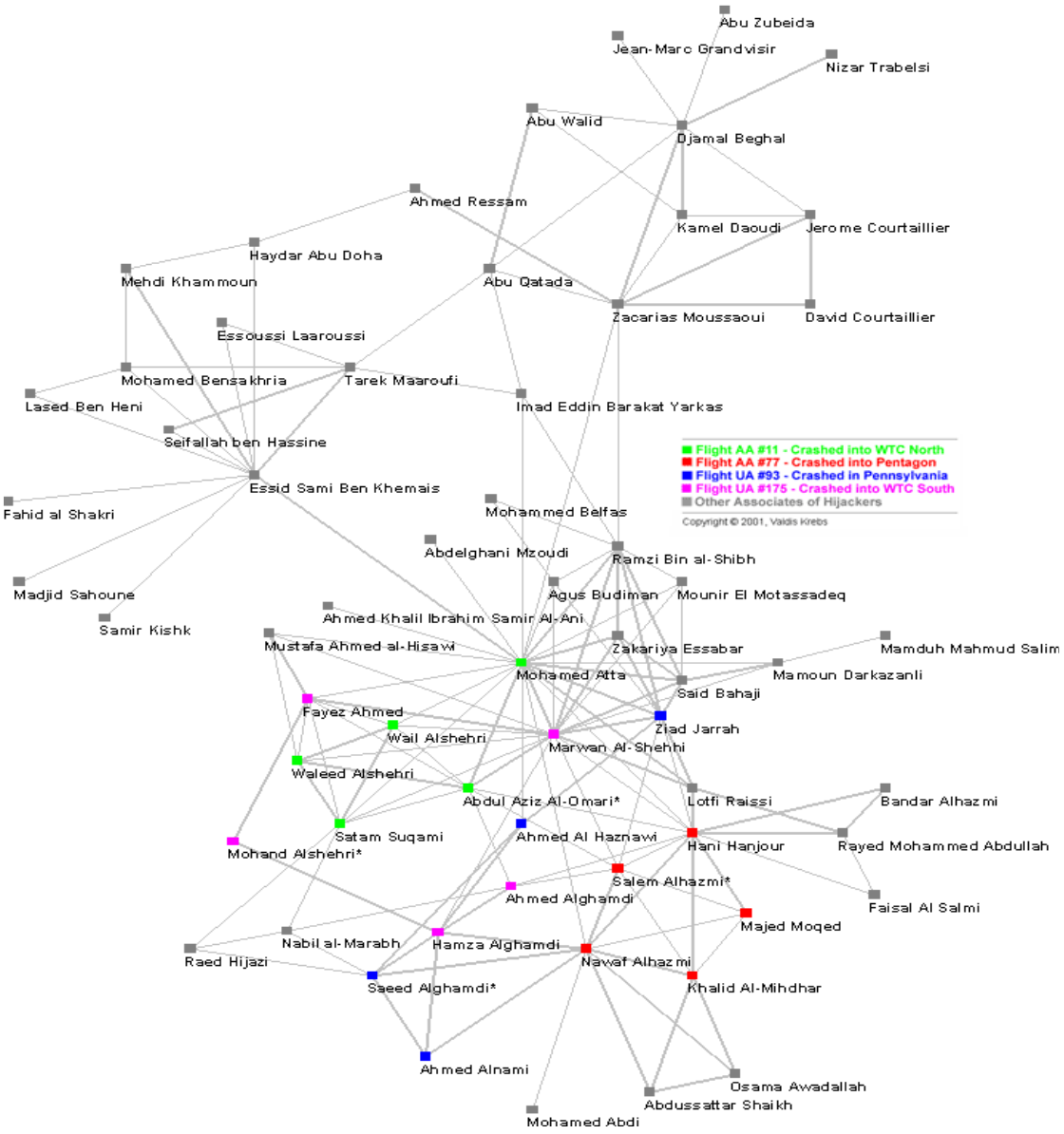


Figura 5[103] – Análise da Rede Terrorista do 9/11

[103] Krebs, V. (2006) *Connecting the Dots*. [disponível em: www.orgnet.com/prevent.html]

Para grupos terroristas e para redes de crime organizado o simples roubo de dados de acesso a contas bancárias, ou o acesso a linhas de crédito significam o acesso a fundos de financiamento para as suas ações. Estes grupos roubam identidades e posteriormente utilizam-nos para obter créditos em diversos bancos. Um dos mais notáveis indivíduos a conseguir uma proeza deste género, financiar atos terroristas com recurso a financiamento pela prática do cibercrime, foi um dos bombistas da al-Qaeda[104], conhecido como o Bombista de Bali.

A sua metodologia de ação pode ser individual ou em pequenos grupos nos quais cada membro exerce uma função na construção de um *malware*, podendo não estarem aparentemente relacionados uns com os outros.

O cibercrime atingiu proporções dramáticas, e uma grande fatia desta razão assenta na necessidade que grandes grupos terroristas ou redes de crime organizado sentem em arranjar fundos de fontes com as quais dificilmente podem ser identificados.

III.5. Vulnerabilidade das infraestruturas de rede elétrica e telecomunicações

> Artigo 2.º
>
> a)«Infra-estrutura crítica» 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

[104] Charette, Robert N. (2007) "Financing Terrorism", IEEE Spectrum [disponível em: http://spectrum.ieee.org/telecom/security/financing-terrorism]

> teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções
>
> Decreto-Lei n.º62/2011, de 9 de Maio[105]

O espaço que hoje concentra as principais ações da vida como a conhecemos é o ciberespaço. Nele estão contidas as redes de controlo de transporte e distribuição energética, bem como as diferentes redes de telecomunicações principais, indispensáveis para o regular funcionamento da sociedade, ou seja a garantia da sua segurança e a promoção dos mercados internacionais[106]. A promoção de uma atividade diária regulada e eficaz passa hoje, então, impreterivelmente por algum ou vários sistemas - o mais provável dos cenários - do ciberespaço.

A União Europeia regulou em 2011, uma diretiva para o quadro de comunicações dentro da União, dada a elevada utilização das redes de comunicação pelos cidadãos dos Estados-Membros na realização das mais variadas atividades[107]. A ENISA é a agência da União responsável pela elaboração de relatórios que permitam visualizar as diferentes situações que ocorrem no ciberespaço, nomeadamente, aqueles que surgem do ciberespaço para os sistemas críticos de cada Estado-Membro. Os quadros seguintes revelam os ataques que causaram danos observáveis pela população em geral, bem como a sua representatividade de impacto em horas de utilização, perpetrados contra os Estados da União no decorrer do ano 2012.

---

[105] Decreto-Lei 62/2011, de 9 de Maio [disponível em: http://www.dre.pt/cgi/dr1s.exe?t=dr&cap=1-1200&doc=20110870&v02=&v01=2&v03=1900-01-01&v04=3000-12-21&v05=&v06=&v07=&v08=&v09=&v10=&v11='Decreto-Lei'&v12=&v13=&v14=&v15=&sort=0&submit=Pesquisar]

[106] Viana, Vítor Rodrigues (2012) *Cibersegurança*, IDN Nação e Defesa nº 133

[107] ENISA (2013) *Power Supply Dependencies en the Electronic Comunications Sector,* [disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies]

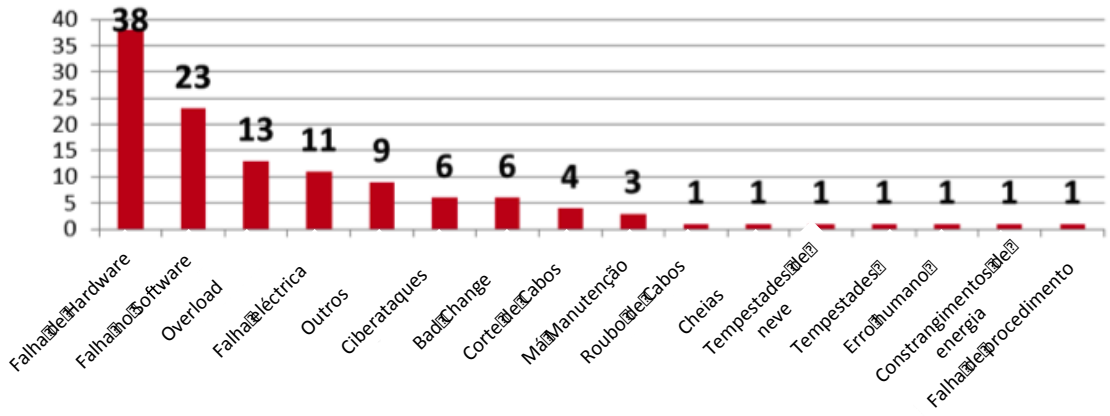


Figura 6[108] - Ataques: causas detalhadas (percentagens por serviço).

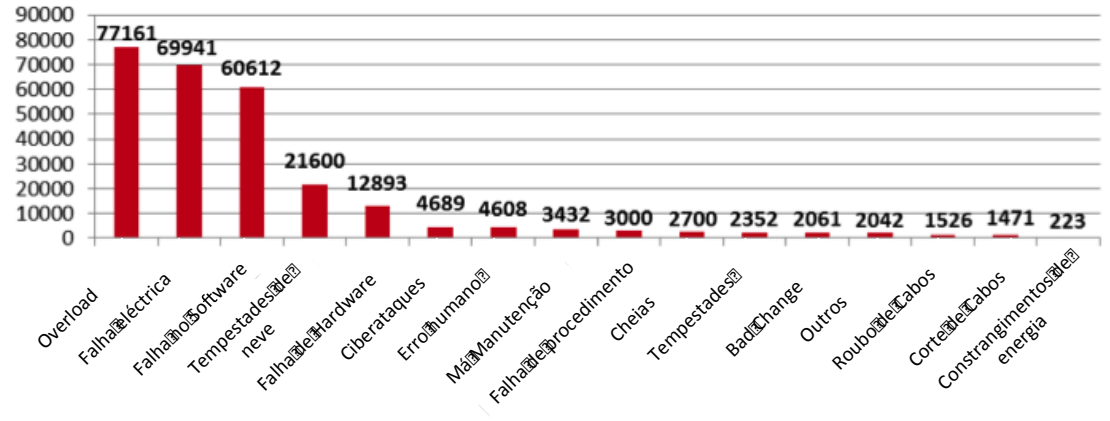
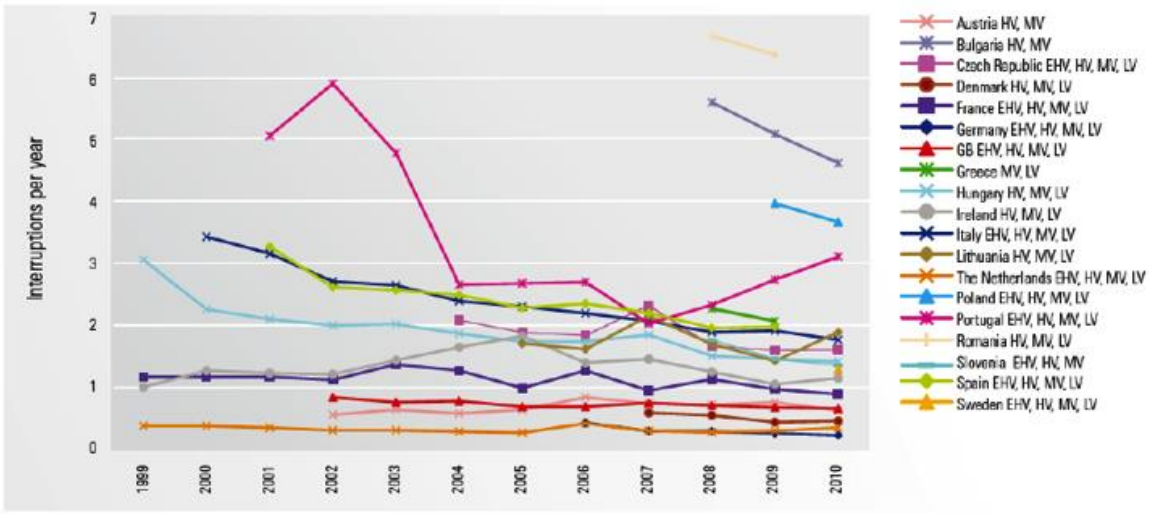


Figura 7[109] - Impacto médio em horas-usuário (em milhares) de causas por incidente.

A Figura 8 demonstra o número de interrupções indesejadas, ocorridas entre 1999 e 2010 na EU.

[108] ENISA (2013) *Power Supply Dependencies en the Electronic Comunications Sector,* [disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies]

[109] idem.



Legenda

O nível de tensão (MAT, AT, MT e BT) refere-se de ocorrência dos incidentes

MAT (EHV): Muito Alta tensão; AT (HV): Alta tensão; MT (MV): Média tensão; BT (LV): Baixa tensão

Figura 8[110] - O número de longas interrupções (não planeada) por ano, excluindo os eventos excecionais.

A necessidade de proteger as infraestruturas críticas de uma nação é de um valor incalculável pois a sociedade pós-moderna depende inteiramente das construções sociais criadas em torno dessas mesmas infraestruturas. Por muito que a tecnologia esteja a evoluir em matéria de ciberdefesa e cibersegurança, essa mesma tecnologia está simultaneamente a evoluir para aplicações ilícitas o que torna a necessidade de proteção de infraestruturas energéticas, financeiras, da banca, água, serviços de emergência e comunicações, vital, constante e permanente. Qualquer quebra em uma destas redes pode provocar acidentes com consequências gravíssimas, devido à crescente interdependência de funcionamento entre estas infraestruturas, que se estabelece como um dominó[111].

[110] ENISA (2013) *Power Supply Dependencies en the Electronic Comunications Sector,* [disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies]

[111] Caldas, Alexandre e Freire, Vicente (2013) "Cibersegurança: das Preocupações à Ação", *Working Paper 2*, Instituto da Defesa Nacional

Imagine-se um sistema financeiro totalmente regulado pelo funcionamento da rede de telecomunicações. No caso de ocorrer uma intrusão de sistema que o interrompa, todos os sistemas e subsistemas com ele interligados e dele dependentes, ficam com pelo menos uma quebra de segurança, que poderia provocar o colapso de todo o sistema financeiro, entre outros de um determinado estado.

Como medida de prevenção e de controlo de danos, foi iniciado em Portugal o Programa Nacional de Proteção de Infraestruturas Críticas, conhecido como PNPIC[112], cujo objetivo era fornecer posicionamento geográfico, bem como informações sobre o funcionamento e procedimento de determinadas infraestruturas em território nacional para que se pudesse efetuar,

> "Uma classificação objectiva da criticidade de cada infraestrutura crítica, a avaliação de interdependências não só funcionais, como económicas, sócias e temporais; a quantificação e modelação de vulnerabilidades e de consequências face às ameaças plausíveis de afetarem as infraestruturas" para a "definição de prioridades na canalização de esforços e recursos para proteção e aumento da resiliência das infraestruturas críticas"
>
> Cibersegurança: das Preocupações à Ação[113]

[112] Decreto-Lei 62/2011, de 9 de Maio [disponível em: http://www.dre.pt/cgi/dr1s.exe?t=dr&cap=1-1200&doc=20110870&v02=&v01=2&v03=1900-01-01&v04=3000-12-21&v05=&v06=&v07=&v08=&v09=&v10=&v11='Decreto-Lei'&v12=&v13=&v14=&v15=&sort=0&submit=Pesquisar]

[113] Caldas, Alexandre e Freire, Vicente (2013) "Cibersegurança: das Preocupações à Ação", *Working Paper 2*, Instituto da Defesa Nacional

Este programa foi concebido para decorrer em algumas fases que se podem dividir em avaliativa, estratégica e implementação, pois inicialmente procuram mapear geográfica e tecnologicamente cada infraestrutura, seguindo com um processo de avaliação de riscos, bem como a delineação de uma estratégia individual, integrada numa estratégia nacional e europeia que procura não só implementar estratégias de prevenção e defesa, como também de mitigar os danos sofridos possíveis em caso de ataque a alguma ou a várias das estruturas críticas que existem, em ambos os espaços nacional e europeu.

Uma parte prática deste programa foi a introdução de sistemas de deteção e intrusão, IDS nas redes de infraestruturas para que fosse, essencialmente possível registar a proveniência dos ataques sofridos e detetar assinaturas de ataque. Os IDS são assim divididos em três grupos que os definem[114]:

1. Método é a captura de dados – verificam se os dados necessários à deteção estão presentes nas estruturas físicas de suporte das infraestruturas ou nas redes que interligam as diferentes estruturas;
2. Arquitetura de sistemas – a deteção de intrusos pode ser efetuada de uma forma centralizada ou distribuída parcial ou totalmente;
3. Estratégia de processamento – pode decorrer de uma deteção de assinaturas, anomalias ou especificações.

Os IDS são eficazes, contudo as dificuldades associadas à sua utilização dificultam a sua implementação e a sua ampla difusão.

A procura de garantia de segurança de Infraestruturas críticas no ciberespaço é algo muito dispendioso económica e tecnologicamente, no entanto é uma situação indispensável dada as particularidades já abordadas acima. É portanto necessário

[114] Escravana, Nelson Nobre; Lima, João e Ribeiro, Carlos (2012) "Ciber(in)segurança da Infraestrtura de Transportes Públicos", *Cibersegurança n.º133*, Lisboa, Nação e Defesa – Instituto de Defesa Nacional

procurar desenvolver práticas mais eficazes e economicamente rentáveis de a conseguir, a segurança das infraestruturas, que ao mesmo tempo acompanhem o desenvolvimento e o crescimento tecnológico observado nos ataques e ameaças perpetrados.

IV. COOPERAÇÃO INTERNACIONAL EM MATÉRIA DE CIBERCRIME

> As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 67/98, de 26 de Outubro.
>
> Art.º 20 - Âmbito da cooperação internacional[115] da Lei n.º 109/09 de 15 de Setembro

Existem vários dispostos legais no que concerne às relações multilaterais, bilaterais e internacionais relativamente à 'recente' ameaça do Cibercrime. Recorrendo essencialmente à posição do Estado Português, enquanto ator Internacional será necessário inicialmente compreender o que o termo Cibercrime comporta.

Ainda que o termo fosse utilizado com recurso à Lei n.º 109/91 Lei da Criminalidade Informática[116], o conceito de Cibercrime, passou a figurar na legislação nacional em 2009, sensivelmente oito anos após o desenvolvimento da Convenção sobre o Cibercrime de 23 de Novembro de 2001[117], em Budapeste. Internacionalmente este ano, foi um marco de viragem na história da balança das relações internacionais. O equilíbrio até então, semi-estável dos atores do panorama internacional, foi quebrado e a dinâmica de relações entre estados, nunca mais seria a mesma.

---

[115] Art.º 20 - Âmbito da cooperação internacional da Lei n.º 109/09 de 15 de Setembro [disponível em: http://dre.pt/pdf1sdip/2009/09/17900/0631906325.pdf]

[116] Lei n.º 109/91, de 17 de Agosto [disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=151&tabela=lei_velhas&nversao=1]

[117] Convenção sobre o Cibercrime, aprovada em Resol. da AR n.º 88/2009, de 15 de Setembro [disponível em: http://dre.pt/pdf1sdip/2009/09/17900/0635406378.pdf]

Quando se fala de atores do sistema internacional, sejam entidades, grupos ou indivíduos que têm condições para a mobilização dos recursos que lhes permitem alcançar os seus objetivos, que têm capacidade para exercer influência sobre os outros atores internacionais e que gozam de uma certa autonomia. O principal ator internacional surge portanto vendo o seu papel ocupado pelo Estado, que enquanto unidade política visa as aspirações humanas fundamentais: a Segurança e o Bem-estar.

Tendo em vista a garantia destas duas condições, foram estabelecidos internacionalmente alguns princípios que buscam garantir a igualdade dos Estados através da manutenção da sua soberania. Nesta matéria, relevamos, que todos os Estados são legalmente iguais, que a sua soberania é plena, mas que existe a condição de respeitar a mesma soberania a outros, estando portanto forçados a cumprir as suas obrigações internacionais completa e conscienciosamente e, ainda a viver em paz com os outros Estados. É nesta fase das relações internacionais que surgem as Organizações Internacionais propriamente ditas, tratando-se por sua vez de estruturas institucionais formais que transcendem as fronteiras nacionais[118], criadas por acordo multilateral entre Estados. Estas traduzem a vontade política de cooperação e são dotadas de organismos permanentes encarregados da concretização dos objetivos delineados para a mesma.

É da necessidade básica de proteção e garantia de segurança que surgem as relações de cooperação, cujos objetivos são convergentes e cuja base das associações e comunidades políticas partilham valores, objetivos, conhecimentos e meios.

> 1 - As Partes deverão conceder-se mutuamente o mais amplo auxílio possível para efeitos de investigação ou de procedimento relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para efeitos de recolha de provas sob a forma electrónica de uma infracção penal.
>
> Convenção sobre o Cibercrime[119]

[118] Lara, António Sousa (2011) Ciência Política - Estudo da Ordem e da Subversão, ISCSP

[119] n.º 1 do Artigo 25.º da Convenção sobre o Cibercrime, aprovada em Resol. da AR n.º 88/2009, de 15 de Setembro [disponível em: http://dre.pt/pdf1sdip/2009/09/17900/0635406378.pdf]

IV.1. A Alteração na Balança de Poderes

Os ataques perpetrados contra o *World Trade Centre* a 11 de Setembro de 2001 em solo Norte-Americano foram individualmente o maior catalisador de instabilidade mundial desde o fim da Segunda Grande Guerra[120]. A tática doravante recorrente, desta Grande Guerra, seria uma de estratégia dissimulada, encoberta, na qual os objetivos de um Estado se sobrepunham aos demais, mas de uma forma não oficial e preferencialmente secreta. Esta ficou conhecida como Guerra Fria[121], e foi predominantemente perspetivada pelos Estados Unidos da América e pela União Soviética. O mundo estrava assim numa nova fase do equilíbrio de poderes.

Colapsaram e simultaneamente emergiram estados e governos, os poderes alteraram-se; no entanto, só a 11 de Setembro de 2001 é que o Mundo, se viu confrontado com uma nova realidade. A guerra já não era motivada somente pela política, economia ou território, mas sim por uma conjugação multifatorial do que em Relações Internacionais se começariam a chamar de fatores despoletadores de conflito. As regras da praxis bélica revelaram-se ineficazes e em alguns casos mesmo inexistentes, levando os atores internacionais à constatação de que o equilíbrio e segurança mundial, dependiam agora, de uma 'contra guerra' mais eficaz, pronta e adequada do que nunca.

Deu-se início ao que seria impensável até à data, ou seja, começaram a ser efetuadas análises sistemáticas do que seriam as fraquezas dos Estados. Cada um autonomamente seria responsável pela avaliação situacional da sua segurança e defesa, investigando portanto, as possíveis ineficiências quer a nível económico, legal, tecnológico, político, militar e ideológico. Aos poucos, o mundo começava a construir barreiras invisíveis, onde outrora figuravam barreiras físicas, entretanto ultrapassadas e destruídas. A fortificação estatal não ficou porém ao nível individual. Existiam e existem organizações Supranacionais que regulam o bom funcionamento dos 'poderes'

[120] Sampaio, Jorge (2006) "Preâmbulo", *Terrorismo e Relações Internacionais - Palestra Gulbenkian*, Gradiva

existentes, buscando garantir que a autonomia dos estados não entra em direta convergência com a rota adotada por terceiros. Seria incorreto assumir que uma organização deste tipo, nomeadamente a ONU e o seu concelho de Segurança, têm o poder decisório final, contudo servem para efeito prático, ideológico, princípios diplomáticos e, em último caso, de necessidades militares. No seguimento desta linha de pensamento, existe também a União Europeia que visa regular o bom funcionamento multifatorial de poderes, referido atrás, dentro do espaço geográfico e económico da Europa e desta, com os seus países vizinhos.

Assim, surgem uma série de Convenções Internacionais, que procuram ressalvar, que da autonomia Estatal em matéria de segurança e defesa, existam pontos comuns que almejem garantir que dentro - ou entre - determinado espaço territorial, político, ou de relacionamento económico se possui uma transparência de informações e de cooperação na medida em que se busca garantir a segurança possível desejada para o 'sistema-mundo'.

> "Os Estados membros do Conselho da Europa e os outros Estados signatários:
>
> Considerando que o objectivo do Conselho da Europa é o de criar uma união mais estreita entre os seus membros;
>
> Reconhecendo a importância de intensificar a cooperação com os outros Estados Partes na presente Convenção;
>
> Convictos da necessidade de prosseguir, com character prioritário, uma política criminal comum, com o objectivo de proteger a sociedade do cibercrime, nomeadamente através da adopção de legislação adequada e do fomento da cooperação internacional;
>
> (...)
>
> Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, prevendo a criminalização desses comportamentos, tal como se encontram descritos na presente Convenção, e a criação de competências suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e a

> acção penal relativamente às referidas infracções, tanto ao nível nacional como ao nível internacional, e adoptando medidas que visem uma cooperação internacional rápida e fiável;
>
> Tendo presente a necessidade de garantir um equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do homem consagrados na Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950), no Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas (1966) e noutros tratados internacionais em matéria de direitos humanos
>
> (...)
>
> Tendo, igualmente, em consideração o Plano de Acção que foi adoptado pelos Chefes de Estado e de Governo do Conselho da Europa na sua Segunda Cimeira (Estrasburgo, 10 e 11 de Outubro de 1997) para, com base nas normas e nos valores do Conselho da Europa, encontrar respostas comuns face ao desenvolvimento das novas tecnologias de informação."
>
> Convenção sobre o Cibercrime[122]

IV.2. Situação Nacional – A abordagem de Portugal ao cibercrime

Em Portugal só em 2009, através da Resolução da Assembleia da República n.º 88/2009, de 15 de Setembro foi aprovada a Convenção sobre o Cibercrime, adotada em Budapeste. Desde esta data não existiram alterações à convenção e em Portugal, embora estejam já estabelecidos os mecanismos, não é ainda comummente praticado o sistema de combate e prevenção ao cibercrime. Não existe ainda uma centralização no âmbito prático, no que concerne à atribuição de competências sobre esta área. As

[122] Preâmbulo da Convenção sobre o Cibercrime, aprovada em Resol. da AR n.º 88/2009, de 15 de Setembro [disponível em: http://dre.pt/pdf1sdip/2009/09/17900/0635406378.pdf]

situações de cibercrime são as que recaem sobre as práticas consideradas como terroristas como disposto na alínea b) do n. 1 do artigo 2. da Lei n.º 17/2011, de 03 de Maio.

> "1- Considera-se grupo, organização ou associação terrorista todo o agrupamento de duas ou mais pessoas que, actuando concertadamente, visem prejudicar a integridade e a independência nacionais, impedir, alterar ou subverter o funcionamento das instituições do Estado previstas na Constituição, forçar a autoridade pública a praticar um acto, a abster-se de o praticar ou a tolerar que se pratique, ou ainda intimidar certas pessoas, grupos de pessoas ou a população em geral, mediante:
>
> a) (...)
>
> b)Crime contra a segurança dos transportes e das comunicações, incluindo as informáticas, telegráficas, telefónicas, de rádio ou de televisão;"

Nesta situação, e no âmbito da cooperação internacional, a entidade externa, procurando o bom funcionamento legal, contacta a entidade competente nacional disponível 24 horas / 7 dias por semanas, como dispostos nos n.º 1, 2 e 3 do artigo 35.º da Convenção sobre o Cibercrime,

> "1 - Cada Parte deverá designar um ponto de contacto que deverá estar disponível vinte e quatro horas por dia, sete dias por semana, a fim de assegurar de imediato a prestação de auxílio nas investigações e nos procedimentos relativos a infracções penais relacionadas com sistemas informáticos, ou na recolha de provas sob a forma electrónica, da prática de infracções penais. Esse auxílio deverá compreender a facilitação ou, se o direito e a prática internos o permitirem, a execução directa das seguintes medidas: a)O aconselhamento técnico;
>
> b)A conservação de dados em conformidade com os artigos 29.º e 30.º;
>
> c)A recolha de provas, prestação de informações de natureza jurídica e localização de suspeitos.

2 -

a) Oponto de contacto de uma Parte deverá dispor de meios para contactar com rapidez o ponto de contacto de uma outra Parte.

b) O ponto de contacto designado por uma Parte deverá assegurar que se pode coordenar de forma célere com a ou as autoridades dessa Parte responsáveis pelo auxílio mútuo internacional ou pela extradição, caso não seja parte integrante dessa ou dessas autoridades.

3 - Cada Parte deverá assegurar que dispõe de pessoal com formação e equipamento de modo a facilitar o funcionamento da rede."

No caso português, a entidade sobre a qual recai esta competência é a Polícia Judiciária, como consta no n.º 1, do artigo 21. da Lei n.º 109/2009 de 15 de Setembro.

Em matéria estritamente de cibercrime não existe ainda a nível nacional uma organização descrita de métodos ou práticas de deteção efetiva, sendo que o que é verificado é uma conjugação entre diferentes serviços e gabinetes que individualmente se encarregam de a desenhar no panorama nacional, perspetivando-a para o exterior, em virtude da preocupação em manter esta 'prática' ativa e em funcionamento, através do cumprimento dos requisitos e padrões internacionalmente previstos. No cenário português, internamente não estão definidas ordens hierárquicas, nem estruturas de aproveitamento e melhor utilização de meios, o que existe efetivamente é uma nomeação para efeitos externos, a Polícia Judiciária.

"As partes deverão cooperar o mais possível entre si para efeitos de investigação ou de procedimento relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para recolha de provas sob a forma electrónica de uma infracção penal, em conformidade com o disposto no presente capítulo, em aplicação dos instrumentos internacionais pertinentes sobre cooperação internacional em matéria penal, de acordos celebrados com base em legislação uniforme ou recíproca e dos respectivos Direitos internos."

Artigo 23.º da Convenção sobre o Cibercrime

Portugal possui capacidades humanas e tecnológicas que lhe permitem ser uma figura de peso no panorama internacional em matéria de cibercrime. Exemplo disso, é que desde a cerimónia protocolar de 4 de Abril de 1949 na qual Portugal foi representado pelo então Ministro dos Negócios Estrangeiros, José Caeiro da Mata, que o país, faz parte de uma Organização Internacional, com um departamento específico para a Comunicação e Sistemas de Informação e com um outro Centro de Excelência reconhecido para a Ciberdefesa Cooperativa, ao qual o país reconhece, desde a época a importância e valor na área da defesa internacional. "(...) Portugal quer afirmar que não vê no Pacto Atlântico Norte mais que um instrumento de defesa e de cooperação internacionais."

Segundo o Coronel Coutinho Rodrigues, as antigas PESC (Política Externa de Segurança Comum), PESD (Política Europeia de Segurança e Defesa), e a recente PCSD (Política Comum de Segurança e Defesa), constituem as pedras basilares que permitem à União Europeia afirmar-se no panorama Internacional, como a única organização internacional com capacidade de cobrir todo o espectro de prevenção, gestão e resolução de crises, independente da sua tipologia, ou do espaço, onde estas decorram ou se percecionem. Desta forma, assumem ainda um carácter unificador, pois é seu intuito estar ao serviço do interesse coletivo dos Estados-membros. Aumentando este carácter de unificação, surge ainda com a assinatura do tratado de Lisboa, a fusão dos cargos de Alto Representante para a Política Externa e de Segurança Comum com a posição de Comissário das Relações Externas, sendo ainda que o Alto Representante de Negócios Estrangeiros e Política de Segurança é simultaneamente Vice-Presidente da Comissão.

A cláusula de Solidariedade presente no mesmo tratado, garante uma articulação entre a segurança interna e internacional, sendo que determina aos estados uma obrigatoriedade de auxílio mútuo nestas matérias.

> "Os Estados-Membros concertar-se-ão no âmbito do Conselho Europeu e do Conselho sobre todas as questões de política externa e de segurança que se revistam de interesse geral, de modo a definir uma

abordagem comum. Antes de empreender qualquer acção no plano internacional ou de assumir qualquer compromisso que possa afectar os interesses da União, cada Estado-Membro consulta os outros no Conselho Europeu ou no Conselho."

"Os Estados-Membros asseguram, através da convergência das suas acções, que a União possa defender os seus interesses e os seus valores no plano internacional. Os Estados-Membros são solidários entre si."

Tratado da União Europeia[123]

Uma das grandes possibilidades dos Estados Membros da União é a facilidade com que se estabelecem acordos bilaterais, que possam mutuamente colmatar as falhas dos estados em questão, nomeadamente no acesso e recurso ao uso de 'forças' e ainda de condições de extradição. Esta última questão foi a única reserva feita pela Assembleia da República Portuguesa, aquando da aprovação da Convenção sobre o Cibercrime, como consta na Resolução da AR n.º 88/2009, de 15 de Setembro[124]

"Artigo 2.º

Reserva

No momento da ratificação da Convenção sobre o Cibercrime, adoptada em Budapeste em 23 de Novembro de 2001, a República Portuguesa formula a seguinte reserva ao artigo 24.º, n.º 5: «Portugal não concederá a extradição de pessoas:

a) Que devam ser julgadas por um tribunal de excepção ou

[123] Artigo 32.º (ex-art. 16.ºTUE) da Versão Consolidada do Tratado da União Europeia como alterado pelo Tratado de Lisboa, de 13 de Dezembro de 2007 [disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:FULL:PT:PDF]

[124] Resolução da Assembleia da República n.º 88/2009, de 15 de Setembro e Convenção sobre o Cibercrime, adoptada em Budapeste em 23 de Novembro de 2001 [disponível em:http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=1505&tabela=leis&ficha=1&pagina=1&]

> cumprir uma pena decretada por um tribunal dessa natureza;
>
> b) Quando se prove que são sujeitas a processo que não oferece garantias jurídicas de um procedimento penal que respeite as condições internacionalmente reconhecidas como indispensáveis à salvaguarda dos direitos do homem, ou que cumprirem a pena em condições desumanas;
>
> c) Quando reclamadas por infracção a que corresponda pena ou medida de segurança com carácter perpétuo.
>
> Portugal só admite a extradição por crime punível com pena privativa da liberdade superior a um ano. Portugal não concederá a extradição de cidadãos portugueses. Não há extradição em Portugal por crimes a que corresponda pena de morte segundo a lei do Estado requerente. Portugal só autoriza o trânsito em território nacional de pessoa que se encontre nas condições em que a sua extradição possa ser concedida."

Quando não exista cooperação Internacional entre os estados requerentes e requeridos, a atuação poderá ser efetuada, tendo como recurso imediato a utilização dos poderes dispostos aos governos centrais em diálogo, sendo que um meio preferencial de atuação poderá ainda recair sobre a Interpol, como disposto na alínea b) do n.º 9 do artigo 27.º da Convenção sobre o Cibercrime, de 23 de Novembro de 2001.

No seguimento da aprovação da Convenção sobre o Cibercrime decorreu dentro do previsto, a adaptação do direito interno, relativamente à adopção e aplicação da Convenção Internacional aprovada em Assembleia da República, de tal modo que no âmbito da cooperação internacional existe uma autonomia em acesso a dados informáticos armazenados em território nacional, desde que os mesmos estejam publicamente disponíveis e, ainda quando a sua disponibilidade não é pública, mas exista uma declaração expressa da pessoa legalmente detentora, enquanto consente na utilização desses mesmos dados, tal como disposto nas alíneas a) e b) do artigo 25.º da Lei n.º 109/2009, de 15 de Setembro, relativamente à Lei do Cibercrime.

IV.3. Portugal - O Enquadramento Legal

Existem hoje, cada vez mais ameaças à integridade de uma nação. Com a era da Globalização e com o surgimento de um novo meio, o ciberespaço, as ameaças não só aumentaram, como sofreram uma grande alteração. Agora é possível perpetrar um ataque devastador sem sair de casa.

Desta forma e com o intuito de manter a integridade nacional, cada Estado almeja uma construção própria nacional, de um dado tipo de estrutura que consiga garantir um mínimo de segurança neste novo meio, a par com os outros que já possuía nomeadamente, as forças armadas e as forças de segurança.

Desta forma e na prossecução deste objetivo, os Estados na sua maioria, dotaram as forças já existentes, de segurança e militares, de novas capacidades, cujo objetivo seria não só atuar em caso de ataque, mas também de prevenção e mitigação do crime por este meio.

No seguimento destas novas estruturas e a par com o que já era praticado, surge a necessidade de cooperação regional e essencialmente internacional. Dada a natureza dos possíveis crimes, a legislação criada e adotada por e para Portugal, é mais restritiva e severa do que em crimes de outras naturezas. Seguindo este principio a necessidade de cooperação é muito mais necessária, uma vez que a localização dos indivíduos, bem como a sua esfera de ações podem figurar-se em milhares de quilómetros de distância entre eles.

A legislação surge portanto como uma forma de padronizar as medidas adotadas internacionalmente no que concerne ao auxílio mútuo entre estados.

A necessidade de criar um centro que conjuga-se todos estes fatores, deu origem ao Centro Nacional de Cibersegurança.

> "No âmbito da Medida 4 do referido plano, cujo desenvolvimento é coordenado pelo Gabinete Nacional de Segurança (GNS), com a colaboração de todas as entidades relevantes em razão da matéria, prevê-se a definição e implementação de uma Estratégia Nacional de Segurança

da Informação (ENSI), que compreende, designadamente, a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança."

Resolução do Conselho de Ministros 42/2012 de 5 de Abril[125]

Em concordância com o crescendo de ameaças e potencialidades, imperou cada vez mais a existência de uma Estratégia da Informação Nacional que, tem vindo a ser delineada no seio dos interesses da Segurança Nacional[126].

Com o surgimento da era tecnológica, assistimos a uma mudança de paradigma e, ao controlo de quase todas as ações direta, ou indiretamente, por meio eletrónico e como tal através da recorrência ao ciberespaço, buscando evitar 'constrangimentos de espaço'. Este novo 'meio' vem simultaneamente facilitar o desenvolvimento e aumentar riscos à segurança de si mesmo.

Finalmente surge aqui, o Centro Nacional de Cibersegurança, na medida em que este é criado como uma estrutura cujo objetivo primordial é suprimir uma necessidade do Estado Português, estando na vanguarda da prossecução e garantia de segurança aos seus cidadãos no 'novo' meio que surgiu.

Segundo Torres Sobral, em entrevista à revista Exame Informática[127], as disputas constantes de tutela e de 'peso' decisório que recaem sobre a formação do Centro Nacional de Cibersegurança (CNC) são revistas por alguns membros de agências nacionais como a causa do atraso na constituição real do mesmo. Estas disputas de poder são de grande importância, sendo que o maior enfâse recai sobre a sua representatividade no cenário internacional, pois será neste mesmo quadro que uma

[125] Resolução do Conselho de Ministros 42/2012, de 5 de Abril [disponível em: http://dre.pt/pdf1sdip/2012/04/07400/0192501926.pdf]

[126] Viana, Vítor Rodrigues, (2012) *6ºSimpósio Internacional de Estratégia de Informação Nacional,* Academia Militar

[127] Exame Informático [disponível em: http://exameinformatica.sapo.pt/noticias/mercados/2012/10/04/centro-de-ciberseguranca-atrasadodevido-a-disputas-entre-ministerios]

decisão interna em detrimento de outras pode preponderantemente influenciar o nível de coação e influências que o Estado Português, projeta no mundo[128]. Advém daqui a importância que o Centro Nacional de Cibersegurança tem para Portugal, no âmbito nacional e também no panorama internacional no que concerne a uma maior eficácia de cooperação internacional em matéria de cibercrime.

O Centro Nacional de Cibersegurança (CNC) surge no cenário de ameaças globais do século XXI em Portugal, para suprir uma necessidade registada no âmbito de segurança e defesa a novas tipologias de ameaças, nomeadamente as que subsistem através do ciberespaço.

> "Há provas de ataques contra os sistemas de informação, nomeadamente devido à ameaça que representa a criminalidade organizada, existindo uma crescente inquietação perante a eventualidade de ataques terroristas contra os sistemas de informação que constituem a infraestrutura vital dos Estados-Membros. Esta ameaça poderá compro- meter a instauração de uma sociedade da informação mais segura e de um espaço de liberdade, de segurança e de justiça, exigindo, portanto, uma resposta ao nível da União Europeia."
>
> DECISÃO-QUADRO 2005/222/JAI DO CONSELHO de 24 de Fevereiro de 2005

> "O processo de globalização e a revolução tecnológica tornaram possível uma dinâmica mundial de integração política, económica, social e cultural sem precedentes. (...)
>
> Mas tornaram, também, possível uma difusão equivalente de ameaças e riscos em todas as dimensões, que incluem (...) o potencial devastador dos ataques, cibernéticos."
>
> n.º 1 , capítulo III do Conceito Estratégico de Defesa Nacional[129]

[128] Freire, Maria Raquel coord. (2011) *Políticа Externa - As Relações Internacionais em Mudança*, Imprensa da Universidade de Coimbra, Coimbra

[129] Conceito Estratégico de Defesa Nacional [disponível em: http://dre.pt/pdf1sdip/2013/04/06700/0198101995.pdf]

Com as 'novas' tecnologias tem-se vindo a registar um abandono da necessidade estática de um computador e de comunicações. Na realidade, esta tecnologia verifica-se cada vez mais como obsoleta, quando a par da sua congénere portável.

Este é o ponto de partida, em larga escala, para a necessidade imperativa de um CNC. A capacidade de defender sistemas de informações e infraestruturas críticas, bem com a salvaguarda contra ataques de sabotagem a lugares externos cujas implicações se verificam internamente, são apenas alguns exemplos dos tipos de ameaças que este centro terá de lidar. Assim é nosso intuito criar um CNC que funcione não só como centro de prevenção e combate mas também como um órgão consultivo a outras forças e instituições na medida que em último caso, se crie uma força conjunta de defesa, ou seja, um bom sistema repleto de bons equipamentos e de pessoal altamente especializado e competente, associadas, por vezes e somente quando em necessidade, a uma *task force* operacional que aja *in loco*.

IV.4. A articulação entre agências

O crescimento exponencial de perigos associados ao ciberespaço trouxe novos desafios às entidades que procuram regular os crimes efetuados através deste meio. Um novo, e cada vez mais recorrente tipo de ataque são as fraudes *online*. Estas provocaram uma evolução nas relações de articulação entre diferentes organismos supre estatais que procuram regular e fiscalizar as ações criminosas no ciberespaço[130].

[130] Regulation (EU) No 526/2013 of The European Parliament and of The Council of 21 May 2013, concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 [disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013: 165:0041:0058:EN:PDF]

Indo ao encontro dos novos desafios de segurança neste meio e procurando colmatar as falhas metodológicas e processuais já verificadas, a União Europeia desenvolveu um novo documento de regulação, para um período de 7 anos, que determina não só as ações da ENISA - European Network Security Agency - como também os procedimentos de articulação com outros organismos europeus de controlo[131].

IV.4.1. ENISA

Esta articulação deriva dos cinco objetivos definidos pela Comissão Europeia, como a meta para a ENISA: (1) Capacidade de auto-resistência, (2) Reduzir significativamente o cibercrime, (3) Desenvolver a CSDP - Política Comum de segurança e Defesa, (4) Desenvolver capacidades tecnológicas para o combate ao cibercrime e por fim (5) Definir e implementar uma política coerente de segurança e defesa no ciberespaço que espelhe os princípios da União[132].

Na prossecução destes objetivos a Comissão Europeia definiu que a ENISA deveria articular as suas ações com alguns organismos europeus em particulares, devido às capacidades excecionais que estes detém ou se perspetiva virem a ter para alcançar estes mesmos objetivos. A si, a União requisitou não só o estabelecimento destas relações, como também o desenvolvimento de equipas de resposta a incidentes nacionais[133] e o apoio regular à realização de exercícios entre os diferentes organismos e organizações da União, bem como entre estes e terceiros fora da União Europeia. Um destes organismos é o recém-criado EC3 - European Cybercrime Centre. Este está

[131] "EU Agency reciever new Regulation for Cyber Security" (2013) [disponível em http://www.pymnts.com/briefing-room/PYMNTS-International/2013/06/eu-agency-receives-new-regulation- for-cyber-security/]

[132] [disponível em: http://www.scl.org/site.aspx?i=ne30498]

[133] Joint Communication to the European Parliament, The Council, The European Economic and Social Commitee and the Committee of the Regions (2013) "CyberSecurity Strategy of the European Union"

sob a alçada da Europol e a sua relação com a ENISA, surge da capacidade que o EC3 tem de regular se as medidas definidas protocolarmente por esta entidade, estão a ser desenvolvidas no âmbito operacional[134].

Deste modo, a União Europeia através da ENISA compromete-se a apoiar o trabalho desenvolvido pelo EC3, facilitando as conversações intraestatais e procurando auxiliar na articulação e aplicação da Lei entre os estados-membros, relativamente à prevenção e combate ao cibercrime.

Contudo, esta articulação pede algo em retorno ao EC3, nomeadamente que a sua ação principal seja o auxílio aos estados membros para que estes consigam extinguir redes de cibercrime relacionados com o abuso sexual de crianças, fraude informática, intrusões e *botnets*. A União Europeia requer ainda, que sejam entregues regularmente, à ENISA pela parte do EC3 relatórios que definam as últimas metodologias de ciberataques, e que definam estratégias possíveis e medidas de ação de combate a possíveis alvos de investigação por cibercrime[135].

A ENISA tem sido alvo de algumas alterações a nível de procedimentos, porém a sua relação com as CERTs, localizados na figura 9, surge na medida necessária da correta aplicação da SRI - Segurança das Redes de Informação.

[134] Joint Communication to the European Parliament, The Council, The European Economic and Social Commitee and the Committee of the Regions (2013) "CyberSecurity Strategy of the European Union"

[135] idem

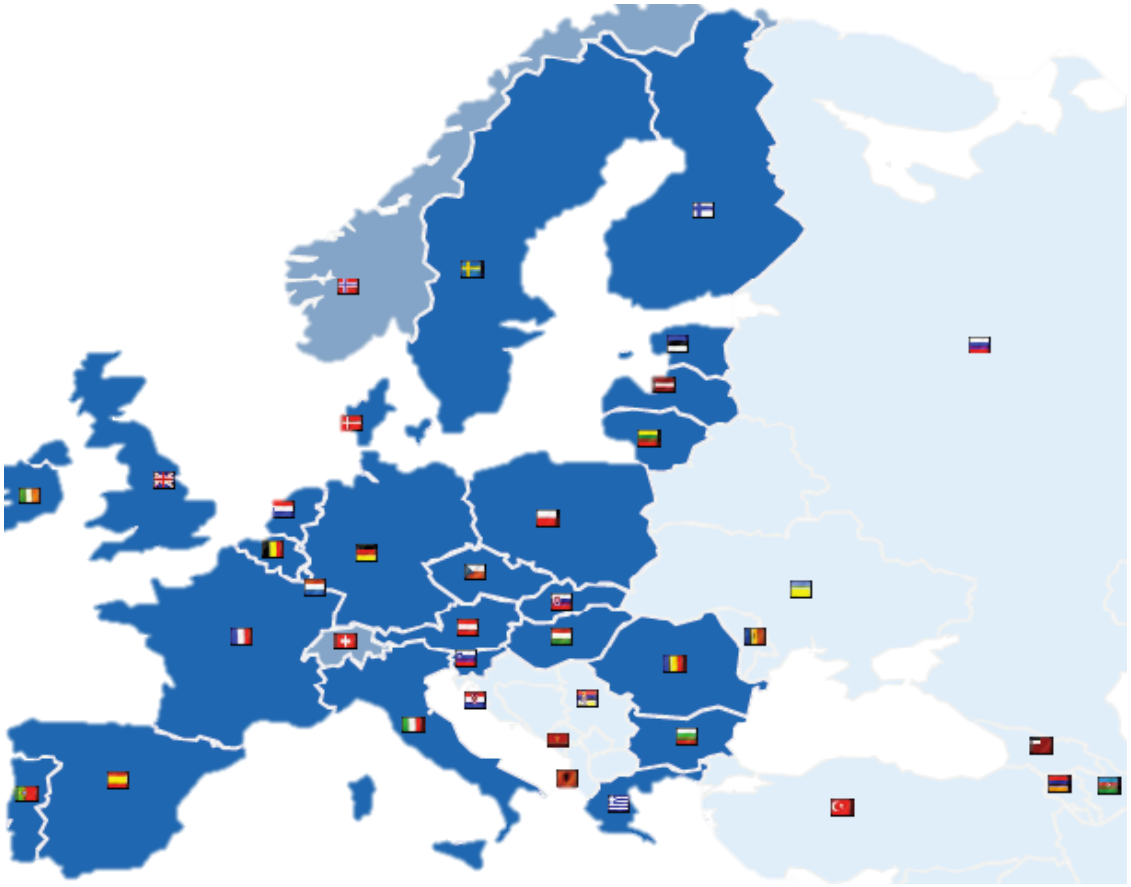


Figura 9[136] - CERT's, *ENISA - CERT Inventory*

Deste modo as CERTs são equipas permanentes de ação rápida a emergências informáticas em organizações ou instituições dos estados membros. A ação da ENISA com esta, como definida nos n.º 31 e 32 da Regulação Nº 526/2013[137], é a de

[136] ENISA (2014) *CERT Inventory – Inventory of CERT teams and activities in Europe.* [disponível em: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe]

[137] Regulation (EU) No 526/2013 of The European Parliament and of The Council of 21 May 2013, concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

assegurar o seu correto funcionamento bem como facilitar o acesso entre diferentes CERTs[138] e assegurar as suas ações dentro e entre os diferentes estados membros.

Desta forma é possível compreender que o papel da ENISA em relação aos CERTs e ao EC3, é o de apoiar financeiramente os mesmos, fornecer indicadores para os seus procedimentos, facilitar o diálogo entre estes e terceiros importantes na prossecução dos objetivos definidos pela ENISA[139], e assim interligar toda a Europa no combate ativo ao cibercrime e a prevenir ciberataques.

Em todo o processo de prevenção, combate e resposta a incidentes informáticos participam diversas entidades a nível Europeu e nacional, nos campos da Segurança das Redes e da Informação, da Repressão e da Defesa. Dada a multidisciplinaridade dos atores e da sua diversidade, uma supervisão europeia não é adequada. Assim é criada uma rede de fluxo de informação a nível da UE e dos governos nacionais que permite agilizar o processo organizativo da prevenção e resposta a incidentes. Também está previsto o envolvimento do sector privado como as empresas ligadas ao sector que as universidades.

[138] ENISA (2011) *A flair for sharing – encouraging information exchange between CERTs. A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe*

[139] n.º 2.1, do Parecer da Comissão de Assuntos Europeus da República Portuguesa à Assembleia da República relativo ao JOIN(2013)1, Comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido.

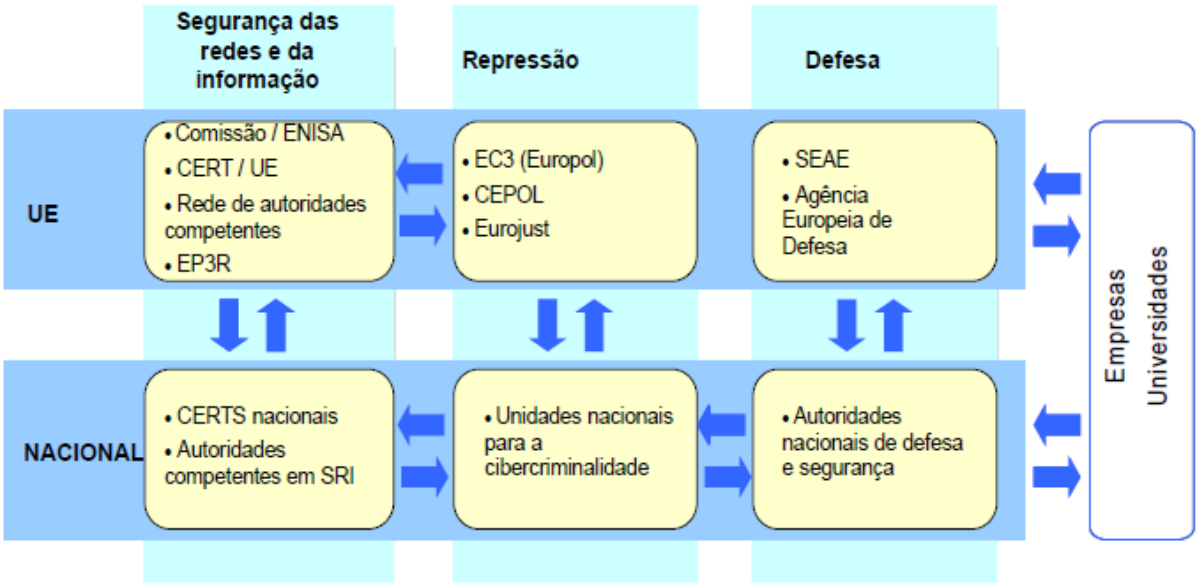


Figura 10[140] - Coordenação entre as autoridades competentes em matéria de SRI/CERT

IV.4.2. CERT-EU

Na *Digital Agenda for Europe*[141], número IP/10/581[142] e MEMO/10/200[143] adotada em Maio de 2010, a Comissão comprometeu-se a estabelecer uma CERT[144] para as instituições da União Europeia (UE), como parte do compromisso desta para uma rede e política de segurança da informação reforçada e de alto nível na Europa.

---

[140] Joint Communication to the European Parliament, The Council, The European Economic and Social Commitee and the Committee of the Regions (2013) *CyberSecurity Strategy of the European Union*. Disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:PT:PDF

[141] Digital Agenda, disponível em http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[142] IP/10/581 Digital Agenda: Comussion outline action plan to boost Europe's properity and well-being, disponível em http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/581&format=HTML&aged=0&language=EN&guiLanguage=en

[143] Digital Agenda for Europe: key initiatives, disponível em http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/200&format=HTML&aged=0&language=EN&guiLanguage=en

[144] Computer Emergency Response Team

Após uma fase piloto de um ano e a realização de vários testes, as instituições da União Europeia decidiram constituir em permanência uma Equipa de Resposta a Emergências Informáticas (Computer Emergency Response Team "CERT-EU") para servir os órgãos, agências e instituições que constituem a União Europeia. Esta equipa deve ser constituída por especialistas em segurança de TI, das principais instituições da EU. A criação da CERT-EU foi mandatada via decisão da Comissão data de 2012/11/11.

A CERT-EU[145] funciona em estreita colaboração com as outras CERTs dos Estados Membros e com empresas especializadas em segurança das TI, para que possa, de forma eficaz e eficiente, responder a incidentes de segurança da informação e ameaças ao ciberespaço, funcionando em permanência, 24 sobre 24 horas por dia, 7 dias por semana.

A missão do CERT-EU é dar apoio às Instituições Europeias para que estas se possam proteger contra ataques maliciosos e intencionais que possam afetar a sua integridade e prejudicar os interesses da União. Desta forma, os serviços que são prestados pela CERT-EU encontram-se divididos em três categorias:

- Anúncios – este serviço visa fornecer informações (por exemplo, cenários de ameaça, análise a vulnerabilidades, novas ferramentas de ataque ou artefactos e ainda medidas de segurança e ou proteção) necessárias para proteger sistemas e redes.
- Alertas e avisos – este serviço procura divulgar informações sobre ataques cibernéticos ou perturbações, vulnerabilidades de segurança, alertas de intrusão, vírus informáticos e fornecimento de recomendações para enfrentar os problemas detectados.
- Coordenação de Resposta a Incidentes – promove uma coordenação da resposta a incidentes de segurança da informação nas instituições e órgãos da União Europeia, em cooperação com os proprietários e fornecedores de peças afectadas da respectiva infra-estrutura de TI, as comunidades europeia e

[145] CERT-EU, disponível em http://cert.europa.eu/cert/plainedition/en/cert_about.html

internacional de *Computer Emergency Response Teams*, operadores de telecomunicações, *ISP*s e outros órgãos privados e públicos (polícia, investigadores e tribunais), dependendo das características de cada caso .

IV.4.3. EC3

O European Cybercrime Centre (EC3)[146] está sobre a alçada da EUROPOL, por definição da Comissão. A ação do centro foca-se no combate contra o cibercrime a nível europeu, contribuindo para uma rápida reação a eventos criminais na Internet.

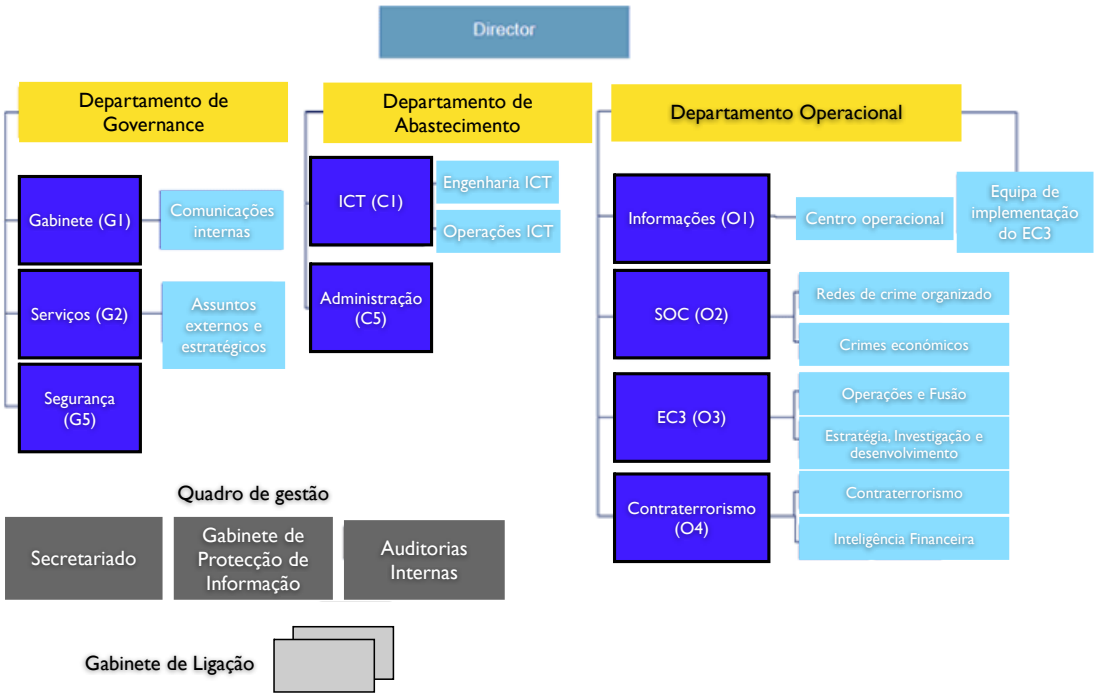


Figura 11[147] - Estrutura da EUROPOL, com o EC3 enquanto subdepartamento influenciador de todo os outros no departamento das operações.

[146] https://www.europol.europa.eu/ec3

[147] Organigrama da Europol. Disponível em https://www.europol.europa.eu/content/page/organisational-structure-157

A sua existência centra-se na ajuda os Estados Membros e às Instituições Europeias em termos operacionais, bem como de concentração de informação para garantir a cooperação internacional entre parceiros.

Em 28 de março de 2012, a Comissão Europeia emitiu uma comunicação intitulada «Luta contra a criminalidade na era digital: criação de um Centro Europeu de Combate à Cibercriminalidade». Dando origem ao EC3, que iniciou atividade a 1 de janeiro de 2013 com um mandato para lidar com as seguintes áreas do cibercrime:

- Fraudes cometidas *online* por grupos organizados e com obtenção de grandes receitas, as *botnets* e a intrusão;
- Exploração e abuso sexual infantil *online*;
- Ataques que afetam os sistemas de informação e infraestruturas críticas.

O EC3 tem sede nas instalações da EUROPOL, a agência policial Europeia em *The Hague,* na Holanda.

Devido ao crescimento das comunicações e das atividades comerciais efetuadas na internet, as ameaças e a prática do cibercrime estão a aumentar muito rapidamente tendo como alvos as pessoas, empresas e instituições governamentais. A União Europeia em virtude de ter infraestruturas de internet avançadas, economias dependentes e sistemas de pagamento fundeados no ciberespaço, tornam-na um alvo atraente para a prática do cibercrime.

A escalada do cibercrime com custos muito significativos para a sociedade civil representa um considerável desafio para as entidades policiais. Relatórios recentes sugerem que as perdas pelas vítimas são de valores totais anuais que rondam os 290 biliões de euros a nível mundial, o que torna esta atividade ilícita geradora de lucros que rondam o 'absurdo'.

As investigações de fraudes *online*, o abuso de crianças e outros crimes normalmente envolvendo muitas vítimas, com suspeitos em diversas partes do mundo, promovem um tipo de operações megalómanas. Na prática, operações desta magnitude não podem ter sucesso se forem apenas efetuadas pelas Policias nacionais.

Esta tipologia de crime alimenta-se da inexistência de fronteiras[148] neste meio requerendo que os corpos policiais colaborem e coordenem mutuamente e além-fronteiras, com outras entidades policiais e privadas. É neste ponto que o EC3 tem as maiores valências.

Em termos de estratégia e prevenção o EC3 analisa grandes volumes de informação provenientes de várias fontes, tendo informações que vão desde investigações em curso, a fontes livres, a análise de comportamento social de abusadores de crianças e burlões.

As necessidades de investigação e desenvolvimento (I&D) são muito importantes, pois permitem conhecer a forma de atuação, a mitigação e a prevenção de ameaças que dependem em grande parte de resultados das diferentes investigações. Assim, o EC3 coordena ativamente as entradas de I&D no programa *Horizon 2020* da Comissão Europeia.

As agências envolvidas no combate à cibercriminalidade não o podem fazer com ferramentas operacionais ultrapassadas, pelo que o EC3 presta apoio à comunidade internacional no desenvolvimento de ferramentas que ajudem na garantia das boas atividades policiais. Devido a ainda não existir uma capacidade operacional necessária para reagir eficazmente à cibercriminalidade em todos os Estados-Membros, a Comissão irá através de programas de financiamento apoiar na identificação das lacunas e no reforço da sua capacidade para investigar a cibercriminalidade. Como missão a Comissão irá trabalhar em estreita cooperação com o EC3, no quadro da Europol e com a Eurojust para harmonizar as abordagens políticas com as melhores práticas na esfera operacional, uniformizando as duas.

Por ainda existirem centros nacionais que não têm o *hardware* e *software* necessário para aquisições e análises forenses, o EC3 apoia e fornece esses serviços

[148] Segundo Richard Hayes, esta inexistência de fronteiras não é total, pois segundo o autor estão, pelo menos, já definidos três grandes territórios e as suas fronteiras no ciberespaço: (1) um ciberespaço governamental, um ciberespaço civil nacional e (3) um ciberespaço internacional. Desta forma é necessária uma ampla cooperação internacional (CERT's)até que se estabeleçam fronteiras mais reais e restritivas. Hayes, Richard (2012)"A Estratégia de Informação Nacional", *5º Simpósio Internacional*, Exército Português

aos Estados-Membros que deles necessitem para as investigações policiais, fornecendo simultaneamente e em colaboração com a CEPOL[149], treino e formação avançada na matéria.

O EC3 fornecerá análises e informações (*Intelligence*), apoiará as investigações, garantirá a investigação forense de elevado nível, facilitará a cooperação, criará canais para a partilha de informações entre as autoridades competentes dos Estados-Membros, o sector privado e outras partes interessadas e assumirá progressivamente o papel de porta-voz das forças policiais.

Em contrapartida a Comissão pede que o EC3 elabore regularmente relatórios estratégicos e operacionais sobre as tendências e as novas tipologias de ameaças, para identificar as prioridades a seguir e definir alvos para a atividade de investigação das equipas dos Estados-Membros especializadas em cibercriminalidade.

Finalmente, sempre que um incidente aparentar estar associado a um crime na área da cibercriminalidade, a Europol/EC3 devem ser informados para que, juntamente com as autoridades policiais dos países afetados, possam iniciar uma investigação, mantendo a cadeia de custódia e a preservação das provas, identificar os autores e, em última instância, garantir que sejam alvo de processo judicial.

[149] European Police College

Considerações Finais

O ciberespaço é um novo meio a ter em consideração. É nele e graças a ele, que decorrem atualmente as maiores transações económicas do mundo, bem como as redes de comunicações e a disseminação de informação. A sua amplitude é tal que deixa um espaço aberto à ocorrência de um sem número de atividades simultâneas. Teoricamente esta característica do ciberespaço seria uma mais-valia, pois permitiria um contacto imediato e à escala global de todas as esferas que estão contidas nele.

Porém observa-se um crescente número de ataques ao sistema do ciberespaço, ou através deste, pelas peculiaridades próprias deste meio. Podemos perspetivar que o ciberespaço seja um conjunto de territórios sobre diferentes *Scopes* e, como em todos os territórios é necessário que ocorram delimitações políticas, legais e físicas.

Já Richard Hayes, no 5º Simpósio Internacional, subordinado ao tema da "Estratégia de Informação Nacional", afirmava existirem pelo menos três territórios, já definidos, distintos no ciberespaço, pelo que a criação de fronteiras nacionais - ou comunitárias, diríamos - no ciberespaço seria um passo a dar no futuro.

Um argumento que consubstancia a necessidade de estabelecer fronteiras no ciberespaço é a identidade dos seus utilizadores pois, muito embora as alterações à sua identidade base, em virtude de se encontrarem num novo meio, possuem os mesmos princípios hedonísticos e os mesmo valores morais adquiridos por anos de construção identitária num meio físico rodeado das suas estruturas simbólicas e sociais, pelo que a necessidade para eles e terceiros da existência de fronteiras no ciberespaço é um prolongamento da ação iniciada há mais de um par de décadas atrás

com o extravasamento das atividades que só existiam fora no ciberespaço para o seu interior.

Deste modo as fronteiras do ciberespaço devem coincidir com as fronteiras físicas e legais para manter um *continuum* na identidade e modo de vida dos que utilizam o ciberespaço.

O ciberespaço constitui um desafio à Ordem Vestefaliana, pois coloca em causa a territorialidade, a soberania e a autonomia de um Estado, verificando-se necessário alterar esses pressupostos.

A existência de uma ciberdefesa e de uma cibersegurança eficazes, são o princípio de criação de fronteiras no ciberespaço, pois estas revelam que um só responsável pela sua segurança seria perfeitamente incapaz de arcar com as necessidades requeridas.

É possível também compreender que a complexidade de ação no ciberespaço, tanto dificulta como facilita em larga escala a deteção como a dispersão respetivamente de vetores de segurança e ameaça.

O grande aumento da cibercriminalidade deve-se portanto às potencialidades do ciberespaço enquanto rede intrincada de acessos que promovem uma interligação rápida e facilitada às fontes que provem o que os cibercriminosos procuram. Surgindo, assim, uma profunda necessidade de criar estruturas nacionais e internacionais que interligadas funcionem como uma rede exclusiva à prevenção do cibercrime, muito como as equipas especializadas no combate à cibercriminalidade fora do ciberespaço. Teoricamente já existem equipas que visam a prossecução não só deste objetivo mas também da prevenção de práticas ciberterroristas, da monotorização e prática de ciberespionagem e finalmente equipas prontas para agir em caso de ciberguerra.

A alteração de poderes a nível mundial pode estar a ser afetada pela utilização do ciberespaço enquanto meio de propaganda e de recurso aos média, mas também devido à visibilidade internacional de vanguarda que ter um centro ou possuir equipas prontas e eficazes transmitem à comunidade Internacional. O ciberespaço é hoje um meio definitivo na denominação de potência internacional, pois exatamente no mesmo patamar que os outros meios, proporciona aos Estados que dele se aproveitam

uma posição de controlo e liderança cujo objetivo último é que os seus ganhos de vitória terão de ser muito superiores às perdas em caso de derrota.

No que concerne à distribuição de poderes a nível internacional existe um fator que é simultaneamente prejudicial ao sistema internacional e à segurança no ciberespaço, a conectividade. Se por um lado é um aspeto positivo e uma razão pela qual o ciberespaço funciona amplamente, é igualmente um aspeto negativo pois é essa mesma abertura a 'tudo' que em caso de falha de segurança pode colocar em causa a segurança dos indivíduos e do próprio estado, situação que se verifica mais difícil em países que possuem um ciberespaço fechado e controlado.

A criação de um Centro Nacional de Cibersegurança é muito mais que o cumprimento de um requisito ou normativa da União Europeia, pois este centro funcionará como espinha dorsal de um meio com uma estrutura própria mais complexa que todas as outras, dadas as particularidades do mesmo que foram sendo abordadas no decorrer do presente trabalho.

Um CNC com as áreas militar e civil agrupadas seria uma nova perspetiva de abordagem à estrutura regular de segurança e defesa, porém o próprio ciberespaço alterou esse paradigma, porque não poderá o centro responsável a nível nacional pelo seu controlo quebrar também com conceções.

Na teoria, os resultados estimam-se positivos pois permitiriam um total conhecimento e controlo tanto de ações de defesa como de segurança, em tempo real e no mesmo espaço. Para além disto, seria não só um rentabilizar de recursos humanos, técnicos e de equipamento, mas de informações, promovendo um espaço de real cooperação aos mais diversos níveis com um fim comum, a procura de uma cibersegurança e ciberdefesa eficazes.

Para este fim, propõem-se a criação de fronteiras no ciberespaço tais como as política e geograficamente estabelecidas. Só neste cenário poderão ser estabelecidas as condições de segurança e defesa desejadas, bem como a eficácia procurada para um recém-criado Centro Nacional de Cibersegurança.

A internet é uma rede complexa de redes. A ação individual, o comportamento e a postura perante a esta são em si a abertura, leia-se, a criação de vulnerabilidades

em pontos e trajetos da rede. Significa que inadvertidamente um individuo, sem qualquer intencionalidade, poderá estar a comprometer a segurança de um sistema, de uma comunidade ainda que, novamente, não se aperceba que as suas ações tivessem qualquer impacto. Reveja-se algo tão simples como a transferência de vírus - independentemente da sua proveniência - quer em suportes físicos como lógicos (USBs ou partilha de ficheiros *online*).

Poder-se-á ter em conta que faz falta a existência de um modelo nacional que permita uma articulação de cibersegurança e ciberdefesa nacional, em ambas as suas vertentes, de sinergia interna e de cooperação externa. A elaboração de uma proposta estruturada apresenta-se muito útil, constituindo possivelmente um campo muito fértil para continuação num trabalho futuro.

O estudo e criação do referido modelo, potenciaria uma interligação das diversas tutelas administrativas com competências para o ciberespaço. Potenciando, igualmente uma maior e melhor cooperação com os seus congéneres internacionais.

Colocam-se ainda outras preocupações, como a eventual entrada mal-intencionada em sub-redes de controlo de gasodutos ou mesmo a *grid* elétrica nacional. O escalar de uma ameaça deste porte, levaria à privação energética por tempo indeterminado e com consequências devastadoras à economia de uma cidade ou mesmo de um pequeno país como Portugal. Dever-se-iam igualmente registar comportamentos sociais e movimentos desestabilizadores.

O poder inerente a esta capacidade técnica poderá levar a uma ciberguerra fria. Imagine-se um país com a possibilidade de reestabelecer uma nova ordem na polaridade mundial, sem recurso ao nuclear. A possibilidade de possuir o mapeamento da *grid* elétrica, de telecomunicações e outros recursos base em sociedade de outros países, pode trazer (à distancia de um *click*) toda uma nova forma de se gerirem acordos diplomáticos.

Se o poder nuclear é em si um meio dissuasor que de uma forma subentendida, pode ditar o fim da primeira potência que o ativar, que dizer sobre quem domine os sistemas de controlo energético ligados física ou logicamente à rede? Como proposta

de investigação futura, deixamos uma eventual análise comparativa: A guerra nuclear e a ciberguerra, que diferenças?

Referências Bibliográficas

Amante, Maria de Fátima (2007) Fronteira e Identidade - Construção e Representação Identitárias na Raia Luso-Espanhola, Lisboa, Instituto Superior de Ciências Sociais e Políticas

Apps, Peter(2012) "As Iraq, Afghan wars end, private security firms adapt", *Reuters.* Disponível em: http://www.reuters.com/ article/2012/10/21/us-usa-arms-contractors-idUSBRE89K02B20121021

Aron, Raymond (1986). Paz e Guerra entre as Nações, Brasília, Universidade de Brasília

Auner, Eric (2013) "As U.S. Drawns down in Afghanistan, Role Continues for Private Security Firms", *World Politics Review.* Disponível em: http://www.worldpoliticsreview.com/trend-lines/13446/as-u-s-draws-down-in-afghanistan-role-continues-for-private-security-firms

(2013) *A Defesa Nacional no Contexto da Reforma das Funções de Soberania do Estado*, Lisboa, Instituto de Defesa Nacional, pp. 7-15. Disponível em: http://www.defesa.pt/Documents/20130307_IDN_reforma_do_estado_soberania_jan2013.pdf

Aziz, Ashar (2013) "The evolution of Cyber attacks and Next Generation Threat Protection", *RSA Conference 2013*, FireEye, Inc.

Barata-Feyo, J. M. Citado em Gonçalves, J. A.B.F.M. (2005) *Sociedade da Informação*, Faculdade de Economia da Universidade de Coimbra. Disponível em: http://www4.fe.uc.pt/fontes/trabalhos/ 2005003.pdf

Baud, J. (2003) *La Guerre Asymétrique ou la Défaite du Vainquer*, L'Art de La Guerre, Éditions du Rocher

Caldas, Alexandre e Freire, Vicente (2013) "Cibersegurança: das Preocupações à Ação", *Working Paper 2*, Instituto da Defesa Nacional

Carvalho, Jorge Silva (2009) "Segurança Nacional, Serviços de Informações e as Forças Armadas", Palestra proferida na Faculdade de Letras de Lisboa a 28 de Maio de 2009

Castells, Manuel (1999), *A Sociedade em rede*, 2ª ed., São Paulo, UNESP

CERT-EU. Disponível em: http://cert.europa.eu/cert/plainedition/en/cert_about.html

Chagas, Polyana Amorim (2011) " Entre o virtual e o real: o sujeito no ciberespaço", *Simsocial – Simpósio em tecnologias digitais e sociabilidade* através de Wertheim

Charette, Robert N. (2007) "Financing Terrorism", IEEE Spectrum. Disponível em: http://spectrum.ieee.org/telecom/security/financing-terrorism

Cimeira Mundial 2005 da ONU. Disponível em: http://www.un.org/spanish/Depts/dpi/portugues/pdf/WorldSummitOutcome-ptREV.pdf

Conceito Estratégico de Defesa Nacional. Disponível em: http://dre.pt/pdf1sdip/2013/04/06700/0198101995.pdf

Convenção sobre o Cibercrime, aprovada em Resol. da AR n.º 88/2009, de 15 de Setembro. Disponível em: http://dre.pt/pdf1sdip/2009/09/17900/0635406378.pdf

Correia, Pedro de Pezarat (2003) *Manual de Geopolítica e Geoestratégia, Conceitos, Teorias e Doutrinas vol. I*, Coimbra

Correia, Pedro de Pezarat (2006) *Políticas de Defesa e Segurança*, Conferência no CCC

Couto, Abel Cabral (1988). Elementos de Estratégia Vol. I, Lisboa, Instituto de Altos Estudos Militares

Dicionário da Real Academia Espanhola, citada em (2013) *Estratégia da informação e Segurança no Ciberespaço,* IDN

Digital Agenda for Europe: key initiatives. Disponível em: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/200&format=HTML&aged=0&language=EN&guiLanguage=en

DL n.º 215/2012, de 28 de Setembro. Disponível em: http://www.dgsp.mj.pt/backoffice/Documentos/DocumentosSite/Legislacao/LO_215-2012.pdf

DL n.º 252/2000, de 16 de Outubro. Disponível em: http://dre.pt/pdf1s%5C2000%5C10%5C239A00%5C57495766.pdf

DL n.º 274/2007, de 30 de Julho. Disponível em: http://dre.pt/pdf1sdip/2007/07/14500/0487204876.PDF

DL n.º 245/95, de 21 de Setembro. Disponível em: http://www.dre.pt/pdf1s/1995/09/219A00/58905896.pdf

DL n.º 200/2001, de 13 de Julho, alterado pela Lei n.º 100/2003, de 15 de Novembro. Disponível em: http://www.emfa.pt/www/conteudos/informacaofap/legislacao/estatcondmilitar/ justmilitar/LeiOrganicadaPoliciaJudiciariaMilitar.pdf

DL n.º 35/2004. Disponível em: http://www.dre.pt/pdf1s/2004/02/044A00/09320941.pdf

DL n.º 62/2011, de 9 de Maio. Disponível em: http://www.dre.pt/cgi/dr1s.exe?t=dr&cap=11200&doc=20110870&v02=&v01=2&v03=1900-01-01&v04=3000-12-21&v05=&v06=&v07=&v08=&v09=&v10=&v11='Decreto-Lei'&v12=&v13=&v14=&v15=&sort=0&submit=Pesquisar

ENISA (2014) *CERT Inventory – Inventory of CERT teams and activities in Europe.* Disponível em http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

ENISA (2013) *Power Supply Dependencies en the Electronic Comunications Sector.* Disponível em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies

ENISA (2011) *A flair for sharing – encouraging information exchange between CERTs. A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe*

Espírito Santo, General Gabriel Augusto do (2009) "Os Efetivos nas Forças Armadas", *Revista Militar*, No. 2484. Disponível em: http://www.revistamilitar.pt/artigo.php?art_id=363

"EU Agency reciever new Regulation for Cyber Security" (2013) Disponível em: http://www.pymnts.com/briefing-room/PYMNTS-International/2013/06/eu-agency-receives-new-regulation- for-cyber-security/

(2013) "EU Cybersecurity Strategy and Directive", *The IT Law Community* [disponível em: http://www.scl.org/site.aspx?i=ne30498]

(2014) "European Cybercrime Centre". Disponível em: https://www.europol.europa.eu/ec3

Exame Informático. Disponível em: http://exameinformatica.sapo.pt/noticias/mercados/ 2012/10/04/centro-de-ciberseguranca-atrasadodevido-a-disputas-entre-ministerios

Fernandes, José Pedro Teixeira (2012) "Utopia, Liberdade e Soberania no Ciberespaço", *Cibersegurança n.º133*, Lisboa, Nação e Defesa – Instituto de Defesa Nacional

Freire, Maria Raquel coord. (2011) *Políticа Externa - As Relações Internacionais em Mudança*, Imprensa da Universidade de Coimbra, Coimbra

Freire, Vicente (2012) "Cibersegurança e Ciberdefesa: a inevitabilidade de adoção de uma estratégia nacional", *Segurança e Defesa*, Maio-Agosto 2012

Friedman, George (2012) *A Próxima Década - Onde temos estado... e para onde nos dirigimos*, Lisboa, D. Quixote

Gasper, Des (2008) *The Idea of Human Security. D*isponível em: http://www.unhistory.org/reviews/Garnet_HumanSecurity.pdf

Halbwachs, Maurice (1992) *On Collective Memory* , Chicago, University of Chicago Press

Hall, Stuart (2002) *A identidade cultural na pós-modernidade*, Rio de Janeiro, DP&A

Hayes, Richard (2012)"A Estratégia de Informação Nacional", *5º Simpósio Internacional*, Exército Português

Huntington, Samuel P. (1996) "A luta de guerrilhas", *Antologia da Guerra Subversiva,* 1ª parte

IP/10/581 Digital Agenda: Comussion outline action plan to boost Europe's propriety and well-being. Disponível em: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/ 581&format= HTML&aged=0&language=EN&guiLanguage=en

Jenkins, Brian M. (1974) International Terrorism: A New Kind of Warfare, California, The Rand Paper Series, The Rand Corporation.

Joint Communication to the European Parliament, The Council, The European Economic and Social Commitee and the Committee of the Regions (2013) "CyberSecurity Strategy of the European Union"

Krebs, V. (2006) *Connecting the Dots*. Disponível em: www.orgnet.com/prevent.html

Lara, António de Sousa (2011) *Ciência Política – Estudo da Ordem e da Subversão*, 6ª edição, Lisboa, Instituto Superior de Ciências Sociais e Políticas

Leary, Mark e Tangney, June (2005) *Handbook of Self and Identity*, Guilford Press

Lei n.º 53/2008 de 29 de Agosto. Disponível em: http://dre.pt/pdf1s%5C2008%5C08%5C16700%5C0613506141.pdf

Lei n.º 63/2007, de 6 de Novembro. Disponível em: http://gnr.pt/documentos/Legislacao/LEI_ORGANICA.pdf

Lei n.º 19/2004, de 20 de Maio. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=227&tabela=leis

Lei Orgânica do Ministério da Administração Interna. Disponível em: http://www.dre.pt/pdfgratis/2006/10/20800.pdf

Lei Orgânica da Polícia de Segurança Pública. Disponível em: http://www.psp.pt/Legislacao/Lei_53-2007.pdf

Lei n.º 29/2003, de 22 de Agosto. Disponível em: http://dre.pt/pdf1sdip/2003/08/193A00/53105312.pdf

Lei n.º 38/2008. Disponível em: http://dre.pt/pdf1s/2008/08/15300/0534505346.pdf

LOIC – Lei n.º 49/2008, de 27 de Agosto. Disponível em: http://www.policiajudiciaria.pt/PortalWeb/content?id={CBD3F401-5D03-492E-9FCF-9396ED545D27}

Lei de Defesa Nacional e das Forças Armadas, Lei n.º 29/82 de 11 de Dezembro. Disponível em: http://ruadosbragas223.home.sapo.pt/DIREITO/Lei_2982_Defesa_Nacional_e_Forcas_Armadas.pdf

Lei n.º 109/09 de 15 de Setembro. Disponível em: http://dre.pt/pdf1sdip/2009/09/17900/0631906325.pdf

Lei n.º 109/91, de 17 de Agosto. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=151&tabela=lei_velhas&nversao=1

Liang, Qiao e Xiangsui, Wang (1999) *Unrestricted Warfare – China's Master Plan to destroy America*, China, People's Liberation Army

Lutz, James M. e Lutz, Brenda (2009) *Global Terrorism*, Londres, Routledge

Margareth (2001) *Uma história do espaço: de Dante à Internet,* Rio de Janeiro, Jorge Zahar

McAfee (2012) *Cyber-security: The vexed question of global rules - An independent report on cyber-preparedness around the world.* Disponível em: http://www.mcafee.com/au/resources/ reports/rp-sda-cyber-security.pdf

Mead, G. H. (1934). *Mind, self, and society*. Chicago, University of Chicago Press

Mesquita, António Arnaldo (2010) "Triplicam as queixas de cidadãos por abuso de autoridade das forças de segurança", *Público.* Disponível em: http://www.publico.pt/portugal/jornal/triplicam-as-queixas-de-cidadaos-por-abuso-de-autoridade-das-forcas-de-seguranca-20615218

Moreira, Adriano (2005) Teoria das Relações Internacionais, Coimbra, Edições Almedina

Novais, Rui Alexandre (2012) "Media e (Ciber)Terrorismo", *Cibersegurança n.º133*, Lisboa, Nação e Defesa – Instituto de Defesa Nacional

Nunes, Paulo Viegas (2013) "Cibersegurança e Estratégia Nacional de Informação: Estruturas de Coordenação Nacional no Ciberespaço", Conferência, Beja, IV SimSIC

Nunes, Paulo Viegas (2012) *Novos Desafios da Segurança e Defesa no Ciberespaço – Conferência PGEES*

Nunes, Paulo Viegas (2012) "A Definição de uma Estratégia Nacional de Cibersegurança", Cibersegurança, N.º133, IDN

Nye, Joseph S. (2012) *O Futuro do Poder*, Lisboa, Circulo de Leitores

Organigrama da Europol. Disponível em https://www.europol.europa.eu/content/page/organisational-structure-157

Pereira, Júlio (2012) "Cibersegurança – O Papel do Sistema de Informações da República Portuguesa", *Segurança e Defesa*, Maio-Agosto 2012, Lisboa, Diário de Bordo

Pignatelli, Marina (2010) *Os Conflitos Étnicos e Interculturais*, Lisboa, Instituto Superior de Ciências Sociais e Políticas

Pires, Nuno Lemos e Ferreira, Rui (2012) "Guerra Assimétrica" – Conferência PGEES'11

Primo, Alex (2007*)* *Interação mediada por computador: comunicação, cibercultura, cognição*. Porto Alegre, Sulina

Proposta de Estratégia Nacional de Cibersegurança, GNS. Disponível em: http://www.gns.gov.pt/media/1247/PropostaEstratégiaNacionaldeCibersegurançaPortuguesa.pdf

Regulation (EU) No 526/2013 of The European Parliament and of The Council of 21 May 2013, concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004. Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

Resolução do Conselho de Ministros 42/2012, de 5 de Abril. Disponível em: http://dre.pt/pdf1sdip/ 2012/04/07400/0192501926.pdf

Ribeiro, António Silva (2009) Teoria Geral da Estratégia: O Essencial ao Processo Estratégico, Coimbra, Edições Almedina

Ricoeur, Paul (2006) *Memory, History, Forgetting*, Chicago, University of Chicago Press

Rodrigues, Alexandre Reis (2013) *Enquadramento Conceptual e Legal da Segurança e Defesa Nacional.* Disponível em: http://database.jornaldefesa.pt/politicas_de_defesa/portugal/JDRI%20031%20200113%20enquadramento%20segurança%20defesa.pdf

Rodrigues, Carlos Coutinho (2012) Contributo para uma "Estratégia abrangente" de gestão de crises, Lisboa, IDN Cadernos, Imprensa Nacional - Casa da Moeda

Rodrigues, Teresa Ferreira (2010) "Dinâmicas Migratórias e Riscos de Segurança – A velha Europa", *Relações Internacionais,* n.º26, Lisboa, IPRI

Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008) *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, Lisboa, FCA, pp. 51

Santos, Rui Teixeira (2012) "À procura dos culpados – A Grande Crise Financeira e Portugal", *Centro de Estudos de Gestão Pública do ISCAD.* Disponível em: http://cegep.iscad.pt/index.php/ noticias/93-a-procura-dos-culpados-a-grande-crise-financeira-e-portugal

Silva Ribeiro, António (2011) *Segurança e Defesa Nacional*, Academia de Ciências de Lisboa

Silva, A. S., & Pinto, J. M. (Eds.). (1999). *Medologia das Ciências Sociais*. Porto, Edições Afrontamento

Storch, Tyson (2012) *Cibersegurança: Pilar de uma sociedade ligada e segura*, Microsoft Trustworthy Computing

Stryker S. (1980). *Symbolic interactionism: A social structural version*. Menlo Park, Benjamin Cummings.

Thompson, John (1998) *A Mídia e a Modernidade - Uma teoria social da mídia*, Petrópolis, Vozes

Tratado da União Europeia (versão consolidada) como alterado pelo Tratado de Lisboa, de 13 de Dezembro de 2007. Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:FULL:PT:PDF

Viana, Vítor Rodrigues (2012) *Cibersegurança*, IDN Nação e Defesa nº 133

Viana, Vítor Rodrigues, (2012) *6ºSimpósio Internacional de Estratégia de Informação Nacional,* Academia Militar

Weber, Keith T. Horst, Shannon (2011) "Desertification and livestock grazing: The roles of sedentarization, mobility and rest", *Pastoralism*, Springer Journal. Disponível em: http://www.pastoralismjournal.com/content/1/1/19

"What is Cybercrime?", Norton, Symantec. Disponível em: http://us.norton.com/cybercrime-definition

Lista de Figuras e Tabelas