ACADEMIA MILITAR

DIRECÇÃO DE ENSINO

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O Papel dos Serviços de Informações no Combate ao Ciberterrorismo:

O CASO PORTUGUÊS

Sandra Núria Basto Perez do Amaral

Dissertação/Trabalho de Projecto para a obtenção do grau de

Mestre em Guerra da Informação

Lisboa

2014

ACADEMIA MILITAR

DIRECÇÃO DE ENSINO

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O Papel dos Serviços de Informações no Combate ao Ciberterrorismo:

O caso português

Sandra Núria Basto Perez do Amaral

Dissertação de Mestrado em Guerra da Informação

Trabalho realizado sob a supervisão:

Orientador Tenente Coronel Proença Garcia

Co-Orientador Coronel Fernando Freire

AGRADECIMENTOS

Este espaço é dedicado a todos os que contribuíram para que fosse possível alcançar mais um objectivo da minha vida, a finalização da dissertação para a obtenção do grau de mestre.

A todos os meus familiares, amigos e colegas que me acompanharam e me motivaram a prosseguir neste caminho nem sempre fácil, um muito obrigada.

No entanto, quero deixar uns agradecimentos a algumas pessoas especiais, sem as quais não teria conseguido certamente levar este barco, desta forma, ao seu destino:

- Ao meu orientador Tenente-Coronel Proença Garcia por ter aceitado desde o primeiro momento orientar a minha tese;
- Ao meu co-orientador Coronel Fernando Freire pela constante motivação ao longo de toda esta dissertação;
- À minha mãe Ana Perez, mãe é sempre mãe em todos os momentos da nossa vida, mas é muito bom ter-se uma mãe que, além desse papel, também é a amiga e a profissional com quem podemos discutir temas e repensar conceitos;
- Ao meu colega e amigo Dr. Armindo Reis Alves pelos preciosos conselhos, pelas longas horas de trocas de ideias e por ter sido um excelente professor, em termos jurídicos, nestes últimos anos;
- Ás minhas queridas amigas Carla Martins Costa, Carla Faria e Ana Rodrigues pela disponibilidade, a amizade é realmente um dos bens mais preciosos;
- Á minha querida amiga Susana Silva por ter feito todo este percurso comigo;
- Ao meu marido Miguel Amaral por existir na minha vida e me dar a estabilidade necessária para estes meus percursos.

Quando vejo uma criança, ela inspira-me dois sentimentos: ternura, pelo que é, e respeito pelo que pode vir a ser. Louis Pasteur

Dedico esta dissertação aos meus filhos Guilherme Amaral e Marta Amaral, não só por todo o tempo que lhes tirei, mas também por representarem a geração do futuro.

Geração essa que poderá, de alguma forma, sofrer todas as consequências de políticas e medidas mal elaboradas e/ou implementadas no contexto do ciberespaço.

Resumo

Quase sem nos apercebermos, a nossa vida em sociedade foi-se transferindo para um novo domínio, o ciberespaço, para onde também migraram todas essas estruturas que suportam o normal funcionamento dos Estados. À conta de um simples clique, deparam-se-nos facilidades e rapidez na resolução de situações e problemas do nosso quotidiano e no acesso à informação e ao conhecimento, abrindo-se novas oportunidades para o estabelecimento de novas relações interpessoais e de negócios.

Estas facilidades e oportunidades que o ciberespaço proporciona, não distinguindo quem a ele acede, trouxeram infelizmente consigo riscos que comprometem não apenas a segurança de pessoas e bens, a economia dos países mas, por vezes, até as próprias seguranças nacional e internacional. São eles os cibercriminosos, os ciberterroristas, os ciberespiões, os ciberrativistas e outros que utilizam igualmente o espaço cibernético para a prática de actos ilícitos e crimes.

De entre todos, os ciberterroristas, pela sua conotação com a violência, com as suas gravosas consequências e com os sentimentos de medo e de angústia que se criam e que caracterizam os actos terroristas, são os que mais têm vindo a preocupar os Estados, levando a que estes tenham definido ou procurem definir as suas políticas estratégicas de cibersegurança, visando a prevenção e o combate ao ciberterrorismo e, bem assim, de outros ataques e crimes cibernéticos. Portugal viu a sua Estratégia Nacional de Cibersegurança aprovada no corrente ano de 2014.

Não revelando-se fácil a destrinça nos crimes praticados por terroristas no ciberespaço, como sendo um de ciberterrorismo ou apenas de um cibercrime, um papel importante na sua detecção / prevenção cabe à *intelligence*, ou seja, aos Serviços de Informações, uma estrutura que dispondo de competências, aptidões e de *know how* específicos, sabe que para se derrotar o inimigo há que primeiramente conhecê-lo e vigiar de perto os seus movimentos.

Palavras-chave: Terrorismo; Ciberespaço; Ciberterrorismo; Cibersegurança; *Intelligence*

Abstract

Almost without us realising it, our life in society has been transferring itself into a new domain, the cyberspace, the place where all the structures which support the normal running of the structures have been migrating. With a simple click, we solve daily problems and access information with ease and speed, opening new opportunities to establish new interpersonal and business relationships.

The ease and the opportunities provided by the cyberspace, regardless of who uses it, have unfortunately brought risks that compromise not only the safety of people and property, the countries' economies but sometimes even national and international security. Those are the cybercriminals, the cyberterrorists, the cyberspies, the cyberactivists and others, who use cyberspace as well to commit unlawful acts and crimes.

Among them all, the cyberterrorists are the ones who are the biggest concern to the states, due to its association with violence, its serious consequences and the feelings of fear and anguish which they generate and which characterise terrorist acts. Therefore, these states have defined or try to define their political strategies concerning cybersafety, aiming to prevent and fight cyberterrorism and other cybernetic atacks and offenses. Portugal had its National Strategy for Cybersafety approved in the current year of 2014.

The unravelling of crimes committed by terrorists in cyberspace is not an easy task, it can be hard to tell the difference between cyberterrorism or a simple cybercrime, the Intelligence play an important role in tracing it and preventing it, a structure with specific skills, competences and know how that is aware that to defeat the enemy, first you have to know it and watch its moves closely.

Keywords : Terrorism; Cyberspace ; Cyberterrorism ; Cyber Security;Intelligence

Acrónimos e Abreviaturas

CIA - Central Intelligence Agency

CERT- Computer Emergency Response Team

CYBINT - Cyber Intelligence/Digital Network Intelligence-gathered from Cyber Space

DoS - Denial of Service

ENISA- European Network and Information Security Agency

FBI – Federal Bureau of Investigation

GEOINT -Geospatial Intelligence

GCS – Gabinete de Coordenador de Segurança

HUMINT – Human Intelligence

IC – Infra-estruturas Críticas

IIC - Infra-estruturas de informação críticas

MASINT - Measurement and Signatures Intelligence

NATO - North Atlantic Treaty Organization (Organização do Tratado do Atlântico Norte)

NSA – National Security Agency

OSINT - Open Source Intelligence

PJ – Polícia Judiciária

SEF – Serviço de Estrangeiros e Fronteiras

SIGINT - Signals Intelligence

SIRP – Sistema de Informações da República Portuguesa

SIS – Serviço de Informações de Segurança

SIED – Serviço de Informações Estratégicas de Defesa

SSI - Sistema de Segurança Interna

TECHINT - Technical Intelligence

TIC - Tecnologias de Informação e Comunicação

UCAT – Unidade de Coordenação Anti-Terrorista

ÍNDICE

Capítulo 1.

INTRODUÇÃO

***" A chamada "presciência" ou "previsão" não pode ser deduzida dos espiritos nem dos deuses, nem por analogia com os acontecimentos passados, nem por cálculos. Ela deve ser obtida por homens que conhecem a situação do inimigo." (*Sun Tzu)**

O fenómeno crescente da globalização e os acelarados avanços tecnológicos, no fundo, as duas faces de uma mesma moeda, impulsionaram, novas dinâmicas de mudança, nos contextos político, social e económico a nível mundial. Trazendo consigo, por um lado, novas formas de interacção e de relacionamento entre os Estados, favoráveis aos repectivos desenvolvimento e progresso, proporcionaram, por outro, fenómenos de homegenização e de interdependência criando-se um terreno propício, por vezes, a situações de fragilização e de dependência dos próprios Estados e, quase sempre, ao derrube das suas fronteiras para a entrada de todo o tipo de ameaças e de crimes, de entre os quais relevam os de natureza terrorista e cibernética, que foram ganhando cada vez mais acuidade, complexidade, sofistificação e imediatismo perante a maior crise económica e financeira das últimas decadas. (RCM nº19/2013)

Segundo o Conceito Estratégico de Defesa Nacional, uma das maiores ameaças à escala global é *o terrorismo transnacional e outras formas de extremismo violento, com impacto altamente desestabilizador*, assim como *o ciberterrorismo e a cibercriminalidade, tendo por alvo redes indispensáveis ao funcionamento da economia e da sociedade da informação globalizada.* Sucede que, estes riscos estão presentes também nas ameaças à segurança nacional, na medida em que, por um lado, *O terrorismo, uma vez que a liberdade de acesso e a identidade de Portugal como uma democracia ocidental podem tornar o país um alvo do terrorismo internacional* e por outro, *a cibercriminalidade, porquanto os ciberataques são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna*[1].

É exactamente esta preocupação que o ciberterrorismo deixa às sociedades modernas que me motivou, por um lado, a reflectir sobre a sua verdadeira dimensão e o realismo do seu impacto, correlacionando-o com os instrumentos legais disponíveis para o seu combate e,

[1] Resolução de Conselho de Ministro n.º 19/2013, publicado no Diário da República, n.º 67, de 5 de Abril de 2013, que aprova o Conceito Estratégico de Defesa Nacional, Parte III, n.º 3.1 - Ameaças e riscos no ambiente de segurança global

por outro, levou-me a ponderar sobre, como a falta de uma cultura de segurança digital em Portugal pode ser uma vulnerabilidade para a cibersegurança nacional.

Terrorismo define-se, na legislação portuguesa[2], como **"***todos os actos criminosos que 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***"**.

Já o ciberterrorismo parece ser entendido como *"ataques ou ameaças altamente nocivas feitas através de computadores por actores não-estatais, contra sistemas de informação, quando conduzidos para intimidar ou coagir governos ou sociedades em prol de objectivos políticos ou sociais. É a convergência de terrorismo para o ciberespaço, onde o ciberespaço se torna o meio de conduzir o acto terrorista. Ao invés de cometer actos de violência contra pessoas ou propriedades físicas, o ciberterrorista comete actos de destruição e perturbação da propriedade digital"*(DENNING,2006). No entanto, nem todos os actos de destruição e perturbação da propriedade digital podem ser considerados de ciberterrorismo, porque autores como Barry Collin (1980),são de opinião, desde a década de 80, de que aqueles têm de conseguir atingir o estado de *ciberterror*[3], ou seja, têm de ser suficientemente destrutivos e perturbadores para criarem o sentimento de medo que seja comparado àquele causado pelos actos de Terrorismo. As infra-estruturas críticas[4] certamente são os principais alvos de ciberterrorismo. Opostamente, há outros autores contemporâneos de Collin como Mark Pollit (1997), que considerava que estes tipos de ataques não seriam exequíveis. De facto, até ao momento, volvidos estes anos, ainda não foi registado, qualquer incidente que pudesse como tal ser classificado.

Sendo as TIC parte–vital integrante dos sistemas de comando e de controlo das infra-estruturas críticas que sustentam o normal funcionamento da nossa sociedade (serviços financeiros, produção e fornecimento de energia, transportes, serviços de emergência na saúde, serviços de produção e distribuição de bens alimentares, etc.) e estando também os governos electrónicos suportados nessas infra-estruturas críticas e informacionais tornaram-se estas um alvo apetecível para as organizações terroristas.

---

[2] Cfr. artigo 2º da Lei n.º 52/2003, de 22 de Agosto

[3] Cyterror – termo criado por Barry Collin em 1980 aquando a defesa da dinâmica do terrorismo na sua transcendia do físico para o virtual e a intercepção e convergência destas duas palavras.

[4] IC – Infraestruturas Criticas, IIC - infra-estruturas de informação críticas

De facto, vive-se numa época de mudança de paradigma social em que a vida das sociedades modernas se transfere do real para o virtual. Essa caixinha mágica permite ao cidadão e empresas interagirem com as autoridades e o Estado, com os outros, transferindo para elas parte da sua vida profissional, empresarial e social, e por isso o mundo virtual tornou-se um importante instrumento condutor do papel interventivo de cada um na sociedade. No meio desta riqueza de disponibilidades e sem se aperceberem, cidadãos, empresas, Estados tornam-se num alvo fácil, porque se vulnerabilizam ou porque possibilitam, ainda que inocente e ingenuamente, a ser pontos de ataques, quais zombies de uma qualquer rede criminosa, colocando em causa *in extremis* a própria segurança nacional.

Paralelamente, a procura de vantagens competitivas leva à convergência de países para programas que conduzam a uma melhor Sociedade de Informação explicitadas muitas vezes no desenvolvimento de (novas) infra-estruturas tecnológicas e de melhores e mais extensas acessibilidades aumentando-se com isso o potencial de ameaça do ciberterrorismo.

É assim que, aproveitando estas vulnerabilidades, e a quase total dependências nos meios tecnológicos, em todas as dimensões da vida em sociedade, as ciberameaças provenientes de grupos terroristas podem constituir-se, *um dos maiores potenciais riscos de ciberataques do futuro por factores de custo-benefício e outras vantagens a ele inerentes, nomeadamente o facto de causarem um significativo impacto psicológico sobre a sociedade e o público sob ataque. Enquanto o Terrorismo tradicional ataca num espaço físico e temporal limitado, o ciberataque parece sobretudo amplificar o impacto psicológico do terrorismo através do medo e da intimidação* (YORAM et al 2011**).**

Poderá não representar o maior perigo segundo Pollit (1997), pensamento que julga-se ainda actualizado, mas é um facto que são muitas as organizações terroristas com a sua presença no ciberespaço, quer seja, sobretudo, para a difusão das suas mensagens políticas, quer seja também para o recrutamento, propaganda, planeamento de acções, angariação de fundos e recolha de informação.

Em 1998, 12 das 30 organizações terroristas listadas no Departamento de Estado dos EUA tinham *websites* e em Janeiro de 2002, investigadores da Universidade de Haifa em Israel encontraram 29 *websites* de 18 organizações na lista do Departamento de Estado. Hoje, seria uma surpresa encontrar um terrorista que não tivesse presença na Web

(DENNING,2009).Em 2008 estimava-se a existência de cerca de 5000 páginas jiahadistas[5].

Não será por isso estranho que a utilização do ciberespaço seja equacionada como um "*vector privilegiado de condução de acções terroristas, tem vindo a assumir uma importância crescente para as sociedades ocidentais, obrigando os estados a rever os fundamentos das suas estratégias de segurança e defesa.* " (NUNES, 2004)

Diante deste enquadramento, cresce a consciência de que podemos estar perante algo novo no terrorismo e, obviamente, questiona-se sobre quais os melhores instrumentos para o seu combate. Sabe-se que, "*enquanto a maior parte dos criminosos quer viver para a sua causa, o enriquecimento, e não morrer por ela (…), alguns terroristas estão preparados para morrer pela sua causa. Este facto redirecciona novamente a tarefa da intelligence para a prevenção. Que por sua vez produz mais uma grande diferença entre o combater terroristas e o combater o crime, porque potenciais terroristas, especialmente no terrorismo doméstico, têm de ser parados antes de actuarem, a decisão de montar a operação tem de começar muito antes. Aos terroristas não pode ser permitido que ataquem, assim sendo têm de ser parados antes (TREVERTONT,2009)"*. Donde, colocam-se perguntas como: terão os ciberterroristas o mesmo perfil que os terroristas tradicionais ou convencionais? Ou serão meros executantes (nomeadamente especialistas) recrutados em regime de *outsourcing*[6] para estas funções específicas e pontuais sob a tutela de grupos terroristas? Serão os *crackers* os novos ciberterroristas (COLLIN,1997)? Será que existe mesmo ciberterrorismo? A prevenção é ajustada? Terá o ciberterrorismo o mesmo significado como é hoje entendido?

No mundo virtual parece que terrorismo (independentemente dos motivos que animam o seu executante) não requer que se morra por uma causa. Será suficiente, para o combate ao ciberterrorismo, dotarem-se os países de ferramentas que permitam a detecção de ataques aos seus sistemas de informação, especialmente os do Estado e das infra-estruturas críticas nacionais, bem como, equipá-los com os meios tecnológicos que lhes permitam gerir situações de crises no imediato? Ou não deve antes continuar-se a estudar os seus actores interpretando os sinais e os rastos que estes vão deixando ao longo dos seus percursos, para

[5] http://techpageone.dell.com/technology/mapping-the-dark-web-of-terrorist-sites/ consultado em 20 de Maio de 2014

[6] Uma técnica administrativa que possibilita o estabelecimento de um processo gerenciado de transferência, a terceiros, das atividades acessórias e de apoio ao escopo das empresas que é a sua atividade-fim, permitindo a estas concentrarem-se no seu negócio, ou seja, no objetivo final

o podermos combater e prevenir? E por outro lado tentar reduzir as vulnerabilidades dos Estados?

Se por um lado, é inquestionável todo o papel desempenhado pela *intelligence* na prevenção e no combate ao terrorismo, qual será o seu papel no ciberterrorismo? Será apenas o de fornecer TI de ponta para o seu combate?

O Conceito Estratégico de Defesa Nacional, num dos seus três Vectores e Linhas de Acção e de Estratégica relativamente ao exercício da soberania consagra, com vista à neutralização de ameças e riscos à Segurança Nacional, a valorização das informações estratégicas, defendendo que *o carácter imprevisível, multifacetado e transnacional das novas ameaças confirma a relevância das informações. Neste contexto, os serviços de informações constituem-se como incontornáveis instrumentos de identificação e avaliação de ameaças e oportunidades em cenários voláteis e complexos*[7]. Pergunta-se : E no combate ao ciberterrorismo qual será o papel dos serviços de informações?

No entanto, há que salientar que os vectores de ataque do ciberterrorismo podem ser considerados os mesmos que os do cibercrime, tendo em conta que o método em si, pode ser o mesmo. Além do mais, as inúmeras actividades ligadas à cibercriminalidade fazem com que se estabeleça, de alguma forma, uma fronteira muito próxima do fenómeno da cibercriminalidade ao do ciberterrorismo, pelo que cabe perguntar se este último não deverá ser tratado como cibercrime. Apesar de, até ao momento, não nos revermos totalmente nessa sobreposição é importante percepcionar como relevar a primazia da *intelligence* na prevenção do ciberterrorismo, diferenciando-a por exemplo da actuação da Polícia criminal (no caso português, a PJ)?

O Serviço de Informações de Segurança (SIS) é, no âmbito do SIRP, o único serviço que integra o elenco das Forças e Serviços de Segurança com competência para exercer funções de segurança interna (n.º 2 do art. 25.º da Lei 53/2008 - Lei de Segurança Interna. Compete-lhe recolher, processar e difundir informações no quadro da Segurança Interna, nos domínios da sabotagem, do terrorismo, da espionagem, incluindo a espionagem económica, tecnológica e científica, e de todos os demais actos que, pela sua natureza, possam alterar ou destruir o Estado de direito democrático, incluindo os movimentos que promovem a violência (designadamente de inspiração xenófoba ou alegadamente

[7] Resolução de Conselho de Ministro n.º 19/2013, publicado no Diário da República, n.º 67, de 5 de Abril de 2013, que aprova o Conceito Estratégico de Defesa Nacional, Parte VI, n.º 1.3. Valorizar as informações estratégicas

religiosa, política ou desportiva) e fenómenos graves de criminalidade organizada, mormente de carácter transnacional, tais como a proliferação de armas de destruição maciça, o branqueamento de capitais, o tráfico de droga, o tráfico de pessoas e o estabelecimento de redes de imigração ilegal[8].

A Polícia Judiciária tem na sua estrutura orgânica uma Unidade Nacional Contra o Terrorismo que, *tem competências em matéria de prevenção, detecção, investigação criminal e de coadjuvação das autoridades judiciárias relativamente aos seguintes crimes: a) Organizações terroristas e terrorismo; b) Contra a segurança do Estado, com excepção dos que respeitem ao processo eleitoral; (…)* [9], e, no que concerne à matéria do cibercrime,[10] a Polícia Judiciária tem competência reservada na investigação de crimes informáticos e praticados com recurso a tecnologia informática[11].

Encontramos, é certo, prevenção no SIS e na PJ. Não se trata propriamente de uma sobreposição, mas de abordagens distintas, em que a Polícia Criminal se preocupa sobretudo com a "prevenção do caso concreto ", ou seja quando existe um forte indício de acto criminal, e os Serviços de Informações se preocupam com a prevenção não só do que é previsível mas também com o que especulativamente pode acontecer.

Numa tentativa de se introduzir alguma coordenação em matéria de segurança no contexto do terrorismo, em território nacional, foi criado no âmbito do Ministério da Administração Interna (MAI),mais especificamente no seio do antigo Gabinete Coordenador de Segurança (GCS), a Unidade de Coordenação Anti-Terrorista (UCAT). Na UCAT, participam todas as entidades com competências específicas ou relevantes para a luta anti-terrorista, nomeadamente o Serviço de Informações de Segurança (SIS), o Serviço de Informações Estratégicas de Defesa (SIED), a Polícia Judiciária (PJ) e o Serviço de Estrangeiros e Fronteiras (SEF), podendo ainda nela participar uma qualquer outra força de segurança, desde que integradas no Gabinete Coordenador de Segurança (GCS), actualmente designado por Sistema de Segurança Interna (SSI).

Mas será que esta estrutura, que está implementada para o combate do terrorismo tradicional ou convencional, será adequada para o combate ao ciberterrorismo? A criação

[8] Página do SIS www.Sis.pt, revisitado em 20 de Maio de 2014
[9] Decreto-Lei n.º 42/2009. DR 30 SÉRIE I de 2009-02-12
[10] Lei do cibercrime Lei 109/2009
[11] Lei Nº49/2008 Artº7 de 27 de Agosto

do Centro Nacional de Cibersegurança[12], no âmbito de uma Estratégia Nacional de Cibersegurança, poderá alterar aquele enquadramento na especificidade ciber?

Como irá Portugal lidar com este novo fenómeno, tendo em conta que os ciberataques em larga escala às infra-estruturas críticas nacionais tornam-se hoje uma potencial ameaça de que os Estados se devem precaver?

Em que estado estão aos TIC em Portugal e qual a literacia digital (cultura de cibersegurança) da sua população para fazer face às crescentes ameaças?

Importa ainda deitar um olhar sobre como garantir a governação no combate ao fenómeno, partindo do pressuposto de que a cibersegurança nacional é nos tempos actuais o garante dos bens jurídicos fundamentais e do normal funcionamento de uma sociedade e do próprio Estado.

Que estratégia ou política nacional para o combate e prevenção do ciberterrorismo no seio de uma Estratégia Nacional de Cibersegurança?

É certo que neste contexto há também um papel e níveis de responsabilidade para a indústria, o meio empresarial, os cidadãos e Estado, mas queremos dar uma especial atenção ao papel que nelas desenvolvem os Serviços de *Intelligence* ou de Informações.

Relativamente ao fenómeno do ciberterrorismo será que os instrumentos que se encontram actualmente em vigor, precisam de ser reformulados à luz de um novo Conceito Estratégico de Defesa Nacional e da inovadora Estratégia Nacional de Cibersegurança, para que o combate seja eficaz?

É neste enquadramento e contexto de algumas incertezas/dúvidas quanto a respostas/soluções que emerge a minha motivação e a pertinência desta dissertação como uma reflexão sobre o assunto e uma tentativa de levantamento de recomendações. Tendo em consideração que o ciberterrorismo é uma possibilidade de ameaça às sociedades modernas, nem sempre latente e provavelmente nunca muito consequente, e que as capacidades de *intelligence*, quer de entidades públicas ou privadas, em proveito da prevenção transportam em si inúmeros mecanismos de resposta senti-me motivada, por força das competências adquiridas em análise de informações no meu contexto profissional, a refletir sobre o real impacto do ciberterrorismo e o papel do SIRP na resposta a estas ameaças. São assim objetivos desta dissertação os seguintes:

[12] O Centro Nacional de Cibersegurança é a entidade responsável pela área de Segurança do Ciberespaço e constitui-se no Artº 2 A Republicação do Decreto-Lei n.º 3/2012, de 16 de Janeiro com as alterações do DL n.º 69/2014, de 09 de Maio

Nesse sentido foi levantada como questão principal (QP) a responder:

- Será o Serviço de Informações o órgão competente para prevenir e combater o ciberterrosimo?

Desta derivam questões subsidiárias (QD) como:

- QD1: Será o Ciberterrorismo uma nova forma de terrorismo?

- QD2: Qual o papel da *Intelligence* na prevenção e combate ao ciberterrorismo?

- QD3 : Qual o papel da *Intelligence* na estratégia de cibersegurança de outros países?

- QD4 : Quais as maiores vulnerabilidades de Portugal ?

Subsequentemente levantamos como hipóteses para validar aquilo a que nos propomos refletir as seguintes:

H1 – O ciberterrorismo não é uma ameaça premente

H2 – A *Intelligence* é principal arma de prevenção e combate do ciberterrorismo

H3 – O factor humano é a principal vulnerabilidade do Estado Português

Metodologia

A opção de metodologia recaiu em realizar-se um estudo de carácter descritivo, baseado na análise documental, bibliográfica, quer de fontes nacionais, quer de fontes internacionais.
Deste modo, a dissertação vai-se desenvolvendo ao longo de 5 capítulos, em que falaremos de conceitos sobre o Terrorismo, o Ciberespaço, o Ciberterrorismo e a Cibersegurança.
Com efeito, procedeu-se ao levantamento do estado da arte nos conceitos chave para este trabalho, ou seja, sobre “Terrorismo”, “Ciberespaço” e “Ciberterrorismo”, e também através da revisão da literatura, de forma a ficarmos munidos dos fundamentos que permitam alicerçar as exposições ao longo do seu desenvolvimento. Consideramos que as obras citadas ao longo da dissertação, necessariamente não as únicas para uma ampla e profunda revisão da bibliografia que seria a desejável mas não exequível, constituem em nosso entender o mínimo indispensável para a realização de um trabalho desta natureza.

Far-se-á uma breve “incursão” sobre que é feito noutros países, em especial daqueles que já dispõem das suas políticas de cibersegurança, para permitir que se retirem orientações e ensinamentos de boas práticas. Na impossibilidade de se contemplarem todos os países, as opções recaíram nomeadamente sobre a Alemanha o Reino Unido e os Estados Unidos América por se revelarem os países mais completos nesta matéria de cibersegurança, mas também sobre a Espanha pela sua proximidade geográfica e pela França pelos conceitos e estrutura da sua estratégia.

Capítulo 2.

DO TERRORISMO AO CIBERTERRORISMO

Pode dizer-se que para o Homem do Séc. XXI o termo Terrorismo traz-lhe de imediato à mente imagens dantescas associadas a destruição de propriedades e de outros bens, a perdas de vidas humanas, a crianças estropiadas e órfãs, a velhos abandonados e vagueando sem norte pelas ruas, a escassez ou falta dos bens essenciais à sobrevivência humana, enfim, imagens essas que os média por vezes não se inibem de explorar visando o aumento das suas audiências.

Pode dizer-se, no fundo, que essas imagens que o Homem do Séc. XXI retém e conserva, vai ao encontro da estratégia das organizações terroristas que procuram, através da instalação de um clima de medo e de insegurança, satisfazer os propósitos que as animam, porque sabem que de outra forma estes seriam mais dificilmente alcançados, por limitações de ordem financeira e humana.

Com a gradual abertura do ciberespaço à comunidade global, indistintamente dos factores nacionalidade, raça, religião, credo e origem social de cada um, também os terroristas encontraram nele um terreno fértil para a prossecução dos seus objectivos. No ciberespaço, e mediante recurso às tecnologias de informação e comunicação, fazem a propaganda às suas ideologias, procuram recrutar novos membros e simpatizantes, estabelecem o diálogo entre si, preparam as suas acções e procuram angariar fundos para as suas causas. E, tal como um qualquer cibernauta também acompanharam as novas formas de comunicação na internet, aderindo igualmente às chamadas redes sociais.

Os incidentes que tiveram lugar em Nova Iorque, em Madrid e em Londres, em datas não tão remotas, e perpetrados por organizações terroristas, levaram, porém, os Estados a centrar a sua atenção em possíveis e eventuais actos terroristas a serem cometidos através do ciberespaço, visando principalmente a destruição das suas infra-estruturas críticas.

Com isso, introduziu-se no léxico internacional o termo ciberterrorismo que se confunde, grosso modo, com os crimes cometidos por terroristas no ciberespaço, mediante recurso a meios informáticos. No entanto, a questão que se coloca é a de saber se um qualquer crime praticado no ciberespaço por terroristas será, *tout court*, classificado como sendo um acto de ciberterrorismo, ou se, tem este assumir determinadas características especiais para que como tal possa ser considerado, e se ciberterrorismo será para já uma ameaça premente.

É o que seguidamente se irá desenvolver.

2.1 TERRORISMO

"A diferença entre o revolucionário e o terrorista reside nos motivos pelo qual cada um se bate. Pois é impossível chamar de terrorista aquele que defende uma causa justa, que se bate pela liberdade, pela libertação de sua terra de seus invasores, dos colonos e dos colonialistas." (Arafat in Lessa e Suppo, 2003)

Segundo o Departamento do Estado dos Estados Unidos da América, mais de 10.000 pessoas foram mortas por actividades terroristas em 2012. O Afeganistão, ocupante do primeiro lugar na lista, com mais de 2.500 mortos é seguido pelo Iraque, pelo Paquistão ,pela Nigéria e pela Rússia, em quinto lugar, com mais de 650 mortos (SILVA e NELMON 2014).

Depois de mais de trinta anos de pesquisas e estudos, ainda não existe uma definição precisa, abrangente e consensual sobre o termo terrorismo, conclui Walter Laqueur do Centro Estratégico de Estudos Internacionais (Center for Strategic and International Studies) (SCHIMD,2004).

Apesar de ser um termo corrente e usual nos média, podendo até ser considerado um dos termos mais mediáticos dos últimos tempos, não existe para a generalidade das pessoas um entendimento preciso sobre o fenómeno do Terrorismo (HOFFMAN,2006). Existem, desde 1936 até à actualidade, cerca de 110 definições sobre o termo.

Através de uma consulta aos dicionários *online* verificamos que a sua definição não é fácil, nem clara. Se num dicionário aparece definido como"*Conjunto de actos de violência cometidos por agrupamentos revolucionários*"[13], noutro aparece como *" prática de actos violentos com fins políticos*"[14] e, noutro ainda, como"*prática de atos violentos (assassinatos, raptos, colocação de bombas, etc.) contra u m governo, uma classe dominante ou pessoas desconhecidas, com o objetivo de fazer impo r determinados objetivos, geralmente políticos*"[15]. Em comum apenas têm a prática de actos violentos. Ora, se numa visão simplista do conceito não existe uma definição única, no campo académico essa definição torna-se muito mais complexa.

[13] "terrorismo", in Dicionário Priberam da Língua Portuguesa [em linha].http://www.priberam.pt/dlpo/terrorismo [consultado em 02-11-2013].
[14] http://www.lexico.pt/terrorismo/ [em linha]. [consultado em 02-11-2013].
[15] *terrorismo* In Infopédia [Em linha]. Porto: Porto Editora, 2003-2013. [Consult. 2013-11-02]. Disponível em: http://www.infopedia.pt/lingua-portuguesa/terrorismo>.

O termo surge originariamente em França, durante a Revolução Francesa de 1789, para caracterizar o "*regime de la terreur*" que se viveu entre 1793-1794. Esse regime foi marcado por execuções e perseguições frequentes e arbitrárias contra os que se opunham ao regime. Esse regime de terror foi legitimado pelo governo revolucionário como uma forma de consolidação do poder, através da criação de um sentimento de intimidação com o intuito de evitar uma qualquer eventual tentativa de contra-revolução (VENTURA et al, 2001).

Embora nos séculos seguintes o termo terrorismo tenha sido conotado ora com o terror provocado por pequenos grupos revolucionários, ora pelo terror provocado por governos autoritários, no entanto, o seu conceito ficou sempre ligado ao que lhe deu origem: "acto de provocar terror", aquando da Revolução Francesa.

É na década de 60/70 do século XX que o terrorismo começa a tomar maiores proporções na Europa com o aparecimento da ETA em Espanha, do IRA na Grã-Bretanha, com as Brigadas Vermelhas em Itália e com as Banden Meinhof na Alemanha. E com estes novos movimentos surgem também novas formas mais violentas de terror como o uso, por exemplo, de cartas armadilhadas e carros bomba.

"*Depois dos atentados de 11 de Setembro, nos EUA, o terrorismo deixou de ser um fenómeno de natureza nacional ou regional, como o IRA ou a ETA. Passou para uma escala internacional, adquirindo uma categoria transnacional* (MARCHUETTA,2012)."

Segundo Hoffman (2006), o fenómeno terrorista é definido por via da construção e exploração do medo, essencialmente através da violência e da intimidação, de forma a fomentar determinadas modificações políticas, sociais, étnicas e/ou religiosas. Sendo o medo uma característica intrínseca e associada ao movimento terrorista, o impacto mais visível da globalização no terrorismo foi a mundialização do medo e alarme social, visto que esta é uma das grandes armas que o terrorismo moderno tem ao seu lado, senão a principal (CARDOSO, 2011).

O terrorismo pode ser considerado como:

- um sistema organizado de extrema e violenta intimidação, de forma a criar instabilidade nos regimes, democráticos ou não (TACKRAH,1987);

- qualquer ação que vise matar ou afetar seriamente civis desarmados ou não-combatentes, com o objetivo de intimidar a população ou compelir a ação de qualquer Estado ou Organização Internacional (KOFI ANNAN[16]);
- ou como uma forma premeditada de violência política, perpetrada por grupos subversivos, ou agentes clandestinos, contra alvos civis, com a finalidade de atingir vasta audiência (Departamento de Estado Norte Americano[17])
- ou ainda como o uso ilícito de força ou violência contra pessoas ou propriedades, de forma a intimidar ou coagir um Governo, a população civil ou outra qualquer dimensão da sociedade, na prossecução de objectivos políticos ou sociais (Federal Bureau of Investigation-FBI).

Segundo a NATO o terrorismo é definido como "*o uso ou ameaça do uso ilegal da força ou da violência contra pessoas ou propriedades com a intenção de condicionar ou intimidar os governos ou sociedades para conseguir objectivos políticos, religiosos ou ideológicos(*AAP-6)".

Também uma definição de terrorismo surgiu no Conselho da União Europeia em 2001, com base num conjunto de acções que poderiam estar incluídos no conceito de agressão terrorista. Acções ou actos intencionais que, pela sua natureza e contexto, podem atingir seriamente um País ou uma organização internacional - tal como se define agressão em termos nacionais - cometidas com o propósito de intimidar seriamente a população, persuadir de forma determinante um governo ou organização internacional para levar a cabo ou omitir determinada acção, ou desestabilizar seriamente ou destruir a política constitucional ou económica, ou as estruturas sociais do País ou Organização internacional.[18]

A falta de uma visão global do fenómeno e, principalmente, de uma definição consensual levou a que Alex Schmid e Jongman fizessem um estudo qualitativo sobre 109 definições de terrorismo, em que era medida a percentagem de referências ao uso de determinadas palavras e expressões dentro das definições do fenómeno e, após uma análise, chegaram à seguinte conclusão

Frequência dos termos referidos:

1. Violência, força 83.5 %

[16] Newsletter, IDN , AGO/SET2005, p.2
[17] USDS 1999, US Department of State, *Patterns of Global Terrorism* - 1998, Washington, DC, 1999.
[18] Council of the European Union: Council Common Position on Combating Terrorism, 27Dec2001

2. Política 65 %

3. Medo, terror enfatizado 51 %

4. Ameaça 47 %

5. Efeitos psicológicos e antecipação das reacções 41.5 %

6. Diferenciação do grupo alvo das vítimas 37.5 %

7. Acções planeadas, sistematizadas e organizadas 32 %

Assim, para estes autores, uma possível definição para terrorismo seria: "*um método de acção marcado pelo sistemático recurso à violência, empregue por indivíduos ou grupos semiclandestinos ou Estados, motivados por razões criminosas ou políticas onde – em contraste com o assassinato – o objecto da violência não corresponde ao alvo da acção. As vítimas imediatas podem ser escolhidas de forma randómica (oportunidade) ou selectiva (representativa ou simbólica) no interior de uma população alvo, servindo como geradores de mensagem. Processos de comunicação baseados na ameaça e violência entre organizações terroristas, as vítimas e os alvos são utilizados para manipular estes últimos, transformando-os em receptores de demandas ou atenção dependendo do objectivo primário da acção, intimidação, coerção ou propaganda*." (SCHIMD & JONGMAN)

A definição académica de terrorismo aceite pelas Nações Unidas, foi adaptada por Alex P. Schmid onde afirma que dada a complexidade e diversidade de perspectivas que existem sobre o terrorismo, não é possível definir adequadamente com uma só definição, sobre o que ocorre com o uso de violência ou a sua ameaça, a que se chama de terrorismo. O terrorismo é um método de reiterada acção violenta inspirada na angústia, utilizado por pessoas, grupos ou Estados, de forma clandestina, por razões idiossincráticas, criminosas ou políticas, por meio das quais - a diferencia do assassinato - o objectivo imediato da violência não corresponde nem o é objectivo final.

Há ainda quem defina o terrorismo como um *método premeditado, politicamente motivado, comunicador de violência ou uma ameaça de violência contra não-combatentes em que as mortes das vítimas têm um valor mais psicológico do que estratégico-funcional e que procura influenciar uma terceira parte, geralmente a parte que dirige a comunidade que é alvo das acções (MAGALHÃES,2004).*

Na verdade, a falta de consenso entre a comunidade académica não se deve unicamente à dificuldade de caracterização do respectivo conteúdo, sendo que hoje já se discute também se, na realidade, existe alguma importância na existência de um conceito sobre o termo. Se, por um lado, uns consideram a existência de um conceito meramente dispensável, outros,

como Ganor (2010) consideram que a importância de um conceito universal é indiscutível para a adopção de políticas para o seu combate.

A importância da sua definição centra-se no facto de se permitir a construção de estratégias comuns, possibilitando-se deste modo a mobilização internacional na sua luta, e no reforço de tratados internacionais e eficazes procedimentos de extradição. Segundo Jessica Stern, da Universidade de Harvard a forma como se definir o conceito irá influenciar de algum modo a forma como será o combate, tendo em conta que se vai definir que dados irão ser recolhidos e analisados para a percepção e prevenção do fenómeno.

A não existência de uma definição consensual sobre o termo também se deve de facto de que a sua acreditação acarreta o risco político de se ter de tomar posições concretas. O que sucede é que, muitas vezes, os seus valores políticos se sobrepõem ao valor legal e, por vezes o terrorismo adequa-se aos interesses particulares dos Estados em determinados períodos e circunstancialismos específicos. A título de exemplo, os "Taliban" e Osama Bin Laden que foram em tempos considerados lutadores da paz (mujahideen) e apoiados pela CIA quando resistiam no Afeganistão contra a sua ocupação pela União Soviética, hoje em dia estão no topo da Lista dos Terroristas Internacionais. A repercussão da actual corrente sobre a preponderância do valor política sobre o valor legal relativamente ao Terrorismo é elevado, levando a que a guerra contra o terrorismo seja selectiva, incompleta e ineficaz (ZEIDAN,2004).

Por outro lado, existe uma falta de uma definição clara entre o que são as lutas legítimas dos povos pela autodeterminação e os actos de terrorismo. E a falta de clareza com que cada um analisa os seus actos, e os interesses intrínsecos que neles persistem, leva a que se legitimem acções de Terrorismo como sendo de Contra-Terrorismo e a captura de reféns como tratando-se de detenções. Segundo Patrícia Eugenia Kreibohm, na óptica de análise das relações internacionais, não raramente aquele que é considerado como terrorista por alguns Estados é geralmente saudado como lutador da liberdade por outros, o que decorre do facto de que a aplicação do termo terrorismo depende do ponto de vista que foi utilizado para analisá-lo e dos próprios interesses, ideias e emoções de seu analista. (KREIBOHM, 2005).

"[...] o termo 'terrorismo' evoca, em linguagem corrente, uma violência extrema, vítimas inocentes, um clima de angústia. Ele remete ao fanatismo e à barbárie. Desde então, ele é frequentemente utilizado para desqualificar o adversário e mobilizar a opinião pública ao seu encontro. Devido a este fato, torna-se difícil defini-lo sem condenar ou absolver, como

testemunham os debates concernentes à ação dos movimentos de libertação nacional e de secessão ou as discussões sobre o terrorismo de Estado.(GUILLAUME,2004)"

Até à data, nenhum instrumento internacional conseguiu com êxito definir o termo terrorismo, embora exista um conjunto de tratados que procuram a repressão de actos terroristas. Tais actos são usualmente tratados em função da acção que foi praticada, seus objectivos e consequências, o que reflecte o mal-estar internacional causado pelo terrorismo como crime internacional (BRANT, 2005).

Uma clara definição de terrorismo proporcionaria não só condições para o estabelecimento de medidas mais eficazes para o seu combate a nível internacional, como também impediria que certos Estados se aproveitassem da imprecisão do termo para qualificar de terrorismo qualquer comportamento ou actuação contrária aos seus interesses, utilizando aquele argumento como justificação para a adopção de respostas, muitas vezes desenvolvidas à margem das Nações Unidas, do Direito Internacional e do Direito Internacional dos Direitos Humanos, como sendo medidas "contraterroristas" ou "antiterroristas".

Pode-se então afirmar que uma tipificação do terrorismo acabaria por proteger duplamente a paz e a segurança internacionais, na medida em que, de forma concomitante, permitiria uma resposta mais eficiente ao flagelo terrorista e impediria a apropriação indevida de tal expressão como justificativa para a adopção de procedimentos unilaterais de represálias (SOUKI).

Torna-se premente, por tudo isto, a adopção de uma definição de terrorismo que seja aceite pela comunidade internacional por forma a reduzirem-se as tensões entre as nações e resolverem-se as crises internacionais.

A utilização do ciberespaço como vector privilegiado de condução de acções terroristas, tem vindo a assumir uma importância crescente. No entanto, a utilização de uma nova arma ou de uma inovação tecnológica para a criação de uma vulnerabilidade estratégica não poderá ser considerada como inovadora (dele próprio) (NUNES,2004).

Muitas são as organizações terroristas com presença no ciberespaço, algumas aparecem de forma explicita outras só são pesquisáveis e acedidas pelos seus membros. O ciberespaço é utilizado para os mais diversos fins, desde recrutamento, propaganda, planeamento de acções, angariação de fundos, recolha de informação e recentemente para o Ciberterrorismo.

É a face do novo terrorismo, um jogo mental que aplica as técnicas violentas do "mundo antigo" às realidades e vulnerabilidades do novo mundo altamente sofisticado e tecnológico. Longe vão os tempos onde as únicas vítimas eram as que, por infortúnio, se encontravam em locais onde ocorriam os atentados. O terrorismo agora é inteligente, bem planeado e direccionado para atingir as bases electrónicas de uma nação (VERTON,2003).

2.2 CIBERESPAÇO

O crescimento sustentado da internet proporcionou a consciencialização dos cidadãos de todo o mundo para a existência de uma nova dimensão virtual, o ciberespaço, que desempenha actualmente um papel central na reformulação das interacções sociais, económicas, culturais que ocorrem numa escala que é global.

Se inicialmente a rede existia apenas como suporte para a partilha de informações, hoje em dia tornou-se um bem essencial de que dependem as infra-estruturas criticas, as áreas comerciais, sociais, industriais entre outras.

Estima-se que estejam ligadas à rede mais de dois biliões de pessoas (2,405,518,376 [19]), um terço da população mundial. Em 2012 cerca 8.7 biliões de dispositivos estavam ligados à rede e estima-se que em 2015 serão 15 biliões[20] de dispositivos ligados.

Desaparece o conceito de território definido através da ideia de controlo sobre fronteiras, podendo essas serem físicas, sociais, simbólicas e culturais. Passa-se a viver uma realidade distinta, na qual as barreiras espaciais, temporais e geográficas já não são tão significativas, quando as redes globais de intercâmbios conectam e desconectam indivíduos, grupos, regiões e até países sob os efeitos globalizantes provenientes da pós-modernidade e/ou modernidade tardia ou alta modernidade (CORRÊA,2004).

"A elevada sofisticação tecnológica e globalização, em todas as suas vertentes, geraram (…) as novas sociedades que são constituídas por células ligadas em rede, que se interconectam em esferas circulares que se vão ampliando (…). A consequência principal, em termos de relações sociais, económicas e políticas, foi uma acentuada

[19] http://www.internetworldstats.com/stats.htm consultado em 15 Abril de 2014

[20] How Many Things Are Currently Connected To The "Internet of Things" (IoT)? Consultado em 10 Abril de 2014 http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/

interdependência entre actores individuais e colectivos, o que imprime uma característica reverberatória a todo o impulso aplicado sobre uma ou poucas células, que se vai amplificando, multiplicando-se em todas as direcções e a grandes distâncias – nos espaços tradicionais, portanto em termos geográficos, e nos novos espaços (SANTOS, LOUREIRO, 2009).”

As prática sociais emergentes com as novas tecnologias de informação e comunicação colocam-nos numa cultura de interconexão generalizada, criando novas formas de mobilidade social e de apropriação do espaço urbano, abrindo-se as portas à criação de uma cibercultura.

Pode-se, com toda a veleidade, enaltecer as possibilidades fantásticas potenciadas pela globalização da informação, desde as que se referem ao valor acrescentado trazido pelas novas tecnologias às que significam uma abissal modificação dos hábitos de vida (um cidadão no mais recôndito ponto do mundo pode aceder a sofisticadas bases de dados ou consultar online os mais reputados especialistas) (CUNHA,1999). Vive-se, então, numa época de mudança de paradigma social em que a vida das sociedades modernas se transfere do real para o virtual, em que as conversas de café deixam de o ser no espaço físico e passam para o espaço cibernético, para as denominadas redes sociais que são, de uma maneira geral, páginas da web que facilitam a interacção entre os membros dispersos pelos mais diversos locais. São usualmente integradas por indivíduos com valores e interesses comuns e com vontade de partilhar informações. O objectivo destas redes é proporcionar diferentes meios de interacção entre pessoas separadas geograficamente por milhares de km de distância, que, à velocidade de um clique, ultrapassam a barreira do tempo e do espaço.

Essa busca de partilha por indivíduos e grupos com interesses comuns, faz com que se criem autênticas comunidades virtuais. O computador, uma ferramenta quase indispensável para a actual vida laboral, académica e funcional de qualquer cidadão, começa a ser utilizada não só para o lazer como também para colmatar as falhas da sociabilização que o stress diário lhes impõe, deixando de ser encarado como mero um utensílio, para ser apreciado como uma extensão da sua própria vida. No fundo, preenchem um vazio há muito deixado pela agitada vida que rodeia o seu quotidiano, e perda de identidade cultural fruto de uma rápida globalização, onde o tempo real não acompanha as necessidades sociais do indivíduo, permitindo não só o intercâmbio com os amigos, como também

reencontrar velhas amizades perdidas no tempo e no espaço. Tudo isto tornam as redes sociais atractivas, e, mesmo, valiosas sob o ponto de vista emocional. As pessoas aderem a elas de "braços abertos", partilhando informações, vídeos, fotografias. O deslumbramento e a mais valia obtida é tal, que as pessoas quase não se questionam sobre a questão de segurança, confiantes de que tudo o que partilham se restringe ao seu grupo de amigos.

Com o desenvolvimento das novas tecnologias, torna-se possível a constituição de um espaço de interconexão entre diversas pessoas, em diferentes lugares do mundo, em tempo real, fazendo não só uso apenas do som , como também de imagens, textos, vídeos, entre outros recursos que privilegiam a interatividade. Estas tecnologias permitiram compreender e incluir, no dia-a-dia, dinâmicas de comunicação, através de equipamentos conectados à Internet, sejam eles computadores, tablets ou smartphones.

As auto-estradas da informação são hoje em dia uma realidade ligando todos os povos e tornando o mundo, como disse Marshall McLuhan, numa "*Aldeia Global*" com um ponto comum: o ciberespaço (BATISTA & RIBEIRO,2010).

O ciberespaço tornou -se o sistema "nervoso" de controlo de um país. Negócios, actividades da Administração Publica (AP) e dos governos e a Defesa operam em significativa parte dele, constituindo uma rede interdependente assente numa infra-estrutura tecnológica de comunicações e informação (VICENTE & CALDAS,2013).

Ao contrário de outros termos do meio informático, o ciberespaço não tem uma definição objectiva, tomando-se como princípio de que é um conceito abstracto para descrever o mundo virtual da era digital. Descrever o ciberespaço como sendo apenas a internet é desprovê-lo de todo um conteúdo de relações múltiplas que o mundo virtual compreende.

O termo ciberespaço surgiu pela primeira vez pela mão de William Gibson, em 1983, numa história de ficção científica onde *o ciberespaço, é uma representação física e multidimensional do universo abstracto da 'informação'. Um lugar pra onde se vai com a mente, catapultada pela tecnologia, enquanto o corpo fica para trás*: *Uma alucinação consensual vivida diariamente por bilhões de operadores autorizados, em todas as nações, por crianças aprendendo altos conceitos matemáticos... Uma representação gráfica de dados abstraídos dos bancos de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz abrangendo o não-espaço da mente; nebulosas e constelações infindáveis de dados. Como marés de luzes da cidade (MONTEIRO,2007).* Só na década de 90 começam a surgir definições menos ficcionadas e, no Dicionário de Comunicação, 2001, é definido como "*um espaço cibernético, um universo virtual*

formado pelas informações que circulam e/ou estão armazenadas em todos os computadores ligados em rede, especialmente a Internet; uma dimensão virtual da realidade, onde os indivíduos interagem através de computadores interligados. Ao falarmos em ciberespaço é comum pensar em algo que não é palpável, algo imaterializado, um lugar distante de nossa realidade, onde relações sociais, culturais, económicas ao se estabelecerem se fazem no imaginário, um ambiente futurístico (RABAÇA et al 2001)".

Já o filósofo francês Pierre Levy define o ciberespaço como o *espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores."* O autor afirma, ainda, que: *Essa definição inclui o conjunto dos sistemas de comunicação electrónicos (aí incluídos os conjuntos de rede hertzianas e telefónicas clássicas), na medida em que transmitem informações provenientes de fontes digitais ou destinadas à digitalização. Insisto na codificação digital, pois ela condiciona o carácter plástico, fluido, calculável com precisão e tratável em tempo real, hipertextual, interactivo e, resumindo, virtual da informação que é, parece-me, a marca distintiva do ciberespaço. Esse novo meio tem a vocação de colocar em sinergia e interfacear todos os dispositivos de criação de informação, de gravação, de comunicação e de simulação. A perspectiva da digitalização geral das informações provavelmente tornará o ciberespaço o principal canal de comunicação e suporte de memória da humanidade a partir do próximo século (*LEVY,1997*).*

Tendo em conta que todos estes conceitos trazem consigo uma certa carga política, também o conceito de ciberespaço se altera consoante o País que o define. Em 2001, a definição de ciberespaço pelo Departamento de Defesa dos Estados Unidos da América limitava-se a um possível ambiente em que a informação digitalizada era comunicada através de redes de computadores[21]. No entanto, em 2003, a Casa Branca definiu o ciberespaço como um sistema nervoso – o sistema de controlo do país, composto por centenas de milhares de computadores, servidores, comutadores, encaminhadores e cabos de fibra óptica interligados que permitia que as infraestruturas críticas funcionassem. [22]

[21] **Dictionary of Military and Associated Terms** [Em linha]. Washington D.C.: Department of Defense, 2010. [Consult. 21 Março 2014]. Disponível em: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

[22] https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf consultado em 14 de Abril de 2014

Para os ingleses, o ciberespaço é um domínio interactivo, composto por redes digitais, que é utilizado para armazenar, modificar e comunicar informação. Inclui a internet, mas também outros sistemas de informação que suportam o mundo empresarial, as infra-estruturas e serviços. Redes digitais essas, que também já suportam o fornecimento de energia e água às nossas casas, ajudam na organização de entregas de comidas e outros bens, e actuam como ferramenta essencial para o desenvolvimento empresarial em todo o Reino Unido. O seu raio de acção aumenta à medida que nos vamos conectando cada vez os equipamentos às redes, nomeadamente as televisões, consolas e até electrodomésticos[23].O Reino Unido com uma população de 63,742,977 (dados de 2014) tinha em 2011, 52,731,209 utilizadores de internet[24].

Na Alemanha, o ciberespaço é definido como: espaço virtual de todos os sistemas de TI ligados a nível de dados numa escala global. A base do ciberespaço é a Internet como uma rede de conexão e transporte universal, acessível ao público, que pode ser complementada e expandida por qualquer número de redes de dados adicionais.[25].

Para os espanhóis, o ciberespaço é o nome dado para o domínio global e dinâmico composto pelas infra-estruturas de tecnologia da informação - incluindo a Internet - redes e sistemas de informação e telecomunicações[26].

Já os Franceses, consideram o ciberespaço como a nova Torre de Babel, onde as várias culturas mundiais são partilhadas e as informações circulam em tempo real[27], considerando ainda que a exclusão do mundo digital leva a que os indivíduos sejam condenados ao isolamento, as empresas sejam arruinadas e as nações se tornem dependentes. Definem o ciberespaço como o espaço de comunicações criado pelas interconexões mundiais processadas por equipamentos digitais automatizadas.

---

23 The UK Cyber Security Strategy , Protecting and promoting the UK in a digital world , November 2011 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf - consultado em 30 de Abril 2014

24 http://www.internetworldstats.com/europa.htm consultado em 20 de Abril de 2014

25 CyberSecurityStrategyforGermany consultado em 30 de Abril 2014https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile

26 Cyber Security Strategy for Spain http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_ESen.pdf consultado em 30 de Abril 2014

27 Information systems defence and security France's strategy http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf consultado em 30 de Abril 2014

Curiosa é definição húngara que chega à precisão de definir o seu próprio ciberespaço: ciberespaço significa o fenómeno combinado de sistemas de informação electrónicos, descentralizados e globalmente interconectados, assim como os processos sociais e económicos que utilizam e se incluem nesses sistemas em forma de dados e informações. O ciberespaço húngaro inclui as partes dos sistemas electrónicos de informação do *e-governement* ciberespaço global, que estão localizados na Hungria, assim como os processos sociais e económicos que aparecem através dos sistemas electrónicos do ciberespaço global, na forma de dados e informações que ocorrem ou são direccionados para ou afectar a Hungria [28].

Apesar das suas potencialidades, o ciberespaço passou também a ser uma oportunidade para as organizações criminosas. No seu início, unicamente para as actividades ilícitas e lucrativas e para o financiamento de actividades terroristas, mas hoje em dia, com o crescente fenómeno do tornou-se ainda mais apetecível para as organizações criminosas e terroristas que a ele poderão deitar mão uma vez que os ciberriscos tornaram-se importantes para causar danos no que respeita às infra-estruturas de informação críticas, executando as acções a custos bem mais reduzidos.

2.3 CIBERTERRORISMO

Tendo em conta que o Ciberterrorismo é *a convergência entre o terrorismo e o ciberespaço*[29] (COLLIN, 1980), a dificuldade de se encontrar uma definição única e consensual sobre o que se entende por ciberterrorismo é a mesma da que se referiu relativamente ao conceito de terrorismo ou mesmo de ciberespaço. O facto do significado do termo ter diferentes definições de acordo com uma série de interesses e o facto de *o terrorista para uns ser o lutador pela liberdade para outros* (PRICHARD & MACDONAL,2004) leva a que dificilmente seja encontrada uma estratégia global para o seu combate, limitando-se os Estados a, cada um por si, criar mecanismos para a sua hipotética prevenção.

[28] National Cyber Security Strategy of Hungary - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/HU_NCSS.pdf consultado em 15 de Maio de 2014

[29] Conceito introduzido pela primeira vez na década de 80 por Barry Collin , "*The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge*",

O termo ciberterrorismo está geralmente associado a ataques e ameaças que, mediante recurso a meios informáticos, produzam ou venham a produzir danos elevados a infraestruturas críticas e a sistemas de informação. São ataques e ameaças feitos por actores não-governamentais[30] com o intuito de coagirem governos ou a sociedade visando atingir objectivos políticos e sociais. É a convergência entre o terrorismo e o ciberespaço, onde este último aparece como a via e/ou local de perpetuação de actos terroristas. Ao invés de cometer a violência directa contra pessoas e espaços físicos, como acontece com o Terrorismo tradicional ou convencional, no ciberterrorismo cometem-se actos de destruição contra a propriedade digital. Para ser considerado como ciberterrorismo, do ataque têm de resultar violência contra pessoas ou propriedades ou pelo menos causar danos "psicológicos" que venham a gerar o medo como sejam por exemplo: ataques que levem à existência de mortes, ferimentos graves, explosões, queda de aviões, contaminação de águas ou perdas económicas em grande escala. Ataques a infra-estruturas críticas com danos sérios ou disrupções podem ser considerados ciberterrorismo dependendo, no entanto, do seu impacto. Ataques que incidam sobre estruturas não essenciais ou que apenas causem danos irrelevantes não podem ser como tal considerados (DENNING, 2006).

No essencial, há também uma diferença a estabelecer-se entre o ciberterrorismo e a ciberguerra a qual centra-se nos seus protagonistas tendo em conta que os autores do ciberterrorismo não são os Estados, mas sim grupos não governamentais. Na ciberguerra o que existe é uma confrontação entre dois Estados que, recorrendo-se ao ciberespaço, para além do ambiente beligerante entre militares, cada um pretende destruir/disromper as infraestruturas criticas e os processos políticos decisórios do adversário. Este conceito pode aplicar-se também a dois grupos organizados de indivíduos, pertencentes a dois Estados distintos.

Um dos factores promissores/facilitadores do ciberterrorismo é que as nações e as suas infra-estruturas críticas estão cada vez mais dependentes das redes de computadores para a sua operacionalidade, criando-se novas vulnerabilidades que passam a ser os novos alvos do ciberterrorismo. Essa dependência é hoje considerada como "o calcanhar de Aquiles " dos Estados tendo em atenção que todas as suas estruturas mais importantes delas dependem. Efectivamente, verifica-se quer ao nível dos Estados quer das organizações,

[30] Poderão ser actores Estado mas isso nunca será assumido e provavelmente nunca associado. Por isso a maioria das vezes serão por grupos ou instituições a mando de governos.

uma cada vez maior dependência, seja dos sistemas de comunicação seja das tecnologias de informação, e é através da exploração destas vulnerabilidades, que se centra a actuação terrorista e a condução das suas acções. É a este nível que as acções terroristas poderão causar um dano e impacto elevados. Os ataques às infra-estruturas críticas nacionais vão-se tornando numa ameaça real. Uma questão complementar é de saber se o medo não é também um aspecto importante a reter na definição.

O ciberterrorismo pode também ser definido como o uso de computadores como armas ou alvos, com motivos políticos, por grupos anti-nacionais ou agentes clandestinos com a intenção de provocar violência ou influenciar o público, de modo a conduzir que um governo altere as suas políticas (WILSON, 2003).

Pode ainda ser entendido na lógica de um conjunto de forças que utiliza as vantagens e as capacidades do terrorismo dito tradicional, assente na exploração das falhas e das vulnerabilidades tecnológicas, com o objectivo de pressionar um Estado e os seus cidadãos, podendo eventualmente criar medo.

É necessário tomar-se consciência, por um lado, que os terroristas não impõem barreiras à sua actuação uma vez que o mundo é o seu campo de actuação e, por outro lado, que existe um profundo desconhecimento sobre as formas que os ataques de carácter terrorista podem assumir, assim como uma falha ao nível da informação sobre o seu real poder disruptivo e impacto social. Na década de 90, Denning considerava 3 níveis de exploração do ciberespaço pelo terroristas :

- Simples/Não estruturado: descrevendo a "*capacidade da organização para conduzir acções básicas de hacking contra sistemas individuais, utilizando ferramentas desenvolvidas por terceiros. A organização possui um fraco nível de análise de alvos, comando e controlo e capacidade de aprendizagem*."
- Avançado/Estruturado: caracterizando a "*capacidade da organização para conduzir ataques mais sofisticados contra múltiplos sistemas ou redes e, possivelmente, modificar ou criar ferramentas básicas de hacking. A organização possui uma análise de alvos elementar, comando e controlo e capacidade de aprendizagem*."
- Complexo/Coordenado: materializando a possibilidade da organização poder "*conduzir ataques coordenados, susceptíveis de provocar uma disrupção massiva contra defesas integradas e heterogéneas (incluindo criptografia). A organização reúne as competências necessárias para criar sofisticadas ferramentas de hacking, revelando uma eficiente análise de alvos, comando e controlo e capacidade de aprendizagem*."

As conclusões deste trabalho apontam para o facto de os custos do desenvolvimento de acções mais disruptivas do que as básicas e tradicionais actividades de *hacking* serem geralmente mais elevados, e que falta à generalidade das organizações e grupos terroristas, o capital humano e a capacidade para operacionalizar um ataque de ciberterrorismo com alguma relevância. O tempo estimado para um grupo terrorista levantar uma capacidade de ciberterrorismo de raiz, até atingir o nível avançado/estruturado, é de 2-4 anos e para atingir o nível complexo/coordenado de 6-10 anos. No entanto, este tempo poderá ser significativamente reduzido se for seguido um processo de *outsourcing*, como alguns dados recolhidos parecem indicar (DENNING, 2000).

O ciberterrorismo poderá assim ser considerado uma ameaça com um impacto futuro mais consistente do que como actualmente se apresenta, posicionando-se como uma ferramenta auxiliar de importância crescente para o terrorismo transnacional.

Independentemente de estratificações parece-nos porém claro que, no entanto, no âmbito do fenómeno do ciberterrorismo, deverá ter-se em conta dois aspectos, sem os quais não seria possível estar a falar-se deste conceito, e que são: por um lado, a existência de alvos susceptíveis de serem atacados, os quais, devido à sua natureza crítica, produzirão um impacto visível e, por outro lado, a existência de pessoas com capacidade e com motivação para perpetrarem essas actividades terroristas.

A forma de actuação dos terroristas no ciberespaço pode ser encarado sob três ópticas: uma primeira identifica-se como os ataques realizados por computadores a centros tecnológicos; a segunda revela-se ao nível da propaganda, através do envio de mensagens e na divulgação do impacto dos ataques realizados; e por fim, uma terceira que respeita ao planeamento da logística necessária à realização de atentados tradicionais, biológicos, ou tecnológicos.

Face ao exposto, revela-se de algum interesse compararem-se as diferenças entre o terrorismo dito tradicional ou convencional e o ciberterrorismo.

No ciberterrorismo ressalta, desde logo, a inexistência de risco físico para o elemento que executa o acto terrorista, uma vez que o campo geográfico da sua actuação é ilimitado. A elevada mediatização do acto terrorista, sempre que o objecto de ataque seja um sistema informático que suporta interesses críticos nacionais, e por último, a relação custo-benefício para se obterem os resultados pretendidos.

Em oposição a aparentes facilidades, o ciberterrorismo requer capacidade e aptidões técnicas quer na fase preparatória quer na fase de execução das acções ciber.

Numa outra perspectiva, é importante saber-se se o ciberterrorismo é uma realidade dos nossos dias, ou se será uma séria ameaça para o futuro, uma vez que através da internet, que possibilitou a aparecimento de um espaço aberto aos *crackers*, não se abrirá também caminho para uma aliança entres estes e as organizações terroristas, com o intuito de provocarem danos, particularmente de natureza económica, sem o exercício da violência. A realização destes ataques não envolve elevados custos e risco, pelo contrário, podem ser realizados em qualquer parte do mundo com baixos custos e risco (DENNING 2009)

As "gerações mais velhas" de cibercriminosos (ou talvez de ciberintrusivos[31]), conhecidos como *hackers*, foram motivados principalmente pela fama, reconhecimento pelos pares e um desejo de aprender mais e testar os limites dos seus conhecimentos. No final da década de 1990 muitos *hackers* tornaram-se em *crackers* e começaram a tirar cada vez mais partido das oportunidades criminais que a Internet se lhes oferecia. Esses criminosos usam o ciberespaço para cometer fraudes bancárias, extorsão através de ameaças de negação de serviço e ataques, fraudes à propriedade intelectual, bem como a fraude de identidade. Em muitos casos, os *crackers* trabalham em grupos, muito embora nem todos se conheçam pessoalmente.

Enquanto os *crackers* se preocupam em roubar dados de organizações, os ciberterroristas preocupam-se em promover destruição massiva. Grupos como Cyber-Jihadad[32] e Cyber são exemplos de alguns grupos de terroristas financiados pelo Estado ."Jihad eletrônica" ou "ciber jihad" [33]como são conhecidos. Normalmente, esses indivíduos e grupos atacam *sites* que contenham valores contrários ao Islão, desfigurando-os ou usando ferramentas de *software* para inundá-los com o tráfego constituindo-se num ataque de negação de serviço (DoS). O maior ataque desta natureza veio em resposta à publicação, em 2006, no Jornal dinamarquês Jyllands-Posen de uma sátira ao profeta Maomé, de que resultou ataques a milhares de *sites* dinamarqueses (DENNING 2011).

Na realidade, vão surgindo indivíduos e grupos que jamais pensariam em detonar uma bomba ou disparar uma arma sobre um ser humano, mas que aparecem hoje como potenciais aliados das organizações terroristas para a concretização dos seus objectivos, como se estas organizações efetuassem um tipo de *outsourcing*

[31] As primeiras gerações era uma espécie de comunidade ética dado que embora intrusos se constituam como uma espécie de testadores á capacidade de intrusão.
[32] http://cyber-jihad.forumt.biz/ (revistado em 3 de Junho 2014)
[33] http://postnito.cz/?p=4966 consultado em 20 Abril de 2014

Resumindo, a utilização do ciberespaço oferece um conjunto de condições que vão ser aproveitadas no desenvolvimento de acções terroristas, tais como:

- Anonimato – não há exposição física do atacante e, caso a operação se transforme num fracasso, o ciberterrorista pode analisar o erro, adquirir experiência e aprender como operar correctamente para ter sucesso na próxima vez, sem colocar em risco a sua identidade e localização. A proliferação dos pontos de acesso anónimos à internet (por ex., os cibercafés), vem também contribuir para o anonimato destes terroristas do ciberespaço;
- O grau de investimento é mínimo comparado com outro tipo de ataque; a sua ação pode alcançar proporções monumentais, dado que se trata de manipular os elementos tecnológicos do adversário ou pelo menos, privá-lo das suas próprias defesas;
- Difusão da sua "cultura terrorista", onde se inclui a sua história, postulado e objectivos a atingir com a sua causa;
- Campanhas de propaganda e mediatização, comunicação dos seus objectivos de forma global e sem grandes encargos, tendo os seus actos, quase sempre, a cobertura dos "media". Os "média" proporcionam aos terroristas um meio para disseminar a sua mensagem de medo e intimidação;
- Obtenção de Informação sobre a tecnologia que pode ser utilizada para fins terroristas;
- Recrutamento – angariação de novos elementos para as suas causas;
- Para o comando e controlo das operações, utilizam a rede como meio de comunicação- activação de maneira remota;
- Para administrar, financiar e para efeitos logísticos de toda a sua actividade;
- A transferência de fundos financeiros – hoje é vulgar realizar depósitos através da Net e fazer movimentos financeiros sem necessidade de comprometer a respectiva identidade.

Para além disso, as organizações terroristas podem realizar também ataques ciberterroristas conjugados com ataques convencionais (sequestro de pessoas importantes, atentados bombistas, ataques com vírus às infra-estruturas críticas de informação, etc.) causando o caos e o pânico nas populações, especialmente àquelas localizadas em contextos urbanos. Todavia, o grau de exposição do ciberterrorista é mínimo comparado com outro tipo de ataque terrorista (não requer manuseamento de explosivos ou missões suicidas) e os seus

resultados podem igualmente alcançar proporções dramáticas. O mundo encontra-se assim, ante um novo tipo de conflito para o qual dificilmente se poderá antever e vigiar a sua extensa fronteira global.

Utilizando a internet como um meio para executar os seus propósitos e os computadores como as suas armas os ciberterroristas tiram proveito da evolução tecnológica produzindo efeitos/impactos sobretudo de natureza disruptiva, com efeitos psicológicos associados, não tanto pelo terror mas sobretudo pela desconfiança. O que é que está seguro? Em que é que eu posso confiar?

Segundo Barry Collin (2007) e com base na definição de Terrorismo podem-se exemplificar alguns actos como sendo de ciberterrorismo:

- O ciberterrorista pode entrar remotamente nos sistemas de controlo de processamento de um fabricante de cereais, alterar os níveis de ferro de um determinado cereal e com isso fazer com que adoeçam e/ou morram as crianças que dele se alimentam em determinado país. O que o ciberterrorista no fundo faz é alterar remotamente a fórmula do produto sem ter de estar na fábrica em questão;
- O ciberterrorista pode colocar um sem número de bombas informatizadas em torno de uma cidade, transmitindo entre si padrões numéricos exclusivos. Programas bombas para a detonação caso uma pare a transmissão. Parando uma dessas transmissões as bombas detonam simultaneamente. Deste modo não necessitam de nenhum "Kamikaze" com coletes de bombas, não necessitam de meios terrestres como camiões e afins, o elevado número de bombas e as combinações dos padrões de transmissão evitam a sua fácil detecção e o seu difícil desactivamento em simultâneo, e o impacto causado pela extensão das explosões é grande. É tudo feito sob controlo remoto;
- O ciberterrorista pode causar distúrbios nos sistemas financeiros, nomeadamente em bancos, alterando as transacções financeiras internacionais e a bolsa de valores. O que fará com que diminua a credibilidade do sistema económico dum país pela perda de confiança do povo. O autor pode estar a executar toda a tarefa num outro continente não se necessitando para isso de invadir violentamente o local, o que poderá ser facilmente detectado e impedido;
- O ciberterrorista pode atacar o sistema de controlo de aviação, fazendo com que se verifique a colisão entre duas aeronaves. Ou então em sistemas de controlo

ferroviário. Fará tudo remotamente sem que sejam necessários recursos humanos acrescidos;

- O ciberterrorista pode alterar remotamente fórmulas de medicamentos nos fabricantes de produtos farmacêuticos, com danos incalculáveis para a vida humana.

Segundo o mesmo autor, estes riscos já estiveram bem mais longe de se tornarem uma realidade, porém, até ao momento, o único caso conhecido e que se aproxima mais a um ataque de ciberterrorismo é o ataque do Stuxnet[34] a duas centrais nucleares no Irão. Na verdade não são conhecidos casos de Ciberterrorismo tal como este tem sido definido, muito embora este termo já tenha feito muitas capas de jornais. Facilmente se confunde ciberterrorismo com ciberactivismo ou mesmo com o cibercrime.

Por vezes tende a confundir-se o ciberterrorismo com o ciberactivismo porque a fronteira que distingue os dois é ténue. O ciberactivismo não é mais do que a convergência do *hacking* com o activismo social e político. O activismo incluiu, por exemplo, a desobediência civil electrónica que leva para o ciberespaço o conceito tradicional de desobediência civil. Segundo Conway (2003), o que distingue os dois conceitos é o grau crescente e progressivo de distúrbio e de destruição que cada um provoca, sendo que o hactivismo se prende com a utilização normal (não disruptiva) da internet em defesa de uma causa, sem o intuito de provocar danos consideráveis. Conway entende ainda que os ciberacktivistas não se vêem como criminosos violentos empenhados na destruição de vidas inocentes, mas sim como os herdeiros daqueles que empregam táticas de invasão e bloqueio no reino de protesto no mundo real.

"As velhas ameaças do mundo real, tornaram-se "cyber-qualquer-coisa-crime" com o advento da internet; expressões como "ciberbranqueamento", "cibertráfico" e

[34] é um vírus informático projectdo especificamente para atacar o sistema operacional SCADA (sistema desenvolvido pela Siemens para controlar as centrífugas de enriquecimento de urânio iranianas). Foi descoberto em junho de 2010 pela empresa bielorrussa de antivírus VirusBlokAda. É o primeiro vírus descoberto que espia e reprograma sistemas industriais. **Siemens: Stuxnet worm hit industrial systems** (Em linha) consultado em 25 de Maio de 2014 http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142

"ciberterrorismo" tornaram-se de utilização comum entre algumas comunidades ligadas à defesa do Estado democrático e manter a paz social (BRAVO,2010).

Existem provas de que a internet é um veículo utilizado para a realização de crimes utilizado seja pelos terroristas, seja pelos chamados grupos de crime organizado. Talvez porque são hoje muitos os grupos terroristas que se servem da internet para criarem as suas páginas para a difusão das suas ideologias, para o aliciamento de novos membros ou para a propaganda das suas acções, o ciberterrorismo esteja nos tempos que correm a absorver uma gradual e crescente atenção e a revela-se uma preocupação para os Estados a nível mundial.

Verifica-se actualmente uma clara tendência da migração dos grupos terroristas, dos *sites* para as redes sociais online onde se incluem não só Facebook, como também o YouTube o Twitter e mais recentemente o Instagram e o Flickr. Esta recente utilização de meios de comunicação que funcionam como uma nova arena em sistemas informáticos sociais abertos a todos, criou novos desafios e mudanças no pensamento estratégico em matéria de segurança nacional.

Um relatório do Departamento de Segurança Interna dos Estados Unidos da América (WEIMANN,2014) fez uma listagem dos grupos de terrorista que usavam o Facebook e concluiu que este era utilizado:

• Como uma via de compartilhar informação operacional e táctica, tais como instruções para o fabrico de bombas, fabrico e manutenção de armas de tiro táctico, etc

• Como uma porta de entrada para acesso a *sites* extremistas e outros conteúdos radicais ligados a outras páginas de grupos ou fóruns de discussão;

• Como um meio de comunicação para a propaganda terrorista e mensagens de ideologia extremistas e radicais;

• Como incitamento à *datamining*[35] e captação de recursos.

A rede social Twitter é talvez aquela com uma maior presença de terroristas. Aproveitando a tendência recente para a cobertura de notícias em tempo real, em que se sacrifica a sua validação e análise em profundidade em prol do imediato, os terroristas têm-se aproveitado dessas falhas para a propaganda e até para causar alguns danos.

[35] é o processo de explorar grandes quantidades de dados à procura de padrões consistentes, como regras de associação ou sequências temporais, para detectar relacionamentos sistemáticos entre variáveis, detectando assim novos subconjuntos de dados.

O principal exemplo disso foi a falsa "notícia de última hora" de um ataque à bomba dentro da Casa Branca, *twitado* pelo Exército Eletrónico Sírio, via uma conta de uma agência de notícias que tinha sido *hackada* em 23 de Abril de 2013. Essa notícia, fez com que a bolsa de Wall Street, sofresse uma perda de $136 biliões de dólares, causada pelo pânico que se gerou nos investidores.

A situação apontada, tal como ela foi descrita, revela a ausência de uma uniformização terminológica no mundo da cibernética, ou seja, um léxico internacional, o que a juntar à falta de uma definição precisa dos conceitos de terrorismo e ciberespaço demonstra bem as dificuldades na definição de políticas de cibersegurança a nível nacional e internacional.

Não obstante esta vertente, os terroristas utilizam o Twitter essencialmente para comunicar com seus simpatizantes. Um exame de 76.000 *tweets* pela Frente al-Nusra relacionados com a Al-Qaeda na Síria revelou que continham mais de 34.000 ligações (PRUSCHA& FISHER 2014).

Esta migração para as redes sociais permitiu também uma melhor e mais eficaz actuação dos denominados “Lone Wolfs” ou lobos solitários, que segundo a definição adoptada pelo pelo Instituto Voor Veiligheids-en Crisis Management[36] que segue as definições do Conselho da Europa relativas ao terrorismo, considera aqueles como actos intencionais cometidos por pessoas:

a. Que operaram individualmente;

b. Que não pertencem a um grupo de terrorismo organizado ou em rede;

c. Que agem sem a influência directa de um líder ou de hierarquia;

d. Cujas tácticas são concebidas e dirigidas pelo próprio indivíduo sem qualquer ordem do exterior.

As organizações terroristas jihadistas estão a estimular o terrorismo praticados por estes lobos solitários, porque revelou-se ser uma táctica eficaz na sua luta global para o estabelecimento do Califado, ou seja, um Estado islâmico.

Esses indivíduos podem encontrar todas as informações que lhes interessa na Internet, tendo em conta que esta apresenta-se como uma plataforma para a motivação ideológica, o incentivo, a justificação, a meta da informação, a instrução e técnicas, tudo num ambiente anónimo.

[36]InstituutVoorVeiligheids-enCrisismanagement Lone-wolf terrorism (em linha) http://www.transnationalterrorism.eu/tekst/publications/Lone-Wolf%20Terrorism.pdf – revisitado em 10 de Junho)

Com o aumento de divulgação de actos terroristas propriamente ditos, de que se relevam os recentes praticados nas estações de comboio na República Popular da China, não quer significar que o ciberterrorismo não seja uma ameaça real, embora não corresponda à antevisão que dele se fazia. Isto, devido sobretudo às medidas preventivas de que os Estados se foram rodeando.

Importa referir que a presença dos terroristas no ciberespaço não tem uma ligação directa com a prática do ciberterrorismo, uma vez que o ciberespaço é, no fundo um espaço utilizado sobretudo para divulgar, recrutar e planear as suas acções, podendo essas acções terroristas, propriamente ditas, não ter lugar no âmbito do próprio ciberespaço.

Contudo, é preocupante a possibilidade de organizações terroristas desempenharem papéis e/ou desenvolverem *software* para empresas e organismos do Estado. Pelo menos um incidente deste tipo é conhecido. Em Março de 2000, a polícia metropolitana do Japão anunciou que o grupo "Aum Shinrikyo", o mesmo que foi responsável pelo atentado no metro de Tokyo em 1995, desenvolveu um *software* com capacidade de georreferenciar veículos automóveis. Veio a saber-se que este tipo de *software* que, de forma dissimulada, albergava "cavalos de tróia", foi vendido por esta organização a várias empresas e instituições, de entre as quais a algumas polícias do Japão (SANTOS et al, 2008).

A crise do Kosovo à qual se chamou "The War of the Web", foi palco de troca e cruzamento de informações de diversas origens, a partir do qual células criminosas delineavam operações. Também na guerra do Iraque a internet teve um papel primordial nas decisões dos ciberterroristas que através de *weblogs* e de *e-mails* trocavam *intelligence* acerca de operações militares dos aliados. Neste teatro de operações a Internet representou formas de contra-informação manobras de diversão e de engodo dos terroristas (SANTOS et al, 2008).

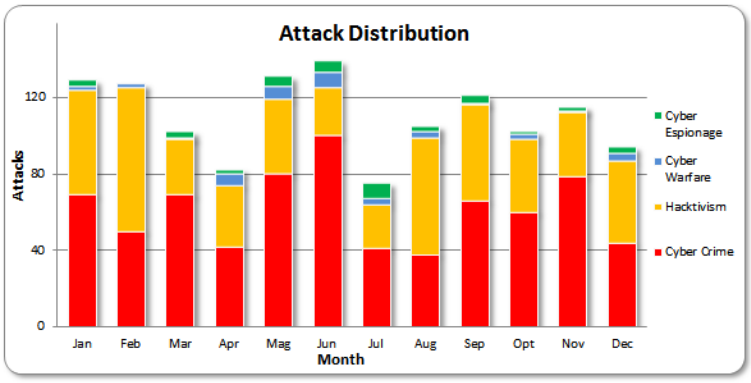
O primeiro ciberataque cometido por terroristas no ciberespaço, mas que nem por isso pode ser denominado como ciberterrorismo, tal como o entendemos, ocorreu em 1997, efectuado pelo grupo de guerrilheiros tâmeis Tigres de Liberação do Tamil Eelam, que denominando-se como *Internet Black Tigers (HIMMA,2007),* inundaram as embaixadas do Sri Lanka com 800 *e-mails* por dia e durante um período de duas semanas. Os *e-mails* continham a mensagem "*Somos os tigres negros e estamos a fazer isto para interromper as comunicações*". Este foi considerado o primeiro ataque executado por terroristas contra sistemas de computadores de um país. Este mesmo grupo também ficou conhecido por praticar ciberataques com o intuito de angariar verbas, tendo para o efeito, nesse mesmo

ano entrado na rede de computadores da Universidade Sheffield em Inglaterra e capturado os nomes de usuário e palavras passe dos utilizadores, usando depois as suas contas de *e-mails* para enviar pedidos de donativos a favor da caridade no Sri Lanka.

O caso mais conhecido e mais grave e pelos média considerado como um ataque de ciberterrorismo a um Estado teve lugar na Estónia em 2007, em que os supostos ciberterroristas atacaram os *sites* do governo, o que para Estônia, um país que tem quase todos os seus serviços na Internet, sendo considerado um país digital, causou vários problemas nesses serviços, afectando directamente a população. Há quem defenda que os apagões no Brasil de 2005 e 2007, respectivamente foram causados por ciberterroristas [37], embora não tenham sido reveladas as conclusões da investigação

O termo ciberterrorismo continua a circular como uma ameaça constante e premente. Porém, como se pode verificar nos quadros abaixo reproduzidos, tanto no ano de 2012, como nos meses de Junho de 2013 e 2014, não houve indícios de ataques de ciberterrorismo:

Ciberataques reportados em 2012, segundo a motivação

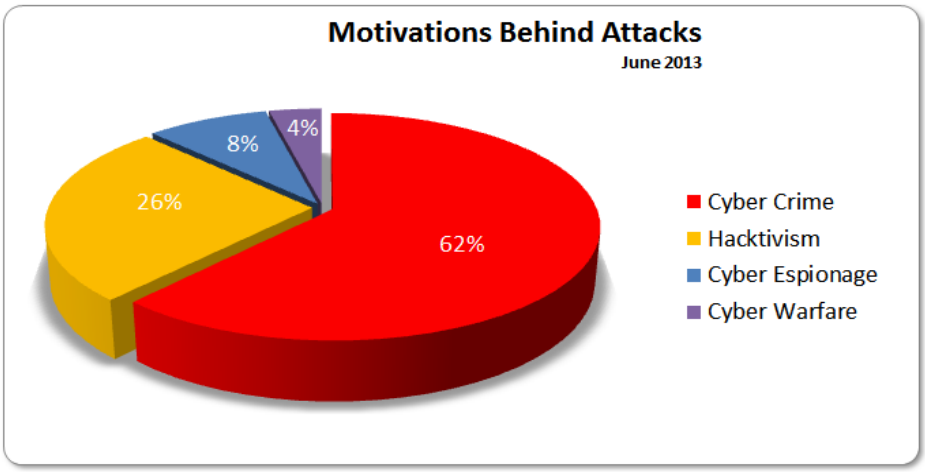


38

Ciberataques reportados em Junho de 2013, segundo a motivação

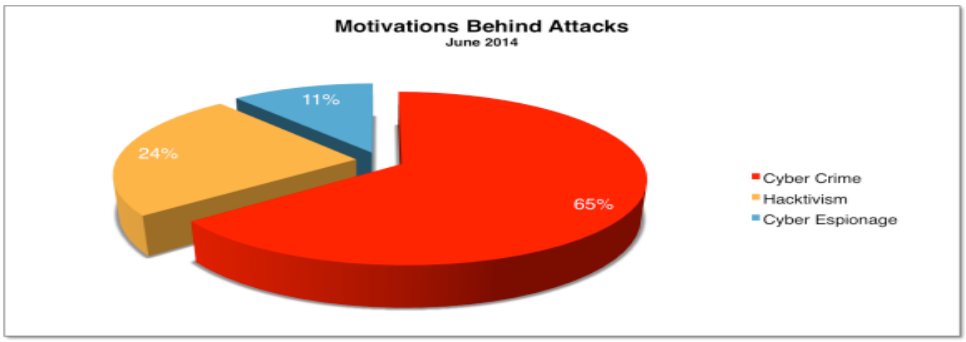
[37] http://revistaepoca.globo.com/Revista/Epoca/0,,EMI105832-15227,00CIBERTERRORISMO+E+GUERRAS+VIRTUAIS+PREOCUPAM+GOVERNOS.html revisitada em 4 de junho 2014

[38] http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/ (revisitado Jun2014)



[39]

Ciberataques reportados em Junho de 2014, segundo a motivação



[40]

O impacto dos resultados dos ataques só são de certo modo alcançados se o carácter espectacular das suas acções for transmitido pelos média, caso contrário é como se não tivessem ocorrido. Entende o General Loureiro dos Santos que "um atentado que não passe para a internet na prática não existe, pois o que interessa é a sua exploração no ciberespaço" (SANTOS, 2006).

Existe uma relação simbiótica de conveniência e exploração mútua (NOVAIS,2012) entre os terroristas e os média. Esta relação resulta da mútua conveniência dos terroristas, que procuram captar a atenção das audiências, e dos média, que buscam factos noticiosos dramáticos que aumentem o seu público e a sua popularidade.

De um modo geral, a investigação tem mostrado que vários processos psicológicos, como a atenção e a memória, tendem a dar prioridade a eventos negativos com forte intensidade emocional, o que pode explicar, em parte, o facto de os média explorarem o terrorismo para aumentar as audiências, proporcionando ao público notícias dramáticas e violentas (ARRIAGA et al).

[39] http://paulsparrows.files.wordpress.com/2013/07/motivations-june-2013.png (revisitado Jun2014)
[40] https://paulsparrows.files.wordpress.com/2014/07/motivations-june-2014.png (consult. Jun2014)

Um curioso exemplo do aproveitamento dos média de notícias ligadas ao terrorismo, em Portugal, foi o recentemente publicado "*Ciberterroristas atacam escolas portuguesas*"[41],o qual constituiu o título de capa de mais do que um jornal nacional. Mas o que na realidade aconteceu foi um simples ataque a alguns *sites* de estabelecimentos de ensino realizado por uns *hackers*.

A forma, muitas vezes gratuita, como as notícias sobre estes eventos se divulgam exercem de certa forma um forte impacto emocional sobre as populações.

O que o ciberterrorismo (ou talvez de forma mais simplista o alarmismo) provoca nas populações é a ampliação do medo tendo em conta que a percepção dos danos que possam eventualmente causar leva a que o pânico se instale mal os primeiros sinais se despontam. Isto, na medida em que sendo o medo uma emoção negativa que causa sofrimento, esse o medo quando colectivo tende a transformar-se em pânico.

Não há espécie com mais medo do que a espécie humana (MARINA,2008).Vivemos entre a lembrança e a imaginação, entre fantasmas do passado e fantasmas do futuro, reavivando velhos perigos e inventando novas ameaças. O medo é uma emoção individual mas contagiosa, ou seja, social. Sendo que os medos sociais, são os que acometem uma sociedade nalgum momento da sua história.

Segundo a psicologia das multidões, as massas são muito influenciáveis, tendo como características o carácter absoluto dos seus juízos, a rapidez dos contágios emocionais, a debilitação ou perda do espírito crítico, o desaparecimento do sentido de responsabilidade pessoal, a subestimação ou o exagero da força do adversário, a sua aptidão para passar repentinamente do horror ao entusiasmo e das aclamações às ameaças de morte (MARINA,2008).

Se, no passado, o medo no homem vinha da natureza e do sobrenatural, hoje o principal perigo para a humanidade vem do próprio homem e das incertezas produzidas pela tecnociência. O aperfeiçoamento dos armamentos, o movimento para uma guerra total, a multiplicação dos actos terroristas provocando cada vez mais vítimas, fazendo crer que o terrorismo está em qualquer lugar e os actos terroristas podem acontecer a qualquer hora, fazem com que a noção de segurança desapareça por completo e seja substituída pelo medo.

[41] http://www.cmjornal.xl.pt/detalhe/cm-tv/atualidade/ciberterroristas-atacam-escolas-portuguesas consultado em 20 de Maio de 2014

É sobretudo nas cidades que se tem mais medo, em especial nas grandes cidades, onde o terrorismo se instala ou se pode facilmente infiltrar, ao mesmo tempo que os danos causados ganham uma maior dimensão e maior visibilidade, o que corresponde a um dos seus objectivos.

Para Hans Jonas (BATTESTIN et al), o maior problema trazido pela tecnologia é o do perigo que não está patente, essencialmente imperceptível: não se trata de uma má utilização da potência tecnológica, mas da sua boa utilização - é isso que torna o perigo cada vez mais ameaçador.

O ciberterrorismo engloba em si mesmo dois tipos de medo, o medo que o ser humano tem do desconhecido mundo cibernético e o terror que o terrorismo provoca.

O Homem necessita representar o medo, atribuir significados comuns a situações, objectos e pessoas que causam temor. A própria representação é uma forma de o tentar controlar, antecipar e conhecer. Ao representá-lo, ele é partilhado e socializado, e, ao mesmo tempo, é ampliado e estendido, e a consequência é que se deseja controlá-lo cada vez mais.

Já na Declaração de Génova sobre o Terrorismo[42] foi destacado que a característica distintiva do terrorismo era o "Medo". Para maximizar o impacto dessa ameaça pública os alvos dos terroristas são maioritariamente civis, criando-se a ideia que qualquer pessoa pode ser um potencial alvo.

Os terroristas querem passar a mensagem que os ataques vêm de forma aleatória e sem aviso, de modo não seja possível prever-se o imprevisível. A sua propaganda baseia-se na disseminação de informação de forma a influenciar a opinião pública de modo a instalar-se o clima de medo. Fazendo com que se adopte o derrotismo como uma filosofia, que a pessoa seja derrotada por essa mesma filosofia. No fundo adoptam como estratégia, a guerra psicológica, que se caracteriza pelo emprego planeado da propaganda e da exploração do fenómeno, com a intenção de influenciar opiniões, emoções, atitudes e comportamentos de grupos com vista a facilitar a execução dos seus objectivos. Tendo como propósito desmoralizar o adversário dando-lhe a sensação de insegurança e descrença no seu êxito, levando-o deste modo à rendição.

Embora o ciberterrorismo não envolva uma ameaça directa de violência, o seu impacto psicológico em sociedades ansiosas, pode ser tão intenso como os efeitos dos atentados bombistas. Além disso, as forças militares e de segurança, que tentam combater e

[42] http://i-p-o.org/GDT.HTM (revisitada em 25 de Maio 2014)

compreender este tipo de ameaça, têm a seu desfavor o facto de existir uma falta de informação ou, pior ainda, excesso de desinformação acerca deste fenómeno.

Em segundo lugar, os órgãos de comunicação social contribuem para esta aura de medo através da colocação nas primeiras páginas dos jornais de casos relacionados com ciberataques (SANTO et al , 2008).

Gerir a percepção pública de medo e do perigo de um ataque terrorista é tão crítica como tomar medidas para protecção contra o próprio ataque real.

No entanto, as armas do tipo convencional destroem as estruturas físicas, as armas lógicas destroem as estruturas lógicas e as armas comportamentais, ou semântica destroem a confiança dos utilizadores nos sistemas de informação e na rede e influenciam a interpretação da informação que circula. O que significa que, no mundo cibernético, o ciberterrorismo é uma ameaça potencial mas com um resultado político muito relativo, tendo em conta que os ataques cibernéticos raramente produzem danos sobre as vidas humanas. Esta será, talvez a principal razão porque o ciberespaço ainda não se tornou a arma preferencial do terrorismo.

Terá o Stuxnet ampliado o risco da efectivação do ciberterrorismo à uma escala alargada?

O Stuxnet , vírus informático projectado especificamente para atacar o sistema operacional SCADA , sistema desenvolvido pela Siemens para controlar as centrifugadoras de enriquecimento de urânio iranianas, pode ser considerada a primeira ciber-arma por ser o primeiro vírus que foi descoberto e que permitiu espiar e reprogramar sistemas industriais. Segundo o Kapersky Lab, produtora de antivírus para o Stuxnet, é um protótipo alarmante de uma arma cibernética.

É um vírus capaz de reprogramar os sistemas sem que seja detectado, uma vez que consegue esconder as mudanças, consegue estar camuflado em mais de 100 mil computadores.

Foi descoberto em Junho de 2010 pela empresa bielorussa de antivírus VirusBlokada e instalou-se na central através de uma *pen* (flash drive) e a contaminação rapidamente se propagou pelos computadores pessoais de funcionários da central nuclear iraniana.

O vírus tinha duas funções, sendo que a primeira era a de fazer com que as centrifugadoras começassem a girar 40% mais rapidamente, durante cerca de quinze minutos, o que causava fissuras nas centrifugadoras de alumínio. A segunda, relaciona-se com a forma como inicialmente se gravavam os dados telemétricos de uma típica operação normal das centrifugadoras nucleares, sem que o alarme soasse, para depois se reproduzir esse registo

para os operadores dos equipamentos. No entanto, as máquinas, ou sejam, as centrifugadoras estavam literalmente a destruir-se sob a acção do Stuxnet sem que os funcionários se apercebessem.

Há quem defenda que o vírus foi desenvolvido por um Estado, nomeadamente os Estados Unidos da América ou Israel porque nenhum outro país teria as competências e aptidões necessárias para o desenvolver. Aliás, nenhum desses países negou as acusações de terem intervido. Curiosamente, o Irão não declarou ter sido atacado.

Segundo Denning (2012) a existência do Stuxnet e o potencial reconhecimento de que as ciberarmas podem causar danos sérios nas infra-estruturas críticas podem levar-nos mais perto de um incidente de ciberterrorismo do que esperávamos. Mas não parece, contudo ser uma ameaça iminente, tendo em conta que a Jihad em todos os seus documentos e sites parece ainda dar a primazia aos ataques físicos reconhecendo, quiçá, as suas faltas de competências imediatas para o desenvolvimento de tais armas, ainda…..

No entanto, o Stuxnet vai provavelmente inspirar, acelerar, e servir como um bloco de construção para o desenvolvimento de novas ciberarmas que têm como alvo dispositivos Infra-estruturas críticas.

Queremos acreditar, porém, que dificilmente o ciberterrorismo passará a ser uma Pearl Harbour digital.

Capítulo 3

A IMPORTÂNCIA DA INTELLIGENCE NA PREVENÇÃO E COMBATE AO CIBERTERRORIMO E QUAL O SEU PAPEL NAS ESTRATÉGIAS NACIONAIS

"Todo o fenómeno é, no princípio, um germe, depois acaba por tornar-se numa realidade que cada um pode constatar. O sábio pensa a longo prazo. É porque tem um grande

cuidado em se ocupar dos germes. A maior parte dos homens tem vistas curtas. É porque esperam que o problema se torne evidente para o atacar.
Quando ele ainda está em embrião, o caso é simples, exige poucos esforços e traz grandes resultados. Quando o problema se torna evidente, cansa-se a resolvê-lo e em geral, todos os esforços são em vão" (Os trinta e Seis Estratagemas)

O ciberespaço nunca conseguiu ser aquele espaço anárquico defendido por John Perry Barlow, em 1996, no seu texto "A *Declaration of the Independence of Cyberspace*" onde defendeu que os governos deveriam manter-se afastados do ciberespaço, uma vez que não tinham o direito moral de o governar pelo que deviam abster-se de criarem quaisquer imposições legislativas reguladoras neste novo espaço social global. De salientar que este pensamento libertário do ciberespaço ainda é acompanhado por muitos movimentos, nomeadamente pelo conhecido grupo de ciberactivistas "Anonymous". Para provar a impossibilidade de tal manifesto Daniel Castro, em 2013 escreveu "*A Declaration of the Interdependence of Cyberspace*" alegando que muito embora a internet não tenha um governo eleito, nem é provável que algum dia o venha a ter, não quer com isso dizer que não é governado. A Internet é regida não só pelas normas e costumes dos seus utilizadores, mas também pelas leis e valores das sociedades em que vivem. O que se pretende não é uma Internet regida pelas nações do mundo mas sim um equilíbrio que reconheça tanto os direitos do indivíduo como os benefícios de uma comunidade bem organizada.
Nos anos mais recentes, os ataques contra as infra-estruturas de informação tornaram-se mais frequentes e complexos, enquanto que, ao mesmo tempo, aqueles que os fazem são cada vez mais profissionais. Dada a abertura e o alargamento dimensional do ciberespaço é possível fazerem-se ataques encobertos e abusarem-se de sistemas vulneráveis como instrumentos para um ataque.
Deste modo, a garantia da segurança do ciberespaço tornou-se no principal desafio para o Estado, para os negócios e para a sociedade, tanto a nível nacional como internacional. Uma estratégia para a cibersegurança (Cyber Security Strategy) leva a que se melhorem as condições de organização nesta área.
Garantir a cibersegurança, proteger os direitos e as infraestruturas de informação exigem grandes esforços por parte dos Estados, tanto a nível nacional como em cooperação com os seus parceiros internacionais. Uma vez que os sistemas de TI encontram-se interconectados numa rede global, incidentes nas infra-estrururas de informação num país podem afectar

também outros países. É por isso que o reforço da cibersegurança recomenda também a aplicação de leis internacionais de conduta, de padrões e de normas. Apenas uma combinação de medidas de política doméstica (interna) e externa será adequada perante a dimensão do problema. Um combate ao crescimento rápido do cibercrime (cybercrime) exige uma colaboração próxima entre os órgãos de polícia criminal a nível mundial.

Com a abertura do ciberespaço a biliões de pessoas distribuídas pelos cinco cantos do globo, abriu-se também a porta à entrada de actores criminosos que, através dele e das suas infra-estruturas e sistemas de informação, procuram satisfazer os seus mais variados intentos.

Neste domínio, a utilização da Internet apresenta-se como o meio privilegiado para a viabilização e concretização dos seus objectivos, dadas a sua difusão e a generalização do seu uso a nível internacional, em larga medida tornadas possíveis pelo crescente abaixamento dos custos dos respectivos equipamentos e de acesso às redes. As redes em banda larga, por seu lado, vieram favorecer a preferência deste uso, na medida em que permite que uma pessoa que esteja num qualquer ponto de uma cidade, vila ou aldeia de um país, que disponha naturalmente das redes adequadas, possa comunicar com outrem num qualquer outro país.

Através da Internet, os Estados comunicam-se entre si, o mesmo sucedendo relativamente às suas empresas, administrações públicas, organizações e instituições públicas e privadas e cidadãos.

As informações que circulam pela Internet são das mais variadas natureza e conteúdos, desde as de simples relações de cordialidade e de amizade, passando pelas de conteúdo científico, literário, económico e político, até às que por vezes tocam nos chamados assuntos de Estado.

Compreende-se, assim, que a natureza e os conteúdos dessas informações comecem a interessar terceiros que vêem que delas possam tirar algum benefício ou proveito.

Por esse facto, indivíduos e famílias são, por vezes, afectadas por actos de chantagem, fraude e extorsão por parte de criminosos que conseguem aceder aos seus dados pessoais; o mesmo tipo de crimes sucedem relativamente às empresas e a grupos profissionais, onde as matérias relativas à propriedade intelectual e dos direitos de autor ganham também um especial peso. Nas áreas judiciais, policiais e militares são inegáveis os nefastos efeitos das informações que caem em mãos criminosas, comprometendo a justiça, a estabilidade, a paz e a segurança do próprio Estado.

Neste âmbito, uma referência especial deve ser dada ao ciberterrorismo que, como a própria palavra indica, relaciona-se com os actos praticados por terroristas, isoladamente, em grupo ou integrados nas respectivas organizações, com o propósito de, sobretudo, e através da internet , divulgarem as suas ideologias, recrutarem novos aderentes, angariarem fundos para as suas actividades de propaganda e trocarem informações com as respectivas organizações, mas também para a prática de crimes que possam pôr em causa a segurança nacional e internacional.

Esta matéria foi, aliás, profusamente desenvolvida no capítulo anterior.

Na verdade, se a gravidade dos crimes ciberterroristas reside não exclusivamente nos efeitos que produzem nos alvos que são atingidos, os quais, para além de poderem colocar em causa as propriedades e as vidas humanas, essa gravidade ganha uma especial acuidade quando tais crimes atingem sobremaneira as infra-estruturas de informação e as infra-estruturas críticas, em redor das quais as economias modernas se desenvolvem, podendo até colocar em risco as seguranças nacional e internacional.

Estes crimes, denominados de cibercrimes, na medida em que são perpetrados no ciberespaço, retiram a confiança dos utilizadores no uso da Internet pela falta de segurança que a mesma oferece, sobretudo pela invasão não consentida da sua privacidade, a que acrescem as eventuais interrupções e roturas dos serviços que são prestados e que não oferecem a garantia de que as suas informações cheguem sempre ao seu destino, donde a sua falta de confiança nos sistemas.

Tendo hoje os Estados a consciência do importante papel que a Internet e outras tecnologias digitais desempenham na vida dos seus cidadãos, no desenvolvimento e crescimento das suas economias, na estabilidade e paz sociais e na própria defesa e segurança nacional, reconheceram estes a necessidade de adoptar um conjunto de medidas de prevenção e de combate aos cibercrimes, onde o ciberterrorismo pode vir a conquistar gradualmente um mais alargado terreno. Tendo em vista principalmente a segurança do ciberespaço, cada Estado tem procurado definir, para o efeito, a sua estratégia com base nos princípios fundamentais que defendem, nos objectivos que pretendem prosseguir e nas linhas programáticas de acção que procuram implementar.

Alguns Estados já viram aprovada a sua Estratégia de Cibersegurança, enquanto que outros estão a lançar-se na sua elaboração. O nosso país, que ainda não colocou em prática essa Estratégia embora já tenha sido aprovado um diploma relativamente ao Centro Nacional de Cibersegurança.

Torna-se interessante e enriquecedor reflectir sobre as estratégias implementadas por outros Países identificando os seus principais eixos estratégicos para, à sua luz, conseguir-se percepcionar aquilo deve ser a nossa estratégia nacional para a cibersegurança.

Tal como em outras áreas, perceber o papel da *intelligence* no combate e prevenção do ciberterrorismo, e qual o seu papel nas estratégias de outros países como uma mais-valia para a criação de mecanismos estruturais para se tentar evitar ou diminuir o impacto do fenómeno.

3.1 A IMPORTÂNCIA DA INTELLIGENCE NA PREVENÇÃO E COMBATE AO CIBERTERRORISMO

Se, por um lado, a abertura de fronteiras em prol de uma crescente economia global facilita e desenvolve os mercados de trocas legais, por outro, são uma porta aberta para esquemas ocultos de economias paralelas muitas vezes suportadas por empresas legítimas, indústrias e serviços ou até instituições financeiras multinacionais que são utilizadas como fachada para suas actividades, tendo como fim último o negócio ilegal nas suas mais variadas formas e tipos, revelando-se o terrorismo como a forma mais grave dessa criminalidade.

Começa-se a ter cada vez mais a noção de que não se pode olhar para a criminalidade como um fenómeno estático, isolado no espaço e no tempo. O seu estudo não deve ser um somatório de dados estatísticos e de gráficos, uma vez que estes, na sua essência, não permitem uma análise aprofundada. Esse estudo deve abranger o fenómeno no seu todo, de uma forma pró-activa, levando-o para além dos factos, testando hipóteses e desenvolvendo inferências. As variadas formas de criminalidade são hoje mais complexas e difusas e de mais difícil detecção, em resultado da utilização do ciberespaço, que, se por um lado proporcionou novas oportunidades, por outro trouxe mais vulnerabilidades.

As grandes batalhas contra a criminalidade dão-se essencialmente em espaços incontrolados, ou seja em zonas sem direito, ou "zonas" cinzentas; espaços intermediários entre territórios realmente policiados por Estados- Nações reais; espaços baldios entre domínios ministeriais ou entre sectores onde operam os serviços. (…) A entidade criminosa ou terrorista opera, na sua maior parte, em zonas fora de controlo (BAUER,RAUFER 2003).

Assim, a globalização exige uma consciente e assumida mudança de atitude, passando-se de uma postura reactiva a uma postura cada vez mais pró activa. Tem de se saber interpretar os sinais e os rastos que o terrorismo vai deixando ao longo do seu percurso, para o poder combater e prevenir, e isso só é possível se for possível identificá-lo, conhecendo os seus espaços, *modi operandis* e seus actores.

Muito embora os órgãos de polícia criminal já comecem a preparar-se para estas novas realidades, nomeadamente através da Criminal Intelligence[43], a primazia da *intelligence* sempre esteve e terá de continuar a estar nos serviços de informações, especialmente se as

[43] Conceito que defende o tratamento e produção de informações por parte dos órgãos de polícia criminal.

acções puserem em risco a segurança de um Estado. No entanto, será uma verdade incontestável que se torna cada vez mais necessária e indispensável uma partilha efectiva de informações entre todos os organismos e instituições aos quais incumbe a defesa da soberania e da segurança dos Estados.

O fenómeno do terrorismo tanto é um problema dos órgãos de polícia criminal como é o dos serviços de informações. Considerando que, após um ataque terrorista, as investigações pós-incidentes são úteis para se determinar certos aspectos do ataque, como o tipo de explosivo utilizado, o meio de entrega e outros meios envolvidos, não será irrelevante conhecer em profundidade o respectivo autor. Para tanto, o cruzamento dos dados apurados ,o confronto das informações recolhidas com alguns padrões estabelecidos vão permitir inferir a identidade do grupo terrorista e antecipar seus eventuais ataques futuros, os propósitos que os animam e as suas relações com outras organizações. Assim, só um trabalho partilhado entre organismos permitirá descobrir padrões semelhantes de actividade terrorista levando-se à detenção dos elementos e impedindo novos actos terroristas.

Esta mudança que resultou da globalização, isenção de fronteiras e criação do ciberespaço, também obrigou a mudanças em toda uma linha de funcionamento dos serviços de informações, que também tiveram eles de adaptar-se às novas realidades. Para se combater eficazmente o inimigo há que em primeiro lugar, descobri-lo neste mundo sem barreiras e sem fronteiras.

A *intelligence* é, ao mesmo tempo um processo e um produto que tem desempenhado um papel importante na diplomacia e na guerra ao longo da história. E, na presente era da informação, cuja velocidade está num simples clique a sua importância tem se revelado ainda maior.

No final de 2000, a CIA não imaginava que a Al-Qaeda teria capacidade para matar milhares de americanos, através de ataques coordenados e executados sobre o próprio solo dos Estados Unidos. Do mesmo modo, não seguiu o aumento do poder da nebulosa Bin Laden, nem foi advertida a tempo da sua decisão de levar a guerra à própria América. A CIA acreditava que os voluntários para as “missões de sacrifício” eram jovens simplórios, vindos de aldeias do interior e que levavam lavagens ao cérebro. Ora, as 19 “bombas humanas” do 11 de Setembro eram todos originários da burguesia, fizeram os seus estudos universitários no Ocidente, e falavam correctamente duas línguas de entre as muitas e diferentes línguas, dispondo de qualificações profissionais e habilitações académicas. O

seu projecto terrorista foi preparado desde longa data e executado sem fraquejar (BAUER,RAUFER 2003)".

A transformação das ameaças tradicionais que deixaram de ser originadas por adversários política e geograficamente identificados e o aparecimento de novos riscos e de novas ameaças originados por adversários múltiplos e com diferentes características de difícil identificação e localização, conduziu a que se aposta cada vez mais na prevenção para que, de alguma forma, os possam tentar evitar.

Emerge então um novo paradigma, genericamente não-governamental, não-convencional, dinâmico, não linear, com regras de empenhamento desconhecidas, pelo menos de um dos lados, com um modo de actuação e doutrina assimétrica e imprevisível, reforçada com o aparecimento de cada vez mais lobos solitários prontos para agirem sozinhos em prol de uma causa (GARCIA,2009). Apesar de estar-se na presença de um novo paradigma a tipologia da ameaça não é alterada, sendo que apenas mudaram os meios utilizados para a sua efectivação e o ciberespaço começa a ser cada vez mais aproveitado para a execução de algumas ameaças.

Não é preciso ter olhos abertos para ver o sol, nem é preciso ter ouvidos afiados para ouvir o trovão. Para ser vitorioso você precisa ver o que não está visível. Sun Tzu"

Tendo em conta a diversidade de ataques possíveis, e tomando como certa a velha máxima "que o bandido está à frente da polícia" torna-se quase impossível dotar os países de todas as tecnologias possíveis para se evitarem com eficácia todos possíveis ataques assim como proteger todos os alvos atacáveis. A velha técnica de se estudar os grupos atacantes e de acompanhar os seus desenvolvimentos continua ainda a ser uma das maiores mais-valias não só na prevenção do terrorismo como no seu combate.

A realização de relatórios prévios permitem à *intelligence* apontar a sua mira sobre um sector ou um grupo, quando um perigo preciso começa a configurar-se, antes da sua passagem ao acto propriamente dito. Se um acto hostil pode apesar de tudo ser perpetuado, o facto de se ter feito um diagnóstico correcto irá permitir que ele não se reproduza.

Para compreender a dimensão do pressentir/revelar/projectar, é necessário eliminar tudo aquilo que intelectualmente engendra a ordem anterior do mundo. "*Todas a interpretações da humanidade e do seu destino pedidas de empréstimo às antigas explicações do mundo, retardam a entrada em jogo daquilo que é* "(BAUER,RAUFER 2003).

Se você conhece o inimigo e se conhece, você não precisa de medo dos resultados de cem batalhas. Se você se conhece, mas não o inimigo, para toda vitória você sofrerá também uma derrota. Se você não conhecer nem você, nem o inimigo, você é um tolo e conhecerá derrota em toda batalha. Sun Tzu

No contexto atrás descrito, deverá assim, a *intelligence* realizar acções de contra terrorismo centradas na prevenção dos actos terroristas. Pode dizer-se que acção preventiva deve incidir privilegiadamente na pesquisa, recolha e análise de informações sobre indivíduos/células/grupos cujas acções se relacionem com actividades de incitamento, apoio, propaganda, radicalização violenta ou recrutamento terrorista – ou actividades criminosas que sirvam de suporte à acção terrorista, denominados "crimes instrumentais" do terrorismo – e ainda a constante monitorização e avaliação das ameaças.

Pesquisa essa, que pode vir da recolha de informações em fontes abertas OSINT[44] ou através da HUMINT[45] nomeadamente através de acções encobertas ou através da SIGINT[46], análise de comunicações ou até através da GEOINT[47], análise geoespacial, ou então a partir da STRATINT[48], *intelligence* estratégica ou da MASINT[49], análise através da obtenção de medidas e assinaturas de eventos, entre outras. A HUMINT tem desempenhado um papel importante na nossa sociedade ao longo dos séculos, uma vez que trabalha, fundamentalmente, com informações retiradas de fontes humanas e comunicação interpessoal. As informações podem ser recolhidas, por meio de operações clandestinas (espiões), de observação directa, das missões diplomáticas (adidos militares) e de contra-espionagem, entre muitos outros meios. A complexidade destas operações requer um elevado grau de preparação para qualquer interrogatório, e extracção de informação. Apesar da prática da HUMINT ser arriscada para quem a usa e de trazer consigo muitos problemas associados, a HUMINT pode recolher pedaços crus de *intelligence* que são muitas vezes mais importantes do que a *intelligence* recolhida pela SIGINT. A HUMINT é

[44] Open Source Intelligence - é o termo usado para descrever as informações, obtidas através de dados disponíveis para o público em geral, como jornais, revistas científicas e emissões de TV.
[45] Human Intelligence - Informações obtidas através de seres humanos, como os espiões tradicionais.
[46] Signals Intelligence - é o termo usado para descrever a actividade da recolha de informações através da interceptação de sinais de comunicação entre pessoas ou máquinas
[47] Geospatial Intelligence – é o termo usado para descrever as informações recolhidas através da referenciação geoespacial
[48] Strategic intelligence - refere-se à recolha, processamento, análise e disseminação de informações que são necessárias para a criação de políticas e dos planos militares a nível nacional e internacional
[49] Measurement and Signatures Intelligence - é o termo usado, para descrever as informações obtidas através da obtenção de medidas e assinaturas de eventos, como explosões atômicas

capaz de encontrar significado nos menores pedaços de inteligência, pedaços esses que podem fazer toda a diferença, até para a própria análise da SIGINT.

Hoje em dia surge uma nova categoria de *intelligence*, a CYBINT[50]- Cyber Intelligence/Digital Network Intelligence- informações recolhidas através do ciberespaço- que advém da conjugação da SIGINT (interceptação de sinais de comunicação entre pessoas ou máquinas.) e da HUMINT, utilizando TECHINT. A necessidade do aparecimento de uma forma de *intelligence* ligada ao ciberespaço deve-se ao aumento da ameaça que nele se verifica. A sua especificidade vai permitir à comunidade *intelligence* redireccionar a sua recolha e análise para o ciberespaço.

O Cybint concentra-se num amplo conjunto de questões e ameaças, bem como a necessidade de exploração e pesquisa de desafios numa base diária em oposição aos outros INTs. Um único avanço tecnológico pode colocar uma nação na dianteira por um considerável período de tempo (TANNER,2014).

Actualmente o processo de formação da maioria dos peritos cibernéticos (*cyberexperts*) é predominantemente focado em aspectos tecnológicos, deixando para trás a área clássica da formação em *intelligence*. Sendo a engenharia social[51] uma ameaça à segurança este handicap na formação põe em causa a eficácia da sua detecção. A falsa sensação de que toda a informação necessária para a prevenção é recolhida na internet faz com que a HUMINT seja muitas vezes esquecida. A maior parte dos produtos que existem para a defesa do ciberespaço de um modo geral são apenas capazes de identificar um ataque quando este está a ser executado, mas a capacidade de prever um ataque ou uma intenção de atacar ainda é limitada. A combinação da HUMINT e engenharia social juntamente com os novos meios tecnológicos, pode em alguns casos, localizar possíveis intrusos, antes da fase de desenvolvimento de um ataque, e em muitos casos, antes de se desenvolver em intenções específicas de ataques.

Segundo Howard Schmidt (coordenador de cibersegurança do Presidente dos EUA até 2012), há que ter uma visão holística da segurança. Existe uma ciber dimensão do mundo físico e existe no mundo físico uma dimensão ciber. Se existir um incidente físico, deliberado ou uma catástrofe natural, e ao mesmo tempo houver uma disrupção no mundo cibernético, a situação pode ser bem mais problemática do que se os incidentes ocorrerem

[50] Para maior desenvolvimento sobre o conceito pode consultar-se http://defensetech.org/2011/01/03/cyber-intelligence/

[51] em segurança da informação, refere-se a engenharia social aquando a prática de interações humanas com o intuito de levar a que se revelem dados sensíveis sobre um sistema de computadores ou de informações

de forma distinta no tempo. Por isso, há que ter a consciência destes dois aspectos de modo a protegermo-nos (VERTON, 2013).

A falta desta visão holística e a excessiva dependência nas tecnologias, ignorando as capacidades do factor humano, leva a que muitas acções sejam condenadas ao fracasso. Segundo Margolis, o padrão que emerge quando reflectimos sobre as falhas de *intelligence* do século XX demonstra que uma única forma de recolha de informações, não é completamente eficaz. O fascínio e foco dos EUA sobre as técnicas de inteligência tem feito com que algumas operações especialmente susceptíveis tenham fracassado quando as áreas de HUMINT não foram abordadas (MARGOLIS,2013).

Conhecendo os grupos de terroristas sobre as formas de Intel utilizada pelos serviços de informações, eles irão utilizar cada vez menos esses meios detectáveis e voltarão às velhas técnicas de comunicação.

3.2 O PAPEL DOS SERVIÇOS DE INTELLIGENCE NAS ESTRATÉGIAS NACIONAIS DE CIBERSEGURANÇA

O combate ao ciberterrorismo implica um reforço das medidas de segurança. Neste âmbito, há que, nomeadamente, prevenir, detectar, actuar nas circunstâncias, averiguar, e provar em tribunal. Estas acções, bem como outras que o referido combate requer, traduzem-se em muitos casos em intromissões na privacidade dos cidadãos, um dos vários aspectos em que o referido combate interfere com as liberdades fundamentais a que estamos habituados nas nossas sociedades democráticas ocidentais. Poder-se-á mesmo afirmar que essa interferência decorre não só do referido combate ao terrorismo mas também do combate à criminalidade em geral embora o caso do terrorismo granjeie no seio das comunidades e da Lei um maior apoio a essa interferência (GOMES).

Muitos são os Estados que já dispõem de estratégias de cibersegurança bem definidas e de estruturas apropriadas.

Country	Strategy Development	Policy Implementation	Public Sector: Policy	Public Sector: Law	Private Sector: For-Profit	Private Sector: Not-For Profit
New Zealand	*Minimal*	*Modest*	*Significant*	*Modest*	*Minimal*	*Significant*
Australia	*Modest*	*Modest*	*Significant*	*Modest*	*Significant*	*Minimal*
UK	*Significant*	*Significant*	*Significant*	*Modest*	*Significant*	*Minimal*
US	*Significant*	*Significant*	*Modest*	*Significant*	*Significant*	*Modest*
Germany	*Significant*	*Significant*	*Significant*	*Significant*	*Modest*	*Minimal*
France	*Modest*	*Modest*	*Modest*	*Significant*	*Modest*	*Modest*
Romania	*Minimal*	*Minimal*	*Significant*	*Modest*	*Minimal*	*Minimal*
Russia	*Minimal*	*Minimal*	*Modest*	*Minimal*	*Modest*	*Minimal*
Belarus	*Modest*	*Significant*	*Significant*	*Significant*	*Minimal*	*Minimal*
Ukraine	*Significant*	*Modest*	*Minimal*	*Minimal*	*Minimal*	*Minimal*
Estonia	*Minimal*	*Minimal*	*Significant*	*Minimal*	*Modest*	*Modest*
Lithuania	*Modest*	*Minimal*	*Minimal*	*Minimal*	*Minimal*	*Minimal*
Latvia	*Significant*	*Minimal*	*Minimal*	*Significant*	*Minimal*	*Modest*
China	*Minimal*	*Minimal*	*Modest*	*Modest*	*Minimal*	*Minimal*

Segundo um estudo comparativo[52] feito pelo "*PRIVACY AND CYBER CRIME INSTITUTE*", são várias as conclusões que podem ser tiradas do quadro acima exposto. Primeiro, os Estados Unidos, Reino Unido e Alemanha são os líderes mundiais em matéria de desenvolvimento e implementação de estratégias de cibersegurança. Em segundo lugar, enquanto que os EUA e o Reino Unido dão um maior papel ao sector privado como parte de suas estratégias, a Alemanha tende a colocar mais ênfase no sector público e no legislativo. Em terceiro lugar, e como se pode esperar os países alinham-se no ciberespaço de acordo com a sua geopolítica. (LEWIN at al, 2011).

Segue-se uma enunciação sumarizada das Estratégias de Cibersegurança dos seguintes países: Alemanha, Reino Unido, França, Espanha e Estados Unidos da América, e qual o papel que os serviços de informações desempenham nessas estratégias. Optou-se pela Alemanha, Reino Unido e EUA por serem os países mais completos em matéria de cibersegurança. Por Espanha pela sua proximidade geográfica a Portugal e pela França pelas semelhanças que tem connosco no sistema judicial[53].

[52] "Securing Cyberspace: A Comparative Review of Strategies Worldwide" , o quadro exposto pode ser consultadoem http://www.ryerson.ca/content/dam/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf

[53] No caso específico da vigilância do terrorismo na Internet, é promovida pelos serviços de informações franceses que ao detectar ameaças especificas reportar ao Ministério Publico Francês. O juiz ou o procurador analisada a ameaça, autoriza o órgão de policia criminal competente a vigiar o/os suspeitos. (UNODC – The use of internet fot terrorist purposes , 2012)

Da leitura dos referidos documentos há um aspecto importante a reter. Encontra-se em todos um denominador comum e que consiste, por um lado, no facto de que esses Estados reconhecem que o sucesso em matéria de cibersegurança não dispensa o reforço da colaboração e da cooperação entre si e, por outro, de que começa a sentir-se a necessidade de aprovação de um conjunto de normas de conduta, justas e responsáveis, que sejam partilhados por todos os Estados ou, pelo menos, por um maior número possível de Estados.

3.3 ESTRATÉGIAS DE CIBERSEGURANÇA DE OUTROS PAÍSES

3.3.1- ESTRATÉGIA DE CIBERSEGURANÇA DA ALEMANHA

No documento da Estratégia de Cibersegurança Alemã, o Estado Federal Alemão reconhece que, fazendo parte de um mundo em crescente conexão, o Estado, as suas infraestruturas críticas, os negócios e os seus cidadãos dependem do funcionamento seguro das tecnologias de informação e da Internet.

O Estado Alemão procurou dar um substancial contributo para assegurar um ciberespaço seguro, de modo a manter e a elevar a prosperidade económica e social do país.

Neste contexto, o nível de cibersegurança alcançado é a soma de todas as medidas nacionais e internacionais que foram tomadas para proteger o acesso às tecnologias de informação e de comunicação, a integridade, a autenticidade e a confidencialidade dos dados no ciberespaço. A cibersegurança deve basear-se numa abordagem abrangente e polivalente, exigindo uma maior partilha e coordenação da informação. A estratégia de cibersegurança concentra-se em abordagens e medidas sociais. São complementadas por medidas tomadas pelo "Bundeswehr[54]" para proteger as suas próprias competências e medidas no âmbito das orientações recebidas para fazer da cibersegurança parte da estratégia preventiva de segurança da Alemanha.

Neste contexto foi criado o Centro Nacional de Ciberresposta (National Cyber Response Center) que depende do Departamento Federal de Informação e coopera directamente com o Departamento Federal de Defesa da Constituição (BSI) e com o Departamento Federal

[54] São as Forças Armadas da Alemanha.

de Protecção Civil de Assistência em Calamidades (BBK). O Departamento Federal de Polícia Criminal (BKA), a Polícia Federal (BPOL), o Departamento Criminal de Alfândegas (ZKA), o Serviço Federal de Intelligence (BND) e outros, participam neste Centro, no âmbito das suas atribuições e competências. O Centro analisa os incidentes e dá as recomendações necessárias para se atuar. O Centro submete regularmente recomendações ao Conselho Nacional de Cibersegurança[55] relativamente a casos específicos. Se a situação de cibersegurança entrar num nível de uma iminente ou efectiva crise, o Centro informará directamente o Secretário de Estado junto do Ministério Federal do Interior.

Assim os serviços de informações fazem parte integrante do Centro Nacional de Ciberreposta trabalhando em cooperação com outros organismos em defesa da segurança nacional. A título de resumo a Estratégia Nacional Alemã[56] para a cibersegurança tem como principais objectivos internos:

1.- Protecção das infra-estruturas críticas.

Trata-se da principal prioridade. Os sectores público e privado devem criar uma reforçada estratégia e uma base organizacional para uma coordenação mais próxima, baseada numa troca intensificada de informações.

Com isto, a cooperação estabelecida no plano de implementação do CIP (Critical Information Protection) será sistematicamente ampliada. Com a colaboração do Conselho Nacional de Cibersegurança, a integração de novos sectores serão apreciados e a introdução de novas tecnologias relevantes será apreciada, e bem assim, quais as medidas protectoras que deverão ser tornadas obrigatórias ou quais as ameaças sobre as quais se deve actuar.

2.-Proteção dos sistemas TIC

[55] Do Conselho fazem parte: a Chancelaria Federal e o Secretário de Estado de cada Departamento de Negócios Estrangeiros, o ministro federal do Interior, o ministro federal da Defesa, o ministro federal de Economia e Tecnologia, o ministro federal de Justiça, o ministro federal das Finanças, o ministro federal de Educação e Investigação. Em certas ocasiões poderão ser convocados outros ministérios. Representantes do mundo dos negócios serão convidados como membros associados. A missão do Conselho é de coordenar os mecanismos de prevenção e as abordagens interdisciplinares de cibersegurança do sector público e do sector privado. O Conselho complementará e interligará a gestão das TI ao nível federal, e o trabalho desenvolvido pelo Conselho de Planeamento das TI na área da cibersegurança a nível político e estratégico.

[56] Cyber Security Strategy for Germany

Em matéria de protecção das infra-estruturas, a atenção deve incidir mais nos sistemas TIC utilizados pelos cidadãos e pelas empresas de média dimensão. Com a preocupação de se considerar a responsabilidade dos fornecedores de TIC sobre a colocação de produtos e de serviços seguros no mercado.

3.- Reforço da segurança das TIC na administração pública

Considerando que a administração pública deve ser o exemplo em matéria de seguranças das TIC sugerem a criação de uma " Network infrastructure" comum, uniforme e segura, na administração federal que será a base para a comunicação electrónica áudio e de informação. Será esta permanentemente monitorizada por forma a detectar as melhorias a introduzir.

4- Controle efectivo do crime no ciberespaço:

Devendo ser reforçadas as capacidades das autoridades responsáveis pela aplicação da lei, do Departamento Federal de Segurança da Informação e do sector privado para combaterem o cibercrime, assim como relativamente à protecção contra a espionagem e a sabotagem.

Para melhorar a troca de conhecimentos (*know how*) o governo federal tenciona criar organismos conjuntamente com a indústria, com o envolvimento de organismos de autoridade que actuarão como consultores.

Para enfrentar a ameaça de um aumento global de cibercrimes, deverá ser feito um esforço para se atingir uma harmonização global das leis, com base na Convenção Cibercrime do Conselho da Europa. Irá considerar se será necessário haver convenções adicionais nesta área, ao nível das Nações Unidas.

5- Utilização de tecnologia segura e de confiança:

A Alemanha continuará e intensificará a investigação sobre a segurança das TIC e sobre a protecção das infra-estruturas críticas.

Serão reforçadas a supremacia tecnológica e a capacidade alemã em todos os níveis de competências estratégicas no âmbito das TIC, incluindo-as nas suas estratégias políticas, desenvolvendo-as ainda mais.

6- Desenvolvimento dos recursos humanos nas autoridades federais

Ao ser atribuída uma importância estratégica à cibersegurança, deve ser examinada como uma prioridade, se será necessário o reforço de pessoal nessas autoridades.

Além disso, a intensificação da mobilidade do pessoal entre as autoridades federais e ações de formação adequadas aumentará a cooperação interministerial.

7- Instrumentos para responder a ciberataques:

Se um Estado quer estar preparado contra ataques cibernéticos, um vasto e coordenado conjunto de mecanismos deve ser criado em cooperação com as suas competentes autoridades.

Com a implementação dos objectivos e medidas estratégicos, o governo federal contribuiu para assegurar a cibersegurança e, assim, a liberdade e a prosperidade na Alemanha.

No entanto os continuados ciberataques a organismos públicos e privados alemães, levaram a que se repensasse as politicas de cibersegurança e que fossem estudadas estratégias alternativas, até à data nenhuma foi efectivamente posta em prática tendo em conta que se começou a criar um excesso de regulamentação e uma sobreposição constante de competências[57].

A estrita separação constitucional de responsabilidades civis e militares cria um desafio para uma abordagem integrada, particularmente no que concerne à defesa (militar) e à *intelligence* (civil).

3.3.2 DEFESA E SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO- A ESTRATÉGIA DE FRANÇA

Em 2008 o Presidente Francês[58] considerou a cibersegurança como uma das grandes prioridades da defesa Nacional. Perante o impacto crescente do ciberespaço no contexto da sua segurança nacional, criou, em 2009, a Agência Nacional de Segurança dos Sistemas de Informação (Agence Nationale de la Sécurité des Systèmes d'Information ou ANSSI[59]) para dar resposta às necessidades das instituições públicas, empresas e cidadãos. Em 2011, o Presidente tomou a decisão de tornar a Agência responsável pela defesa dos sistemas de informação a acrescentar ao seu papel de segurança. A ANSSI depende directamente do primeiro ministro embora seja supervisionada pelo Secretário Geral para a Defesa Nacional. Funciona como coordenador da acção governamental e nas suas missões incluem-se o fornecimento de meios seguros às agências de comunicações, inspeccionando

[57] http://www.lexology.com/library/detail.aspx?g=1f872876-3d23-44e7-a8f1-92a9be8d080b revisitado em 23 de Junho 2014

[58] "The French Whitepaper on defence and national security 2008," Présidence de la République, June 2008 consultado em 15 de Abril de 2014

[59] http://www.ssi.gouv.fr/fr/anssi/organisation/ revisitado em 2 de Junho de 2014

os sistemas de governo, actuando como um CERT do governo, fornecendo certificação de sistemas de protecção de segredos de Estado, agindo como um ponto de contacto e internacional oferecendo formação.

Sob a dependência da ANSSI funciona o Centro Operacional de Segurança dos Sistemas de Informação (COSSI) que tem como objectivo exercer uma monitorização continua, detectando e alertando para a existência de incidentes e/ou vulnerabilidades que possam colocar em causa a segurança das informações do Estado ou a sistemas importantes da sociedade de informação. Coordenando as estratégias e o planeamento de medidas de reposta aos ataques cibernéticos.

O ANSSI funciona como estrutura autónoma não integrando nele outros serviços nomeadamente o Serviço de Informações francês com a competência para a prevenção do terrorismo a Direcção Geral para a Segurança Externa (DGSE)[60] no entanto a DGSE tem lugar no Comité Estratégico para a Segurança dos Sistemas de Informações[61], que propõe as orientações estratégicas que deverão ser seguidas na agência.

A estratégia francesa assenta em quatro OBJETIVOS principais:

1.- Tonar-se uma potência mundial em ciberdefesa:

Mantendo a sua independência estratégica, a França deve trabalhar no sentido de assegurar a sua presença no círculo das nações líderes na área da ciberdefesa. Assim, beneficiará dos efeitos multiplicadores da cooperação, tanto a nível operacional como na implementação de uma estratégia unificada para enfrentar as ameaças.

2.- Salvaguardar a capacidade da França para tomar decisões através da protecção da informação relacionada com a sua soberania

As autoridades governamentais e os atores de gestão de crises devem ter os recursos para comunicar em qualquer situação e em total confidencialidade. As redes que respondem a estas necessidades devem ser alargadas, principalmente a nível local.

Para assegurar a confidencialidade da informação que circula nestas redes, exige a segurança desses produtos. Há que ter conhecimentos especiais para os desenhar e optimizar o seu desenvolvimento e métodos de produção.

3.- Reforçar a cibersegurança das infra-estruturas críticas nacionais

Um ataque bem-sucedido num sistema crítico de informação francesa pode ter graves consequências humanas e económicas. Em estreita colaboração com importantes

[60] http://www.defense.gouv.fr/english/dgse revisitada em 20 de Junho 201
[61] Décret n° 2009-834 du 7 juillet 2009 Artº7

fabricantes de equipamentos e operadores, o Estado deve actuar no sentido de garantir e melhorar a segurança destes sistemas críticos.

4.- Assegurar a segurança no ciberespaço

Em termos de luta contra o cibercrime, a França promoverá o reforço da sua actual legislação e da sua cooperação judicial internacional. De modo a atingir esses objectivos, são definidas sete áreas de acção:

- Antecipar e analisar o ambiente, de modo a tomar as decisões apropriadas.

-Detectar e impedir ataques, alertar e apoiar as potenciais vítimas.

- Fortalecer e perpetuar as capacidades científicas, técnicas, industriais e humanas de modo a manter a independência

- Proteger os sistemas de informação do Estado e os operadores de infraestruturas críticas para garantir uma melhor resiliência nacional

- Adaptar a legislação francesa para incorporar desenvolvimentos tecnológicos e novas práticas

- Desenvolver colaboração internacional, iniciativas nas áreas de segurança dos sistemas de informação, ciberdefesa e combate ao cibercrime de modo a melhorar a protecção dos sistemas nacionais de informação

- Comunicar, informar, e convencer com vista a aumentar a compreensão da população francesa sobre a dimensão dos desafios relacionados sobre a segurança dos sistemas de informação.

3.3.3 A ESTRATÉGIA DE CIBERSEGURANÇA DO REINO UNIDO

No Reino Unido, a Estratégia Nacional de Segurança que foi definida em 2011 considerou o ciberataque como uma ameaça que punha em causa as informações, os respectivos sistemas e a economia do país.

Para o combater, foi definido um plano estratégico de quatro anos, que se estenderá assim até 2015, no qual será investida uma verba de 650 milhões de libras. A distribuição deste orçamento sugere que Comunidade de inteligência britânica seja uma entidade chave em questões de cibersegurança, com destaque ao papel relevante da agência de *intelligence* de comunicações do governo (GCHQ) (ROBINSON Et al, 2013). Estando incluído no orçamento verbas para acções de partilha de SIGINT com o Ministério da Defesa, entidade

reconhecida na estratégia como tendo um papel importante na melhoria da compreensão e redução das vulnerabilidades e ameaças no ciberespaço (OCDE2012)[62].

Para efectivar a estratégia foi criado um gabinete Garantia de Cibersegurança da Informação (OCSIA Office of Cyber Security and Information Assurance) que apoia o Ministro do Gabinete e o Conselho de Segurança Nacional. É à OCSIA que cabe a estratégia nacional de cibersegurança. Tem como missão o fornecimento de orientação estratégica, apoio à educação, conscientização e formação, trabalhando em parceria com o sector privado, o Gabinete da Informação (OGCIO) para garantir a resiliência e a segurança das infra-estruturas do governo, interagindo ao mesmo tempo com parceiros internacionais. É um órgão de coordenação sendo o papel do OCSIA aproveitar a estreita cooperação e coordenação entre as diversas agências a nível nacional e departamentos e promover a criação de política comum. O OCSIA, juntamente com o Centro de operações para a cibersegurança (CSOC)[63]a, trabalha com departamentos e serviços governamentais, tais como o Ministério do Interior, o Ministério da Defesa, a agência de *intelligence* de comunicações do governo (GCHQ) , Grupo de segurança electrónica de comunicações, Centro para a Protecção da Infra-Estrutura Nacional e de Negócios. Além destes, as políticas de segurança envolvem, o regulador das comunicações (OFCOM) o Gabinete do Comissário de Informação e Departamentos de polícia, como a Agência do Crime Organizado e da Unidade e-crime da Polícia Central.

A estratégia inglesa reforça a centralização dos serviços de informações e do Ministério da Defesa na compreensão do fenómeno e na redução das ameaças e vulnerabilidades.

São quatro os objectivos principais dessa Estratégia:

1º Objectivo: Atacar o cibercrime e tornar o Reino Unido num dos lugares mais seguros do mundo para se fazerem negócios no ciberespaço.

Abordagem :

a) Travar os cibercrimes:

- Reduzindo as vulnerabilidades online
- Restringindo as actividades criminosas online

[62] OECD (2012), "Cybersecurity Policy Making at aTurning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", OECD Digital Economy Papers, No. 211, OECD Publishing

[63] Este centro criado pela estratégia de segurança em 2009 , foi criado para monitorizar activamente a saúde do ciberespaço, proporcionar o conhecimento da situação colectiva, permitir uma melhor compreensão dos ataques contra redes da uk e coordenar a resposta a incidentes e fornecer informação e aconselhamento sobre os riscos para as empresas e para o público. Funciona como uma multi-agência organizada pelo GCHQ.

- promovendo parcerias mais eficazes

b) Tornar mais seguro fazer negócios no ciberespaço:

- Aumentado os alertas e a visibilidade das ameaças
- Protegendo as informações e os serviços
- Fortalecendo uma cultura que domine os riscos
- Promovendo a confiança no ciberespaço.

2º Objectivo: Tornar o Reino Unidos resistente a ataques cibernéticos e ser capaz de defender os seus interesses no ciberespaço.

Significa reorganizar e recentrar os recursos para encontrar novas formas de se reforçar a segurança nacional

3º Objectivo: O Reino Unido quer ajudar a moldar um ciberespaço aberto, estável e vibrante, que a sua população possa utilizar com segurança e que apoie as sociedades abertas.

Abordagem:

a) Ajudando a moldar o desenvolvimento do ciberespaço:

- Promovendo um ciberespaço aberto e interoperacional
- Promovendo as liberdades e os direitos fundamentais

b) Protegendo o estilo de vida:

- Assegurando a segurança sem se comprometer os valores

4º Objectivo: O Reino Unido disponha de conhecimentos cruzados, aptidões e competências de que precisa para sustentar os objectivos de cibersegurança.

Abordagem:

a) Alargando o conhecimento:

- Construindo uma agenda de investigação cruzada
- Aprofundando a compreensão das ameaças, vulnerabilidades e riscos

b) Elevando as aptidões:

- Construindo uma cultura que entenda os riscos e capacite as pessoas a usarem o ciberespaço e melhorando as aptidões de cibersegurança em todos os níveis.

c) Desenvolvendo as capacidades:

- Construindo capacidades técnicas
- Aumentando as competências para responder a incidentes.

As metas a atingir são de que todas as medidas que foram apontadas coloquem, em 2015, o Reino Unido numa situação em que:

- as leis estão a travar os cibercriminosos
- os cidadãos sabem o que devem fazer para se protegerem
- uma cibersegurança eficaz seja vista como positiva para o negócio no Reino Unido
- um bem sucedido sector de cibersegurança tenha sido estabelecido
- os serviços públicos online são seguros e resistentes
- as ameaças ás infraestruturas e à segurança nacional foram confrontadas.

3.3.4 ESTRATÉGIA DE CIBER SEGURANÇA DE ESPANHA

Em Espanha, a Estratégia de Cibersegurança é adoptada sob, e em alinhamento com a Estratégia Nacional de Segurança de 2013, que incluiu a cibersegurança nas suas 12 áreas de acção.

A Estratégia Nacional de Cibersegurança é, assim, um documento que fornece ao governo espanhol as bases para o desenvolvimento das disposições da Estratégia Nacional de Segurança sobre a protecção do ciberespaço, de modo a implementar a prevenção contra ciberataques, a defesa, detecção, acções de resposta e de recuperação contra ciberataques.

A estratégia de segurança destaca a questão da cibersegurança como eixo fundamental da sociedade e do sistema económico espanhol, destacando o papel do Centro Nacional de Inteligência (CNI) como fundamental ao nível da prevenção. De realçar que já em 2002 o CNI[64] foi designado como responsável em garantir a segurança das tecnologias de informação na administração pública

A Estratégia Espanhola compõe-se de 5 Capítulos:

1º Capitulo - Ciberespaço e a sua segurança – traça as características que definem o ciberespaço, as oportunidades que este oferece e as implicações de segurança por dele se depender. Mostra as características particulares que são comuns às ciberameaças e a elevada dependência da economia e dos serviços no ciberespaço o que faz aumentar os riscos e as ameaças com um grave impacto na segurança nacional.

2º Capítulo – Objectivos e princípios orientadores de cibersegurança – Estabelece como objectivo geral a definição de linhas gerais de orientação relativamente ao uso seguro do ciberespaço, através de uma visão abrangente que envolve a coordenação das autoridades públicas, o sector empresarial e os cidadãos, seguindo o caminho das iniciativas

[64] Cortes Generales, Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. 2002

internacionais neste campo, relativamente às leis nacionais e internacionais e em linha com outros documentos estratégicos nacionais e internacionais.

A Estratégia fixa seis objetivos específicos:

- Assegurar que os sistemas de informação e de comunicação utilizados pelas autoridades públicas tenham um elevado nível de segurança e de resiliência
- Fortalecer os sistemas de informação e de comunicação que são utilizados pelo sector privado em geral e pelos operados de infra-estruturas críticas em particular
- Reforçar as capacidades de prevenção, detecção, reacção, análise, recuperação, resposta, de investigação e de coordenação perante actividades terroristas e crimes no ciberespaço
- Alertar os cidadãos, profissionais, empresas e as autoridades públicas sobre os riscos derivados do ciberespaço
- Ganhar e manter o conhecimento, aptidões, experiência e capacidades tecnológicas para suportar os objectivos de cibersegurança
- Contribuir para aumentar a cibersegurança na esfera internacional

As principais linhas orientadoras da cibersegurança são: a liderança nacional e a coordenação de esforços; a partilha de responsabilidades; a proporcionalidade, racionalidade e eficiência; a cooperação internacional.

3º Capítulo – Define as linhas de acção na cibersegurança nacional.

Definem-se oito principais Linhas de Orientação:

- Capacidade para prevenir, detectar, responder e recuperar relativamente a ciberataques
- Segurança dos sistemas de informação e de comunicação que suportam as autoridades públicas
- Segurança dos sistemas de informação e de comunicação que suportam as infraestruturas
- Capacidade para investigar e actuar sobre o ciberterrorismo e sobre o cibercrime
- Segurança e resiliência das tecnologias de informação e de comunicação no sector privado
- Conhecimento e aptidões
- Cultura de cibersegurança

Envolvimento internacional

Estrutura organizacional:

a) Conselho Nacional de Segurança, presidido pelo Primeiro-ministro

b) Comissão Especializada de Cibersegurança, que apoia o Conselho Nacional de Segurança, assistindo o Primeiro-ministro na direcção e coordenação da Política de Segurança Nacional na área de cibersegurança.
c) Comissão Especializada de Situações (que lida com as situações de crise no campo da cibersegurança).

3.3.5 ESTRATÉGIA INTERNACIONAL DE CIBERSEGURANÇA DOS ESTADOS UNIDOS DA AMÉRICA

O presidente Barack Obama e a secretária de Estado, Hillary Rodham Clinton, apontaram a questão cibernética como uma das principais prioridades da política externa dos EUA. O presidente emitiu uma Revisão da Política Nacional para o Ciberespaço em 2009. Em maio de 2011, o governo divulgou a Estratégia Internacional para o Ciberespaço expondo nossas prioridades de política externa referentes ao espaço cibernético. A secretária Hillary Clinton descreveu essas prioridades como "um novo imperativo para a política externa que o Departamento de Estado vem pondo em prática e na qual continuará a ter um papel fundamental"[65].
A missão da cibersegurança é assim, uma missão do Executivo, centralizada na pessoa do Presidente. Assim é escolhido de entre os membros do gabinete da Casa Branca um coordenador de cibersegurança, que trabalha em conjunto com o gabinete federal de informações e com Conselho Nacional de Economia.
Dentro da Secretaria da Segurança Nacional é criado um Gabinete de Cibersegurança e Comunicações(CS&C)[66] que tem como missão assegurar a segurança, a resiliência e a confiança nas infra-estruturas nacionais de comunicação no ciberespaço. O CS&C trabalha para prevenir ou minimizar as disrupções nas infra-estruturas de informações críticas, a fim de proteger o público, a economia e os serviços governamentais. Liderando os esforços para proteger o governo federal, o domínio ". Gov" as redes do governo civil e de colaborar activamente com o sector privado, aumentando a segurança do domínio ". Com". Além disso, o Centro de Cibersegurança Nacional e Integração de Comunicações (NCCIC) monitoriza o ciberespaço 7 dias por semana, 24 horas por dia.

[65] www.state.gov/cyber - visitado em 15 de abril de 2014

[66] http://www.dhs.gov/office-cybersecurity-and-communications revisitado em 15 de Junho 2014

Nos Estados Unidos da América o director da Agência Nacional de Segurança (NSA) é cumulativamente o directo do Centro de Comando do Ciberespaço.

Para os EUA, definem-se como os cinco princípios a que devem subordinar-se as normas no ciberespaço:

- Apoio das liberdades fundamentais
- Valorização da privacidade
- Respeito pela privacidade
- Protecção contra o crime
- Direito de auto-defesa

No que concerne a aspectos a serem considerados pelos Estados na elaboração da respectiva legislação relativamente à cibersegurança:

-Interoperacionalidade global - os Estados devem actuar no âmbito das suas autoridades para ajudarem a assegurar a interoperacionalidade de uma Internet que seja acessível a todos

- Estabilidade das redes – Os Estados devem respeitar a livre circulação na configuração das suas redes nacionais, assegurando que não interferirão arbitrariamente nas redes internacionalmente interconectadas

- Acesso seguro – Os Estados não devem arbitrariamente privar ou interromper o acesso individual à Internet ou outras tecnologias em rede

- Administração partilhada – a administração da Internet não deve estar limitada ao governo, mas deve incluir todos os parceiros adequados

- Cibersegurança face a Diligência – os Estados devem reconhecer e actuar, sob a sua responsabilidade, para proteger as infra-estruturas de informação e para tornar seguros os sistemas nacionais contra danos ou má utilização.

Numa abordagem estratégica os EUA comprometem-se a preservar e a fortalecer os benefícios das redes digitais às suas sociedades e economias, com a consciência que o crescimento destas redes trazem novos desafios para a sua segurança nacional e a da sua economia, bem como para a comunidade global. Preparando-se para enfrentar esses desafios enquanto preservam o seu código de princípios.

Pretendem os EUA que o seu papel no futuro ciberespaço tenha cumpra os seguintes objectivos :

- Objectivo diplomático: os EUA trabalharão para criar incentivos e construir um largo consenso e um ambiente internacional no qual os Estados- reconhecendo os valores

intrínsecos de um ciberespaço aberto, interoperacional, seguro e de confiança – trabalhem conjuntamente e atuem como parceiros responsáveis

- Objectivo de defesa: Os EUA, juntamente com outras nações, colaborarão para encorajar comportamentos responsáveis e oporem-se àqueles que procuram destruir redes e sistemas, dissuadindo e actuando contra actores malévolos, e reservando-se o direito para defender estas estruturas nacionais vitais, como julgar necessário e apropriado

- Objectivo de Desenvolvimento: Os EUA facilitarão a capacidade de construir a cibersegurança além das suas fronteiras, bilateralmente ou através de organizações multilaterais, de modo que cada país disponha dos seus meios para proteger as sua infra-estruturas, reforçar as redes globais, e construir parcerias no consenso sobre redes abertas, interoperacionais, seguras e de confiança

Relativamente às politicas os EUA defendem a seguinte linha de actuação :

- Economia: Manter um ambiente de comércio livre que encoraja inovações tecnológicas no âmbito da acessibilidade e redes ligadas globalmente; proteger a propriedade intelectual, incluindo o segredo de negócios comerciais contra roubo; assegurar o primado da interoperacionalidade e a segurança dos padrões técnicos, determinados tecnicamente por peritos

- Protecção das redes nacionais: promover a cooperação no ciberespaço, particularmente sobre normas de conduta para os Estados e cibersegurança , bilateralmente e em linha com organizações multilaterais e parceiros multinacionais; reforçar intrusões e disrupções das redes americanas; assegurar uma administração forte de incidentes, resiliência, e capacidades de recuperação de infra-estruturas de informação; melhorar a segurança da cadeia de fornecimento de alta tecnologia, em consulta com as indústrias.

- Estado de direito: Participar em pleno no desenvolvimento de políticas internacionais de cibercrime; harmonizar leis internacionais de cibercrime, alargando o acesso à Convenção de Budapeste; focalizar as leis de cibercrime no combate de actividades ilegais, não restringindo o acesso à Internet; recusar a terroristas e outros criminosos a faculdade para explorarem a Internet para operações de planeamento, financiamento e ataques.

- Militarmente: reconhecer e adaptar às crescente necessidades militares por redes seguras e de confiança; construir e reforçar as existentes alianças militares para combater potenciais ameaças no ciberespaço; aumentar a cooperação no ciberespaço com aliados e parceiros para aumentar a segurança colectiva.

- Administração (governance) da Internet: priorizar a abertura e a inovação relativamente à Internet; preservar a segurança e a estabilidade das redes globais, incluindo no domínio no sistema de nomes (DNS); promover e reforçar a entrada de parceiros para a discussão sobre assuntos de administração (governance)
- Desenvolvimento internacional: facultar os necessários conhecimento, formação e outros recursos a países que procuram construir capacidades técnicas e de cibersegurança; desenvolver e partilhar permanente e regularmente as boas práticas internacionais em cibersegurança; elevar as competências dos Estados para combater o cibercrime- incluindo formação dos agentes de autoridade, especialistas forenses, juristas e legisladores; desenvolver relações com políticos para elevar a construção de capacidade técnicas, proporcionando contactos regulares entre peritos e seus colegas do governo americano
- Liberdade na Internet: suportar os atores da sociedade civil para alcançarem plataformas seguras e de confiança para as liberdades de expressão e de associação: colaborar com a sociedade civil e organizações não governamentais para estabelecerem mecanismos de segurança protegendo as suas actividades na Internet contra intrusões digitais ilegais; encorajar a cooperação internacional para a protecção da privacidade dos dados comerciais; assegurar a interoperacionalidade de uma Internet acessível a todos.

Capítulo 4

O CASO PORTUGUÊS

A criminalidade originada pelas novas tecnologias, como a internet, comunicações *wireless*[67] e outras redes de computadores têm trazido muitos problemas às polícias de todo o mundo não só pela sua difícil detecção como também devido à falta de legislação actualizada e eficaz para a combater.

É também no contexto das Tecnologias da Informação e Comunicações (TIC) e da internet, que surgem novas formas de radicalismo associadas a outros actores não estatais, cujo poder é tendencialmente crescente, como seja o ciberterrorismo, enquanto variante do terrorismo dito tradicional ou convencional.

O ciberterrorismo é um termo de ainda difícil definição que não se encontra legislado em qualquer código português.

Esta nova linha de actuação emergente, que é o ciberterrorismo, que se traduz na exploração das oportunidades proporcionada pelo ciberespaço, como vector privilegiado na condução de acções terroristas, e das vulnerabilidades dos Estados, no que concerne à massiva utilização das tecnologias de informação e comunicações na gestão das chamadas infra-estruturas críticas nacionais, não pode ser negligenciada ou ignorada, pelo que deve fazer parte das actuais preocupações das unidades políticas estatais com atribuições de responsabilidade na segurança nacional.

É chegado o momento de indagar como o direito português encara quer o fenómeno terrorista, quer a ocorrência do ciberterrorismo. Tal como nos ordenamentos jurídicos da generalidade dos países ocidentais, este tipo de actividades ou dos actos em que encontram expressão são prevenidos e combatidos pelos meios considerados mais adequados e eficazes.

[67] Uma rede sem fio (ou comunicação sem fio) refere-se a uma passagem aérea sem a necessidade do uso de cabos – sejam eles telefônicos, coaxiais ou ópticos

4.1 LEGISLAÇÃO PORTUGUESA

Os Estados são pessoas jurídicas de direito internacional que se formam para defesa dos interesses das comunidades de cidadãos que os integram. O impulso agregador radica, *prima facies*, na segurança de cada pessoa singular individualmente considerada e daqueles a quem, não tendo voz, ele possa chamar seus. Tratava-se – e trata-se ainda – de proteger a vida ou a integridade física e a propriedade, face às agressões externas e às investidas que, no quadro da comunidade a que cada pessoa pertence, são desferidas pelos seus pares.

Para o que nos interessa, a Constituição da República Portuguesa (adiante designada por CRP) declara Portugal, na conjugação dos seus artigos 1º[68] e 2º[69], como um Estado soberano. Na especificação das tarefas fundamentais do Estado, vertidas no artigo 9º do mesmo diploma, os constituintes não quiseram deixar de destacar nas duas primeiras alíneas, das oito que constituem a norma, aquilo que são, de facto, os interesses primeiros dos cidadãos, quais sejam o de "garantir a independência nacional "[70] e o de "garantir os direitos e liberdades fundamentais"[71].

Na forma tradicional, a defesa nacional constitui uma incumbência do Estado e "tem por objectivos garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas", tal como se prescreve no artigo 273º da CRP. Na Lei de Defesa Nacional, aprovada pela Lei Orgânica n.º 1-B/2009, de 7 de Julho[72], esta espécie de definição é vertida no n.º 1 do artigo 1º, ampliando-se, no n.º 2 do mesmo artigo, o conceito para abranger "o cumprimento dos compromissos internacionais do Estado no domínio

[68] "Portugal é uma República soberana, baseada na dignidade da pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária".

[69] "A República Portuguesa é um Estado de direito democrático, baseado na soberania popular, no pluralismo de expressão e organização política democráticas, no respeito e na garantia de efectivação dos direitos e liberdades fundamentais e na separação e interdependência de poderes, visando a realização da democracia económica, social e cultural e o aprofundamento da democracia participativa".

[70] A alínea a) deste artigo 9º da CRP completa-se incluindo o segmento que, nesta nota, se sublinha: "Garantir a independência nacional e criar as condições políticas, económicas, sociais e culturais que a promovam".

[71] A alínea b) deste artigo 9º da CRP completa-se incluindo o segmento que, nesta nota, se sublinha: "garantir os direitos e liberdades fundamentais e o respeito pelos princípios do Estado de direito democrático".

[72] Este diploma foi primeiramente publicado como Lei n.º 31-A/2009, de 7 de Julho, tendo sido posteriormente rectificado para Lei Orgânica n.º 1-B/2009, de 7 de Julho, pela Declaração de Rectificação n.º 52/2009, de 20 de Julho, que o republicou na íntegra.

militar"[73]. A defesa militar do Estado é incumbência exclusiva das Forças Armadas, nos termos do artigo 275º da Constituição.

Na outra vertente, a CRP (artigo 272º, n.º 1) atribui à polícia as funções de "defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos". Vislumbram-se, aqui, dois planos de actuação das polícias, a segurança pública e a investigação criminal. No plano da conflitualidade jurídica dos cidadãos, prevê a Constituição (cfr. artigo 202º, n.ºs 1 e 2[74]) e as leis (tais como o Código Civil ou o Código do Trabalho) a intervenção dos tribunais, no exercício da função jurisdicional, seja na jurisdição cível, do trabalho ou administrativa e fiscal. Prevê-a igualmente na jurisdição penal, mediada contudo pelo labor do Ministério Público e das polícias, no que tange à investigação criminal. O Ministério Público é a entidade judiciária com competência "para exercer a acção penal"[75], tal como as polícias têm por função "defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos"[76]. Importa densificar os conceitos de segurança interna e de investigação criminal e, para isso, vamos socorrer-nos de dois diplomas basilares, a Lei de Segurança Interna (adiante designada pela sigla LSI)[77] e a Lei de Organização da Investigação Criminal (enunciado à frente pela sua sigla, LOIC)[78]. Dispõe o n.º 1 do artigo 1º que "segurança interna é a actividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática." Especificando e alargando o conceito, o n.º 3 do mesmo artigo estipula que "as medidas previstas na presente lei destinam-se, em especial, a proteger a vida e a integridade das

[73] O texto da norma é o seguinte: "A defesa nacional assegura ainda o cumprimento dos compromissos internacionais do Estado no domínio militar, de acordo com o interesse nacional."
[74] "1. Os tribunais são os órgãos de soberania com competência para administrar a justiça em nome do povo.
2. Na administração da justiça incumbe aos tribunais assegurar a defesa dos direitos e interesses legalmente protegidos dos cidadãos, reprimir a violação da legalidade democrática e dirimir os conflitos de interesses públicos e privados."
[75] Integrando o n.º 1 do artigo 219º da CRP, que dispõe: "Ao Ministério Público compete representar o Estado e defender os interesses que a lei determinar, bem como, com observância do disposto no número seguinte e nos termos da lei, participar na execução da política criminal definida pelos órgãos de soberania, exercer a acção penal orientada pelo princípio da legalidade e defender a legalidade democrática."
[76] Constante do n.º 1 do artigo272º da CRP: "A polícia tem por funções defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos."
[77] Aprovado pela Lei n.º 53/2008, de 29 de Agosto, rectificada pela Declaração de Rectificação n.º 66-A/2008, de 28 de Outubro de 2008.
[78] Aprovada pela Lei n.º 49/2008, de 27 de Agosto, com a alteração introduzida pela Lei n.º 34/2013, de 16 de Maio.

pessoas, a paz pública e a ordem democrática, designadamente contra o terrorismo, a criminalidade violenta ou altamente organizada, a sabotagem e a espionagem, a prevenir e reagir a acidentes graves ou catástrofes, a defender o ambiente e a preservar a saúde pública". O conceito de segurança interna sobreleva o de segurança pública e inclui a investigação criminal. No Conselho Superior de Segurança Interna[79], têm assento[80] o Primeiro-ministro, que preside, os Vice-Primeiros-Ministros, os Ministros de Estado e da Presidência, se os houver, os Ministros da Administração Interna, da Justiça, da Defesa Nacional, das Finanças e das Obras Públicas, Transportes e Comunicações, os Presidentes dos Governos Regionais, os Secretários-Gerais do Sistema de Segurança Interna e do Sistema de Informações da República Portuguesa, o Chefe do Estado-Maior-General das Forças Armadas, dois deputados designados pela Assembleia da República por maioria de dois terços dos deputados presentes, desde que superior à maioria absoluta dos deputados em efectividade de funções e, também, o comandante-geral da Guarda Nacional Republicana, os directores nacionais da Polícia de Segurança Pública, da Polícia Judiciária e do Serviço de Estrangeiros e Fronteiras e os directores do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança, a Autoridade Marítima Nacional, o responsável pelo Sistema de Autoridade Aeronáutica, o responsável pelo Sistema Integrado de Operações de Protecção e Socorro, o director-geral dos Serviços Prisionais. O Procurador-Geral da República pode participar nas reuniões, por iniciativa própria, sempre que o entenda ou a convite do presidente deste Conselho[81]. O presidente pode, ainda, "convidar a participar nas reuniões os ministros que tutelem órgãos de polícia criminal de competência específica e outras entidades com especiais responsabilidades na prevenção e repressão da criminalidade ou na pesquisa e produção de informações relevantes para a segurança interna, designadamente os dirigentes máximos de outros órgãos de polícia criminal de competência específica"[82].

O Conselho Superior de Segurança Interna, enquanto "órgão interministerial de audição e consulta em matéria de segurança interna"[83], que assiste o Primeiro-ministro "nomeadamente na adopção das providências necessárias em situações de grave ameaça à

[79] De acordo com o artigo 11º da LSI, os outros dois órgãos que compõem o Sistema de Segurança Interna são o Secretário-Geral e o Gabinete Coordenador de Segurança.
[80] Em conformidade com o artigo 12º, n.º 2, da LSI.
[81] Como se estipula no artigo 12º, n.º 4, da LSI.
[82] Como se prevê no n.º 6 do mesmo artigo 12º da LSI.
[83] Estatuição do n.º 1 do artigo 12º da LSI.

segurança interna"[84], integra membros do Governo, representantes da Assembleia da República, dos Governos Regionais, das Forças Armadas, a que acresce a Autoridade Marítima Nacional[85] e o Sistema de Autoridade Aeronáutica[86], dos Serviços de Informações, dos órgãos de polícia criminal dotados de competência genérica, a que acresce o Serviço de Estrangeiros e Fronteiras[87], do Sistema Integrado de Operações de Protecção e Socorro[88] e dos Serviços Prisionais, a que se poderá juntar o Procurador-Geral da República[89]. O número de entidades que participam no sistema e a sua diversidade funcional aconselharam que se criasse um órgão - o Secretário-Geral do Sistema de Segurança Interna - com competências de coordenação, direcção, controlo e comando operacional no quadro do sistema (cfr. artigo 15º da LSI), definidas, respectivamente, nos artigos 16º a 19º da Lei de Segurança Interna.

Importa desagregar funções, em ordem a evidenciar a principal missão dos intervenientes neste Sistema, centrando-nos, sempre que possível, na prevenção e combate ao terrorismo e ao ciberterrorismo. A Lei de Organização da Investigação Criminal define, no seu artigo 1º, investigação criminal como "o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo". Não é despiciendo sublinhar que, "a direcção da investigação cabe à autoridade judiciária

[84] Como se prevê no artigo 13º, n.º 1, da LSI.
[85] Entende-se por autoridade marítima "o poder público a exercer nos espaços marítimos sob soberania ou jurisdição nacional, traduzido na execução dos actos […] que contribuam para a segurança da navegação, bem como no exercício de fiscalização e de polícia", tal como se estatui no artigo 3º do Decreto-Lei n.º 43/2002, de 2 de Março.
[86] Pela Lei n.º 28/2013, de 12 de Abril (artigo 4º, n.º 1), a "Autoridade Aeronáutica Nacional é a entidade responsável pela coordenação e execução das atividades a desenvolver pela Força Aérea na regulação, inspeção e supervisão das atividades de âmbito aeronáutico na área da defesa nacional."
[87] O SEF é, de acordo com o disposto no artigo 1º, n.º 1, da sua lei orgânica, aprovada pelo Decreto-Lei n.º 252/2000, de 16 de Outubro, "um serviço de segurança […] que, no quadro da política de segurança interna, tem por objetivos fundamentais controlar a circulação de pessoas nas fronteiras, a permanência e atividades de estrangeiros em território nacional, bem como estudar, promover, coordenar e executar as medidas e ações relacionadas com aquelas atividades e com os movimentos migratórios."
[88] "O SIOPS visa responder a situações de iminência ou de ocorrência de acidente grave ou de catástrofe", como se estipula no artigo 1º, n.º 2, do Decreto-Lei n.º 134/2006, de 25 de Julho. Este diploma, mas não esta norma, foi objecto de duas alterações legislativas, levadas a cabo pelos Decretos-Lei n.ºs 114/2011 e 72/2013, respectivamente, de 30 de Novembro e 31 de Maio.
[89] O Procurador-Geral da República preside à Procuradoria-Geral da República e compete-lhe "dirigir, coordenar e fiscalizar a actividade do Ministério Público e emitir as directivas, ordens e instruções a que deve obedecer a actuação dos respectivos magistrados", nos termos do disposto nos artigos 12º, n.ºs 1, alínea a) e n.º 2, alínea b), do Estatuto do Ministério Público, neste se dispondo (artigo 1º e 2º, n.º 1), igualmente, que "o Ministério Público representa o Estado, defende os interesses que a lei determinar, participa na execução da política criminal definida pelos órgãos de soberania, exerce a acção penal orientada pelo princípio da legalidade e defende a legalidade democrática, nos termos da Constituição, do presente Estatuto e da lei" e "goza de autonomia em relação aos demais órgãos do poder central, regional e local".

competente em cada fase do processo" e que esta autoridade é assistida na investigação pelos órgãos de polícia criminal", nos termos dos n.ºs 2 e 3 do artigo 2º da LOIC[90]. Esta solução prende-se com a natureza de órgão de soberania (cfr. artigo 110º da CRP) que é atributo dos tribunais, a que está conferida "competência para administrar a justiça", tal como se estipula no artigo 202º, n.º 1, da Constituição. Aliás, compete ao Ministério Público "dirigir a investigação criminal, ainda quando realizada por outras entidades", sendo esta instituição judiciária "coadjuvada pelos órgãos de polícia criminal" no exercício destas funções, como se prescreve no artigo 3º, n.ºs 1, alínea h) e 3, do Estatuto do Ministério Público[91]. A Lei de Organização da Investigação Criminal enuncia os órgãos de polícia criminal de competência genérica, nas três alíneas do n.º 1 do artigo 3º: a Polícia Judiciária, a Guarda Nacional Republicana e a Polícia de Segurança Pública. Os restantes órgãos de polícia criminal "possuem competência específica", nos termos do n.º 2 do mesmo artigo 3º. A uns e a outros compete "coadjuvar as autoridades judiciárias na investigação", bem como "desenvolver as acções de prevenção e investigação da sua competência ou que lhes sejam cometidas pelas autoridades judiciárias competentes"[92].

Dispõe o artigo 7º, n.º 2, da LOIC, que "é da competência reservada da Polícia Judiciária, não podendo ser deferida a outros órgãos de polícia criminal, a investigação dos […] crimes" de "organizações terroristas e terrorismo" (alínea l). No n.º 3 do mesmo artigo e diploma, dispõe-se: "é ainda da competência reservada da Polícia Judiciária a investigação dos seguintes crimes, sem prejuízo do disposto no artigo seguinte: l) Informáticos e praticados com recurso a tecnologia informática (alínea l) e os com ele conexos (alínea o).

Na fase de inquérito, o Procurador-Geral da República, ouvidos os órgãos de polícia criminal envolvidos, "defere a investigação de um crime referido no n.º 3 do artigo anterior a outro órgão de polícia criminal desde que tal se afigure, em concreto, mais adequado ao bom andamento da investigação" e, designadamente, quando as condições para a realização da investigação não ofereçam dificuldades de monta, de acordo com a previsão do n.º 1[93] do artigo 8º. Mas já assim não será (cfr. n.º 5 do mesmo artigo e

[90] Era já essa a solução constitucional constante do artigo 202º, n.º 3, da CRP, em que se dispõe: "No exercício das suas funções os tribunais têm direito à coadjuvação das outras autoridades."
[91] O Estatuto foi aprovado pela Lei n.º 47/86, de 20 de Agosto, tendo a Lei n.º 60/98, de 27 de Agosto, aditado o n.º 3 ao artigo 3º, a que, no texto, se faz referência.
[92] Em conformidade com o artigo 3º, n.º 4, da LOIC.
[93] Ou seja, na redacção das quatro alíneas deste normativo, quando (a) existam provas simples e evidentes, na acepção do Código de Processo Penal; (b) estejam verificados os pressupostos das formas especiais de processo, nos

diploma) se "a investigação assum[ir] especial complexidade por força do carácter plurilocalizado das condutas ou da pluralidade dos agentes ou das vítimas" (a), se os factos [tiverem] sido cometidos de forma altamente organizada ou assum[ir]em carácter transnacional ou dimensão internacional (b) ou, ainda, se a investigação reque[rer], de modo constante, conhecimentos ou meios de elevada especialidade técnica (c).

Nesta conformidade, prevê o artigo 2º, n.º 2, da Lei n.º 37/2008, de 6 de Agosto[94], que a Polícia Judiciária (adiante designada por PJ) "prossegue as atribuições definidas na presente lei, nos termos da Lei de Organização da Investigação Criminal e da Lei Quadro da Política Criminal." Para além das atribuições em sede de prevenção e detecção criminal previstas no artigo 4º do diploma, estabelece-se que "as competências da PJ respeitantes à investigação criminal são as definidas na Lei de Organização de Investigação Criminal".

Dispõe o artigo 6º da LOIC que "é da competência genérica da Guarda Nacional Republicana e da Polícia de Segurança Pública a investigação dos crimes cuja competência não esteja reservada a outros órgãos de polícia criminal e ainda dos crimes cuja investigação lhes seja cometida pela autoridade judiciária competente para a direcção do processo, nos termos do artigo 8.º".

Para além desta competência no domínio da investigação criminal[95], a Guarda Nacional Republicana (adiante designada por GNR) tem outras atribuições, como sejam as constantes das alíneas b), i) e j) do n.º 1 do artigo 3º da Lei 63/2007, de 6 de Novembro[96], de que se destacam a de "garantir a ordem e a tranquilidade públicas e a segurança e a protecção das pessoas e dos bens", a de "proteger, socorrer e auxiliar os cidadãos e defender e preservar os bens que se encontrem em situações de perigo, por causas provenientes da acção humana ou da natureza" e a de "manter a vigilância e a protecção de pontos sensíveis, nomeadamente infra-estruturas rodoviárias, ferroviárias, aeroportuárias e portuárias, edifícios públicos e outras instalações críticas".

De forma semelhante, a Polícia de Segurança Pública (de seguida mencionada por PSP) tem, para além da competência para investigar crimes, atribuições de outra ordem, de que se salientam as referidas nas alíneas b), i) e j) do n.º 1 do artigo 3º da Lei n.º 53/2007,

termos do Código de Processo Penal; (c) Se trate de crime sobre o qual incidam orientações sobre a pequena criminalidade, nos termos da Lei de Política Criminal em vigor; ou (d) a investigação não exija especial mobilidade de actuação ou meios de elevada especialidade técnica".

[94] Diploma que aprovou a orgânica da Polícia Judiciária.

[95] Cfr. artigo 3º, alínea e) do diploma orgânico da GNR.

[96] O diploma, que aprovou a orgânica da GNR, foi objecto de correcção pela Rectificação n.º 1-A/2008, de 04 de Janeiro.

de 31 de Agosto, que aprovou a orgânica desta força de segurança. Uma vez que estas atribuições têm a mesma exacta descrição das que acima foram transcritas para a GNR, não se justificará, aqui, proceder a esta remissão para o parágrafo anterior.

Este núcleo de funções, tradicionalmente associado a estas duas entidades, permite denominá-las forças de segurança e enquadra-las na actividade de polícia de segurança, por oposição às de polícia administrativa e judiciária. A GNR é uma "força de segurança de natureza militar, constituída por militares organizados num corpo especial de tropas" que integra os "sistemas nacionais de segurança e protecção", estipulando-se que "as forças da Guarda são colocadas na dependência operacional do Chefe do Estado-Maior-General das Forças Armadas, através do seu comandante-geral, nos casos e termos previstos nas Leis de Defesa Nacional e das Forças Armadas e do regime do estado de sítio e do estado de emergência", nos termos dos n.ºs 1 e 2 do artigo 1º e n.º 2 do artigo 2º do diploma orgânico da GNR. A PSP é, por sua vez," uma força de segurança, uniformizada e armada", cujas atribuições são, "em situações de normalidade institucional", " as decorrentes da legislação de segurança interna e, em situações de excepção, as resultantes da legislação sobre a defesa nacional e sobre o estado de sítio e de emergência", em conformidade com o disposto nos artigos 1º, n.º 1 e 3º, n.º 1, do seu diploma orgânico.

"Aos serviços de informações incumbe assegurar, […], a produção de informações necessárias à salvaguarda da independência nacional e à garantia da segurança interna", como se estabelece no artigo 2º, n.º 2, da Lei n.º 30/84, de 05 de Setembro[97]. O diploma define as bases gerais do Sistema de Informações da República Portuguesa (adiante designado por SIRP) e integra, para além dos serviços de informações (Serviço de Informações Estratégicas de Defesa e Serviço de Informações de Segurança), o Conselho Superior de Informações, o Secretário-Geral do Sistema de Informações da República Portuguesa e, com competências fiscalizadoras, o Conselho de Fiscalização do Sistema de Informações da República Portuguesa e a Comissão de Fiscalização de Dados do Sistema de Informações da República Portuguesa, como consta das alíneas e), f), b), d), a) e c), do artigo 7º.

Dispõe o artigo 20º da Lei Quadro do Sistema de Informações da República Portuguesa "o Serviço de Informações Estratégicas de Defesa é o organismo incumbido da

[97] A Lei n.º 30/84, de 5 de Setembro, alterada pelas Leis n.ºs 4/95, de 21 de Fevereiro, 15/96, de 30 de Abril, e 75-A/97, de 22 de Julho, foi republicada na íntegra, em anexo, com as alterações aprovadas pela Lei Orgânica n.º 4/2004, de 06 de Novembro, constitui a Lei Quadro do Sistema de Informações da República Portuguesa.

produção de informações que contribuam para a salvaguarda da independência nacional, dos interesses nacionais e da segurança externa do Estado Português". O artigo 21º da Lei Quadro estipula que "o Serviço de Informações de Segurança é o organismo incumbido da produção de informações que contribuam para a salvaguarda da segurança interna e a prevenção da sabotagem, do terrorismo, da espionagem e a prática de actos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido". A Lei Quadro do SIRP afirma o princípio da exclusividade, explicitando que a produção de informações com estas finalidades se realizam "exclusivamente mediante as atribuições e competências dos serviços previstos na presente lei" (cfr. artigo 2º, n.º 1), sendo "proibido que outros serviços prossigam objectivos e actividades idênticos aos dos previstos na presente lei"(cfr. artigo 6º). Para além das entidades fiscalizadoras integradas no SIRP (Conselho de Fiscalização e a Comissão de Fiscalização de Dados), a lei rodeia de todas as cautelas a actividade dos serviços de informações, desde logo proibindo que sejam "desenvolvidas actividades de pesquisa, processamento e difusão de informações que envolvam ameaça ou ofensa aos direitos, liberdades e garantias consignados na Constituição e na lei" (cfr. artigo 3º, n.º 1), o que determina que os "serviços de informações [fiquem] sujeitos a todas as restrições legalmente estabelecidas em matéria de defesa dos direitos, liberdades e garantias perante a informática" (cfr. n.º 2 do mesmo artigo 3º), explicitando-se, ainda, que "cada serviço só pode desenvolver as actividades de pesquisa e tratamento das informações respeitantes às suas atribuições específicas" (cfr. artigo 3º, n.º 3). Fica, igualmente, vedada aos "funcionários ou agentes, civis ou militares", destes serviços "exercer poderes, praticar actos ou desenvolver actividades do âmbito ou competência específica dos tribunais ou das entidades com funções policiais", sendo-lhes "expressamente proibido" "proceder à detenção de qualquer indivíduo ou instruir processos penais" (cfr. artigo 4º, n.ºs 1 e 2).

A completar o edifício do Sistema de Informações, a Lei n.º 9/2007, de 19 de Fevereiro, que estabelece a orgânica do Secretário-Geral do SIRP e algumas alterações na estrutura do SIRP, do SIED e do SIS, institui o Conselho Consultivo do SIRP, bicameral, reunindo, por isso, com diferente composição, conforme as matérias se inscrevam nas atribuições do SIED ou do SIS (cfr. artigo 15º). Sendo um órgão de consulta do Primeiro Ministro, podendo ser objecto de delegação no Secretário-Geral do SIRP. Os directores e os directores-adjuntos do SIED e do SIS "participam no conselho consultivo do SIRP, independentemente do âmbito da sua reunião. O director-geral de Política de Defesa

Nacional[98] do Ministério da Defesa Nacional, o director-geral de Política Externa[99] do Ministério dos Negócios Estrangeiros e o responsável pelo organismo de informações militares[100] são membros do conselho consultivo no âmbito das atribuições do SIED, enquanto, no domínio das atribuições do SIS, são membros do mesmo conselho o comandante-geral da Guarda Nacional Republicana, o director nacional da Polícia de Segurança Pública, o director nacional da Polícia Judiciária e o director-geral do Serviço de Estrangeiros e Fronteiras.

Como se vê, os serviços e organismos articulam-se, veem a sua actividade coordenada cooperam e trocam informações em instâncias que propiciam esse contacto. As competências são aquelas que a lei atribui, mas os poderes legislativo e executivo apontam paulatinamente para uma cooperação que seja, ela própria, fomentadora de um eficaz e eficiente exercício daquelas competências.

O combate e a repressão do terrorismo beneficia, ainda, no plano nacional, das políticas europeias adoptadas em sede de política externa e de segurança comum (PESC) e do que se designa por "espaço de liberdade, segurança e justiça", no quadro da União Europeia, da qual Portugal é Estado membro. É neste âmbito que, em cumprimento da Decisão Quadro n.º 2002/475/JAI, do Conselho, de 13 de Junho, foi publicada a Lei n.º 52/2003, de 22 de Agosto, apelidada de lei de combate ao terrorismo, tipifica os crimes praticados por grupos terroristas e define a moldura penal, tendo presente a gravidade dos danos infligidos por estas associações criminosas, ideologicamente marcadas e que, pela variedade dos meios utilizados eram condenados a penas concebidas para o criminoso comum, cujo grau de ameaça é significativamente menor.

"Transpondo para a ordem jurídica interna as Directivas n.ºs 2005/60/CE, do Parlamento Europeu e do Conselho, de 26 de Outubro, e 2006/70/CE, da Comissão, de 1 de Agosto, relativas à prevenção da utilização do sistema financeiro e das actividades e profissões especialmente designadas para efeitos de branqueamento de capitais e de financiamento do terrorismo", a Lei n.º 25/2008, de 5 de Junho, "estabelece medidas de natureza preventiva e repressiva de combate ao branqueamento de vantagens de

[98] Para maiores desenvolvimentos, pode consultar-se o Decreto Regulamentar n.º4/2012, de 18 de Janeiro, que aprovou a orgânica da Direcção-Geral de Política de Defesa Nacional.
[99] A orgânica da Direcção-Geral de Política Externa foi aprovada pelo Decreto Regulamentar n.º 11/2012, de 19 de Janeiro.
[100] Presentemente com a designação de Centro de Informações e Segurança Militares, em conformidade com o disposto nos artigos 3º, n.º 1, alínea e), 28º e 29º do Decreto-Lei n.º 234/2009, de 15 de Setembro.

proveniência ilícita e ao financiamento do terrorismo", dando-se, assim, mais um passo no cerco às actividades terroristas e à criminalidade com ela conexa.

Da mesma forma que se procura separar, como dois continentes, a segurança interna da segurança externa, assim se procura restringir as competências de natureza preventiva dos órgãos de polícia criminal, reservando-as para os serviços de informações que, por sua vez, não podem proceder a actos de investigação criminal.

Quando guardas da Guarda Nacional Republicana ou agentes da Polícia de Segurança Pública procedem a policiamento de proximidade[101] ou quando inspectores da Polícia Judiciária vigiam ou fiscalizam estabelecimentos que possam ocultar actividades de receptação ou comercialização ilícita de bens[102], estamos perante actos típicos de prevenção criminal. A Constituição da República determina, no n.º 3 do seu artigo 272º, que "a prevenção dos crimes, incluindo a dos crimes contra a segurança do Estado, só pode fazer-se com observância das regras gerais sobre polícia e com respeito pelos direitos, liberdades e garantias dos cidadãos". E, no n.º 2 do mesmo artigo, estipula que "as medidas de polícia são as previstas na lei, não devendo ser utilizadas para além do estritamente necessário". A medida das competências das diferentes polícias pode encontrar-se na regulação constante do Código do Processo Penal, da Lei de Segurança Interna e dos diplomas orgânicos de cada uma entidades com competências policiais. O diploma que aprova a orgânica da PJ[103] distingue as competências de investigação criminal das de prevenção criminal e, quanto a estas, especifica alguns domínios de intervenção, no diploma que define as competências dos seus departamentos (ali designados por unidades). A circunstância de a PJ dispor de um sistema de informação criminal, "visando o tratamento e difusão da informação"[104], não atribui a este órgão de polícia criminal competência para tratamento e análise das informações que tem ao seu dispor em moldes semelhantes aos que a lei confere aos serviços de informações. De facto, o Decreto-Lei n.º 352/99, de 3 de Setembro, limita a utilização daquele sistema a organizar e a manter actualizada a informação necessária ao exercício das competências atribuídas, por lei, à PJ, em sede de investigação criminal e de prevenção criminal (cfr. artigo 1º), estipulando, no

[101] Ver, para a GNR, o artigo 3º, n.º 1, na conjugação das alíneas a), b) e c), da Lei n.º 63/2007, de 6 de Novembro, diploma que aprovou a orgânica da GNR. Para a PSP, consultar o artigo 3º, n.º 1, na conjugação das alíneas a), b) e c), da Lei n.º 53/2007, de 31 de Agosto, diploma que aprovou a orgânica da PSP.
[102] Competência da Unidade de Informação de Investigação Criminal da Polícia Judiciária, inscrita no artigo 14º, n.º 2, do Decreto-Lei n.º 42/2009, de 12 de Fevereiro, diploma que estabelece as competências das unidades da Polícia Judiciária.
[103] Lei n.º 37/2008, de 6 de Agosto.
[104] Cfr. artigo 8º da Lei n.º 37/2008.

artigo 2º, n.º 1, que " a recolha de dados pessoais para tratamento […] limita-se ao estritamente necessário à prevenção de um perigo concreto ou à repressão de infracções penais determinadas". Sublinhe-se que a utilização para fins de prevenção criminal deve ser entendida em sentido restrito, isto é, limitada às competências que a lei, especificadamente, atribui à PJ, uma vez que, havendo indícios de ter ocorrido a prática de um crime ou actos preparatórios conducentes à sua execução, haverá que transformar o procedimento em Inquérito[105] e, logo que possível, fazer intervir as autoridades judiciárias, em conformidade com o disposto no Código do Processo Penal (cfr. artigos 241º e 248º, que se articulam com a competência conferida aos órgãos de polícia criminal pelo artigo 55º, n.º 2[106]).

Os serviços de informações não encontram a sua actividade vinculada à comissão de um crime, podendo dizer-se que a sua função é a de "produzir informações que contribuam para a salvaguarda da segurança interna e a prevenção da sabotagem, do terrorismo, da espionagem e a da prática de actos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido"[107]. Acrescente-se que os serviços de informações continuam, todavia, vinculados a actuar com respeito pelos "direito liberdades e garantias consignados na Constituição e na lei"[108]. Sublinhe-se ainda que a produção de informações engloba várias actividades, designadamente "de pesquisa, análise, interpretação, classificação e conservação de informações" (cfr. artigo 5º, n.º 3, da Lei n.º 9/2007). Num certo sentido, dir-se-ia que o SIS é um serviço com competências de prevenção criminal. Seria útil um estudo que se debruçasse sobre o conceito de prevenção criminal que ajudasse a separar as águas, porquanto o SIS não sendo organicamente um serviço de prevenção criminal (designação que, para já, se deve reservar às polícias), parece sê-lo, parcialmente, quanto aos seus fins, sem que fique descaracterizado como serviço de informações.

[105] Dispõe o artigo 262º do CPP que "inquérito compreende o conjunto de diligências que visam investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles e descobrir e recolher as provas, em ordem à decisão sobre a acusação" (n.º 1) e que "[…] a notícia de um crime dá sempre lugar à abertura de inquérito" (n.º 2).

[106] Norma que dispõe: "Compete em especial aos órgãos de polícia criminal, mesmo por iniciativa própria, colher notícia dos crimes e impedir quanto possível as suas consequências, descobrir os seus agentes e levar a cabo os actos necessários e urgentes destinados a assegurar os meios de prova".

[107] Trata-se da missão do Serviço de Informações de Segurança, tal como se encontra descrita no artigo 21º da Lei Quadro do Sistema de Informações da República Portuguesa. Neste particular, não cabe trazer à colação o Serviço de Informações Estratégicas de Defesa, vocacionado para a segurança externa.

[108] Cfr. artigos 3º, n.º 1 e 6º, n.º 1, respectivamente, das Leis n.º 4/2004, de 6 de Novembro e Lei n.º 9/2007, de 19 de Fevereiro.

4.2 ESTRATÉGIA PORTUGUESA DE CIBERSEGURANÇA

O Conceito Estratégico de Defesa Nacional considera como uma das ameaças e riscos à segurança global, o ciberterrorismo e a cibercriminalidade, tendo por base que têm como alvo redes indispensáveis ao funcionamento da economia e da sociedade da informação globalizada[109]. E como um dos principais riscos e ameaças à segurança nacional "A cibercriminalidade, porquanto os ciberataques são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna"[110].

Segundo o mesmo conceito estratégico para se reduzir o nível da ameaça "No domínio da cibercriminalidade, impõe -se uma avaliação das vulnerabilidades dos sistemas de informação e das múltiplas infraestruturas e serviços vitais neles apoiados. Neste domínio, definem -se como linhas de ação prioritárias: garantir a proteção das infraestruturas de informação críticas, através da criação de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN); definir uma Estratégia Nacional de Cibersegurança, montar a estrutura responsável pela cibersegurança, através da criação dos órgãos técnicos necessários; sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática e levantar a capacidade de ciberdefesa nacional.

O Relatório Anual de Segurança Interna, 2013, diz que "cumpre mencionar a multiplicidade de riscos e de ameaças relacionadas com o ciberespaço, em particular no domínio do activismo, da espionagem e do terrorismo, que tiveram particular destaque em 2013 designadamente no que concerne à actividade dos estados ou organizações que desenvolvem ou patrocinam actividades crescentemente agressivas neste domínio"[111]. E que do ponto de vista da ameaça terrorista foram observados determinados fenómenos que alicerçam e potenciam as acções terroristas. Ainda no que concerne ao cibercrime Portugal não ficou imune a tentativas de infiltração de sistemas de informáticos do Estado, ocorridas

[109] Resolução de Conselho de Ministro n.º 19/2013, publicado no Diário da República, n.º 67, de 5 de Abril de 2013, que aprova o Conceito Estratégico de Defesa Nacional

[110] Resolução de Conselho de Ministro n.º 19/2013, publicado no Diário da República, n.º 67, de 5 de Abril de 2013, que aprova o Conceito Estratégico de Defesa Nacional III , 3.2

[111] http://www.portugal.gov.pt/media/1391220/RASI%202013.pdf Relatório de Segurança Interna 2013 – revisitado em 5 de Junho de 2013

no contexto de campanhas internacionais, aparentemente visando, o acesso a informação privilegiada, persistindo a dificuldade da atribuição, de forma conclusiva, da origem dos ataques.

Assim, tornou-se cada vez mais premente a objectivação de uma estratégica nacional de cibersegurança., embora tenha sido definido pela Comissão Europeia, que, até ao final de Dezembro de 2012, todos os Estados-membros deviam ter os respectivos Centros Nacionais de Cibersegurança operacionais.

A 9 de Maio do corrente ano de 2014 no diário da República, foi publicado o Decreto-Lei 69/2014 onde consta a sua efectiva regulamentação. O Centro Nacional de Cibersegurança, doravante designado por CNCSeg estará integrado no Gabinete Nacional de Segurança até ao ano 2017 onde voltará a ser novamente avaliada a sua eficácia. O Gabinete Nacional de Segurança que viu a sua autonomia consagrada no Decreto-Lei n.º 3/2012 alterado pelo Decreto-Lei n.º 162/2013 depende directamente do 1º Ministro ou a Ministro a quem ele delegar.

Actualmente o GNS tem como missão e atribuição[112] :

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

2 - No âmbito do GNS funciona o Centro Nacional de Cibersegurança, doravante designado por CNCSeg, que tem por missão contribuir para que o país o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.

3 - O GNS prossegue as seguintes atribuições:

[112] Artº 2 Republicação do Decreto-Lei n.º 3/2012, de 16 de Janeiro com as alterações do DL n.º 69/2014, de 09 de Maio

a) Garantir a articulação e a harmonização dos procedimentos relativos à segurança da informação classificada em todos os serviços, organismos e entidades, públicos ou privados, onde seja administrada tal informação, designadamente e em especial, os da Administração Pública, das forças armadas e das forças e serviços de segurança, bem como no âmbito das organizações, reuniões, programas, contratos, projetos e outras atividades internacionais em que Portugal participe;

b) Assegurar, nos termos dos instrumentos de vinculação do Estado Português, a proteção e a salvaguarda da informação classificada emanada das organizações internacionais de que Portugal faça parte ou das respetivas estruturas internas, nomeadamente no âmbito da Organização do Tratado do Atlântico Norte (OTAN), da União Europeia (UE), Unidade Europeia de Cooperação Judiciária (EUROJUST) e da Agência Espacial Europeia (AEE), bem como de outros Estados com os quais tenha sido celebrado acordos de segurança;

c) Exercer em Portugal os poderes públicos cometidos às autoridades nacionais de segurança, nomeadamente nas áreas da credenciação de segurança, segurança das comunicações, distribuição e outras, nos termos das normas aprovadas pelas entidades internacionais competentes;

d) Proceder ao registo, distribuição e controlo da informação classificada, bem como de todos os procedimentos inerentes à sua administração, de índole nacional ou confiadas à responsabilidade do Estado Português, garantindo que o material cripto é objeto de medidas específicas de segurança e administrado por canais diferenciados;

e) Fiscalizar e inspecionar os órgãos de segurança que detenham, a qualquer título e em qualquer suporte, informação classificada sob responsabilidade portuguesa, dentro e fora do território nacional;

f) Avaliar, acreditar e certificar a segurança de produtos e sistemas de comunicações, de informática e de tecnologias de informação que sirvam de suporte ao tratamento, arquivo e transmissão de informação classificada e proceder à realização de limpezas eletrónicas;

g) Promover o estudo, a investigação e a difusão das normas e procedimentos de segurança aplicáveis à proteção e salvaguarda da informação classificada, propondo a doutrina a adotar por Portugal e a formação de pessoal especializado nesta área da segurança;

h) Credenciar as empresas que pretendam exercer as atividades de comércio e indústria de bens e tecnologias militares, nos termos da Lei n.º 49/2009, de 5 de agosto;

i) Credenciar entidades públicas e privadas para o exercício de atividades industriais, tecnológicas e de investigação, quando tal seja exigido por disposição legal ou regulamentar;

j) Exercer as competências de autoridade credenciadora e de fiscalização de entidades que atuem no âmbito do SCEE, bem como no quadro do regime jurídico dos documentos eletrónicos e da assinatura eletrónica;

l) Atuar como autoridade responsável pela componente codificada do Sistema GALILEO, credenciar os pontos de contacto nacionais no âmbito da sua componente de segurança e efetuar a gestão de chaves quando da respetiva operação;

m) Exercer as demais atribuições que lhe sejam atribuídas por lei.

No que concerne às Competências do Centro Nacional de Cibergurança[113] :

1 - Na prossecução da sua missão, o CNCSeg possui as seguintes competências:

a) Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques;

b) Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança;

c) Exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais;

d) Contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais;

e) Promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança;

f) Assegurar a produção de referenciais normativos em matéria de cibersegurança;

g) Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança;

h) Assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do planeamento civil de emergência, no quadro definido pelo Decreto-Lei n.º 73/2013, de 31 de maio;

i) Coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros;

[113] Artº 2 A Republicação do Decreto-Lei n.º 3/2012, de 16 de Janeiro com as alterações do DL n.º 69/2014, de 09 de Maio

j) Exercer as demais competências que lhe sejam atribuídas por lei.

2 - O disposto no número anterior não prejudica as atribuições e competências legalmente cometidas a outras entidades públicas em matéria de segurança do ciberespaço e é exercida em coordenação com estas, através de elementos de ligação designados para o efeito, bem como em cooperação com entidades privadas que exerçam funções naquela matéria.

3 - O CNCSeg atua ainda em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo, devendo comunicar à Polícia Judiciária, no mais curto prazo, os factos de que tenha conhecimento relativos à preparação e execução de crimes.

No fundo a Estratégia Nacional de Cibersegurança portuguesa segue as linhas orientadoras das estratégias de outros Estado, definida sempre por orientação política. Sendo que à semelhança de outros o seu principal desafio é o de estimular uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, ao mesmo tempo que garante a proteção e defesa da sua infraestrutura de informação crítica. Neste âmbito, considera-se que o principal desafio de Portugal se coloca essencialmente ao nível da Garantia da Informação garantindo a Confidencialidade, a Integridade e a Disponibilidade.

Este desiderato requer tanto a implementação de processos de Segurança da Informação como de mecanismos de cibersegurança e ciberdefesa.

Assim, o País deverá procurar atingir os seguintes três objectivos principais:

1 -Garantir a Segurança no Ciberespaço:

As ameaças aos sistemas de informação são dirigidas simultaneamente aos serviços públicos, privados, às empresas e aos cidadãos. Os serviços públicos deverão servir como exemplo para a sociedade e deverão ser capazes de melhorar a protecção dos sistemas de informação e a informação de que são guardiões.

Campanhas de informação e alerta deverão ser implementadas, tendo como alvos principais os cidadãos e as empresas.

Ao mesmo tempo deverá ser elaborada legislação que promova a melhoria da cibersegurança, a luta contra o cibercrime e ainda a promoção da cooperação judicial e internacional.

Para garantir a Segurança do Ciberespaço, foram identificadas as seguintes linhas de acção estratégica:

• Analisar o ambiente de informação e antecipar eventuais ataques de forma a tomar as decisões apropriadas, acompanhando os últimos desenvolvimentos tecnológicos, analisando e antecipando ameaças a fim de estar na vanguarda;

• Detectar e bloquear ataques, alertar e apoiar as potenciais vítimas;

− Portugal deverá desenvolver capacidade de detecção de ataques aos seus sistemas de informação, especialmente os do Estado e infraestruturas críticas nacionais. Estes sistemas deverão permitir alertar as entidades relevantes, ajudar a entender a natureza dos ataques e a criar as necessárias contramedidas.

− De modo a gerir toda a informação recolhida pelas nossos sensores de detecção e monitorização ou fornecidos pelos nossos parceiros, a fim de se obter uma visão real da situação das redes nacionais e se necessário gerir situações de crise, o Centro Nacional de Cibersegurança deve ser equipado com uma sala de situação e com meios humanos e tecnológicos adaptados aos desafios.

− De modo a responder às principais crises que afectem ou ameacem a segurança dos sistemas de informação ou os operadores de infraestruturas críticas, o Estado deverá ser capaz de rapidamente impor as medidas necessárias, incluindo o isolamento de redes. Para atingir este objectivo, o Centro Nacional de Cibersegurança é a entidade nacional responsável pela defesa dos sistemas de informação.

• Estimular e potenciar as capacidades científicas, técnicas, industriais e humanas do país de forma a manter a independência nacional neste domínio;

• Adaptar a legislação nacional de forma a incorporar os desenvolvimentos tecnológicos e novas práticas.

• Desenvolver iniciativas de cooperação internacional em áreas ligadas à segurança dos sistemas de informação, cibercrime, ciberdefesa e luta contra o terrorismo de forma a proteger melhor os sistemas de informação nacionais;

• Comunicar e informar de forma a influenciar e a aumentar a compreensão da população portuguesa relativamente à extensão dos desafios relacionados com a segurança dos sistemas de informação.

• Fortalecer a Cibersegurança das Infraestruturas críticas nacionais;

• Defender os Interesses Nacionais e a Liberdade de Acção no Ciberespaço.

A visão clara das implicações/necessidades associadas a cada um dos objectivos, permitirá definir uma orientação (geral e específica) traduzida em linhas de acção concretas, destinadas a reforçar o potencial estratégico nacional no ciberespaço.

Neste contexto, identificam-se as seguintes linhas de cação estratégica para cada um dos objetivos enunciados:

2 -Fortalecer a Cibersegurança das Infraestruturas Críticas Nacionais;

A nossa sociedade está cada vez mais dependente dos sistemas de informação e das redes, particularmente da INTERNET, pelo que os ataques a estes sistemas podem ter graves consequências humanas e económicas.

O Estado deve trabalhar para garantir e melhorar a segurança das Infraestruturas Críticas Nacionais, em colaboração estreita com as operadoras de telecomunicações e os detentores dessas infraestruturas.

Para fortalecer a Cibersegurança das Infraestruturas Críticas Nacionais foram identificadas as seguintes linhas de ação estratégica:

• Reforçar a Segurança das TIC nas Redes do Governo e da Administração Pública;

• Reforçar a Segurança dos sistemas de informação do Estado e dos operadores das infraestruturas críticas para assegurar uma maior resiliência (capacidade de sobrevivência) nacional.

3- Defender os Interesses Nacionais e a Liberdade de Acção no Ciberespaço:

As autoridades governamentais e os atores relacionados com a gestão de crises deverão ter os meios disponíveis para comunicarem em qualquer situação e com confidencialidade. Para garantir a confidencialidade da informação nestas redes, são necessárias tecnologias de segurança, que teremos que desenvolver nas nossas Universidades e Centros de Investigação.

Para defender os interesses nacionais e a nossa liberdade de ação no ciberespaço, assegurando a protecção da informação e a Soberania Nacional foram identificadas as seguintes linhas de ação estratégica:

• Reforçar iniciativas nacionais estruturantes da “Sociedade de Informação e do Conhecimento”;

• Proteger e defender os mecanismos de Governação Eletrónica do Estado;

• Levantar a Estrutura Nacional de Cibersegurança e Ciberdefesa;

• Estabelecer mecanismos de cooperação nacional e internacional, neste âmbito.

De forma transversal, as atividades desenvolvidas no âmbito da implementação da Estratégia Nacional de Cibersegurança, contribuirão decisivamente para uma utilização

mais racional e coerente dos recursos disponíveis, estimulando esforços cooperativos e gerando as sinergias necessárias para reforçar as capacidades nacionais no ciberespaço.

4.3 O ESTADO DAS TIC'S EM PORTUGAL E A AUSÊNCIA DE UMA CULTURA DE SEGURANÇA DIGITAL COMO VULNERABILIDADE

Sendo as TIC partes vitais dos sistemas de comando e de controlo das infra-estruturas críticas das sociedade dos nossos dias (serviços financeiros, a produção e fornecimento de energia, transportes, serviços de emergência na saúde, serviços de produção e distribuição da alimentação, etc.)e, estando inclusivamente os governos electrónicos suportados nas TIC, estas começam a ser um alvo apetecível para as organizações terroristas.

Numa época em que se vive à escala global, onde as informações circulam à velocidade da luz, os Estados tendem a modernizar-se, adaptando-se da melhor forma possível aos desafios que esta nova realidade lhes oferece.

De facto, um país que se encontre e viva num ambiente de concorrência a nível global só conseguirá vantagem competitiva se desenvolver novas infra-estruturas tecnológicas, se for capaz de inovar e de ser empreendedor.

O *E-governmen*[114]*t* surge como a resposta dos Estados a estes novos desafios, visando melhoria contínua da sua produtividade, competitividade e da qualidade dos serviços que prestam. Para isso torna-se necessária a promoção de uma Administração Pública cada vez mais eficiente e eficaz explorando todo o potencial das Tecnologias de Informação e comunicação, não perdendo de vista o seu alinhamento estratégico que será a integração do seu sistema de informação de suporte e a sua área de "negócio".

A União Europeia tomou iniciativas e-Gov e promoveu a Interoperabilidade Pan-Europeia. Para o efeito, surge em 22 de Abril de 2009 a Resolução Legislativa do Parlamento Europeu contendo medidas de interoperabilidade relativamente às administrações públicas europeias (ISA): "O objectivo do programa ISA é apoiar a cooperação entre as administrações públicas europeias mediante a facilitação da interacção electrónica transfronteiriça e intersectorial eficiente e *eficaz* entre essas administrações, incluindo *as entidades que exercem, por conta destas, funções de carácter público, por* forma a

[114] Governo Electrónico

permitir o fornecimento de serviços públicos electrónicos que secundem a aplicação das políticas e a realização das actividades comunitárias"[115].

Portugal segue a tendência e apresenta o Plano Tecnológico,o Prace e o Simplex.

Segundo os dados do IMD (Institute for Managementent and Development*)*, no World Competitiveness Yearbook 2009[116], Portugal é o 3º País mais competitivo na Europa do Sul, ocupando o 16º lugar na União Europeia e é o 31º país no ranking mundial de *e-government* .

Como reforço do definido na "Estratégia de Lisboa " surge o i2010, lançando a Comissão uma nova política integrada para sociedade de informação em consonância total com o novo ciclo da Estratégia de Lisboa, contribuindo para o seu objectivo central, o crescimento sustentado e o emprego com o intuito de responder a novos desafios, nomeadamente a info-exclusão e a info-acessibilidade.

O projecto da Agenda Digital da Comissão Europeia, tendo como principal objectivo definir um roteiro que maximize o potencial social e económico das TIC, definiu como objectivo que em 2020, toda a população da União Europeia deverá ter acesso à Internet a velocidade de pelo menos 30mbp/s. Em 2011, a Comissária Neelie Kroes revelou que 10% dos objectivos já estavam alcançados.

A par deste investimento no *e-government* tem-se denotado, porém um desinvestimento na educação e na formação, não obstante os apoios do QREN para a área da formação. Na verdade, deixamos de ter altas taxas de analfabetismo mas passámos a ter grandes taxas de iliteracia, deixámos de ter um número elevado de info-excluídos e passamos a ter um número elevado de info-iletrados ou iletrados-digitais. O avançar do *e-government* com a subsequente desmaterialização e desburocratização dos processos, levou a que se tornasse obrigatório o recurso às novas TIC para a resolução de algumas questões da vida do quotidiano do cidadão comum, assim como o computador deixou de ser um objecto estranho para passar ser um objecto usual em qualquer lar português (nos lares das regiões da Grande Lisboa e do Grande Porto e nos das classes sociais mais elevadas é maior a penetração deste equipamento -61.8% e 77.6%, respectivamente-, mas é precisamente nas outras regiões do Continente e nas classes sociais mais baixas que mais tem aumentado a taxa de posse de um computador no lar. Nos lares das classes média baixa e baixa a posse

[115] Posição do Parlamento Europeu aprovada em primeira leitura em 22 de Abril de 2009 tendo em vista a aprovação da Decisão *2009/.../CE* do Parlamento Europeu e do Conselho sobre soluções de interoperabilidade para as administrações públicas europeias (ISA)

[116] http://jpn.icicom.up.pt/2009/05/20/portugal_ultrapassa_espanha_no_ranking_da_competitividade.html

de computador quase quadruplicou nesta década, passando de 10.9% para 39.9% e nos lares fora das regiões da Grande Lisboa e do grande Porto aumentou mais de duas vezes, passando de 21.9% em 1997 para 50.5% em 2007[117]).

Com a necessidade de se alcançarem as metas políticas definidas em questões de TIC proporcionam-se computadores a custos reduzidos sem que aos seus possuidores lhes fosse proporcionada uma formação adequada quanto à sua utilização, passando-se, desta feita, de uma sociedade de info-excluídos a uma de info-iletrados. Assim, aos poucos as novas tecnologias vão fazendo parte do quotidiano do cidadão: *"Mais de um milhão de computadores foram distribuídos no âmbito dos programas e.Escolas e e.Escolinhas a estudantes, docentes e trabalhadores em formação profissional. Um ambicioso Plano Tecnológico da Educação está a fazer das nossas escolas ambientes de aprendizagem de referência na modernidade e na inovação. Portugal tem hoje uma das maiores taxas de penetração de banda larga móvel do mundo e é o País com mais computadores portáteis por mil habitantes*" [118]

Portugal é o terceiro país da Europa no ranking de utilizadores de redes sociais, com 2, 5 milhões de adeptos, 84,4 % do total de utilizadores nacionais[119]. Os adeptos das redes sociais vão desde jovens estudantes a governantes do nosso país.

Segundo um estudo publicado pela UMIC- Agência para a Sociedade do Conhecimento (2010) sobre a penetração das TIC em Portugal:

- 92%, 90% e 30% das pessoas (de 16 a 74 anos) com, respectivamente, educação superior, secundária, e de 9º ano ou inferior, utilizam computador.
- 91%, 87% e 26% das pessoas (de 16 a 74 anos) com, respectivamente, educação superior, secundária, e de 9º ano ou inferior, utilizam Internet
- 97% e 98% dos estudantes usam, respectivamente, Internet e computador
-39% dos agregados familiares dispõem de ligações em banda larga à Internet.
-A penetração do Serviço Telefónico Móvel na população é 137%.
-96% das empresas têm computadores, valor que é 100% para as médias e as grandes empresas.
-92% das empresas têm acesso à Internet, e 81% em banda larga

[117] Estudo Netpanel da Marketest
[118] Relatório Plano Tecnológico - Conselho Consultivo de 09 de Julho de 2009
[119] Diário de Noticias edição de 22-02-2009

-Todos os organismos e serviços da Administração Pública Central, Regional e Local dispõem de ligações à Internet,

- 92% dos organismos da Administração Pública Central têm presença na Internet

- 99% das Câmaras Municipais tem presença na Internet.

Segundo os dados do estudo Netpanel da Marktest, o domínio " hi5.com" liderou em número de páginas visualizadas pelos portugueses no primeiro semestre de 2009, na navegação que realizaram a partir de casa.

Ora, a par desta massiva campanha de se dotarem os lares portugueses com estas novas tecnologias, não tem sido proporcionadas, acções de formação a estes novos utilizadores no que concerce às matérias de utilização e segurança. Exemplo disso foi a campanha do computador "Magalhães" ofertado a quase todas as crianças do 1º Ciclo Ensino Básico , em que foi-lhes dada uma máquina e não a formação,tornando esses computadores um convite a visitantes indesejáveis.

Portugal tem actualmente 4,7 milhões de utilizadores do Facebook[120]

Uma passagem rápida pelo Twitter ou pelo Facebook é suficiente para se constatar que em Portugal os adeptos vão desde estudantes, empresários, deputados ou mesmo governantes.

Se por um lado as redes sociais permitem o intercâmbio entre os seus membros, trocas comerciais, recrutamento e partilha de conhecimento, por outro são utilizadas por crackers e hackers para recolherem informações através dos mais variados vírus informáticos , podendo através de sniffers conseguem obter não só as informações publicadas pelos utilizadores (que pensam só poderem ser acedidas pelas suas redes sociais) mas também toda a informação contida no computador infectado, desde contas bancárias a cartões de crédito . Além disso, as redes sociais já são utilizadas por grupos terroristas, tal como se referiu no capítulo 2.

Quantas pessoas reconhecem se uma determinada página da Internet que está a ver preenche os requisitos de uma página segura? Quantos empregados de uma empresa sabem o que devem procurar? Todos que usam a Internet devem saber o que é o pequeno símbolo que quase sempre aparece em algum lugar de uma página na Web, com a forma de um cadeado. Eles devem saber que quando o cadeado está fechado, o *site* foi certificado como sendo seguro. Quando o cadeado está aberto ou o seu ícone não existe, o site Web não é autenticado como genuíno, e todas as informações transmitidas não estão criptografadas.

[120] Diário de Noticias – 4 de Fevereiro de 2014

Entretanto, um atacante que consegue comprometer os privilégios administrativos de um computador da empresa pode modificar ou corrigir o código do sistema operacional para alterar a percepção do- utilizador daquilo que está realmente acontecendo. Por exemplo, as instruções de programação no *software* do browser que indicam que o certificado digital de um site Web é inválido podem ser modificadas para desviar da verificação. Ou então, o sistema pode ser modificado com algo chamado root kit, instalando uma ou mais backdoors no nível do sistema operacional, que são mais difíceis de serem detectadas(MITNICK & SIMON,2013).

A ingenuidade, o deslumbramento, o espírito de partilha e a falta de informação sobre o ciberespaço de quem adere às redes sociais, aliados à facilidade de acesso e à sua popularidade, leva a que as redes sociais sejam algo "muito apetecível" para ser utilizado como "arma", em ordem a desenvolver um ataque cibernético, por quem possui os necessários conhecimentos técnicos e pretende utilizar a Internet como plataforma de guerra.

Assim, estes mesmo utilizadores que são os principais destinatários do *e-government*, e muitas vezes os responsáveis pela sua implementação, que dotados de uma quase identidade digital podem através do seu computador resolver todos os assuntos burocráticos da sua vida pessoal e profissional, são os que ao utilizar o ciberespaço como extensão da vida social, partilham informações sem o mínimo cuidado de segurança devido aos parcos conhecimentos que têm de informática, do ciberespaço, e, uma total ausência de uma cultura de segurança da informação.

Diariamente o Facebook é confrontado com 600.000 ciberataques[121]. Ora, o Facebook que conta com mais de 60 milhões de membros, e é utilizada diariamente por milhares de pessoas, permite a criação de aplicações através de um simples clique. As aplicações do Facebook conseguem compreender todos os requisitos das aplicações da web. Neste contexto, pode-se optar por dois caminhos simples para a construção de aplicações: ou se faz o *download* do programa "Developer Application", que requer conhecimentos de programação, uma vez que tem de utilizar-se a linguagem FBML (Facebook Markup Language – que no fundo é a programação em HTML com as *tags* especificas para aceder ao facebook) para se alojar dentro do "Facebook Canvas" ou então, através da ajuda de

[121] http://www.computerweekly.com/news/2240106175/Facebook-admits-to-600000-cyber-attacks-a-day

uma aplicação do próprio facebook, para se criarem "questionários " com o *upload* de fotografias, por exemplo.

Diariamente são criadas milhares de aplicações em forma de questionários e,se é certo que a maioria é inocente não se poderá atestar de forma alguma que todas o sejam.

A titulo de uma experiência pessoal,criou-se um questionário com a ferramenta do Facebook, a elaboração do questionário que permitia o upload de fotografias (que à partida poderiam conter códigos maliciosos o que não sucedeu neste caso). Finalizado o questionário, enviaram-se os "convites" para os "amigos" que rapidamente o preencheram, em seguida os "amigos" dos "amigos" preencheram-no e, como existem "amigos" em vários continentes, esse mesmo o questionário circulou à volta do mundo. Este pequeno teste serviu para confirmar quão fácil é para um leigo em informática construir uma aplicação numa rede social. Ora, se para um leigo é fácil, como não o será para quem pretenda fazer dela uma arma de guerra cibernética.

A popularização de *software*s que visam mitigar as ameaças à segurança da informação acabou por produzir uma noção enganadora nos utilizadores a respeito da plena eficácia desses *softwares* na protecção das próprias organizações e na supressão de qualquer ameaça. Essa noção equivocada pode ser originada pela obtenção de informações parciais sobre o assunto, ou pela falta da conscientização adequada (LIANG et al), e é um factor humano que pode provocar acréscimo de vulnerabilidade, pois ocasiona um comportamento imprudente dos utilizadores em relação aos Sistemas de Informação.

A "falsa confiança" que é criada em redor das redes, faz com que, muito facilmente, qualquer um adira a uma qualquer aplicação e que siga um qualquer *link*, especialmente se aquela for sugerida por um membro da sua rede. Assim, basta um membro instalar uma aplicação para facilmente se transformar os computadores de inocentes utilizadores em "zombies" (bootnets). Qualquer utilizador pode fazer uma experiência , bastando colocar uma aplicação na sua página pessoal e monitorizar por quantas pessoas é esta partilhada em apenas um dia . Os gestores das redes sociais estão atentos a estes fenómenos, mas, devido à enorme dimensão das redes e à crescente oferta de mecanismos de partilha e de interacção que nelas se têm desenvolvido para torná-las mais atractivas, tem sido difícil conciliar os mecanismos de segurança com as ofertas de partilha.

Em 2013, 318.000 contas do Facebook foram atacadas por um *software* denominado *Pony*, o *malware*[122] que atacava o sistema quando o utilizador visitava um website ficando automaticamente contaminado, permitindo aos *hackers* acesso a todas as informações sensíveis contidas nos computadores. Apesar de ser um vírus antigo e já bastante usual nas mensagens dos *e-mail's*, tomou este uma outra proporção nas redes sociais, uma vez que a população cibernética começou a estar alertada para o risco de contaminação através dos *e-mails*, tomando um cuidado redobrado na sua utilização, enquanto que permanecia ingenuamente passivo em relação aos perigos das redes sociais. Ainda este ano, o Facebook foi invadido por outro vírus de nome "*LOL*" que continha uma extensão " .Zip" e que circulou através de mensagens privadas infectando os sistemas e apoderando-se das próprias contas de Facebook.

Há uns anos, um grupo de investigadores criou uma aplicação para o Facebook com o intuito de estudar a segurança das redes. A aplicação denominada "Photo of the Day" ,permitia aos utilizadores beneficiar todos os dias de uma foto da "National Geographic" onde os investigadores tinham previamente inserido uma aplicação "Facebot". Todos os utilizadores da rede que utilizaram a aplicação ficaram infectados tornando-se em "botnets" enviando de imediato mensagens para um alvo, produzindo um ataque DNS.

É sabido que as organizações terroristas utilizam a Internet para inúmeros propósitos tais como recrutamentos, comunicações, propaganda, fraudes e intrusões. Com a crescente popularidade que as redes sociais têm ganho e com a dificuldade de controlar eficazmente a sua segurança, estas poderão ser utilizadas como uma nova arma do ciberespaço para atacar organizações.

É possível detectar a origem de um ataque, mas não é possível determinar quem operou o computador para o praticar. Um grupo terrorista com ajuda de um *cracker* pode desenvolver um vírus que se instala num computador de um simples adolescente e este, sem o saber, ao utilizar seu computador numa determinada data pode causar um atentado de forma intencional.

[122] Malware significa "software malicioso". Malware é qualquer tipo de software não desejado que é instalado sem a sua autorização [em linha] consultado em 20 de Junho de 2014 http://www.microsoft.com/pt-pt/security/resources/malware-whatis.aspx

Aproveitando a iliteracia informática dos seus membros, as vulnerabilidades das redes e a dificuldade do seu controlo, grupos menos bem intencionados, infiltram-se, inserem vírus, uns com intuito de tirarem proveito ilícito, outros pelo simples prazer da destruição.

No entanto, o que as torna extremamente perigosas é a sua utilização por parte de organizações terroristas como meio de ataque cibernético. Este cenário poderá converter-se em realidade se não forem tomadas as devidas medidas de segurança até porque o *e-government* é cada vez mais uma realidade global, o que torna uma guerra cibernética muito mais acessível. E as redes poderão ser uma porta aberta para um ataque em massa aos Estados por parte de grupos radicais.

Em 2013 a Agência Europeia ENISA (Agência Europeia para a segurança das redes e da informação) lançou um comunicado a alertar para os altos riscos de ciberataques a organizações empresariais e governamentais dos estados membros através de ataques cibernéticos com técnicas antigas, embora utilizadas de uma forma mais inteligente e com um mais amplo campo de actuação. Através do envio de um e-mail contendo um link para uma página da internet que contem um *malware* instalado permite o atacante ganhar controlo sobre a maquina e começar a recolher informações. Através da informação recolhida o atacante procede a novos ciberataques até conseguir atingir o fim proposto. Os anti-virus instalados e os programas anti-phising nem sempre detectam este tipo de ataques tendo em conta que são métodos utilizados há muito tempo e até à data utilizados em pequena escala, passando ao largo das companhias fabricantes de anti-virus[123].

Se é certo que na "virtualização do Estado" se prevêem as medidas de segurança para a protecção das IIC (infra-estruturas de informação críticas), o mesmo não se poderá dizer da implementação de uma cultura de segurança da informação. Em Março deste ano, devido aos sucessivos ataques aos *sites* das escolas portuguesas, o Ministério da Educação proibiu o acesso dos alunos a redes sociais através dos computadores das escolas[124].

Essa caixinha mágica que permite ao cidadão resolver todas as suas questões, é mesma que ele utiliza para jogar, para partilhar vídeos e fotografias com amigos que se encontram do outro lado do mundo, para estabelecer novas amizades, tudo fruto da mudança do paradigma para uma nova sociabilização virtual e, ao fim e ao cabo, para se contaminar ou para se tornar num zombie de uma qualquer rede terrorista, pondo em risco *in extremis* a Segurança Nacional.

[123]ENISA *Cyber-attacks – a new edge for old weapons* FN01_2013 [2013/03/13]

[124] http://cmtv.sapo.pt/atualidade/detalhe/ciberterroristas-atacam-escolas-portuguesas.html

Esta imagem, talvez um pouco caricaturada, é infelizmente real. E não falamos aqui apenas do cidadão comum a quem foi dada uma ferramenta sem livro de instruções completo, os info-iletrados, mas também daqueles que com alguma responsabilidade se deslumbram com a popularidade que o mundo virtual lhes proporciona e se esquecem por completo das regras da segurança da informação. A segurança tem de deixar de ser encarada como uma questão meramente técnica mas acima de tudo estratégica e humana, uma vez que todo o processo de segurança se inicia e tem o seu término no ser humano.

O quadro abaixo reproduzido reflecte em síntese os vários recursos dos sistemas de informação e respectivas vulnerabilidades [125]:

Recursos de sistema	Vulnerabilidades
1. Pessoal	a) Acesso a informação, equipamentos e aplicações críticas; b) Nível de formação e de conhecimentos; c) Probabilidade de erro humano; d) Falta de idoneidade, compromisso e ética; e) Frustrações no trabalho.
2. Instalações	a) Quebra de segurança física; b) Segurança não implementada de raiz com as instalações; c) Limitações ou localização inapropriada das instalações
3. Hardware de Rede	a) Configurações físicas mal executadas; b) Acessos inseguros; c) Ferramentas de administração deficientes; d) Más políticas de segurança; e) Falta de planos de contingência; f) Falta de renovação de equipamentos; g) Hardware não testado; h) Deficiente firmware; i) "Bugs" ou configurações deficientes; j) Políticas de integração deficientes; k) Interrupções de energia; l) Danos físicos.
4. Software de Rede	a) A Não alteração da configuração base; b) Passwords de origem não alteradas; c) Protocolos inseguros; d) "Bugs"; e) Má administração e exploração do software; f) Heterogeneidade de software; g) Falta de análise de logs; h) Simetrias de confiança (trust Symmetry); i) Simetrias de transitivas (Trust Transitivity); j) Políticas de integração deficientes; k) Software não testado.
5. Dispositivos Periféricos	a) Localização;

[125] Santos, Paulo , Bessa Ricardo, Pimentel Carlos – Cyberwar , O fenómeno, as tecnologias, e os actors FCA Editora informática – Jan 2008

	b) Segurança física deficiente; c) Políticas de Segurança e de pessoal; d) Conexões não autorizadas ou fantasma; e) Dispositivos não testados.
6. Dispositivos de armazenamento	a) Gestão ineficiente; b) Inexistentes ou más políticas de segurança; c) Falta de políticas de acesso; d) Falha de equipamentos; e) Dispositivos em ambiente não controlado; f) Dados residuais.
7. Sistemas Operativos	a) Passwords de origem não alteradas; b) "Bugs"; c) Características de segurança fora de uso; d) Más especificações; e) A não actualização de "releases" e de "updates"; f) Má gestão das configurações de segurança; g) Indefinição ou deficiente aplicação das políticas de segurança.
8. Software de Nível de Sistema	a) Políticas de acesso; b) Passwords de origem não alteradas; c) A não actualização de "releases" e de "updates"; d) Má gestão das configurações de segurança.
9. Aplicações de Nível de sistema	a) Políticas de acesso; b) A não actualização de "releases" e de "updates"; c) Má gestão das configurações de segurança; d) Ambiente de desenvolvimento.
10. Dados Operacionais	a) Deficiente política de backups e de recovery; b) Falta de planos de contingência; c) Corrupção de dados.

126

Segundo Vance et al. (2012), as organizações sofrem, em regra e anualmente, uma brecha na segurança, devido a uma violação das políticas de segurança da informação. Os autores estimam que mais da metade de todas as violações de segurança são directa ou indiretamente causados por falha de um colaborador ao cumprir os procedimentos de segurança. Ainda de acordo com Vance et al. (2012), uma série de abordagens comportamentais têm sido propostas na literatura para explicar a importância do cumprimento dessas políticas, ou para explicar as razões dos abusos(VANCE et al 2012).

Quando as ameaças à segurança não são percebidas como eminentes, os esforços em seguir as normas e boas práticas em segurança da informação podem ser considerados desnecessários, improdutivos e apenas uma formalidade normativa (HERATH et al, 2009).

[126] Santos, Paulo , Bessa Ricardo, Pimentel Carlos – Cyberwar , O fenómeno, as tecnologias, e os actors FCA Editora informática – Jan 2008

Assim sendo, a par de todas as políticas de cibersegurança que se pretendam implementar torna-se premente um investimento na literacia digital promovendo uma verdadeira cultura de segurança na utilização no ciberespaço também na óptica do utilizador.

A protecção contra este tipo de ameaça é uma responsabilidade partilhada. Os Estados, seja por intervenção legislativa, seja pela criação de instrumentos técnicos adequados, têm um papel importante quer na prevenção quer na preparação para a eventual resposta a uma emergência.

Por outro lado, a segurança das redes e da informação passa, também, por uma utilização segura e consciente da tecnologia por parte dos indivíduos, em casa ou no trabalho, por um maior enfoque na componente de segurança dos seus produtos por parte dos fabricantes de equipamento e produtores de software e pela aplicação de metodologias de análise de risco e políticas de segurança da informação nas empresas[127].

[127] O CERT (Computer Emergency Response Team) Portugal , surgiu no ano de 2002 e tem como missão contribuir para o esforço de cibersegurança nacional nomeadamente no tratamento e coordenação da resposta a incidentes, na produção de alertas e recomendações de segurança e na promoção de uma cultura de segurança em Portugal. Esta série de textos é da autoria de especialistas do CERT.PT e insere-se na campanha do Mês Europeu da Cibersegurança, que teve lugar em Outubro de 2013.

Capítulo 5

CONCLUSÃO

Do que foi referido nos capítulos anteriores e das situações e dos factos que foram apontados para melhor os consubstanciar, infere-se que:

- O ciberespaço é um domínio interactivo constituído por todas as infra-estruturas técnicas de informação e de comunicação, no qual se incluiu a Internet, que permite que pessoas, quaisquer que sejam a sua nacionalidade, raça, religião, credo e ideologia se possam, independentemente do ponto do globo onde se encontrem, comunicar entre si, cooperar, progredir e prosperar.

- Com o ciberespaço materializou-se em larga medida o conceito de " aldeia global" com que o mundo dos nossos dias tem vindo a ser caracterizado. Perante a facilidade e a velocidade como as informações hoje circulam, possibilitadas pelos avanços tecnológicos verificados nas estruturas e nos sistemas de informação, pode dizer-se que foram ultrapassadas as barreiras de distância e do tempo. De facto, as informações e as comunicações que são presentemente estabelecidas correm em tempo real.

Refira-se, a propósito, que a World Wide Web (W.W.W.) tendo começado em 1991, mantém hoje em linha cerca de 2 biliões de pessoas, ou seja, cerca de 1/3 da população mundial. De salientar que com o aparecimento da WWW pela progressiva difusão das comunicações móveis e de banda larga mostrou os limites da visão idealista dos fundadores da internet.

- A Internet e outras tecnologias digitais estimulando cada vez mais o diálogo transnacional, favorecem não apenas a pessoa, a título individual, pela oportunidade de acesso a novos conhecimentos, mas também os Estados, seja no desenvolvimento da sua economia, seja na resolução de situações e de problemas para as quais careçam de ajuda ou da solidariedade da comunidade global.

- As sociedades, por virtude da sua inclusão no ciberespaço, estão a transformar-se.

- No que ao cidadão comum diz respeito, a internet faz parte hoje da sua vida diária, pois, é através dela que toma conhecimento do que se passa na sua localidade, no seu país e no mundo; resolve grande parte das situações e dos problemas que surgem no seu quotidiano, sejam os que se prendem com as suas actividades familiares e domésticas, seja no seu relacionamento com os organismos e serviços públicos, seja até para estabelecerem e manterem a relação de proximidade com colegas, familiares e amigos, através das vulgarmente designadas redes sociais.

Pode dizer-se que o individuo que se excluiu do mundo digital caminha para o isolamento.

- Relativamente ao sector público, são irrefutáveis os benefícios que advêm do uso da Internet e de outras tecnologias digitais, e que se traduzem, por um lado, na comodidade para os cidadãos que não terão de deslocar-se aos organismos e serviços públicos para tratarem de assuntos que os envolvem ou afectam, até simplesmente para cumprirem os seus deveres de cidadania, quão seja o pagamento dos seus impostos, enquanto para a própria administração pública, por seu lado, abre-se o caminho para a sua simplificação administrativa e burocrática, com os seus reflexos nos custos com as despesas do seu funcionamento e também para que esta estabeleça relações de uma maior proximidade com os cidadãos.

Pode dizer-se que com o ciberespaço as administrações públicas democratizaram-se, significando-se com isso que as exigências dos cidadãos por uma maior transparência no desenvolvimento das suas políticas sectoriais e responsabilidade dos respectivos agentes cresceram, podendo comprometer a " accountability " dos governos.

Ainda no contexto do sector público, não são irrelevantes as implicações que resultam do uso da Internet e outras tecnologias digitais pelas estruturas policiais e militares, seja para efeitos de logística, de uma permanente actualização e modernização, seja em termos dos respectivos contributos para a manutenção da estabilidade e da segurança nacional e internacional.

- No sector privado, mais concretamente no chamado mundo dos negócios, a Internet e outras tecnologias digitais, conduziram, por um lado, a novos modelos organizacionais e de gestão das empresas, com reflexo na competitividade e na produtividade, e a inovações e, por outro lado, possibilitaram a abertura de novos mercados sendo hoje possível que uma empresa que se encontra sediada em Portugal, faça os seus negócios com outras estabelecidas em qualquer um outro país do mundo e que, à velocidade de um clique possa resolver os problemas que entretanto possam ter surgido.

Pode dizer-se que a economia de um país desenvolve-se hoje no ciberespaço e que o seu crescimento assenta sobremaneira em redes electrónicas de informação.

Porém, as vantagens da globalização do ciberespaço e a crescente generalização do uso, a nível mundial, da Internet e de outras tecnologias digitais, trouxe novos problemas e novos desafios para a comunidade global.

- Questões que se prendem com os direitos e liberdades fundamentais do Homem e com a segurança nacional e internacional passaram a absorver uma crescente atenção dos Estados e dos respectivos governantes.

- O ciberespaço, aliado ao uso massificado da internet, transformou-se num terreno propício e favorável à prática de actos ilícitos e de crimes, com a entrada naquele de actores maliciosos e de organizações terroristas. Com a vantagem de se tratarem da prática de actos que não envolvem grandes custos para a sua perpetração, poderem ser executados à distância, isto é, de um qualquer ponto do globo e de serem reduzidos os riscos para os seus autores por dificuldades e, por vezes impossibilidade, na sua identificação.
- No que reporta ao cidadão comum, o roubo de identidade para efeitos de acesso à sua conta bancária ou a obtenção e revelação dos seus dados pessoais e profissionais para efeitos de extorsão ou chantagem, são alguns dos exemplos de cibercrimes que são praticados, a que não são também alheios a pedofilia e o aliciamento e exploração de crianças, ou de mulheres, para a prostituição, e que vão ganhando também o seu terreno.
- Para a economia, a internet que se apresenta como uma janela para o mundo, sendo através dela que as empresas dão conta da sua presença e existência, que os engenheiros, gestores, economistas, académicos, cientistas e profissionais das mais diversas profissões e especializações trocam entre si, a nível mundial, os seus conhecimentos, os quais conduzirão à definição de novos conceitos, a novas descobertas, inovações, invenções, o ciberespaço abriu as portas a cibernautas criminosos para a prática dos seus crimes, podendo alguns comprometer a própria segurança nacional. Neste domínio, relevam os crimes contra a propriedade intelectual, designadamente, a espionagem intelectual e comercial, as patentes, as marcas e os direitos de autor.

Com vista a minimizarem-se os riscos e a prática de cibercrimes, os países foram rodeando-se das necessárias e adequadas medidas reactivas e pró-activas para os contornar e combater, por forma a que tanto os cidadãos como os sectores publico e privado continuem a utilizar esse espaço cibernético , com confiança e segurança. Isto, na medida em que os utilizadores, seja como uma pessoa singular ou colectiva, têm de ter a confiança de que não há rupturas no envio dos seus dados e que a respectiva privacidade não será violada.

- Tratam-se de medidas que vão das mais simples, quão sejam a realização de acções de formação e campanhas de sensibilização junto dos cidadãos e nas empresas sobre os riscos pelo uso inapropriado da Internet e dos cuidados a ter para os prevenir e combater, passando por outras mais complexas como sejam a manutenção da segurança das suas infra-estruturas críticas, tendo em vista a preservação da sua integridade, evitando as

rupturas, até à produção de legislação específica no contexto de combate ao cibercrime. Donde,

- Os Estados estão conscientes de que o ciberespaço tornou-se um terreno onde os sucessos económicos se ganham ou se perdem, com os seus evidentes reflexos na prosperidade e no bem-estar das suas populações, e onde a segurança nacional e internacional pode ou não ficar comprometida.

-Os Estados vão igualmente ganhando a consciência de que, apesar de cada um, isoladamente, terem adotado as melhores e mais eficazes medidas domésticas de defesa da cibersegurança, esta só será mais amplamente conseguida se derem as mãos e unirem os seus esforços para a definição de um conjunto de regras de conduta, justas e responsáveis, em matéria de cibersegurança e que seja por todos partilhado.

- Analisadas as estratégias de cibersegurança de 5 países constatou-se que, apesar de terem algumas diferenças na sua implementação, visam todas dois objectivos interligados: proteger a sociedade contra ciberameaças, uma vez que se tornaram mais dependentes do ciberespaço e, fomentar a segurança cibernética como essencial para o maior desenvolvimento da economia;

Para o Reino Unido a dependência do interesse do país no ciberespaço é vasta, afectando o cidadão individual, quase todos os aspectos do governo, a indústria, a infra-estrutura nacional, o transporte e a forma como a economia funciona; para a Espanha, grande parte da estabilidade do país e a prosperidade económica dependerá da segurança do ciberespaço. Segundo a França, o nível actual de ataques contra sistemas de informação, revela um alto potencial de desestabilização da vida quotidiana, podendo levar à disrupção das redes que são fundamentais para a vida da nação e à negação do funcionamento da capacidade militar. Para os Estados Unidos da América o ciberespaço fornece uma plataforma para a inovação e prosperidade e os meios para melhorar o bem-estar geral em todo o mundo, que toca praticamente tudo e toda a gente. A Alemanha, por seu lado pretende manter e promover a prosperidade económica e social e salienta que a garantia de segurança cibernética se transformou num desafio central para o Estado, empresas e sociedade e que é uma questão vital para o século XXI;

Na verdade, a Comunidade Europeia não tem uma abordagem única para a segurança cibernética como sucede com a NATO que criou, em 2007, um Centro de Excelência de Cooperação em Ciberdefesa, com a participação activa de 28 países. No entanto, a Comunidade Europeia tem uma responsabilidade política que abrange as áreas de

cibersegurança civil, cibercrime, a cooperação policial e de justiça penal no ciberespaço, sendo que essas responsabilidades em toda a Comunidade Europeia continuam a ser prerrogativa dos governos nacionais, donde as estratégias nacionais de cibersegurança serem diferentes entre os países que a compõem.

- O ciberespaço, sendo um mundo sem fronteiras, embora haja quem pense que possa delimitá-las, abriu as portas a uma panóplia de oportunidades, seja para os Estados, para as suas organizações, para as suas empresas e para os seus cidadãos, mas deixou-as entreabertas para agentes maliciosos que, individualmente, em grupo ou integrados em organizações, descobriram a sua via para cometerem actos ilícitos e crimes.

- Grosso modo, tais actos, na medida que perpetrados no ciberespaço e mediante recurso a meios informáticos ,têm sido classificados de cibercrimes, no entanto, tendo em conta a intenção da sua prática e quem os pratica podem ter designações específicas. Donde, falar-se de ciberespionagem, de ciberterrorismo, de ciberativismo, etc. e, com isso relacionado, sobre a necessidade de se definirem políticas de cibersegurança para a prevenção e combate a tais actos.

- O Terrorismo, termo que surgiu originariamente em França no SEC XVIII e que ainda hoje não tem uma definição internacionalmente aceite, devido às conotações politicas a que se associa, é um acto com cada vez mais visibilidade num mundo global onde as notícias correm mundo em questões de segundos. Numa época onde as notícias negativas e sensacionalistas vendem mais nos média que as noticias positivas e realistas, o terrorismo tem sido vezes demais manchete de jornais e abertura dos serviços noticiosos, trazendo consigo a sensação que se está mais próximo de nós do que na realidade o está. Os actos terroristas de 11 de Setembro nos Estados Unidos, seguidos dos atentados em Espanha e no Reino Unido fizerem estremecer o mundo ocidental que se julgava seguro e impenetrável a tal violência.

- Esta passagem do mundo real ao virtual, levou a que os grupos criminosos, nomeadamente os terroristas se adaptassem com intuito de conseguir atingir os objectivos da melhor forma possível.

- O ciberespaço tornou-se também um terreno aberto para a prática de actos terroristas, com a vantagem de estes poderem ser executados sob o anonimato, sendo difícil quando não impossível a identificação do seu autor ou autores, poderem ser cometidos a partir de um qualquer ponto do globo e sem que este ou estes ponham em risco as suas próprias

vidas e por envolverem custos reduzidos, salvo a posse dos conhecimentos técnicos exigíveis para a respectiva prática.

- A prática de um crime cometido no ciberespaço por um terrorista, porém, nem sempre pode ser classificado como um acto de ciberterrorismo, não passando aquela frequentemente da esfera do chamado cibercrime. Isto, na medida em que, para ser-se qualificado de ciberterrorismo é necessário que ele apresente as caraterísticas de um acto terrorista tradicional ou convencional, onde a violência, a destruição de propriedades e de vidas humanas e, sobretudo, a criação de sentimentos de terror e de pânico sobressaem e sejam preponderantes.

- O que move os terroristas a recorrerem ao ciberespaço é a possibilidade de, através da internet, mais facilmente poderem fazer a propaganda das suas ideologias, de poderem aliciar novos membros e simpatizantes, de estabelecerem o diálogo com outros membros, de prepararem as suas ações, de incitamento à " datamining" e para angariarem fundos para as suas causas.

- À semelhança da restante comunidade cibernética, também os terroristas vão acompanhando a evolução das novas formas de comunicação no ciberespaço, pelo que os seus sítes na internet têm vindo a ser completados com o seu crescente envolvimento nas chamadas redes sociais, muito porque têm conhecimento de que os serviços de informações os têm sob vigilância, mas principalmente porque estas oferecem maiores audiências e outras possibilidades na sua utilização. Além disso, o seu envolvimento nas redes sociais permitem-lhes inscrever e participar em fóruns restritos, possibilitando-lhes fazer passar as suas mensagens, recrutar novos seguidores e simpatizantes e aliciar, mediante uma recompensa monetária, os especialistas informáticos que possam ser-lhes úteis para a execução de uma determinada acção. O ciberterrorista, qualificado para a prática de um acto terrorista pela via informática, tanto pode ser um membro de uma qualquer organização terrorista, amante de uma causa e que por ela dá a sua vida, como pode ser um perito informático sem qualquer ligação a uma organização terrorista e que age a soldo desta, recrutado em regime de outsourcing. Ou ser até simplesmente um simples apaixonado por ideais extremistas e radicais e que atua por sua própria conta e em defesa daqueles ideais – são conhecidos como os Lone Wolf ou Lobos Solitários que, por vezes, são incentivados pelas organizações terroristas para a execução de uma determinada acção.

- A enorme dificuldade, porém, de se destrinçar um acto praticado por terroristas no ciberespaço e mediante recurso a meios informáticos como sendo um acto de ciberterrorismo de um outro acto, praticado pelos mesmos autores e pelas mesmas vias, como sendo um acto de cibercrime, tem levado os responsáveis pelas questões de cibersegurança e os estudiosos da matéria a analisarem os casos e as situações que tiveram lugar nestes domínios. Até à data não ocorreu nenhum ataque de ciberterrorismo, tal como se entende, uma disrupção das infra-estruturas criticas causando danos físicos graves e perda de vidas. No entanto, os vírus como o Stuxnet, podem levar à efectivação dos actos terroristas no ciberespaço, colocando em risco as infra-estruturas críticas. Porém esse risco não parece evidente tendo em conta todos os procedimentos e conhecimentos que são necessários para o desenvolvimento de vírus dessa envergadura. Ainda no início do mês de Junho, alguns países, nomeadamente a Alemanha, a República Checa, a Áustria, entre outros, perderam o rasto nos seus radares de 13 aviões, durante cerca de 25 minutos, que sobrevoavam o espaço aéreo europeu. Esse "blackout"[128] aconteceu por duas vezes levando as investigações a considerar que os sistema de tráfego aéreo tinham sido *hackados*. Este incidente está a ser investigado pela Agência Europeia para Segurança da Aviação sendo a causa ainda desconhecida, embora possa estar conotado com exercícios militares[129].

Perfilha este entendimento Denning para quem os incidentes até agora verificados apresentam características de se tratarem de actos de ciberativismo, de ciberespionagem ou simplesmente de actos de protesto contra uma determinada situação. Isto, na medida em que o ciberterrorismo, tal como o terrorismo, têm subjacentes uma ameaça constante que paira sobre a mente das populações e servem-se do medo para alcançarem os seus objectivos. Esse medo que impele o Homem para agir de determinada maneira para se livrar da ameaça e da ansiedade que lhe produz e que o leva, por um lado, a ceder as suas liberdades individuais aos que lhe prometem a sua segurança ou, inversamente, a aumentar a sua desconfiança sobre as respectivas instituições. É através dessa guerra psicológica causadora do medo que faz com que as populações estejam em constante alerta, temendo esse algo que desconhecem e que pode até nunca vir a acontecer.

[128] http://www.independent.ie/world-news/europe/cyberterrorism-fear-after-13-jets-vanish-from-radar-30353858.html consultado em 20 de Junho
[129] http://www.reuters.com/article/2014/06/13/us-europe-airplanes-safety-idUSKBN0EO1CW20140613 consultado em 20 de Junho

Aparentemente Portugal não é um país de elevado risco no que concerne a ataques ciberterroristas, tendo em conta o último Relatório Anual de Segurança Interna (RASI) sobre o terrorismo em Portugal onde se afirma que os riscos em 2013[130] :

Do ponto de vista da ameaça terrorista foram observados determinados fenómenos que alicerçam e potenciam as acções terroristas, de forma a continuar a garantir a protecção da segurança das pessoas, das infra-estruturas críticas nacionais, dos grandes eventos e dos sistemas electrónicos de informação. À semelhança do que sucedeu os últimos anos permaneceu como questão central a detecção de indícios que revelassem de forma mediata ou imediata, o envolvimento de cidadãos nacionais ou de estruturas sediadas em território nacional no activismo, na propaganda, no apoio logístico ou no financiamento de redes terroristas internacionais. Suscitou idêntica atenção o movimento de cidadão nacionais para palcos da Jihad, em particular com destino a regiões onde a Al-qaeda e afiliadas procuraram reforçar a sua posição, com destaque para a Síria, ou em direcção a regiões sobre a influência da Al-qaeda no Magreb islâmico e de grupos terroristas de carácter regional, como o Mali. Efectivamente a situação da Síria emergiu com particular destaque, em função do elevado contingente de combatentes que para ali se deslocaram oriundos de vários países da União Europeia, bem como da presença naquele país de grupos terroristas, alguns com ligações à AQ-CORE que tem interesses ocidentais como alvos prioritários. Sobressai ainda riscos de eventuais conexões ao nosso pais de antigos elementos das estruturas operacionais de redes terroristas separatistas ou revolucionárias – ainda que desactivadas- designadamente através da utilização de Portugal como local de retaguarda e células que se encontrem adormecidas.

- É preciso, no entanto, não esquecer-se que Portugal faz parte da Comunidade Europeia que, embora em situação de crise económico-social, mantem-se como uma das suas potências.

- Um outro aspecto a ter em conta especialmente no cerne da Comunidade Europeia é o crescimento dos partidos extremistas, como se constatou nas últimas eleições europeias, que trazem consigo ideais radicais. O crescimento da crise económica, o descrédito do sistema político e a ausências de valores estruturais especialmente nas populações mais jovens levam a que se aumente a tendência de crescimento de forças radicais, contribuindo

[130] Relatório de Segurança Interna 2013 http://www.portugal.gov.pt/media/1391220/RASI%202013.pdf revisitado em 1 de Junho de 2014

para o aumento de grupos extremistas "anti-europa" que poderão ser no futuro uma ameaça séria e real à segurança nacional.

A recolha de informações é a arma mais poderosa na luta para desmantelar as redes terroristas e prevenir-se os seus ataques.

- Dadas as naturezas complexa e multifacetada de relações que o terrorismo tem associadas, dificilmente será consensual um seu conceito abrangente e aceite por toda a comunidade internacional, pelo que dificilmente se alcançará uma legislação universal à altura dos seus riscos, donde o combate não se revelar uma tarefa facilitada. A prevenção torna-se, assim, a principal estratégia para a eliminação ou redução dos seus efeitos.

- A legislação portuguesa apresenta-se, por ora, em matéria de cibersegurança, ao mesmo tempo complexa e confusa, não tanto devida à profusão de normativos existentes, mas pela dispersão por várias entidades e organismos de competências e de atribuições na prevenção e no combate verificados no ciberespaço, sem que haja, para o efeito, uma definição clara e concisa sobre a entidade à qual caberá superintender, supervisionar, orientar, dirigir e coordenar as suas necessárias e as mais apropriadas acções.

Exemplo disso, é a criação recente do Centro Nacional de Cibersegurança, em que se estabelece que " O CNC SEG. actuará em articulação e em estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo, devendo comunicar à Polícia Judiciária, no mais curto prazo, os catos de que tenha conhecimento relativos à preparação e execução de crimes".

Ora, a referência de que o CNCSeg actuará em articulação e em estreita cooperação com os responsáveis pela ciberespionagem, pela ciberdefesa, pelo cibercrime e pelo ciberterrorismo, sem que se explicitem quais sejam os organismos responsáveis por cada uma das referidas áreas e sem que, principalmente, se definam claramente não apenas o âmbito, mas os limites das respectivas competências, parece indiciar que cada um tenderá a agir isolada e autonomamente.

- A prevenção, apresentando-se como uma das mais eficazes armas de combate ao ciberterrorismo, julga-se que, na situação portuguesa, para além de se pensar em dotar o país de uma estrutura de cibersegurança, há que avançar-se rapidamente na implementação de uma cultura de segurança digital, sob pena de todos os esforços poderem revelar-se inglórios.

- Os Serviços de Informações do país encontram-se, por seu lado, limitados no seu campo de actuação por impedimentos legais que urgem ser ultrapassados. A sua quase

impossibilidade de socorrerem-se da HUMINT e da SIGINT, restringindo-se à utilização da OSINT para efeitos de obtenção e recolha de informação, é bastante limitadora da sua capacidade interventiva.

Não obstante considerar-se que a área do Ciberterrorismo deva manter-se no âmbito das competências dos Serviços de Informações, há que reconhecer-se que no âmbito de combate ao ciberterrorismo as acções pró-activas prevalecem sobre as acções reactivas, onde a recolha de informações não se compadece com as limitações impostas pela restrição de uso de determinadas técnicas.

Importa neste contexto sublinhar que o ciberterrorismo previne-se combatendo o terrorismo, assim como a partilha de informações com outros organismos de segurança nacionais, sobretudo com a polícia criminal, ou seja com a Polícia Judiciária, o órgão com a competência reservada para a investigação dos crimes de terrorismo, e com o Serviço de Estrangeiros e Fronteiras (SEF), o órgão de polícia criminal responsável pela averiguação e investigação de actividades relacionadas com a prática do crime de auxílio à imigração ilegal e de crimes conexos, revela-se simplesmente indispensável.

- No mundo da globalização onde as fronteiras da informação, do saber e do conhecimento, das relações interpessoais e entre os Estados, dos negócios e da livre circulação de pessoas e bens tendem a reduzir-se, dificilmente se compreende que estas fronteiras persistam na organização interna dos Estados em que os seus serviços, instituições e organismos públicos mantem-se fechados nas respectivas torres de marfim, trabalhando virados para o próprio umbigo.

Se, nas estratégias de cibersegurança que alguns dos Estados referidos neste trabalho já reconhecem da necessidade de adoptarem regras de conduta que sejam aceites e partilhados por outros Estados, espera-se que a estratégia de cibersegurança para o país, recentemente aprovada, para além da atenção a dispensar-se àquele aspecto, seja capaz de introduzir, na prática, uma mudança na cultura de interacção e de cooperação entre as entidades e organismos com competências nesse domínio, a começar pela oportuna e salutar troca e partilha de informações entre si.

- Esta nova cultura de serviço público, que importa introduzir-se no Estado, mais concretamente, nas estruturas que o suportam para que possa desempenhar, mais eficiente e eficazmente, as principais funções que lhe cabe prosseguir, sugere e justifica que as instituições académicas colaborem na mudança pretendida, investindo em estudos e

trabalhos de investigação que, sem se descuidarem dos respectivos aspectos teóricos, a principal atenção se focalize em resultados/ conclusões práticos que deles possam obter-se.

Na sequência do trabalho ora apresentado sobre o ciberterrorismo, não será despiciendo referir-se o número assaz significativo de organismos e de estruturas que, directa e indirectamente, encontram-se envolvidos na sua prevenção e combate, sem que, no entanto, haja sido indicada uma entidade independente e com autoridade bastante que supervisione, coordene, oriente e acompanhe em permanência os incidentes que estejam ou possam vir a verificar-se nesse domínio. Por outro lado, tendo em atenção a estrutura weberiana da nossa administração pública, independentemente da natureza dos serviços que cada um presta, em que uma qualquer informação pedida a um organismo sob a tutela de ministros distintos percorre uma escala hierárquica inconcebível até que esta chegue às mãos do seu destinatário, mais se justifica que, em questões tão sensíveis quão sejam de terrorismo e de ciberterrorismo, a essa entidade seja permitida que possa até, quiçá, obter pessoal e presencialmente as informações pretendidas, sem que os responsáveis hierárquicos e máximo do organismo visitado fiquem melindrados. Além de que os diplomas orgânicos dos serviços e organismos públicos, usualmente redigidos em termos vagos e imprecisos, principalmente em matérias relativas a competências e atribuições, não raramente dão origem a duplicações e a sobreposições que, a haver, poderá revelar-se um sério entrave incompatível à celeridade que se deseja alcançar no tratamento desses incidentes.

A realização de um trabalho de investigação, de algum fôlego, que passe por um levantamento exaustivo das estruturas e organismos com intervenção, directa ou indirecta, na área do terrorismo e do ciberterrorismo, a identificação das respectivas tutelas e a existência ou não de eventuais delegações de competências e respectivo âmbito; por uma análise dos respectivos diplomas orgânicos, comparando os conteúdos das suas competências e atribuições, das ordens de serviço internas quando os haja, a identificação da unidade ou subunidade orgânica que da apontada área se ocupa e seus níveis de dependência hierárquica, os recursos humanos disponíveis e respectivas qualificações e o confronto entre o que encontra-se legislado com o que efectivamente se faz na prática; por proceder, através da realização de entrevistas pessoais junto de entidades que, de alguma forma, tiveram intervenção nesse domínio, visando a recolha das suas experiências e opiniões, e finalizando com a apresentação de propostas concretas, suportadas em modelos

de organização e estruturas adoptados por alguns países europeus que se revelem mais adequados às características do nosso país, designadamente, situação geográfica, dimensão territorial e populacional, movimentos migratórios e pelas fronteiras aéreas, sistema económico e fluxos financeiros, nível de governo electrónico e principais vulnerabilidades… apresenta-se-me como um desafio.

Bibliografia

ARRIAGA, Patrícia ; NELSON Felix ; Eduardo Ulrich – **Psicologia das crises e das catástrofes: o importante papel de factores cognitivos e afectivos na percepção de risco de terrorismo**. In CARVALHO, Marina, coord. Estudos sobre intervenção psicológica em situações de emergência, crise e catástrofe. Portimão : ISMAT, 2011. [Consult. 25 Março 2014]. Disponível em: https://repositorio.iscte-iul.pt/bitstream/10071/3253/1/2011_Emo%c3%a7%c3%b5es_Terrorismo_PA.pdf

BAUER, Alain; XAVIER, Raufer – **A Globalização do Terrorismo**. Lisboa: Prefácio, 2003. 290 p. ISBN 972-8563-87-6.

BARLOW, John Perry – **A Declaration of the Independence of Cyberspace** [Em linha]. San Francisco : The Electronic Frontier Foundation, 1996. [Consult. 21 Jun. 2014]. Disponível em https://projects.eff.org/~barlow/Declaration-Final.html

BATISTA, Gonçalo; RIBEIRO, Carlos – Ciberterrorismo: a nova forma do crime no Séc. XXI, como combatê-la. **Proelium – Revista da Academia Militar**. ISSN 1645-8826. Série VI, n.º 1 (2004), p. 29 a 64.

BATTESTIN, Cláudia; GHIGGI, Gomercindo – **O Princípio Responsabilidade de Hans Jonas: um princípio ético para os novos tempos**. Thaumazein: Revista on-line semestral do Curso de Filosofia [Em linha]. Ano III, n.º 6 (Outubro 2010). [Consult. 15 Jun. 2014]. Disponível em http://sites.unifra.br/Portals/1/ARTIGOS/numero_06/battestin_5.pdf. ISSN 1982-2103

BRAVO, Rogério – **Geopolítica, geoestratégia e ciberespaço. Notas Introdutórias** [Em linha]. San Francisco : Academia.edu., 2014. [Consult. 21 Jun. 2014]. Disponível em http://www.academia.edu/5543845/Geopolitica_geoestrategia_e_ciberespaco_Notas_introdutorias

BRANT, Leonardo Nemer Caldeira – **O Tribunal Penal Internacional como agente jurisdicional no combate ao Terrorismo**. In AMBOS, Kai ; JAPIASSÚ, Carlos Eduardo Adriano, Org. Tribunal Penal Internacional: Possibilidades e Desafios. Rio de Janeiro: Lumen Juris, 2005, p. 149-161.

CARDOSO, Tatiana de Almeida Freitas Rodrigues – **Os impactos da globalização no terrorismo**. Revista Eletrônica de Direito Internacional. [Em linha]. Vol. 8, 1.º semestre (2011), p. 289–329. [Consult. 26 Março 2014]. Disponível na Internet: http://www.cedin.com.br/revistaeletronica/volume8/arquivos_pdf/sumario/Tatiana%20Cardoso.pdf. ISSN 1981-9439

CASTRO, Daniel – **A Declaration of the Interdependence of Cyberspace** [Em linha]. Framingham : Computerworld, 2013. [Consult. 21 Jun. 2014]. Disponível em http://www.computerworld.com/s/article/9236603/A_Declaration_of_the_Interdependence_of_Cyberspace

COLLIN, Barry – The Future of Cyberterrorism. Crime & Justice International Journal. ISSN 1096-8733. Vol. 13, n.º 2 (March 1997), p. 15

CONWAY, Maura – **Hackers as Terrorists? Why It Doesn't Compute.** ***Computer Fraud and Security*** [Em linha]. N.º 12 (December 2003), p. 1-8. [Consult. 14 Maio 2014]. Disponível na Internet: http://doras.dcu.ie/493/1/comp_fraud_12_2003.pdf. ISSN 1361-3723.

CORRÊA, Cynthia Harumy Watanabe – **Comunidades virtuais gerando identidades na sociedade em rede**. *Revista Ciberlegenda* [Em linha]. N.º 13 (2004) [Consult. 15 Jun. 2014]. Disponível em http://www.uff.br/ciberlegenda/ojs/index.php/revista/article/view/226/122

DENNING, Dorothy E. – **Whither Cyber Terror?** [Em linha] Brooklyn : 10 Years After September 11. A Social Science Research Council Essay Forum [Consult. 15 Jun. 2014]. Disponível em http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/.

DENNING, Dorothy E. – **Stuxnet: What Has Changed?.** Future Internet [Em linha]. N.º 44 (2012), p. 672-687. [Consult. 15 Jun. 2014]. Disponível em http://faculty.nps.edu/dedennin/publications/Stuxnet%20-%20What%20Has%20Changed%20-%20Future%20Internet%20-%20final.pdf. ISSN 1999-5903 .

DENNING, Dorothy E., **Terror's Web: How the Internet is Transforming Terrorism**. In JEWKES, Y; YAR, M., ed. – Handbook on Internet Crime [Em linha]. [Oxford] : Willan, 2009. [Consult. 15 Jun. 2014]. Disponível em http://faculty.nps.edu/dedennin/publications/Denning-TerrorsWeb.pdf

DENNING, Dorothy E. **– A View of Cyberterrorism Five Years Later**. In HIMMA, Kenneth Einar, ed. **–** Internet Security: Hacking, Counterhacking, and Society. Boston: Jones and Bartlett, 2006. Chapter 7. ISBN 978-0763735364.

Dictionary of Military and Associated Terms [Em linha]. Washington D.C.: Department of Defense, 2010. [Consult. 21 Março 2014]. Disponível em: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

FREIRE, Vicente ; CALDAS, Alexandre – **O Ciberespaço: desafios à Segurança e à Estratégia. In Segurança Internacional: Perspetivas Analíticas**. Lisboa: Imprensa Nacional-Casa da Moeda e Instituto da Defesa Nacional, 2013. ISBN 978-972-27-2168-4**.** p. 81-151.

GANOR, Boaz – **Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter**? [Em linha]. [Herzliya] : International Institute for Counter-Terrorism (ICT), 2010 [revisitada em 31 de Maio 2014]. Disponível em http://www.ict.org.il/Article/1123/Defining%20Terrorism%20-%20Is%20One%20Man%E2%80%99s%20Terrorist%20Another%20Man%E2%80%99s%20Freedom%20Fighter

GARCIA, Francisco Proença – **La Transfromation de la Inteligência**. [Em linha] In Boletin de Informacion Nº313, Centro Superior de Estudios de La Defensa Nacional, Ministério de Defensa de España,2009. [Consult. 15 Jun. 2014] Disponível em: http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/Boletines_de_Informacion/ficheros/BOLETIN_DE_INFORMACION_DEL_CESEDEN_313.pdf

GOMES, José Emílio Amaral – **Notas digitais**. [Em linha]. Lisboa: Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI). [Consult. 15 Jun. 2014]. Disponível em: http://www.apdsi.pt/uploads/news/id547/4.8_jose%20emilio%20gomes_070626.pdf

GUILLAUME, Gilbert. **Terrorismo e Justiça Internacional**. In: BRANT, Leonardo Nemer Caldeira, coord. *O Brasil e os Novos Desafios do Direito Internacional.* Rio de Janeiro: Forense, 2004. p. 27-37.

HIMMA, Kenneth Einar – **Internet Security: Hacking, Counterhacking, and Security**. Burlington: Jones and Bartlett, 2007. ISBN 0763735361.

HERATH, Tejaswini ; RAO, H. Raghav – **Protection motivation and deterrence: a framework for security policy compliance in organisations**. European Journal of Information Systems. ISSN: 0960-085X. Vol.18, n. º 2 (April 2009), p. 106-125.

HOFFMAN, Bruce – **Inside Terrorism**. New York: Columbia University Press, 2006. ISBN 0231126999.

KREIBOHM, Patricia Eugenia. **El terrorismo Contemporáneo como Problema Teórico: categorías de análisis, debates e interpretaciones**. In BESOER, Fabián; BRIEGER, Pedro; DERGHOUGASSIAN, Khatchik. *Terrorismo Siglo XXI.* Buenos Aires: Ediciones Suárez, 2005.

LEVIN, Avner, Paul Goodrick Daria IlKina – **Securing Cyberspace : A Comparative Review of Strategies Worldwide .**PRIVACY AND CYBER CRIME INSTITUTE Ryerson University. [em linha] (Consult. Em 29 de Abril de 2014) disponível em :http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf

LEVY, Pierre **– Cyberculture.** Paris: Éditions Odile Jacob, 1997, ISBN: 9782738105127.

LIANG, H; XUE, Y. – **Understanding security behaviors in personal computer usage: a threat avoidance perspective**. Journal of the Association for Information Systems. ISSN 1536-9323. Vol. 11, n.º 7 (2010), p. 394-413.

MAGALHÃES, Ana Manuel Ferreira Malheiro de – **A importância de uma definição de terrorismo.** Jornal de Defesa e Relações Internacionais. [Em linha]. (2004) [Consult. 1 Abr. 2014]. Disponível em: http://www.geografiaparatodos.com.br/index.php?pag=sl228

MARCHUETA, Maria Regina – **Reflexões Sobre o Terrorismo Internacional**. [Coimbra] : Edições Duarte Reis, 2003. 88 p. ISBN 9789728745066

MARGOLIS, Gabriel – **The Lack of HUMINT: a Recurring Intelligence Problem**. Global Security Studies [Em linha]. Vol. 4, n. 2 (Spring 2013), p.43-60. [Consult. Em 14 Maio 2014]. Disponível na Internet: http://globalsecuritystudies.com/Margolis%20Intelligence%20(ag%20edits).pdf

MARINA, José António – **O MEDO: Tratado sobre a valentia**. 1.ª edição. Lisboa : Sextante Editora, 2008. ISBN 978-989-8093-29-5.

MARTINS, A.G. Lourenço ; Marques , J. A. Garcia; Dias, Pedro Simões – **Ciberlaw Em Portugal : O direito das tecnologias da informação e comunicação** (Lisboa): Edição Centro Atlântico . 1ªEdição 2004. ISBN 972-8426-95-X

MITNICK, Kevin, D. ; SIMON, William, L. – **Mitnik – A arte de enganar - Ataques de hackers: controlando o fator humano na segurança da informação** [Em linha]. São Paulo : Pearson Education, 2003. [Consult. 12 Março 2014]. Disponível em: https://doutrina.ensino.eb.br/docs/Kevin_Mitnick-A_Arte_de_Enganar.pdf . ISBN: 85-346-1516-0.

MONTEIRO, Silvana Drumond – **O Ciberespaço: o termo, a definição e o conceito**.

Revista de Ciência e Informação [Em linha]. V.8, n.º 3 (Junho 2007). [Consult. 29 Abril 2014]. Disponível na Internet: http://www.dgz.org.br/jun07/Art_03.htm

NOVAIS, Rui Alexandre – "**Media e (Ciber) Terrorismo**. Nação e Defesa. Lisboa : IDN. ISSN 0870-757X. N.º133 (2012), p. 89-103.

NUNES, Viegas – **Ciberterrorismo: aspectos de segurança. Revista Militar. [Em linha].** ***Nº2433,*** **(Outubro 2004). [Consult. 27 Maio 2014]. Disponível na Internet:** http://www.revistamilitar.pt/artigo.php?art_id=428**. ISSN** 0873-7630.

36 Estratagemas, Os – Manual Secreto da Arte da Guerra Chinesa. São Paulo : Landy, 2007. 240 p. ISBN 8576290960.

PRICHARD, L. E. ; MACDONALD, J. J. – **Cyber Terrorism: a study of the extent of coverage in computer security textbooks**. Journal of Information Technology Education. ISSN-1547-9714. Vol. 3 (2004), p. 279-289.

PRUCHA, Nico ; FISHER, Ali – **Tweeting for the Caliphate: twitter as the new frontier for Jihadist propaganda**. CTC Sentinel [Em linha]. Vol. 6, n. 6 (June 2013). p. 19-23. [Consult. 11 Março 2014]. Disponível na Internet: https://www.ctc.usma.edu/wp-content/uploads/2013/06/CTCSentinel-Vol6Iss62.pdf

RABAÇA, Carlos; BARBOSA, Gustavo G. – **Dicionário de comunicação**. 2.ed. rev. e atual. Rio de Janeiro: Campus, 2001. 560 p. ISBN 978-85-7244-834-5

ROBINSON, Neil [et al]. – **Cyber-security threat characterization**. Stockholm : Swedish National Defence College, 2013.

RODRIGUES, José Narciso da Cunha – **Internet e Globalização**. In MONTEIRO, António Pinto, coord. – *As Telecomunicações e o Direito na Sociedade da Informação*. Coimbra : Instituto Jurídico da Comunicação, 1999, p. 343-347. ISBN 972-98462-0-0.

SANTOS, Loureiro dos, General – **O Império Debaixo de Fogo, Ofensiva Contra a Ordem Internacional Unipolar**. Mem Martins: Edições Europa-América, 2006. 295 p. ISBN 972-1-05668-5.

SANTOS, Loureiro dos, General – **As guerras que já aí estão e as que nos esperam se os políticos não mudarem**. Mem Martins : Edições Europa-América, 2009. 384 p. (Estudos e Documentos). ISBN 9789721060647.

SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos – **Cyberwar, O fenómeno, as tecnologias, e os actores**. [Coimbra]: FCA Editora Informática, 2008. 288 p. ISBN 9789727225972.

SILVA JR, Nelmon J. – **Pressupostos acadêmicos acerca do terrorismo** [Em linha]. [Consult. 29 Abril 2014]. Disponível em: http://www.conteudojuridico.com.br/pdf/cj046875.pdf

SCHMID, Alex P. ; JONGMAN, Albert J. **– Political Terrorism: A New Guide to Actors, Authors, Concepts, Databases, Theories, and Literature**. Harvard : Harvard University. ISBN 1412804698.

SOUKI, Hassan Magid de Castro – **Terrorismo e Direito Internacional: reflexões acerca do fenômeno terrorista no século XXI**. Revista Eletrônica de Direito do Centro Universitário Newton Paiva [Em linha]. [Consult. 28 Abr. 2014]. Disponível na Internet: http://npa.newtonpaiva.br/direito/?p=1177

TANNER, Ashley – **Examining the need for a cyber intelligence discipline**. Journal of Homeland and National Security Perspectives [Em linha]. Vol.1, nº 1 (2014), p. 38-48. [Consult. 28 Abr. 2014]. Disponível na Internet:https://journals.tdl.org/jhnsp/index.php/jhnsp/article/view/16/11

TREVERTONT, Gregory F. – **Intelligence for an Age of Terror**. Cambridge : Cambridge University Press, 2009. ISBN 0-07-222787-7

TZU, Sun – **A Arte da Guerra**. Lisboa: Editorial Futura, 1974.

WEIMANN, Gabriel – **New Terrorism and New Media** [Em linha]. Research series, Vol. 2. Washington, D.C. : Wilson Center, 2014. [Consult. 15 Maio 2014]. Disponível em: http://www.wilsoncenter.org/publication/new-terrorism-and-new-media

WILSON, Clay – **Computer attack and cyberterrorism: vulnerabilities and policy issues for Congress.** [Em linha]. Washington, D.C. : Library of Congress, 2003. [Consult. 15 Maio 2014]. Disponível em: http://fas.org/irp/crs/RL32114.pdf

VANCE, A.; SIPONEN, M. ; PAHNILA, S. – **Motivating IS security compliance: Insights from Habit and Protection Motivation Theory**. Information & Management. Amsterdam : Elsevier. ISSN 0378-7206. Vol. 49, nrs. 3-4 (May 2012), p. 190-198.

VENTURA, J. P. ; NASCIMENTO, J. M. – **Violência, Terrorismo e Psicologia: uma abordagem exploratória**. Revista Portuguesa de Ciência Criminal. Coimbra : Coimbra Editora. ISSN 0871-8563. Vol. 11, n.º 4 (Out-Dez. 2001), p. 633-698.

VERTON, Dan – **Black Ice: The Invible Threat of Cyber- Terrorism**. New York : McGraw-Hill, 2003. ISBN 0072227877.

YORAM, Schweitzer ; GABI, Sibon ; EINAV, Yogev – **Cyberspace and Terrorist Organizations, Military and Strategic affairs**. Military and Strategic Affairs [Em linha]. Vol. 3, n. 3 (December 2011), p. 39-47. [Consult. 28 Abr. 2014]. Disponível na Internet: http://d26e8pvoto2x3r.cloudfront.net/uploadimages/Import/(FILE)1333532806.pdf

ZEIDAN, Sami – **Desperately Seeking Definition: The International Community's Quest for Identifying the Specter of Terrorism**. Cornell International Law Journal. Cornell : Cornell University Law School. ISSN 0010-8812. (2004).