Universidade Nova de Lisboa

Faculdade de Direito

Perspectiva do ciberterrorismo como uma ameaça real e concretizável

Dissertação apresentada para obtenção do grau de
Mestre em Direito e Segurança

(Orientação: Professor Doutor Armando Marques Guedes)

Suzana Sobral

Janeiro de 2013

Agradecimentos

As primeiras palavras de agradecimento vão para o Professor Doutor Armando Marques Guedes, sempre apresentando paciência, disponibilidade e por ter aceite ser meu orientador, demonstrando acreditar que conseguiria concretizar este trabalho.

Ao Professor Doutor Bacelar Gouveia e a todos aqueles que leccionaram neste VII Mestrado de Direito e Segurança agradeço por terem permitido que aprendesse um pouco mais.

Ao Tenente-Coronel Proença Garcia, agradeço a sua disponibilidade, o tempo que dispensou para conversar e oferecer sugestões.

Ao Tenente-Coronel Mário Ley Garcia, pela disponibilidade que demonstrou e na ajuda que me deu na organização de ideias.

Ao Coronel Fernando Freire, agradeço a sua generosidade e paciência, por todo o tempo que despendeu e por toda a ajuda que me deu.

A todos agradeço os conhecimentos que me transmitiram.

ÍNDICE **Página**

Resumo

O ciberterrorismo é um fenómeno recente. Esta dissertação pretende demonstrar que o ciberterrorismo constitui uma ameaça à segurança interna, que pode ser levada a cabo.

O ciberterrorismo constitui por isso um desafio acrescido para a cibersegurança, que não tem sido vista na óptica da segurança interna.

Não existe em Portugal uma estratégia de cibersegurança, não havendo igualmente legislação adequada e eficaz.

Procedemos ao enquadramento do ciberterrorismo como uma transferência da prática terrorista para o novo campo do ciberespaço.

A criação do "*The Tallinn Manual on the International Law Applicable to Cyber Warfare* e do "*National Cyber Security Framework Manual"*, pelo *Cooperative Centre*, da Estónia, reconhecido pelo OTAN, como forma de resposta às ciberameaças, demonstra que a legislação está a progredir para o âmbito dos conflitos cibernéticos.

Relativamente ao enquadramento jurídico do combate ao terrorismo, a sua dispersão e inadequação espelha a falta de consenso internacional existente quanto às concepções de terrorismo e verifica-se a não convergência do direito internacional com o direito regional.

Quanto ao ciberterrorismo, não é contemplado na legislação nacional, da União Europeia ou internacional.

Palavras-chave: Terrorismo, ciberterrorismo, cibersegurança.

Introdução

A escolha deste tema foi um processo onde existiram mais dúvidas do que certezas. Quando decidimos pela escolha do tema, considerámos que actualmente, não perspectivamos a nossa vida em sociedade sem computadores e sem *Internet*. Hoje, os particulares, as empresas e os Estados utilizam os computadores e a *Internet* nas comunicações, nos negócios e nas infra-estruturas críticas. Estas, concebidas pela União Europeia como: "… as instalações físicas e de tecnologia da informação, redes, serviços e bens, os quais, se forem interrompidos ou destruídos, provocarão um sério impacto na saúde, na segurança ou no bem-estar económico dos cidadãos ou ainda no funcionamento efectivo dos governos dos Estados-Membros." (COM (2004) 702 final).

De uma forma ou de outra, todas as dimensões da nossa vida estão ligadas ao mundo computacional e ao ciberespaço.

A sociedade é vista e tratada como uma "rede" de "interconexões e dependências" em vez de uma "estrutura." "O Estado não exercerá seus poderes de outra forma a não ser por meio do controle da rede. E assim a impossibilidade de exercer o controle sobre a rede irá enfraquecer as instituições políticas de forma irreversível". (Zygmunt Bauman, 2009).

No entanto, apesar do mundo das tecnologias em que vivemos e das oportunidades que oferece, a violência é também parte integrante da vida humana, afectando milhões de pessoas em todo o mundo, vítimas de conflitos armados cruéis que têm como consequências essencialmente um sofrimento atroz, pobreza, injustiça, humilhação, medo, terror e deixam o rasto de uma devastação material, mas mais marcante, deixam o rasto de uma devastação psicológica que perdura no tempo.

Desde 1946 que os conflitos armados provocaram milhões de mortes, refugiados e pessoas deslocadas, não obstante os conflitos tradicionais entre Estados terem diminuído. A conflitualidade actual contrasta assim, com a cultura de paz preconizada internacionalmente, em especial ao nível das Nações Unidas.

A polemologia, cujas investigações se baseiam na paz negativa e tinha como característica fundamental o paradigma da exclusividade do uso da violência armada pelos Estados soberanos, actualmente está colocada em

causa pelo terrorismo. O Estado-nação está em declínio, porém não se verifica na mesma proporção, um decréscimo da violência organizada (Martin van Creveld, 1991).

O novo fenómeno dos actores não estatais e o crescimento de adeptos do radicalismo islâmico, cujos objectivos e forma de actuação não são claros, em acréscimo às oportunidades da globalização e do ciberespaço, ofereceram ao terrorismo dimensões confortáveis para a sua actuação.

O ataque da organização terrorista *Al-Qaeda*, em 11 de Setembro de 2001 nos Estados Unidos da América, alterou o modo de perspectivar a segurança e as relações internacionais.

Em 2003, no documento do Conselho Europeu "Estratégia Europeia em Matéria de Segurança*"* foram reconhecidos quais os maiores riscos de segurança enfrentados: o terrorismo global, os Estados fracos ou enfraquecidos, a violência religiosa dos grupos extremistas, os conflitos regionais na vizinhança da Europa e o abastecimento energético. Neste documento é referida a vulnerabilidade dos sistemas de informação, a mais recente vaga de terrorismo tem ligações ao extremismo religioso e que os conflitos podem levar "ao extremismo, ao terrorismo e ao fracasso dos Estados e oferece, além disso, oportunidades à criminalidade organizada."

Em 2004, no Relatório das Nações Unidas: "*A more secure world: our shared responsibility", Report of the High-level Panel on Threats, Challenges and Change*", é referido que todas as formas de terrorismo são proibidas, por qualquer uma das 12 convenções internacionais sobre o combate ao terrorismo, pelo Direito Internacional, pelas convenções de Genebra ou pelo Estatuto de Roma. (Francisco Proença Garcia, 2006).

Em 2005, o Conselho da União Europeia, adoptou a "Estratégia Antiterrorista da União Europeia" (14469/4/05), onde se afirma, "…requer um trabalho a nível nacional, europeu e internacional no sentido de reduzir a ameaça do terrorismo e a nossa vulnerabilidade a atentados".

Posteriormente, em 2008, no Relatório sobre a Execução da Estratégia Europeia de Segurança (S407/08)[1], é dito que: "A ameaça do terrorismo e da criminalidade organizada adquiriu uma nova dimensão que se faz sentir dentro

[1] Disponível: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/PT/reports/104638.pdf.

das nossas próprias sociedades.” e ainda”… continua a ser uma das maiores ameaças à nossa subsistência.” O mesmo texto refere que foram identificadas em 2003 várias ameaças em matéria de segurança que se mantiveram mas outras agravaram-se e tornaram-se mais complexas. Ao nível da cibersegurança é mencionado relativamente à cibercriminalidade que “…os atentados contra sistemas informáticos tanto privados como governamentais que ocorreram nos Estados-Membros, vieram conferir a este tipo de criminalidade uma nova dimensão, revelando o seu potencial como nova arma económica, política e militar”.

O mundo não está mais pacífico, embora nos últimos anos continue a ocorrer um decréscimo das despesas militares em consequência também da evolução da tecnologia. A guerra total tem vindo a ser substituída pelas guerras regionais e conflitos internos de fraca intensidade.

Com o avanço das tecnologias e o acesso fácil ao ciberespaço, o ciberterrorismo, transposição do fenómeno terrorista para o ciberespaço, possibilitado pelo uso de computadores e da *Internet*, constitui um instrumento de poder no campo dos conflitos assimétricos.

A segurança e a paz mundiais estão em risco. A ameaça da concretização de ciberataques terroristas, coloca desafios acrescidos à cibersegurança, uma vez que o seu escopo não pode ser apenas possibilitar a acessibilidade, integridade e confidencialidade dos computadores e redes de computadores, ou uma navegação segura na rede e na prevenção do cibercrime.

O ciberterrorismo pode evoluir para uma nova forma de conflito. A legislação vigente em Portugal, relativamente à cibersegurança, embora não abundante, acompanha com algum atraso a evolução do ciberespaço.

O facto de não existirem a nível internacional, definições consensuais académicas e jurídicas de terrorismo, suas tipologias, de ciberterrorismo, de guerra, de cibercrime, de cibersegurança, causa um enorme entrave à cooperação entre os Estados.

O argumento fundamental deste trabalho é verificar se:

- O ciberterrorismo é um fenómeno concretizável.

No âmbito da dissertação identificámos como questões derivadas:

- O que significa ciberterrorismo?

- A diferenciação entre terrorismo e ciberterrorismo justifica-se?

- Concretizou-se algum ciberataque terrorista ou suspeita-se da sua preparação?

- Que medidas tomar para enfrentar o fenómeno?

De modo a provarmos o nosso argumento central, apresentamos no Capítulo I, a globalização e o fracasso dos Estados como um potencializador de crescimento do terrorismo e no Capítulo II, expomos as vantagens do ciberespaço para levar a cabo potenciais actos terroristas, bem como várias noções de ciberterrorismo e exemplos de ciberataques.

Para a elaboração desta dissertação, fizemos uma revisão da literatura no âmbito dos estudos sobre o fenómeno do terrorismo, essencialmente após o 11 de Setembro de 2001, dos estudos sobre a problemática do ciberterrorismo, da cibersegurança, e procedemos a uma recolha das convenções internacionais, regionais, do direito da União Europeia e direito interno no âmbito da segurança e do terrorismo.

A nossa opção incidiu na realização de uma exposição de carácter descritivo, essencialmente com base em análise bibliográfica, artigos científicos e académicos, artigos de publicações periódicas e legislação em vigor nacional e internacional.

Procedemos ao levantamento das áreas abordadas, através da revisão de bibliografia, artigos publicados, sítios da *Internet*, seminários e conferências a que assistimos, de forma a garantir uma sustentação sólida para os objectivos que pretendemos atingir.

Os conteúdos e citações presentes neste trabalho, provenientes da língua inglesa, são traduzido nosso e quanto à legislação consultada em inglês optámos por manter essa mesma versão, sempre que possível.

Este trabalho não foi realizado conforme o novo acordo ortográfico.

Estrutura da dissertação

No Capítulo I

Pretendemos demonstrar que a inexistência de uma definição consensual académica e legal ao nível internacional de terrorismo, bem como a sua tipificação torna difícil, por exemplo, a compreensão do fenómeno do

terrorismo, faz cair o discurso sobre o terrorismo e o ciberterrorismo no campo popular, gerando mais confusão, bem como impossibilita a cooperação entre os Estados. Abordámos algumas definições de instituições relevantes nacionais e internacionais. Realizámos uma breve contextualização do terrorismo nos pós 11 de Setembro de 2001 e perspectivamos a globalização e o fracasso dos Estados como um potencializador do fenómeno do terrorismo.

No Capítulo II

Perspectivamos o ciberespaço como um novo instrumento de poder, onde a assimetria de forças não impede um actor individual de lançar um ciberataque com capacidades disruptivas e destrutivas às infra-estruturas críticas de um país. Verificamos que os próprios Estados utilizam estes actores não estatais para efectuar ciberataques, uma vez que de facto o ciberpoder dos países está nas mãos de privados.

Consideramos o espectro das ciberameaças, no qual o ciberterrorismo constitui uma ameaça séria no escalonamento de um conflito.

Verificámos que a *Internet* é um meio que aumenta o risco da concretização de um ciberataque terrorista, apesar de ter vindo a ser usada por terroristas essencialmente para delinear e dirigir ataques convencionais, divulgar a sua ideologia, manipular as populações e os meios de comunicação, recrutar e treinar novos terroristas, recolher informações sobre alvos potenciais e controlar operações. Os tipos de armas criadas para utilização no ciberespaço podem ter capacidade letal, sendo uma ameaça gravíssima à segurança interna.

No Capítulo III

Apurámos que não existe uma concepção de cibersegurança ao nível internacional, mas no entanto, parece existir acordo quanto à sua concepção, sendo referida a óptica da confidencialidade, acessibilidade e integridade, na maioria das estratégias de cibersegurança. Não obstante, as estratégias focam a consolidação dos mercados internos de cada país, não perspectivando assim a cibersegurança numa óptica de segurança interna.

As principais organizações internacionais, União Europeia, OSCE, Conselho da Europa, OTAN e ONU, não têm tido o papel pretendido a nível da

cibersegurança na prevenção contra o ciberterrorismo. Apenas no âmbito do Conselho da Europa a Convenção Cibercrime, é o diploma mais relevante, sendo por isso recomendado pela OTAN.

No Capítulo IV

Abordamos os vários acordos internacionais multilaterais, acordos regionais, legislação da União Europeia e legislação interna, ressaltando apenas algumas das suas características relevantes para a perspectiva de inexistência de definições de terrorismo, acto terrorista, de menções ao ciberterrorismo e de um combate eficaz ao terrorismo.

Verificámos a inexistência de um acordo internacional que unifique todos os acordos existentes, referente ao combate ao terrorismo e a inexistência de legislação europeia eficaz, bem como interna no combate ao terrorismo, o mesmo se passando com o fenómeno do ciberterrorismo.

No Capítulo V

Apresentamos as respostas de uma forma sintética às questões derivadas, um pequeno contributo para a resolução do problema do ciberterrorismo finalizamos este trabalho com uma breve conclusão.

Capítulo I – O terrorismo no contexto actual

"Chega mais perto e contempla as palavras.
Cada uma tem mil faces secretas sob a face neutra e te pergunta sem interesse pela resposta, pobre ou terrível, que lhe deres: trouxeste a chave?"
Carlos Drummond de Andrade

1.1 - A problemática da definição de terrorismo

Vasta literatura diz-nos que o termo "terrorismo" surgiu na Revolução Francesa (1793/94) como forma de denominar os comportamentos dos revolucionários liderados por Robespierre. Foi sempre relacionado desde o início da História, a fanatismos religiosos, às guerras santas, a assassínios de hereges, à Inquisição e surge actualmente ligado a fundamentalismos muçulmanos, cristãos, judaicos e hindus.

No entanto, o termo "terrorismo" entendido como método de combate/ acção entrou para os discursos já na década de 30 do século passado. (Alex P. Schmid, 2011).

A definição de terrorismo é controversa, como tal, não tem sido possível obter consenso quanto à sua conceptualização.

Relativamente à definição da proposta de revisão consensual académica de terrorismo (*The revised academic consensus definition of terrorism* (Rev. ACDT 2011)) e ao anteprojecto da definição legal, proveniente da Comissão Ad Hoc para o Terrorismo do Sexto Comité da Assembleia Geral das Nações Unidas, no seu artigo 2, integrada nas negociações da Convenção Compreensiva sobre Terrorismo Internacional (*Comprehensive Convention on International Terrorism*), adiada para 2013, existe uma discrepância enorme.

Na definição académica consensual revista em 2011 consta o seguinte:

> *"1. Terrorism refers, on the one hand, to a doctrine about the presumed effectiveness of a special form or tactic of fear-generating, coercive political violence and, on the other hand, to a conspiratorial practice of calculated, demonstrative, direct violent action without legal or moral restraints, targeting mainly civilians and non-combatants, performed for its propagandistic and psychological effects on various audiences and conflict parties;*

2. Terrorism as a tactic is employed in three main contexts:

(i) illegal state repression,

(ii) propagandistic agitation by non-state actors in times of peace or outside zones of conflict and

(iii) as an illicit tactic of irregular warfare employed by state- and non-state actors;

3. The physical violence or threat thereof employed by terrorist actors involves single-phase acts of lethal violence (such as bombings and armed assaults), dual- phased life-threatening incidents (like kidnapping, hijacking and other forms of hostage-taking for coercive bargaining) as well as multi-phased sequences of actions (such as in 'disappearances' involving kidnapping, secret detention, torture and murder).

4. The public (-ized) terrorist victimization initiates threat-based communication processes whereby, on the one hand, conditional demands are made to individuals, groups, governments, societies or sections thereof, and, on the other hand, the support of specific constituencies (based on ties of ethnicity, religion, political affiliation and the like) is sought by the terrorist perpetrators;

5. At the origin of terrorism stands terror – instilled fear, dread, panic or mere anxiety -spread among those identifying, or sharing similarities, with the direct victims, generated by some of the modalities of the terrorist act – its shocking brutality, lack of discrimination, dramatic or symbolic quality and disregard of the rules of warfare and the rules of punishment;

6. The main direct victims of terrorist attacks are in general not any armed forces but are usually civilians, non-combatants or other innocent and defenceless persons who bear no direct responsibility for the conflict that gave rise to acts of terrorism;

7. The direct victims are not the ultimate target (as in a classical assassination where victim and target coincide) but serve as message generators, more or less unwittingly helped by the news values of the mass media, to reach various audiences and conflict parties that identify either with the victims' plight or the terrorists' professed cause;

8. Sources of terrorist violence can be individual perpetrators, small groups, diffuse transnational networks as well as state actors or state-sponsored clandestine agents (such as death squads and hit teams);

9. While showing similarities with methods employed by organized crime as well as those found in war crimes, terrorist violence is predominantly political – usually in its motivation but nearly always in its societal repercussions;

10. The immediate intent of acts of terrorism is to terrorize, intimidate, antagonize, disorientate, destabilize, coerce, compel, demoralize or provoke a target population or conflict party in the hope of achieving from the resulting insecurity a favourable power outcome, e.g. obtaining publicity, extorting ransom money, submission to terrorist demands and/or mobilizing or immobilizing sectors of the public;

11. The motivations to engage in terrorism cover a broad range, including redress for alleged grievances, personal or vicarious revenge, collective punishment, revolution, national liberation and the promotion of diverse ideological, political, social, national or religious causes and objectives;

12: Acts of terrorism rarely stand alone but form part of a campaign of violence which alone can, due to the serial character of acts of violence and threats of more to come, create a pervasive climate of fear that enables the terrorists to manipulate the political process". (Alex P. Schmid, 2011).

No anteprojecto de definição legal do Sexto Comité Ad Hoc, da Assembleia Geral das Nações Unidas, no seu artigo 2 (Anexo II)[2], consta o seguinte:

"*Article 2*

1. Any person commits an offence within the meaning of the present Convention if that person, by any means, unlawfully and intentionally, causes:

(a) Death or serious bodily injury to any person; or

(b) Serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility or to the environment; or

(c) Damage to property, places, facilities or systems referred to in paragraph 1 (b) of the present article resulting or likely to result in major economic loss;

when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

2. Any person also commits an offence if that person makes a credible and serious threat to commit an offence as set forth in paragraph 1 of the present article.

[2] Disponível: http://www.un.org/documents/ga/docs/57/a5737.pdf.

3. Any person also commits an offence if that person attempts to commit an offence as set forth in paragraph 1 of the present article.

4. Any person also commits an offence if that person:

(a) Participates as an accomplice in an offence as set forth in paragraph 1, 2 or 3 of the present article; or

(b) Organizes or directs others to commit an offence as set forth in paragraph 1, 2 or 3 of the present article; or

(c) Contributes to the commission of one or more offences as set forth in paragraph 1, 2 or 3 of the present article by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either:

(i) Be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of an offence as set forth in paragraph 1 of the present article; or

(ii) Be made in the knowledge of the intention of the group to commit an offence as set forth in paragraph 1 of the present article".

Existem mais de duzentas e cinquenta definições académicas, governamentais e intergovernamentais de terrorismo. Uma das primeiras definições será de Robespierre e remonta a 1794 (Alex P. Schmid, 2011):

"*La terreur n'est autre chose que la justice prompte, sévère, inflexible ; elle est donc une émanation de la vertu ; elle est moins un principe particulier qu'une conséquence du principe général de la démocratie appliqué aux plus pressants besoins de la patrie*".[3]

Deste modo, a melhor forma de chegar a uma definição será desagregar as definições existentes e discutir os seus atributos individuais, as suas dimensões e encontrar o que há de comum entre elas (Alex P. Schmid, 2011).

Existem dez elementos comuns que resultam da comparação entre as definições académicas e legais existentes, e abarcam o cerne das características fundamentais de terrorismo:

- Uso demonstrativo de violência contra seres humanos;
- Ameaça de mais violência;
- Promoção deliberada do terror ou medo num grupo alvo;

[3] Disponível: http://ihrf.univ-paris1.fr/spip.php?article609.

- Direccionado a civis, não combatentes e inocentes;
- Intenção de intimidação, coerção e/ou propaganda;
- Método, táctico ou estratégico para travar um conflito;
- Importância da comunicação dos actos de violência a grandes audiências;
- Natureza ilegal, criminal e imoral dos actos violentos;
- Predominância de um carácter político do acto;
- Uso como ferramenta psicológica de conflito para mobilizar ou imobilizar sectores do público. (Alex P. Schmid, 2011).

De acordo com Schmid e Jongman, (1988) terrorismo consiste:

"[a]n anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group, or state actors, for idiosyncratic, criminal or political reasons, whereby – in contrast to assassination – the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organizations), (imperilled) victims, and main targets are used to manipulate the main target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily used."

A Organização das Nações Unidas (ONU) adaptou e adoptou a definição de Schmid e Jongman (1988) da seguinte forma:

"*Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-)clandestine individual, group, or state actors, for idiosyncratic, criminal, or political reasons, whereby - in contrast to assassination - the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat - and violence-based communication processes between terrorist (organization), (imperiled) victims, and main targets are used*

to manipulate the main target (audience(s), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought." (Alex P. Schmid, 2011)

A Organização do Tratado do Atlântico Norte (OTAN), refere que terrorismo é:

"*The unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives*."[4]

No caso do Departamento de Estado dos Estados Unidos da América (*U.S. Department of State*) o terrorismo é entendido como:

"…premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."[5]

O Departamento de Defesa dos Estados Unidos (*The United States Department of Defense*) define terrorismo como:

"*The unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political*."[6]

O *Federal Bureau of Investigation* (FBI) diferencia terrorismo doméstico de terrorismo internacional[7]:

"*Domestic terrorism is the unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction committed against persons or property to intimidate or coerce a government, the civilian*

[4] Disponível: http://www.fas.org/irp/doddir/other/nato2008.pdf.
[5] Disponível: http://www.state.gov/documents/organization/195768.pdf.
[6] Disponível: http://ra.defense.gov/documents/rtm/jp1_02.pdf.
[7] Title 18, United States Code, Part 1, Chapter 113B, section 2331 (as amended by section 802 of the USA Patriot Act).

population, or any segment thereof in furtherance of political or social objectives.

"International terrorism involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.[8]

Quanto ao Parlamento Europeu, numa Resolução do Parlamento Europeu sobre a dimensão externa da luta contra o terrorismo internacional (2006/2032 (INI)) é dito que terrorismo é:

> "Para além dos actos já referidos nas convenções em vigor, qualquer acto destinado a causar a morte e lesões corporais graves a um civil ou a um não combatente, quando o propósito do dito acto, pela sua natureza ou pelo seu contexto, seja intimidar uma população ou obrigar um governo ou uma organização internacional a realizar um acto ou abster-se de o fazer.
> (Definição proposta inicialmente pelo Grupo de Alto Nível das Nações Unidas sobre Ameaças, Desafios e Mudança, no relatório de 2 de Dezembro de 2004)."[9]

Por detrás do terrorismo está assim, o terror. O que os terroristas fazem é manipular as nossas emoções, manipular o nosso medo. Medo de uma morte repentina e violenta, tentando maximizar a ansiedade e incerteza, de forma a manipular vítimas actuais e futuras e todos aqueles que com eles se identificam. O que querem que se pense é: "Serei eu a seguir?" "Terror é um medo induzido que transforma um estado de espírito num estado caracterizado por um medo intenso de uma ameaça perigosa a nível individual e por um

[8] Disponível: http://www.fbi.gov/stats-services/publications/terrorism-2002-2005.
[9] Disponível: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:287E:0524:0535:PT:PDF.

clima de medo a nível colectivo. As soluções típicas para este estado de espírito são a fuga ou procurar esconderijo." "Terrorismo é uma actividade, um método ou táctica que produz uma consequência fisiológica e tem o objectivo de produzir terror. Cria um nível de ansiedade (incerteza, tensão e medo) que não corresponde necessariamente a um nível de ameaça actual." (Alex P. Schmid, 2011).

Acto terrorista será assim, o acto praticado, sistemática ou esporadicamente, com recurso à violência, por qualquer agente político ou não político.

Terrorismo será o método de violência, consubstanciado na prática de acções terroristas com objectivos políticos

Por fim, grupo terrorista será um grupo, com motivações políticas, que elege a acção terrorista como única estratégia ou como complemento da sua prática da violência.

Essencialmente, a não existência de uma definição consensual universal, entre outras razões, deve-se ao facto do fenómeno ter uma natureza controversa, ao carácter estigmatizante, não criminalizador e não legitimador do termo "terrorismo" e à existência de uma pluralidade de terrorismos. (Alex P. Schmid, 2011).

Vasta literatura refere o facto de existirem similaridades relativamente às noções de terrorismo, crime organizado e violência política, tornando a tarefa da conceptualização ainda mais complexa.

A definição de crime organizado, também não é consensual, no entanto …"Phil Williams adopta uma resposta interessante, na linha de Clausewitz, ao considerar o Crime Organizado como a continuação do negócio por meios criminosos; possui uma estrutura de base em rede, que aparentemente pode parecer de estrutura caótica mas, na realidade, apresenta-se com uma forma organizacional sofisticada, marcada por três características distintivas: associação com finalidade criminosa, corrupta e violenta (Williams, 2000, 185-186). (Francisco Proença Garcia, 2006).

De acordo com a Convenção das Nações Unidas contra o Crime Organizado Transnacional, de 15 de Novembro de 2000, assinada por Portugal em 12 de Dezembro de 2000 e ratificada apenas em 10 de Maio de 2004, um grupo criminoso organizado consiste:

”Article 2, (a) … *a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*;”

Podemos dizer, que tanto o terrorismo como o crime organizado, possuem organização, utilizam a mesma estratégia de financiamento e as mesmas práticas. Quanto à distinção essencial entre terrorismo e crime organizado, o terrorismo visa a alteração de situações políticas e o crime organizado visa a obtenção de ganhos económicos.

Em relação à violência política, esta possui as mesmas motivações do terrorismo: a existência de vítimas e audiência, a alteração da liderança política ou do sistema político. A diferença está no grau de alteração do sistema social pretendido. Há uma enorme variedade de formas e tipos de violência política. O terrorismo é uma subcategoria de violência política. Existe uma enorme lista de categorias, formas e manifestações de violência política. Alguns exemplos são: a greve de fome, dano de propriedade pública, justiça política, tortura, assassinatos, limpezas étnicas, golpes de estado, guerras civis, genocídio, etc. Como táctica, método e forma, o terrorismo pode ser utilizado por uma quantidade enorme de actores. (Alex P. Schmid, 2011).

As ciências sociais contribuíram muito para o estudo académico do terrorismo, mas o seu estudo ainda não atingiu o grau de “ciência dura”, porque não existe uma definição consensual de terrorismo e uma base de dados com a cronologia de incidentes terroristas, que possibilite uma análise séria (Magnus Ranstorp, 2007).

1.2 - A dificuldade na tipificação do terrorismo

A tipologia tem vindo a ser definida como uma selecção abstracta, combinada e acentuada de uma série de critérios com referências empíricas. As tipologias variam de acordo com as seguintes axiologias: relação entre o tipo e experiência real, grau de abstracção aplicada, o propósito do tipo, contexto temporal a que se aplica, o escopo espacial e a sua função. As vantagens da tipificação são entre outras, a clarividência conceptual

(importante no que toca à violência política e terrorismo), a disciplina (não somente uma ordenação da informação), a simplificação de informação complexa (incisiva e não apenas simplista) e a sua aplicação prática. Todavia, a utilidade da tipificação está dependente das necessidades de quem a usa. (Alex P. Schmid, 2011).

Existe uma grande quantidade de formas de abordar a problemática do terrorismo e as linhas conceptuais adoptadas, devido ao vasto número de contextos em que o terrorismo se desenvolve.

A amálgama de motivações e circunstâncias em que o terrorismo ocorre é relevante e vai desde os Estados que admitem a sua impunidade, aos que não têm qualquer constrangimento em que haja vítimas inocentes, e aos verdadeiros fanáticos que acreditam que os seus aparentes nobres e justificados actos justificam os meios pérfidos utilizados.

A problemática torna-se mais complexa quando o terrorismo é usado como único instrumento ou quando é usado como complemento de outros instrumentos tácticos.

As tipologias básicas do terrorismo são (Alex P. Schmid, 2011):

- Grupos milenares e religiosos;
- Grupos etno-nacionalistas;
- Grupos racistas de direita;
- Grupos revolucionários de esquerda e anarquistas;
- Esquadrões da morte justiceiros e paramilitares;
- Terroristas estatais ou patrocinados por estados;
- Organizações criminais com emprego de tácticas terroristas;
- Grupos de uma causa;
- Indivíduos psicologicamente perturbados e terroristas imitadores;
- Lobos solitários e terroristas da resistência sem líder.

Quanto às motivações para o terrorismo, estas são algumas das principais (Alex P. Schmid, 2011):

- Vingança;
- Intimidação e desorientação para alcançar a diminuição da moral do oponente;
- Exigências com chantagem política de modo a obter concessões;
- Propaganda;

- Provocação para obter reacção;
- Disrupção de fontes de abastecimento;
- Criação de mártires;
- Construção moral de uma imagem de força dos terroristas;
- Eliminação de forças oponentes;
- Extorsão de dinheiro para financiar campanhas de violência.

Relativamente às tácticas utilizadas pelos terroristas, as principais são (Alex P. Schmid, 2011):

- Distribuição de listas de mortes de pessoas a serem assassinadas;
- Punição (ex. mutilações);
- Violação em massa para humilhação dos indivíduos opositores do sexo masculino;
- Rapto com pedido de resgate ou concessões políticas;
- Tomada de reféns com ocupação para negociação coerciva;
- Desvio de aeronaves e sequestro para chantagem política;
- Assassinato de figuras políticas relevantes para aterrorizar outras;
- Incêndio ou bombardeamento de objectos icónicos para o oponente;
- Assaltos indiscriminados ou focalizados em espaços públicos;
- Colocação de engenhos explosivos;
- Sequestros com tortura e assassinato;
- Gravação de imagens para posterior transmissão televisiva;
- Tortura para intimidação;
- Ataques por bombistas suicidas;
- Massacres em larga escala;
- Envenenamento em massa;
- Uso de armas convencionais.

A investigação do terrorismo torna-se cada vez mais relevante devido ao incremento do terrorismo transnacional. Mesmo sendo sete vezes menos frequente que o terrorismo nacional, o terrorismo transnacional tem tido relevância no seu perfil. O apoio financeiro e político a grupos terroristas agora vem de um campo regional mais alargado, o que se reflecte no termo “terrorismo global”. No entanto, será mais correcto falar em “terrorismo inter-regional” ou “terrorismo além-fronteiras”, uma vez que nem a *Al-Qaeda* opera a nível mundial. (Alex P. Schmid, 2011).

"…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." (Maria Regina Marchueta, 2003).

Optaremos doravante por denominá-lo terrorismo transnacional.

A predominância da dedução na construção das tipologias é evidente. Apenas uma minoria dos autores, utilizou a indução empírica, sendo que a maioria usou fontes secundárias e retirou conclusões das suas próprias interpretações. (Alex P. Schmid, 2011).

A multiplicidade de factores implicados no desenvolvimento, nas operações e na etiologia dos grupos terroristas torna a abordagem a uma tipologia compreensiva muito difícil. Porém, se os objectivos da descoberta das relações, gerando hipóteses, desenvolvendo teorias e identificando novas áreas de investigação se mantiverem interactivas e confirmadas por dados empíricos trarão resultados na categorização de grupos terroristas e seus comportamentos fora dos seus ambientes de múltiplos partidos e conflitos. (Alex P. Schmid, 2011).

Uma vez que não existe consenso quanto à tipologização das várias formas de terrorismo, referimos apenas como exemplo, que de acordo com o Relatório TE-SAT 2012, a Europol considera a existência de sete tipos de terrorismo: religioso, etno-nacionalista, separatista, de esquerda, anarquista, de direita, de uma única causa[10].

1.3 - Perspectiva do terrorismo após o 11 de Setembro de 2001

Os acontecimentos do 11 de Setembro, marcam uma viragem na forma como se passou a perspectivar o terrorismo, o combate ao terrorismo e as relações internacionais. A agenda política alterou-se, passando o terrorismo e a segurança a ter o papel principal nas agendas políticas, com especial enfoque na cooperação entre Estados. Estados Unidos da América, União Europeia, Japão, Rússia e China, reforçaram as suas alianças. No entanto, o sistema internacional manteve-se. Os Estados Unidos da América continuam como potência hegemónica.

[10] Disponível: https://www.europol.europa.eu/sites/default/files/publications/europoltsat.pdf.

No dia 11 de Setembro de 2011, uma organização, a *Al-Qaeda*, lança um ataque nos Estados Unidos da América, cujo impacto teve uma escala global nunca vista, uma vez que foi possível por todo o planeta, assistir ao ataque em directo e em tempo real pelas televisões. A acção terrorista com o maior impacto da história, destruiu totalmente as duas torres gémeas do *World Trade Cente*r, símbolos capitalistas, e parcialmente o edifício do Pentágono em Washington, símbolo do poder militar americano. Com o desvio de quatro aviões civis por dezanove muçulmanos suicidas e usados como projécteis, esta acção causou mais de três mil mortes.

A *Al-Qaeda* (a base) surge no Afeganistão e surge a partir de outra entidade chamada *Makhatab al-Khidamat* (MAK - Escritório de Serviços), durante o domínio soviético, nos anos 80 do século XX. O MAK, liderado por Abdullah Azzam, mais tarde transforma-se num novo movimento dirigido por Abu Ebeida El-Banshiri e mais tarde Osama Bin Laden viria a tomar o seu lugar, internacionalizando este movimento. O objectivo era o de incitar, organizar e apoiar a luta dos *mujahedin* a nível mundial. Bin Laden era um milionário saudita, *wahabita* (deriva do apelido de Muhammad bin Abd al Wahhab, criador de um movimento religioso muçulmano na Arábia central em meados do século XVIII, que preconizava que um muçulmano deve fazer *Bay'ah* (“juramento de fidelidade ao seu governante” muçulmano durante sua vida, para assegurar a sua redenção depois da morte e este governante deve jurar fidelidade ao seu povo enquanto governar). Este juramento deve ser feito segundo a *shariah* (lei islâmica).

Bin Laden, economista e engenheiro, formado na Arábia Saudita, considerava-se um *mujahedin* na *jihad*. Foi armado pela *Central Intelligence Agency* (CIA) com o patrocínio da Arábia Saudita para levar a cabo a *jihad* contra a ocupação soviética do Afeganistão. Durante algum tempo, Bin Laden preferiu chamar à organização, Frente Internacional para a *Jihad* contra os Judeus e os Cruzados. Bin Laden considerava a *jihad* uma luta contra os regimes islâmicos que julgava corruptos e contra todos os “infiéis” que ocupam o Islão. Em 1991, rebela-se contra o rei Fahad, por este ter concedido aos EUA autorização para aquartelar as tropas americanas na Arábia Saudita durante a guerra contra o Iraque para libertação do Kuweit. Bin Laden considerou esta presença como “infiéis” que profanavam o berço do Profeta, o território mais

sagrado de todo o Islão. Refugiou-se no Sudão e com outros islamitas durante a década de noventa, tornou a *Al-Qaeda* o centro disseminador do terrorismo islâmico.

O objectivo geopolítico desta organização é a reunião do mundo islâmico da *Umma* ("comunidade" mundial de todos os muçulmanos) numa mesma entidade político-religiosa regida pela *sharia*. Líderes terroristas islâmicos pretendem reconquistar por exemplo, Portugal e Espanha, por na Idade Média terem sido dominadas pelo Islão. Defende a *Al-Qaeda*, que as fronteiras desenhadas pelo colonialismo europeu, terão que desaparecer e o Islão tem que se difundir para todos os países. Os muçulmanos emigrados e seus descendentes não podem integrar-se nas sociedades de acolhimento. Este objectivo não teve início na *Al-Qaeda*, mas sim nos diversos movimentos terroristas religiosos islâmicos que pretendem restabelecer o califado (abolido aquando da revolução liderada por Kemal Atatürk (1919-23)) que pretendeu tornar a Turquia num Estado secular ou colocá-lo sob a direcção de um colégio de doutores (políticos e teólogos).

Ao longo dos anos noventa a *Al-Qaeda* realizou vários atentados contra alvos americanos, colaboraram com o regime fundamentalista islâmico dos *taliban*, também treinados e equipados pela CIA, na luta contra os afegãos da Liga do Norte e instalaram campos de treino para os terroristas *mujahedin*.

Foi a primeira instituição privada clandestina que apoiou e patrocinou grupos terroristas, como o faziam alguns Estados soberanos, mas possui uma estratégia vantajosa relativamente a estes, porque não sendo um Estado, pode passar à margem da legislação internacional. Não tem território, povo, infra-estruturas importantes nem governo, por isso não tem o problema de poder sofrer retaliações por parte das vítimas. Não obstante, tem algumas capacidades dos Estados, como a obtenção de recursos, serviços de informações entre outros. Retira partido da *Internet* como estratégia, por exemplo para disseminar a sua causa, recrutar novos seguidores, movimentar fundos provenientes de financiamentos, entre outros e utiliza empresas de comunicação como forma de manipulação mediática.

Após o episódio do 11 de Setembro, as alterações que ocorreram foram essencialmente as seguintes:

- Aumento da busca e análise de informação sobre as actividades terroristas;
- Reforço na captura de suspeitos de actividades terroristas;
- Cooperação entre governos, forças de segurança e agências de informação;
- Procura e supressão das redes de financiamento do terrorismo;
- No Islão pioraram as divergências entre os chamados "fundamentalistas" religiosos apoiantes de Bin Laden, os religiosos "moderados" e os "laicos" que condenaram os ataques e similarmente têm vindo a recusar os métodos cruéis utilizados;
- Foram reduzidos os constrangimentos nas acções contra os Estados que patrocinam o terrorismo;
- Os Estados Unidos da América criaram uma aliança com a "Liga do Norte" no Afeganistão, para combater a força *taliban*, tendo instituído um governo laico eleito de forma democrática e juntamente com a OTAN têm combatido os *taliban*;
- Os Estados Unidos da América em 2003 conduziram uma ofensiva cinética contra o Iraque, um dos países patrocinadores do terrorismo transnacional, numa coligação com trinta e oito países;
- Aumento na angariação de novos militantes islâmicos;
- Repressão policial no ocidente e no Islão;
- A *Al-Qaeda* afirmou-se como modelo e adepta de muitos grupos terroristas sunitas;
- O Irão utiliza o grupo terrorista libanês *Hezbollah* e patrocina o terrorismo xiita, dando uma nova importância a este fenómeno que utiliza os desentendimentos entre cristãos e muçulmanos e subdivide-se em duas redes, uma rede constituída por grupos terroristas sunitas de inspiração *wahabita* ligada aos sunitas e outra rede, a salafista (que surgiu no Egipto no século XIX, cujo objectivo primordial do movimento era reformar a doutrina islâmica de forma a adaptá-la à actualidade, é liderada pela *Al-Qaeda* e pelo Irão através dos serviços de informações, da Guarda Revolucionária e pelo *Hezbollah*);
- Alguns Estados islâmicos, anteriormente apoiantes do terrorismo estão a balizar esses apoios (porém mantêm-nos, como a Síria por exemplo) e

outros deixaram de dar o seu apoio (como é o caso do Afeganistão e do Iraque);

- Os sunitas (cerca de 80% a 90% dos muçulmanos, consideram-se os sucessores directos do profeta Muhammad Maomé) e os xiitas (os restantes, que não concordam e preconizam que o sucessor deveria ser Ali, o genro do profeta), possuem uma rivalidade que é transposta para as relações entre os grupos terroristas, uma vez que ambos actuam sem que cooperem ou se bloqueiem;

- Há sinais de cooperação entre o *Hezbollah* e grupos sunitas da Palestina no conflito com Israel;

- Há indícios ataques terroristas de grupos xiitas contra sunitas e de sunitas contra xiitas;

- Progressiva participação em actividades terroristas de muçulmanos com nacionalidades europeias e norte americanas e de pessoas convertidas ao islamismo;

- Hoje a literatura sobre o terrorismo pode ser encontrada nas ciências sociais, militares e recentemente também na criminologia;

- Muitos dos novos especialistas adoptaram a noção de Walter Laqueur (1987):

"O terrorismo é o uso da ameaça ou uso da violência, um método de combate, ou estratégia para atingir determinados alvos com o objectivo de provocar um estado de medo na vítima, sendo impiedoso e não conforme com as regras humanitárias, e a sua publicidade é um factor essencial na estratégia terrorista"

e outros preconizam que há um "Novo Terrorismo", qualitativamente diferente do terrorismo não estatal anterior a 1995, aquando do ataque químico no metropolitano de Tóquio que terá deixado treze mortos e anterior a 2001 aquando do ataque às Torres Gémeas e Pentágono nos Estados Unidos da América;

- As pesquisas empíricas não aumentaram proporcionalmente à produção de novas publicações. Verificou-se uma eliminação do trabalho de outros, com uma agenda direccionada politicamente, comercialmente por aqueles que estavam ligados à indústria do contra-terrorismo interno e também por oportunismos pessoais. Entre 2001 e 2008, de acordo com Andrew Silke (*Contemporary terrorism studies: issues in research,*

London, Routledge, 2009), foram publicados 2281 livros sobre terrorismo. Este facto criou uma sobrecarga, fazendo com que provavelmente os melhores trabalhos sejam subestimados, deixando de ser possível distinguir entre pesquisa e produtos laterais. (Magnus Ranstorp, 2007, Alex P. Schmid, 2011, et al).

Hoje as nossas sociedades estão organizadas em rede, mas os terroristas similarmente organizam-se em rede. Num relatório executado sobre o financiamento do terrorismo, por Jean-Charles Brisard e exibido ao Presidente do Conselho de Segurança das Nações Unidas em 2002, é referido que "…durante trinta anos os países ocidentais lidaram geralmente com organizações terroristas de estrutura simples, a maior parte das vezes entidades locais desorganizadas (Europa, Médio Oriente e Ásia) ou apoiadas pelo Estado (*Hezbollah* e outras). Com este novo tipo de terrorismo a "Al-Qaeda alterou inteiramente o nosso conhecimento e avaliação das organizações terroristas ao criar a base de uma complexa confederação de militantes que agregam redes de apoio financeiro". A fim de sustentar "os seus objectivos criminosos, esta organização conseguiu construir uma complexa teia de apoios ou instrumentos políticos, religiosos, económicos e financeiros." (Adriano Moreira, 2009).

1.4 – Um potencializador: o problema da globalização e o fracasso dos Estados

A globalização embora tendo trazido factores de unificação e de cooperação, trouxe ao mesmo tempo riscos e desafios que até então eram inexistentes e que transpõem as fronteiras geopolíticas dos Estados, tornando as suas estruturas e os seus modelos de governação desadequados para operar na nova ordem mundial. O fenómeno da globalização, tanto é organizativo como desagregador nos efeitos que gera na vida das pessoas, das regiões e nações, nas relações internacionais, provocando confusão entre as causas e os efeitos.

A globalização, é um fenómeno mundial que resultou de dois acontecimentos fundamentais, o surgimento de novos meios de transporte e tecnologias e a queda do muro de Berlim, que terminou com a Guerra-Fria e o

com um mundo bipolar, em que dominavam os Estados Unidos da América e a ex-União Soviética.

Com o fim da Guerra Fria eclodiram uma vaga de conflitos tribais e étnicos, até então contidos, tendo como consequência o desmembramento de Estados como a Jugoslávia, ex-URSS e Afeganistão, passando a ser considerados “Estados falhados”. O cunho religioso destes conflitos torna mais difícil a sua resolução. Estes “Estados falhados” têm uma componente nacionalista que concorre para a fragmentação dos Estados, particularmente aqueles que possuem governos repressivos e autoritários e uma componente, a globalização, que salienta o seu declínio económico, tornando mais difícil a sua governação, não conseguindo assim, competir na economia mundial. O fim da Guerra Fria, por sua vez, trouxe o declínio do modelo de Estado moderno vestefaliano e em consequência o fim do paradigma do uso da violência como um privilégio exclusivo. A guerra entre Estados deu lugar a conflitos armados desligados dos Estados ou de quaisquer políticas governativas inerentes.

As guerras de hoje desenrolam-se mais dentro dos Estados e menos entre Estados, os confrontos assumem características irregulares e são de baixa intensidade.

O novo mundo unipolar esbateu a noção do espaço físico e a noção de soberania dos Estados, e de forma subtil alterou culturas através da divulgação em massa pelos meios de comunicação, de estereótipos sociais do chamado primeiro mundo.

Os Estados ao perderam o privilégio exclusivo do uso da força, também perderam o controlo da recolha, tratamento, gestão e difusão da informação. Estes poderes do Estado, passaram para os novos intervenientes no espaço global sem as referências as tradicionais de território, nação e população.

O fenómeno da globalização modificou a forma como se gere o espaço e o tempo. Chegar ao outro lado do planeta é cada vez mais rápido e mais fácil. Agora, a necessidade de definir e governar o espaço comum é fundamental para os Estados terem capacidade para decidir e dominar. No entanto, com a globalização vieram novos problemas para a segurança interna dos Estados, sobretudo: o terrorismo e o crime organizado transnacional (especialmente o crime económico e financeiro, o narcotráfico, o tráfico de armas, o tráfico e

exploração de seres humanos). A segurança “apresenta-se agora como um conceito global.” (Paulo Pereira de Almeida, 2009).

O sistema capitalista espalhou-se, o mundo passou a ser como um espaço único, onde se ignoram as fronteiras geográficas e onde a relação entre tempo e espaço tende a ser comprimida. Todavia, a internacionalização do processo de trabalho, as novas tecnologias e a mobilidade do capital, trouxeram, para além de oportunidades, grandes problemas. “A prosperidade crescente de uma área urbana em Singapura pode ter suas causas relacionadas, via uma complicada rede de laços económicos globais, ao empobrecimento de uma vizinhança em Pittsburgh cujos produtos locais não são competitivos nos mercados mundiais.” (Anthony Giddens, 2000).

A procura desenfreada por recursos para alimentar o capitalismo e as suas vertentes de industrialização e o desenvolvimento económico, desviou as atenções da maioria dos governos para o que é essencial na vida humana, o bem-estar. Nas agendas políticas dos governos actuais, releva o crescimento do PIB, o necessário aumento de acumulação de capital, da população e o progresso tecnológico. Porém, o crescimento económico não é a condição fundamental e bastante para que se adquira desenvolvimento, é apenas uma forma de diminuir a pobreza e uma forma exequível para atingir o bem-estar social. Desenvolvimento deve, acima de tudo, ser a existência de uma distribuição da riqueza e de todas as condições que rodeiem a qualidade de vida das sociedades. Contudo, no mundo global em que vivemos assiste-se sim a uma distribuição assimétrica de recursos, de riqueza e de justiça social.

Apesar de a “sociedade global” ter feito doutrina a nível internacional, como sinónimo de homogeneidade, em que a globalização teve neste processo o papel principal, “…levanta-se a fronteira do conhecimento, ou a fronteira tecnológica, …que se interpõe entre o mundo do Norte, dos países ricos, industrializados e detentores dos meios técnicos e humanos necessários para aceder a esse conhecimento, e o mundo do Sul, dos países pobres, endividados e, alguns, situados ainda na Idade Média da produtividade industrial”. Este desequilíbrio existente no ciberespaço gera exclusão e não dá voz a milhões de pessoas. A cibercensura afecta cerca de 80% da população mundial, uma vez que cerca de quarenta e cinco países impediram o livre acesso aos meios de comunicação social e à *Internet* estrangeira, como é o

caso da China, Cuba, Sudão e Vietname. Daí que sempre que os principais dirigentes políticos se reúnem, existem sempre manifestações contra a globalização com a exigência de um novo contrato social global. (Maria Regina Marchueta, 2002).

A fronteira do conhecimento separa dois mundos e ao mesmo tempo continuará o processo da centralização, especialização e hierarquia sob controlo das potências avançadas, gerando desigualdades entre países e regiões e em consequência os riscos de ocorrência de conflitos.

A pretexto da segurança, os Estados tentam limitar o acesso aos recursos económicos estratégicos, aliando a política à economia, para atingir os seus objectivos, violando sistematicamente os direitos fundamentais.

O papel das corporações transnacionais, das instituições intergovernamentais e das organizações não-governamentais é cada vez mais relevante em detrimento dos Estados.

A globalização pode ter efeitos perversos, como a exclusão social, a repressão da liberdade de expressão e da democracia, a eclosão de movimentos sociais de luta por uma vida digna. O grande problema reside na articulação entre o bem-estar do indivíduo e a organização ao nível global.

O desenvolvimento, o progresso tecnológico e industrial e a sua aplicação à indústria bélica continuam, a expensas da degradação ambiental.

Não sabemos por quanto tempo a humanidade suportará as desigualdades globais a que assistimos. O sentimento generalizado é o de que os cidadãos não se sentem representados pelo poder político e a classe política é sinónimo de corrupção e de burocracia.

Todos estes elementos constituem o campo fértil para o crime organizado e para o terrorismo, facultando santuários para os seus campos de treino, depósitos de armas e núcleos de comunicações, sem o problema de possíveis intromissões externas da comunidade local, escapando assim ao controlo da sociedade internacional. O seu objectivo não é assim assumir a governação destes Estados, apenas os usam para atingir os seus objectivos, não lhes interessando que se tornem estáveis, como é o caso do Afeganistão. Os grupos terroristas tendem a usurpar práticas criminosas para sua sustentação, empenhando-se nas práticas do contrabando, tráfico de seres

humanos, armas, narcóticos, como no caso da Bósnia e Kosovo, ao cultivo e fabrico de droga, como o faz por exemplo a *Al-Qaeda* no Afeganistão.

A ausência de um governo e instituições eficientes nestes Estados proporciona o recrutamento de uma fatia da população descontente que não tem meios de subsistência capazes. Normalmente a estratégia terrorista passa por realizar um pacto com as autoridades, em que são oferecidos serviços, compensações financeiras ou materiais avultadas.

Em conclusão, o terrorismo é altamente complexo e globalizado, sendo por isso tratado como um campo de estudos autónomo.

A falta de acordo ao nível internacional quanto às concepções académica e legal, impede a cooperação internacional, tornando esta questão um problema gravíssimo, uma vez que permite práticas inumanas e o sofrimento de pessoas a um nível inqualificável, tais como tortura, escravidão, genocídio, entre outras. No entanto, a existência de uma concepção legal não é uma garantia para extinguir o problema do terrorismo, mas a falta de uma concepção de terrorismo deixa assim, o campo aberto ao arbítrio dos objectivos políticos, discurso popular e impede a cooperação entre Estados. (Alex P. Schmid, 2011).

Na falta de uma definição de terrorismo universal e de uma teoria geral de terrorismo, a construção de tipologias pode ser um instrumento muito útil para podermos entender o terrorismo. Não obstante, ”Se não fosse pelas etiquetas, poderíamos confundir os terroristas e as vítimas - como aquele soldado britânico anónimo, em Kosovo, que compartilhou suas dúvidas com Chris Bird, correspondente do Guardian: "Creio que fomos mal informados sobre o Exército de Libertação do Kosovo. Eles são terroristas e nós ganhamos essa guerra para eles. Não só os sérvios, mas os albaneses étnicos também têm medo deles." (Zygmunt Bauman, 2009). Os progressos teóricos que poderão vir a existir no campo do estudo do terrorismo terão por base o progresso da tipologia que por sua vez terá a sua base no progresso da conceptualização. No entanto, muita cautela é necessária, uma vez que “O conceito de "terrorismo" fica particularmente conveniente quando alguém em algum lugar decide resistir à opressão com uma arma na mão, ainda mais se resistem aos governos que há muito tempo deixaram de resistir ao "programa

globalizante" norte-americano de livre-comércio e fronteiras abertas.” (Zygmunt Bauman, 2009).

Após os ataques de 11 de Setembro a Nova Iorque e Washington pela *Al- Qaeda*, os serviços de informações e investigadores tomaram consciência que tinham negligenciado esta organização terrorista. Os estudos do terrorismo passaram a colocá-lo campo da segurança nacional e interna.

Acresce que hoje estarmos a viver uma crise ao nível mundial, não só económica e financeira, mas que está a atravessar todas as dimensões da vida, impedindo um combate eficaz ao terrorismo. Os nossos direitos, liberdades e garantias vão sendo restringidos em nome da segurança, mas a verdade é que o mundo não está mais seguro, tendo em conta que de Janeiro a Novembro de 2011 o número de ataques terroristas passou de cerca de 400 para ultrapassar os 600, tendo no entanto voltado a diminuir (de acordo com o *Global Terrorism Database*).

Depois do 11 de Setembro de 2001, ocorreram outros ataques, como por exemplo, na estação de comboios de Atocha, em Madrid, no dia 11 de Março de 2004, tendo provocado cerca de 190 mortes e mais de 1800 feridos. No dia 7 de Julho de 2005, em Londres, aconteceu outro ataque, desta vez a um autocarro, que causou cerca de 50 mortes.

Podemos assim concluir, que as consequências dos atentados do 11 de Setembro ainda não terminaram, bem como ainda não se denotaram consequências da morte de Osama Bin Laden, pelas forças militares americanas. Poderemos ter futuramente surpresas, consubstanciadas em acontecimentos novos e possivelmente mais graves.

Os conflitos actuais não são apenas consequência da competição política e de políticas de poder. São igualmente um efeito das progressivas desigualdades na distribuição da riqueza, da injustiça social, do crescimento populacional e degradação ambiental, que por sua vez levam à insatisfação social e desencadeiam fenómenos de violência generalizada.

As discussões sobre a paz e a segurança, na presente ordem internacional, são hoje mais complexas, sendo necessária uma visão fora do tradicional pensamento de que o Estado é o único detentor do uso exclusivo da força.

A prevenção dos conflitos exige assim, políticas que reforcem o tecido social e uma melhor governabilidade das comunidades, de modo a debelar a origem dos conflitos.

Capítulo II – O terrorismo no ciberespaço: o ciberterrorismo

"Eu penso que as tecnologias são moralmente neutras até que nós as aplicamos. É só quando os usamos para o bem ou para o mal que elas se tornam boas ou más".
William Gibson

2.1 - O ciberespaço como espaço de poder: a assimetria

Hoje, nas sociedades inseridas num mundo globalizado e centradas em rede, a *Internet* e o ciberespaço são o centro de todas as interacções. O acesso ao ciberespaço através da *Internet* é nos dias de hoje, nas sociedades livres e industrializadas, um gesto comum.

Até há cerca de um século, a humanidade apenas tinha dois domínios físicos onde operava: a terra e o mar. Depois surgiu o terceiro, o espaço aéreo e em 1957 surgiu o quarto domínio, o espaço sideral e vasta literatura enumera o quinto domínio, o ciberespaço. (Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Para Walter Gary Sharp (1999), o ciberespaço é considerado como:

> *"…environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web."* (Dan Kuehl, 2003).

Já para Dorothy Denning (1999), o ciberespaço é entendido como:

> *"… the information space consisting of the sum total of all computer networks*." (Dan Kuehl, 2003).

Apenas daremos estes exemplos, uma vez que existem muitas maisdefinições, tanto de autores como de instituições civis e militares.

O domínio do ciberespaço tem, entre outras, duas características fundamentais que o distinguem dos outros: a primeira é a sua matriz física que permite o uso do espectro electromagnético como significando fluxos, e a segunda é a primazia que dá ao uso da tecnologia. A informação ao ser criada, armazenada, modificada, trocada, ou explorada, depende para tal do uso da energia electromagnética e componentes electrónicos. (Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Com o ciberespaço ao qual o ser humano pode e é estimulado a aceder, onde se concentra uma quantidade de informação imensurável, nesse mundo virtual, onde se reflectem os problemas do mundo físico, surgiram conjuntamente problemas que afectam a governação e a política.

Com a tecnologia, os conceitos de espaço e de tempo foram restringidos, a *Internet* mudou o campo de actuação para o ciberespaço e é agora neste espaço, que interagem as redes, numa confluência de todas as dimensões sociais, económicas, políticas e militares.

Os novos actores não estatais intervêm na cena internacional, dotados de recursos financeiros, humanos, tecnológicos, entre outros e aqui reside o grande perigo para as sociedades modernas. Actores não identificados e não identificáveis, sem objectivos definidos ou definíveis, podem igualmente ter acesso ao ciberespaço, passando a ter estes também um novo instrumento de poder. Estes novos actores para além de terem autonomia própria, estão a ser mobilizados por Estados, de uma forma aberta ou encoberta, para executar ciberataques.

Hoje "… um actor individual, dotado de um computador e das necessárias competências técnicas, poder "deitar abaixo" a rede eléctrica de um País como os Estados Unidos. Esta assimetria, faz com que este País, detentor de uma superioridade militar convencional à escala global, tenha que desenvolver os mecanismos necessários para evitar o que muitos autores designam por "*Pearl Harbor* digital". (Viegas Nunes, 2004).

Mesmo com as mais avançadas técnicas o mais provável é que não se consiga identificar o agente do ataque, porque a rede possibilita o anonimato. Por isso, uma significativa quantidade de Estados tem interesse em manter e tolerar organizações que possam ser implicadas em todo o tipo de actividades

ligadas ao ciberespaço. O caso do ciberataque à Estónia, cujo governo atribuiu a autoria do ataque ao governo russo, é um bom exemplo.

O ciberpoder de um país tem três dimensões:

- Coordenação entre elementos operacionais e políticas dentro das estruturas estatais;
- Coerência entre as políticas adoptadas a nível de alianças internacionais e estruturas legais;
- Cooperação de actores não estatais (sociedade civil e empresas). (Alexander Klimburg, 2011).

As primeiras duas dimensões são importantes, mas na terceira reside a real capacidade dos países, ou seja, no sector privado. Para existir uma capacidade integrada de um país ao nível da criação de um ciberpoder, é necessária a cooperação dos actores não estatais, ou seja, nas democracias modernas é um desafio atrair os seus próprios cidadãos. Os Estados têm que confiar nos seus cidadãos, mas estes também devem poder confiar no Estado. A China e a Rússia já demonstraram possuir essa capacidade. Os piratas informáticos chineses estão por detrás de um sem número de ciberataques a diversos países. A natureza destes ataques não será estatal, mas serão patrocinados pelo Estado chinês. O Exército de Libertação do Povo, constitui uma milícia com unidades destinadas à guerra da informação. Estima-se que esta milícia seja composta por 25.000 soldados recrutas que estudam em universidades estatais. (Alexander Klimburg, 2011).

Já em 1999, dois dos então Coronéis do Exército de Libertação do Povo, Qiao Liang e Wang Xiangsui publicaram o livro com o título "*Unrestricted Warfare"*, no qual preconizam que, a melhor forma de suplantar a superioridade tecnológica dos Estados Unidos da América pelos países em desenvolvimento, é com o recurso a tácticas específicas, propondo entre outras: *hacking websites*, ataques a instituições financeiras, terrorismo, uso dos *media* e guerra urbana. Nesta obra é referido ainda que não haverá regras e nada será proibido, uma vez que os países fortes é que fazem as regras nas relações com os países mais fracos e que os Estados Unidos da América não cumprem as normas das Nações Unidas, criam normas novas quando as anteriores não servem os seus interesses e que se não cumprirem as suas próprias regras o mundo inteiro não confiará nelas.

Os piratas informáticos patriotas, agentes de cibercrimes e agentes reformados dos serviços de informações russos também foram identificados como estando na origem de diversos ataques. Cerca de 40% do cibercrime global, em 2007, foi da responsabilidade destes três actores não estatais russos. (Alexander Klimburg, 2011).

As operações psicológicas e políticas (PSYOP) e a subversão de Estados, organizações e movimentos internacionais são características do ambiente estratégico da actualidade. Apesar de ocorrerem em tempo de paz, as actividades a elas ligadas estão estreitamente ligadas a acções que poderão ser disruptivas ou mesmo violentas.

Com a *Internet*, movimentos, organizações, indivíduos, têm agora à disposição um espaço de projecção dos seus interesses a nível global. O ciberespaço é uma ferramenta estratégica de comunicação global, que permite a angariação de recursos, adeptos, possibilita a divulgação de conteúdos, imagens, documentos, em tempo real.

A expansão do ciberespaço constitui uma forma de exponenciar as capacidades de controlar estrategicamente os centros de poder habituais. O desafio está em conseguir atingir o equilíbrio entre os objectivos fundamentais do Estado, a segurança e o bem-estar.

Na dimensão do ciberespaço, desenvolvimento é de alguma forma, sinónimo de sistemas cada vez mais competitivos e sofisticados, que possibilitam produzir, armazenar, proteger e difundir cada vez mais informação, que posteriormente pode ser convertida em conhecimento e este em sabedoria. (José Dinis, 2005).

Desta forma, quem controlar o ciberespaço tem maior acesso à informação e de algum modo controla-a. Quem controlar a informação tem uma capacidade ampliada para influenciar audiências, sociedades e culturas, ou seja, tem a possibilidade de controlar todas as dimensões da vida.

2.2 – O espectro das ameaças: cibercrime, *hacktivismo*, ciberespionagem, ciberterrorismo e ciberguerra

O ciberespaço é um novo espaço de actuação humana, um recurso que nos permite realizar uma série de actividades, como ter acesso à informação,

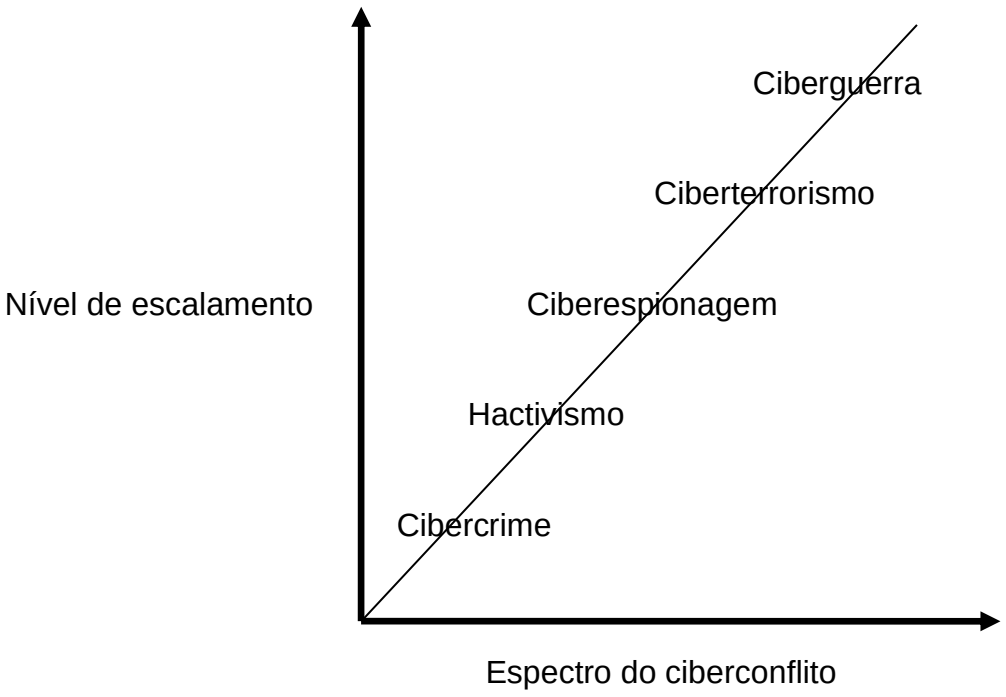
comunicar, realizar negócios, entre outras, mas é também um espaço onde existem ameaças que influenciam o seu funcionamento.

O ciberespaço é assim, um campo de confluências que nos concede oportunidades, mas é ao mesmo tempo perigoso, porque integra várias ameaças, contudo, não é um espaço de liberdade que se auto-regula.

A Major da *United States Air Force*, Bonnie N. Adkins, em 2001, num estudo para o *Air Command and Staff College, Air University*, perspectivou o espectro do ciberconflito. Este desenvolve-se por escalões, que constituem as ciberameaças, no qual surge em primeiro lugar o cibercrime, em segundo lugar o *hacktivismo*, em terceiro lugar a ciberespionagem, em quarto lugar o ciberterrorismo e por fim, em quinto lugar a ciberguerra. A mesma autora adopta a definição de ciberterrorismo de Dorothy Denning (2001), considerando-o um:

> "Ataque premeditado e politicamente motivado contra informação, sistemas de computadores, programas de computadores, e dados, que resulta na violência contra não combatentes por grupos não estatais ou agentes clandestinos".

Michael Ronczkowski (2011), baseando-se em Bonnie Adkins (2001) configurou esquematicamente o espectro das ciberameaças do seguinte modo:



Já para Dorothy Denning (1999), as ciberameaças, podem assumir as seguintes formas:

- Intervenção social: o "Ciber-activismo", "*Ciber-hacktivismo*", "Ciber-vandalismo" ou "*Ciber-graffiti*";
- Acções criminosas: *hacking*, *cracking*, "Cibercrime" ou "Ciberterrorismo";
- Actos de guerra: "Ciberguerra", Guerra de Comando e Controlo ou Guerra Electrónica.

Quanto aos agentes que preconizam estas ameaças: "O nível da ameaça pode ir dos amadores, que têm acesso à *Internet* e que simplesmente se dedicam a acções exploratórias de *hacking* mas sem grande impacto, até à condução de acções de Guerra de Informação por parte de Estados". (Viegas Nunes, 2004).

Cibercrime

Não existe igualmente uma definição consensual académica e jurídica internacional de cibercrime, mas a maioria das definições focam o uso de computadores ou redes de computadores como meio de praticar actos ilícitos como o *spamming* (muitas vezes associados a processos de intrusão), fraude, pornografia infantil e furto de informação. Os métodos utilizados podem ser os mesmos que usam os *crackers* ou os *acktivistas*, distinguindo-se pelas motivações.

O crime informático, ou cibercrime, está a tornar-se um negócio altamente organizado na *Internet*, onde os próprios agentes dos crimes publicitam programas disruptivos para venda ou aluguer. Os grupos criminosos tentam recrutar engenheiros informáticos de topo e utilizam tácticas de negócio modernas para manterem actualizados os seus produtos, com as mais recentes funcionalidades. Usam a *Internet* como meio de aumentar a sua rede de computadores controlados remotamente, aos quais se atribui a designação de *botnet* ou *zombies* (mortos-vivos), possibilitando assim ataques em enxame, com o objectivo de infectar o maior número possível de computadores, distribuir *spam* ou negar o acesso à *Internet* ou serviços pelos legítimos utilizadores.

Com a sofisticação dos códigos maliciosos existente actualmente, a expansão do crime informático constitui uma ameaça à segurança interna, uma

vez que é usado, não só por redes de crime organizado, mas igualmente por terroristas, para obtenção de apoios financeiros, branqueamento de capitais, incitamento ao cometimento de crimes, entre outros.

O tráfico de droga está relacionado com o crime informático, uma vez que os traficantes estão entre os maiores utilizadores de encriptação para comunicar, branquear capitais e dirigir operações de entrega de droga.

Quanto às características do cibercrime, podem considerar-se as seguintes como fundamentais:

- Normalmente é conduzido através de uma conexão à *Internet*;
- Pode ser levado a cabo através de dispositivo portátil de armazenamento de dados (uma *pen* por exemplo);
- Realizado anonimamente e sem que a vítima perceba;
- Transnacional;
- As redes sociais e profissionais são um instrumento para ter acesso a informação pessoal ou de empresas para cometer fraude, furto de identidade, extorsão, sabotagem, ofensas à integridade física, entre outros;
- Possibilidade de obtenção de ganhos avultados;
- Contratação de especialistas e piratas informáticos por parte de grupos criminosos e terroristas para execução dos crimes;
- Formação de alianças entre piratas informáticos e grupos criminosos ou terroristas, que rapidamente podem ser dissolvidas quando necessário;
- Os clientes dos agentes dos crimes podem ser quaisquer pessoas, incluindo terroristas;
- As redes de computadores infectadas podem ser alugadas;
- Instrumento para obter ganhos para financiamento de acções terroristas. (Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Relativamente às principais ferramentas e processos utilizados pelos agentes de crimes informáticos, podem determinar-se os seguintes:

- *Botnets*;
- Códigos maliciosos alojados em sítios da *Internet*, que são instalados nos computadores dos utilizadores quando estes acedem a sítios como o *Youtube*, por exemplo;

- Furto de identidade, que ocorre normalmente quando se compra produtos em sítios da *Internet* ou quando se acede *on-line* às contas bancárias e é feito através da instalação de um código malicioso também instalado pelo próprio utilizador, sem este saber. Estes dados normalmente são para venda;
- Ameaça interna, usada por quem tem acesso a instalações de organizações, que através de uma *pen*, por exemplo, furta dados de um computador ou rede de computadores ou danifica os meios físicos ou lógicos;
- Pirataria e produtos contrafeitos, a primeira consubstanciada no furto de propriedade intelectual, cópia ilegal de programas de computador, música, filmes e quaisquer outros elementos digitais;
- Branqueamento de capitais, perpetrada através de pagamentos electrónicos "fictícios" (através do sistema *PayPal*, por exemplo) de serviços realizados anonimamente, casinos virtuais, leilões, serviços bancários, venda de acções e títulos, cartões inteligentes que armazenam e transportam fundos. São utilizadas conjuntamente as chamadas "mulas", que são indivíduos, muitas vezes adolescentes, contratados muitas vezes para trabalhar a partir das suas casas, mas na realidade estão a participar em operações ilícitas. (Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Hacktivismo

É um fenómeno recente e consiste essencialmente num tipo de conduta *hacker* com motivações políticas ou sociais, com o objectivo de influenciar governos e públicos. Este comportamento é considerado, pelo menos, como uma desobediência civil, contra alvos específicos com capacidade de decisão e o seu meio de protesto é feito sobretudo é feito através da desconfigurarão de páginas da *WWW* ou um DDoS. Um exemplo típico é aquele em que o *hackitivista* entra sem autorização num sítio de *Internet* e desconfigura a página inicial colocando uma outra imagem. (Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz, 2009, Dorothy Denning, 2007,2011, Bonnie N. Adkins, 2001).

Ciberespionagem

A ciberespionagem é realizada com o objectivo de obtenção de ganhos económicos e políticos, contra indivíduos, empresas e governos, utilizando técnicas de furto de informação considerada sigilosa e pode ser levada a cabo por indivíduos, empresas ou mesmo Estados. Em 2007 percebeu-se que a sua dimensão era muito maior do que a que se supunha, quando por exemplo em Inglaterra, o MI5 enviou uma carta a cerca de trezentos empresários britânicos, em que acusava formalmente o Estado chinês de patrocinar espionagem à economia inglesa, incluindo sistemas de computadores, banca e serviços financeiros. O mesmo está a acontecer a outros Estados, como os Estados Unidos da América e Canadá. (Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Ciberterrorismo

A ideia da utilização do ciberespaço para a condução de ataques terroristas foi ganhando consistência ao longo do tempo.

Já em 1998 ocorreram incidentes políticos com envolvimento de *crackers* na Índia e do Paquistão, onde foram lançados ataques de vírus e ataques DDoS, na sequência das tensões entre estes países. A inovação destes ataques consistiu no facto de terem sido utilizados *botnets*.

Em 2003, um *worm* denominado "*SQL Slammer*", alastrou pela *Internet* com o propósito de sobrecarregar servidores e tornar impossível o acesso à *Internet*, através da exploração de vulnerabilidades no sistema *SQL Server 2000*, um programa de gestão de base de dados da *Microsoft*. Entre outros efeitos, deu-se a inacessibilidade do serviço de caixa automático do *Bank of America*, em Seattle, nos Estados Unidos da América, houve interrupções no serviço de atendimento de urgências e a Continental Airlines teve que cancelar vários voos devido a erros no sistema de passagens electrónicas e de *check-in.*

Outro exemplo com bastante impacto, foi o ataque à Estónia em 2007. A Estónia é um país largamente dependente da *Internet*, uma vez que praticamente todos os seus serviços são fornecidos via electrónica, tendo assim uma grande vertente *eGovernment* ou *eDemocracy*, porque inclusivamente os cidadãos têm a capacidade de votar por via electrónica, daí ser conhecido por "*eEstónia*". Em Abril de 2007, o governo da Estónia alterou o

lugar de uma estátua em Tallinn, em memória aos soldados russos falecidos na 2ª Grande Guerra Mundial, aquando da ocupação alemã. O governo russo, bem como os russos que residem na Estónia desde a ocupação soviética, fizeram várias ameaças, houve actos de vandalismo, pilhagens, feridos e uma vítima mortal. Continuamente, seguiram-se semanas de ataques DDoS e de *defacement*. Este ciberataque teve como alvos, páginas da *Internet* privadas, de partidos políticos, do governo, bancos, sistemas de fornecimento de energia eléctrica, gás, entre outros. O governo da Estónia comparou o ataque a um ataque terrorista, tendo indicado, através de uma série de indícios não validáveis, o governo russo como autor. Por sua vez, o governo russo negou a sempre a autoria dos ataques, bem como se recusou a prestar apoio na resolução do problema, sabendo-se, no entanto, que a sua origem era a Rússia.

Em 2008, na Lituânia, ocorreram ataques a mais de trezentos sítios de *Internet*, aquando da decisão do governo lituano de deixar de utilizar os símbolos soviéticos.

Igualmente em 2008, vários países descobriram um *worm* nos seus sistemas de comunicações estratégicos, que ficou conhecido como "*Confiker*". Este *botnet* infecta um computador e pode por si, disseminar-se para outros automaticamente, sem interacção humana. Foi desenhado por engenheiros de topo que já eram profissionais na altura, com o propósito, por exemplo, de paralisar sistemas de defesa e negar o acesso a sítios de *Internet* fornecedores de anti-vírus. Terá infectado cerca de dez milhões de computadores, em mais de duzentos países, que utilizavam o sistema operativo *Windows*, e provavelmente foi controlado a partir da Ucrânia.

Em 2010, o incidente que ficou conhecido como "operação Aurora", um ataque contra a *Google Corporation,* e outras empresas das áreas tecnológica, de defesa e financeira, consistiu na abertura remota de uma *backdoor* que permitiu ter acesso aos computadores através da instalação de um programa malicioso. Foi o primeiro ataque a empresas comerciais, no qual foi usada criptografia sofisticada para desenhar este *malaware* até então desconhecido.

Ainda em 2010, foi descoberto um *worm* denominado "*Stuxnet*". Sobre este iremos deter mais a nossa atenção devido às suas particularidades. Este *worm* foi colocado nas instalações nucleares iranianas de Natanz, no Irão, e

teve a capacidade de alterar a frequência das correntes eléctricas que fornecem energia às centrifugadoras, fazendo com que alterassem a velocidade e os intervalos das frequências durante meses, com o intuito de parar o enriquecimento de urânio. Aparentemente, infectou milhares de outros computadores e afectou muitos outros países, entre eles a China, India, Indonésia, Inglaterra, Estados Unidos, embora com o poder destrutivo já mais limitado. Foi desenhado por isso, para se autoreplicar e infectar computadores que não estão ligados à *Internet*. Este vírus tem características fortes técnicas, porque é um sofisticado programa de computador com a capacidade de penetrar e controlar sistemas remotos de uma forma quase autónoma. É um programa malicioso de nova geração que foi lançado no ciberespaço contra alvos determinados e com a capacidade de autodestruição caso o *worm* não detectasse o programa específico associado ao programa iraniano de enriquecimento de urânio. Foram exploradas as vulnerabilidades do sistema de palavras passe *Siemens*, que acede ao *Windows*. (James Farwell, 2011).

As centrais nucleares não estavam ligadas à *Internet* de acesso público, pelo que, foi necessário que primeiramente se estudasse a forma como funcionavam as centrifugadoras, depois se testasse o *worm* e posteriormente, alguém que o introduzisse num disco de armazenamento de dados portátil pertencente a um dos cientistas iranianos, para finalmente este introduzir o *worm* nas instalações nucleares. Todo este processo revela que houve um trabalho de *intelligenge*, que seguramente demorou anos, até conseguir obter estas capacidades. A grande inovação deste *worm*, reside no facto de ter a capacidade de atacar e reprogramar o computador alvo.

Fragmentos do código, relações entre indivíduos e correlações no ciberespaço, sugerem uma ligação entre o código usado pelo *worm* com a crescente comunidade russa de programadores que estão fora da Rússia, mas trabalham para o mercado da programação. Neste tipo de comunidade não há uma diferença clara entre os programadores que apenas executam tarefas específicas para os equipamentos SCADA da Siemens e em seguida trabalham para criar jogos de computador *on-line* pertencentes a empresas israelitas na Irlanda e Inglaterra. (Andrew Foltz, 2012).

Este acto terá sido levado a cabo pelos Estados Unidos, Alemanha, Inglaterra e Israel (James Farwell, 2011), com a colaboração do grupo

Mujahedeen-e-Khalq (MEK) (de acordo com o Global Research). O MEK era considerado uma Organização Terrorista Estrangeira (*Foreign Terrorism Organization) pelo U.S. Department of State* (Departamento de Estado Americano) desde 10 de Agosto de 1997. Na sequência deste ataque ter vindo a público, o grupo terrorista MEK, que desde 2001, aquando da sua renúncia pública ao terrorismo, exigia a sua remoção da lista dos grupos terroristas, alcançou a sua pretensão, o que foi feito em 28 de Setembro de 2012, através da Ordem Executiva 13224, do Departamento de Estado americano.

Podemos concluir assim, dadas as especificidades deste ataque, que existe agora uma preocupação acrescida para a comunidade internacional, uma vez que por detrás deste ataque estão Estados, na sua maioria, detentores de democracias consolidadas, que combatem o terrorismo, mas que utilizaram os serviços de uma organização terrorista, para lançar um ataque a outro Estado.

Não se sabe ao certo quais terão sido as consequências exactas do *Stuxnet*, no entanto, atrasou com certeza o programa de enriquecimento de urânio iraniano por alguns anos. (Andrew Foltz, 2012).

O enriquecimento de urânio pelo Irão é considerado uma ameaça, pois se o Irão possuir armamento nuclear concorrerá com as outras potências a nível bélico.

Porém, o Irão não acusou este ataque, o programa nuclear foi restabelecido num espaço de tempo considerado curto, talvez umas semanas, o que revela que as vulnerabilidades da central nuclear iraniana foram sobreavaliadas, não correspondendo assim o efeito do ataque aos níveis de recursos despendidos, uma vez que apenas atrasou durante algum tempo o programa de enriquecimento de urânio iraniano. A importância estratégica do *Stuxnet* reside no facto de denotar uma evolução da guerra computacional que está a ocorrer bem longe de Washington e que conduz esta evolução é a indústria do cibercrime (James Farwell, 2011).

Não obstante, este ataque, estabelece uma demonstração de força por parte dos agentes que o levaram a cabo, poderá constituir um caso de estudo e terá pelo menos servido de exercício de treino para eventuais ataques semelhantes.

Ciberguerra

A ciberguerra tem como objectivos essenciais:

- A invasão dos sistemas do adversário, para furto, corrupção de informação ou destruir a informação ou mesmo os respectivos sistemas ou redes de computadores;

- A negação de serviços;

- Alteração semântica da informação;

- *Defacement.* (Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Assim, é uma parte da componente militar (pode ser exclusivamente guerra de informação) de qualquer guerra que pode ser exercida, nomeadamente pela sociedade civil e é normalmente coordenada pelas entidades políticas.

A diferença entre a ciberguerra e outro tipo de ataque está na intensidade, a organização e no dano provocado ou se o mesmo for conjugado com um ataque tradicional ou uma declaração de guerra por um Estado inimigo. (Bonnie N. Adkins, 2001).

John Arquilla e David Ronfeldt (2001), entendem que a ciberguerra é utilizada para "Conduzir operações militares de acordo com determinados princípios da informação".

Dorothy Denning (2000) refere que a ciberguerra é o conjunto de "…acções com vista a obter a superioridade de informação para a estratégia nacional militar afectando a informação do adversário e dos seus sistemas ao mesmo tempo que defendemos os nossos".

Uma vez que estes autores contribuem para os estudos com vista à criação de uma nova doutrina militar americana pós-Guerra Fria, estas concepções denotam a perspectiva da ciberguerra na sua dimensão militar, ou seja, têm em consideração a capacidade de defesa dos sistemas, das redes e da informação, e a vertente defensiva e ofensiva.

A criação do *The United States Cyber Command* (USCYBERCOM) em 2009, composto por "…duzentos e quarenta mil homens e mulheres". (Marques Guedes, 2011) e do *The National Cybernetic Taskforce*, pelo Estado israelita em 2011, por exemplo, denotam já uma capacidade significativa dos Estados no âmbito da ciberguerra.

Quanto à China e Rússia, parece que criaram capacidades ofensivas, pois constantemente saem a público notícias onde são acusados de ciberataques a vários países.

No entanto, não existe uma definição internacional consensual académica ou legal de guerra. Apenas existe a definição de agressão, adoptada pela Organização das Nações Unidas pela Resolução da Assembleia Geral 3314 (XXIX), em 1974, na qual consta no seu "Artigo I:

> "Agressão é o uso da força armada por um Estado contra a soberania, a integridade territorial ou a independência política de outro Estado, ou de qualquer outra forma incompatível com a Carta das Nações Unidas, tal como estabelecido na presente definição".

O debate à volta das novas guerras e velhas guerras nos estudos de segurança tem a sua equivalência nos estudos do terrorismo. Parece haver uma convergência de conceptualização entre guerra e terrorismo. (Alex P. Schmid, 2011).

Podemos classificar a guerra como regular, integrando o uso dos três níveis: estratégico, táctico e operacional, e irregular ou assimétrico, onde entram os actores não estatais, sem que haja um campo de batalha no mar, terra ou ar e sem objectivos claros. As empresas militares privadas, utilizadas como um novo instrumento, constituem uma nova forma de intervenção nos conflitos retirando ao Estado o privilégio exclusivo de uso da força. A guerra foi desmilitarizada, porque hoje os alvos também são civis e não só militares, a violência é extrema e o terror é usado por não-combatentes em todas as dimensões sociais. A guerra de hoje é mais frequente, estratégica, urbana e subversiva. Agora as operações militares são desenvolvidas em terra, mar, ar, espaço e nos novos ambientes electromagnéticos, tendo passado para o ciberespaço, com a evolução das tecnologias de informação.

As tecnologias de informação e a informação são agora usadas também como uma arma. Neste contexto, a preocupação-chave é a obtenção da superioridade de informação em cada confronto ou conflito.

A inclusão das tecnologias de informação e comunicação nos conflitos fez surgir primeiramente o termo "guerra electrónica", posteriormente de

“guerra de comando e controle da informação e operações de segurança”, depois o de “operações de segurança de rede e operações psicológicas”, que evoluíram depois para o conceito de “operações de informação” que agora integra todos os conceitos anteriores. (Viegas Nunes, 2005, António Jesus Bispo, 2004).

Podemos concluir que a *Internet* é, simultaneamente, a porta para o ciberespaço e desenvolvimento a ela associados, e é o terreno de planeamento, preparação logística de actividades das forças militares e um teatro de operações.

2.3 – O ciberterrorismo no espectro da conflitualidade

O conceito de ciberterrorismo foi utilizado pela primeira vez na década de 80, por Barry Collin, investigador no “*Institute for Security and Intelligence*”, para se referir à junção dos termos ciberespaço e terrorismo.

Mais recentemente, foram criados conceitos controversos que emergiram principalmente de organizações de pesquisa e da indústria da consultadoria e segurança. É o caso dos termos “ecoterrorismo”, “narcoterrorismo”, “agroterrorismo”, “terrorismo biológico”, “químico e nuclear”, “ciberterrorismo”, “terrorismo suicida”, entre outros termos utilizados. O termo “ciberterrorismo” é usado de forma exagerada e abusiva para descrever uma variedade de situações que envolvem computadores e *Internet*. Porém, até hoje ainda não se viu um incidente onde deliberadamente, civis fossem assassinados através de ciberataques e onde o propósito fosse influenciar (impressionar, intimidar e coagir) uma terceira parte. (Alex P. Schmid, 2011).

Os ataques mais severos DDoS, geralmente são levados a cabo por *crackers*, por exemplo para extorquir dinheiro das vítimas, ou colocar os competidores fora do mercado. Os ataques de *hackers* são perpetrados para apenas satisfazer o ego e a curiosidade dos mesmos. Ambos são categorias de piratas informáticos. Ataques com objectivos políticos ou sociais, não têm sido intimidatórios e serão mais actos de protesto e não de terrorismo. Logo, estes actos poderão ser considerados *hacktivismo* e não terrorismo. (Dorothy Denning, 2005).

Com a progressiva utilização da *Internet*, passaram a existir diferentes ameaças e ataques maliciosos dirigidos contra os sistemas integrados em rede e ao mesmo tempo houve uma ampliação do número de alvos. Presentemente há a possibilidade de um ciberataque poder ser planeado e executado apenas por uma pessoa e a partir de um computador, utilizando uma rede não segura ou pouco segura, portanto de fácil acesso, de terceiros, tendo como alvo a propriedade digital ou a disrupção das infra-estruturas críticas de um país desenvolvido.

Para Mark Pollitt (1997), analista forense do FBI, ciberterrorismo:

> *"…is the premeditated, politically motivated attack against information, computersystems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents."*

O *National Infrastructure Protection Center* (NIPC), a instituição que tem a cargo a implementação de instrumentos de protecção das infra-estruturas governamentais dos EUA, definiu em 2003 "ciberterrorismo" como:

> "…um acto criminoso perpetrado através de computadores que resulta em violência, morte/ou destruição e que gera o terror com o objectivo de coagir um governo a alterar as suas políticas." (Viegas Nunes, 2004).

O ciberterrorismo definido por Dorothy Denning (2000)[11], surge como:

> "*Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks*

[11] Disponível: http://www.fas.org/irp/congress/2000_hr/00-05-23denning.htm.

against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."

A mesma autora, em 2007, afirmou que as ciberameaças terroristas não eram maiores que em 2001. Contudo, já em 2011, explicou que o ciberconflito actual tem origem sobretudo nas redes socias, é levado a cabo por actores não estatais que lançam os ciberataques por razões políticas e sociais e acrescenta que com a motivação dos actores e as vulnerabilidades dos sistemas, o ciberterrorismo pode passar de uma ameaça teórica a algo real.

Em 2012, esta autora relata que, em 2010, no fórum *jihadista al-Shamukh*, apelava-se a ataques contra sistemas SCADA, com o argumento de que poderiam ser utilizados para causar uma explosão massiva numa central eléctrica ou nuclear. Acrescenta ainda, que o *Stuxnet* trouxe uma visão dos danos que pode causar, o que nos pode aproximar mais do ciberterrorismo, mas não considera a ameaça eminente. Em conclusão, refere que apesar dos terroristas terem expressado algum interesse em ataques semelhantes ao *Stuxnet,* aparentemente, não terão capacidade nem meios para conduzir ciberataques devastadores. Pelo menos a curto prazo, o *Stuxnet* teve pouco impacto no âmbito do ciberterrorismo, contudo tem de continuar-se a prestar atenção à ameaça.

Barry C. Collin (1996), apontou a meio da década de 90, uma série de hipóteses que os terroristas podiam explorar através do ciberespaço, que iam desde o ataque a fábricas de cereais com o objectivo de atingir crianças, ataques à banca de um país até atingir o colapso, ataques ao tráfego aéreo e ferroviário com o objectivo de aviões e comboios chocarem, provocando centenas de mortes ou ataque a uma conduta de gás para alterar a pressão até causar uma explosão.

Todavia, Mark Pollit (1997), quase na mesma altura, considerava que estes ataques não seriam exequíveis uma vez que existem meios e processos de controlo suficientes para que não ocorram ciberataques a este nível.

Similarmente, em tempo mais recente, Jerry Brito e Tate Watkins (2011)[12], consideram que existe um discurso alarmista proveniente de Washington, que prevê cenários catastróficos, para justificar as actuais políticas americanas relativas à cibersegurança, no que diz respeito aos gastos e à legislação. Defendem inclusivamente que o público deve ter acesso a provas, mesmo que confidenciais, de que realmente existem ciberameaças, antes de serem promulgadas quaisquer leis.

Actualmente, não nos parece possível concordar completamente com Mark Pollit, Jerry Brito e Tate Watkins, depois dos ataques que ocorreram contra a Estónia ou contra as centrais nucleares iranianas em Natanz com o *worm Stuxnet*.

Em 1999, o *Center on Terrorism and Irregular Warfare* da *Naval Postgraduate School*, definiu três níveis de capacidade ciberterrorista:

- Simples/Não estruturado: *hacking* contra sistemas individuais, com recurso a ferramentas desenvolvidas por terceiros, com fraco nível de análise de alvos, comando e controlo e capacidade de aprendizagem;
- Avançado/Estruturado: ataques mais sofisticados contra múltiplos sistemas ou redes e modificação ou criação de ferramentas básicas de *hacking*, com uma análise de alvos elementar, comando e controlo e capacidade de aprendizagem;
- Complexo/Coordenado: ataques coordenados, com a capacidade de provocar uma disrupção massiva contra defesas integradas e heterogéneas, incluindo a criptografia, com capacidade para criar ferramentas sofisticadas de *hacking*, já com uma eficiente análise de alvos, comando e controlo e capacidade de aprendizagem.

Viegas Nunes (2004), entende que o tempo necessário para que um grupo ou organização leve a cabo um ataque que atinja o nível avançado/estruturado, é de dois a quatro anos e para atingir o nível complexo/coordenado de seis a dez anos.

Quanto às armas que podem ser utilizadas para fins terroristas, estes são os tipos:

[12] Disponível: http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy.

- Convencionais, que possuem capacidade de destruição física de equipamentos. São utilizadas para atacar fundamentalmente estruturas físicas dos suportes da informação impossibilitando o uso de certos serviços. Com este objectivo são usadas:

  - Munições de Radiofrequência (RF), que podem ser impulsionadas por sinais de rádio, podem ser adaptadas a granadas de mão, de morteiro ou de artilharia;

  - Bombas de impulso electromagnético, que geram impulsos electromagnéticos que operam como uma onda de choque e provocam danos no alvo, idênticas às consequências de descargas eléctricas dos relâmpagos;

  - Dispositivos Electromagnéticos Transitórios – TED's ("*Transient Electromagnetic Device*") para realizarem o controlo *TEMPEST* (*Transient ElectroMagnetic Pulse Emanation Standard*), actividades de supervisão e defesa dos conteúdos dos computadores a ataques externos, mesmo que um computador não esteja ligado a uma rede[13]. As vantagens deste tipo de armas relativamente às armas convencionais são o baixo custo, a sua resistência temporal, podem atacar alvos únicos ou múltiplos e não são letais, se ajustadas em conformidade.

- Lógicas[14], com o objectivo de atacar a lógica operacional dos sistemas de informação, inserindo atrasos ou comportamentos indesejados no seu funcionamento, através das seguintes técnicas:

  - Envio de vírus informáticos, introduzidos num computador com a finalidade de destruir programas;

  - Bombas Lógicas, instaladas nos sistemas operativos dos computadores, mantêm-se em hibernação até receberem uma ordem específica para serem activados, desencadeando a destruição dos sistemas hospedeiros;

[13] Em 1985, Van Eck mostrou que existiam semelhanças entre os PC e as emissões de radio e TV, utilizando uma antena direccional e um bom amplificador de sinal conseguia vigiar as emissões.

[14] As bombas lógicas, possuem capacidade de destruição massiva, tendo já sido usadas pela CIA em 1982, para destruir um gasoduto soviético. Uma bomba lógica foi programada para redefinir as velocidades que bombeavam o gasoduto e as configurações das válvulas de modo a produzir pressões muito acima das suportáveis pelas juntas e soldaduras. O resultado foi a maior explosão não nuclear e um incêndio observados do espaço, com dimensões nunca vistas. (Alexander Klimburg, 2011).

- *Back Doors* e T*rap Doors*, são mecanismos construídos dentro de um sistema, de modo a aceder à sua informação num momento posterior à sua instalação;
- *Worms*, vírus que se propagam de forma independente, destruindo os sistemas operativos;
- Cavalos de Tróia, que facultam a entrada de intrusos sem que o utilizador perceba. Apesar de supostamente inofensivos quando são activados têm um alto poder destrutivo;
- *Virtual Sit-Ins* e *Blockades*, que possibilitam o bloqueio do acesso ao equipamento;
- *E-mail Bombs*, que sobrecarregam as caixas de entrada de e-mail com mensagens não solicitadas;
- DDoD's, entre outros mecanismos que permitem desligar e destruir sistemas de transmissão de dados e *hardware*.

- Comportamentais, com a finalidade de destruir a confiança dos utilizadores nos sistemas de informação e na rede que os sustém, e manipular a interpretação da informação que neles circula (PSYOP), também muito usadas pelo terrorismo convencional. (John Arquilla, David Ronfeldt, 2001).

Todas estas possibilidades, a concretizarem-se, teriam como consequências no caso de uma disrupção em cascata, o terror e a insegurança da população, a paralisação do Estado, perdas económicas elevadíssimas, directas e indirectas na recuperação, constituindo por isso uma ameaça séria à segurança interna.

Em 1997, Andrew Rathmell, defendeu que a convergência das tendências tecnológicas e sócio-políticas, sugeria que o ciberterrorismo poderia ser a onda do futuro. Acrescentou que se a guerra vai ser conduzida no ciberespaço e se os combatentes do futuro vão ser irregulares, logo, o ciberterrorismo seria o paradigma lógico do conflito futuro. Referiu ainda que grupos de oposição violenta iriam continuar a perseguir os seus tradicionais alvos políticos, membros das forças de segurança, civis inocentes e infra-estruturas físicas e económicas do Estado e que com a crescente importância da infra-estrutura de informação, significa que se tornariam um novo alvo.

2.4 - O uso da *Internet* para prática terrorista

A *Internet*, a rede mundial de comunicações ou a "rede das redes", usada inicialmente para fins militares, começou a sua viagem de crescimento em 1969, aquando da criação do projecto *Advanced Research Projects Agency Network* (ARPANET), que ligou os computadores de quatro universidades americanas.

Este projecto foi desenvolvido pela *Advanced Research Projects Agency* (ARPA), cujo objectivo era a inter-ligação das bases militares e departamentos de pesquisa americanos, de um modo fiável em caso de ataques nucleares ou de precisão (Armando Marques Guedes, 2007).

Contudo, a Internet, teve um crescimento de tal modo elevado, que de acordo com o *Cisco Visual Networking Index 2011*[15], está previsto que em 2015:

- O tráfego anual de IP's terá a capacidade de perto de um *zettabyte* (966 *exabytes*, que equivale um trilião de Bytes);
- Circulará a cada cinco minutos pelos IP's globais um *gygabite* (equivalente a todos os filmes feitos até hoje);
- O número de aparelhos ligados a redes IP será o dobro da população mundial (7 biliões de pessoas).

Este tráfego servirá para todo o tipo de actividades desde comunicar, colaborar, discutir, consumir e combater.

Vasta literatura refere que a *Internet* tem, sete características fundamentais que fazem dela um instrumento privilegiado:

- Meio de comunicação rápido (em tempo real);
- Fácil acesso;
- Baixo custo;
- Permite a disseminação de informação complexa;
- Comunicação anónima graças à moderna encriptação;
- Pode ser utilizada a partir de redes públicas.

[15] Disponível: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.

Estes atributos permitem que a *Internet* seja um bem estratégico valioso para ser usado com fins terroristas. Passou por isso, a ser uma ferramenta poderosa à disposição de terroristas, como meio complementar do terrorismo convencional, para actividades como comando e controlo de operações terroristas, para comunicarem entre si, interceptar comunicações, disseminar mensagens de ódio e violência, propaganda[16], partilhar informação, divulgar causas, recrutar, obter informação, entre muitas outras funcionalidades. Para este facto contribui por exemplo, a perda de espaços físicos, como o Afeganistão, o conhecido santuário de inúmeros terroristas, tendo aqueles sido substituídos por uma parte do espaço cibernético. A *Internet* é assim usada por grupos terroristas para operações de influência, através do controlo da sua imagem junto de audiências alvo e nos meios de comunicação social, para manter um nível de apoio e tolerância na sua comunidade. A maioria dos sítios de *Internet* de grupos terroristas foca a sua história, os seus líderes, os fundadores, objectivos políticos, religiosos, sociais ou ideológicos, as suas justificações para atingir esses objectivos e deixam de lado o uso de meios violentos. Utilizam ainda grupos de conversação com um fim agregador, de unidade e colectividade, entre os seus membros. As campanhas de propaganda permitem moverem-se livremente nas suas comunidades.

O uso da *Internet* tornou-se tão importante, ao ponto da *Al-Qaeda* e Irão terem como objectivo a criação de navegadores próprios de *Internet*, como o *Google* ou o *Firefox*, com o objectivo de bloquear as ideias ocidentais, obviamente, sem que os utilizadores sequer se apercebam.

Ainda relativamente à *Al-Qaeda*, consta no livro "*The 39 Principles of Jihad*" um apelo directo para os especialistas em computadores usarem as suas capacidades e experiência para destruir sítios de *Internet* americanos, judeus, seculares e moralmente corruptos. Em 2003 também, um afiliado da *Al-Qaeda* anunciou a abertura na *Internet* de uma universidade para as ciências da *Jihad*. O anúncio foi disseminado pelo Centro de Informação Islâmico, que já anteriormente tinha divulgado mensagens de Bin Laden e denotou que já havia especialistas em *jihad* electrónica. (Dorothy Denning, 2007).

[16] Através de blogs, redes sociais, correio electrónico, sítios na Internet, fóruns, entre outros.

O *Hamas* (Movimento da Resistência Islâmica da Palestina, fundado em 1987 é um grupo terrorista cujo objectivo é a luta contra a existência do Estado de Israel) e o *Hezbollah* (“Partido de *Allah*”, fundado em 1982 no Líbano, como resposta à invasão deste país por Israel) usam os seus sítios da *Internet* para chegar às crianças através de caricaturas, banda desenhada, jogos de computador, entre outros. Estes métodos são uma parte das operações psicológicas (PSYOP) utilizadas para ensinar à juventude palestiniana, os princípios e o ódio aos judeus e aos ocidentais. (Dorothy Denning, 2005).

A *Internet* tem sido um meio de conflito entre actores não estatais, mas igualmente entre países, tais como Israel e a Palestina, Tailândia e a China, Paquistão e a Índia, EUA e China.

Há ainda a destacar o papel das mulheres, embora não seja claro como são influenciadas ou influenciam as estruturas terroristas. No entanto, sabe-se que nos movimentos de extrema-direita e *jihadistas*, a *Internet* é utilizada pelas mulheres de uma forma bem activa, no recrutamento, propaganda, disseminação e para comunicarem entre si. Um exemplo carismático é o do *Canadian Heritage Alliance*, um grupo que advoga a supremacia branca, liderado por Melissa Guille e cujo sítio na *Internet* é gerido por esta na sua casa em Londres. (Magnus Ranstorp, 2007).

Apesar dos terroristas possuírem esta ferramenta valiosa, a *Internet*, até hoje ainda não ocorreu nenhum ciberataque que possa considerar-se terrorista. (Alex P. Schmid, 2011). Ao que parece usam a *Internet* fundamentalmente para planear e conduzir ataques convencionais, disseminar a sua ideologia, manipular as populações e os meios de comunicação, recrutar e treinar novos terroristas, recolher informações sobre alvos potenciais e controlar operações.

Contudo, tendo em consideração as armas existentes que podem ser utilizadas pelos terroristas, as convencionais, as lógicas e as comportamentais, os recursos monetários e humanos que detêm, e o acesso facilitado ao ciberespaço, podemos concluir que o seu objectivo não é o lançamento de ataques em larga escala, porque caso o fosse, com toda a probabilidade já teriam executado esses mesmos ataques. Tal, no entanto, não nos permite concluir que não o farão.

2.5 - O ciberterrorismo como uma ameaça à segurança interna

Vivemos na “era da informação”, e para que o desenvolvimento e bem-estar sociais sejam garantidos, têm que ser asseguradas a segurança e a protecção das infra-estruturas críticas e de informação dos Estados. Estas infra-estruturas críticas englobam entre outros, as telecomunicações, a distribuição de energia eléctrica, gás e água, sistemas de transportes, banca e serviços financeiros e serviços de emergência.

Do ponto de vista estratégico, o lançamento de um ciberataque ou ataque de informação, tem para alguns autores correspondência a um bombardeamento, no contexto actual de informação, caso as suas consequências sejam a morte de civis, o objectivo seja político e provoque terror na comunidade. Neste enquadramento, as armas da guerra de informação poderão ser consideradas como de “disrupção massiva” (Martin Libicki, 1996), apresentando a sua utilização, segundo Viegas Nunes (2004), um enquadramento estratégico semelhante ao das armas de destruição massiva.

As infra-estruturas de informação e o ciberespaço são actualmente imprescindíveis à vida da chamada “sociedade de informação”, sendo o seu correcto funcionamento de um interesse vital para a livre circulação da informação e para todos os processos e serviços que dependem do fluxo dessa informação. Não sendo a Infra-estrutura de Informação Nacional (IIN) inteiramente segura, pode ser alvo de ataques que buscam explorar as vulnerabilidades e insuficiências existentes, o que impõe que seja garantida a sua protecção e defesa, obrigando assim a uma revisão dos actuais conceitos de Segurança e Defesa. (Viegas Nunes, 2004).

A “era industrial” deu lugar à “era da informação” e hoje, nas relações de poder, os recursos e os alvos a atingir são as informações. (Alvin Toffler, 1980). Os ciberataques à informação têm uma grande vantagem estratégica em relação aos ataques cinéticos, que é o facto de, com menos custos, criarem um impacto menor na opinião pública, mas também podem ser utilizados para produzir as condições necessárias para um ataque militar convencional.

Começa a criar-se na comunidade internacional a percepção de que esta espécie de ameaças torna necessária a adopção de contra-medidas e a criação de uma estratégia de cibersegurança preventiva e reactiva.

Podemos dizer que os ciberataques com motivações políticas aumentaram, tornando a possibilidade da existência de ciberataques terroristas numa nova linha de acção do terrorismo pós-moderno, em que os actores antagónicos possuem forças assimétricas.

A supremacia militar no campo de batalha não garante a segurança, porque no caso dos terroristas a sua capacidade de inovação é enorme no que toca a tácticas assimétricas. No caso da hegemonia militar dos Estados Unidos da América, quanto mais os terroristas se sentirem dominados e ressentidos, mais incentivados estarão a criar respostas não convencionais.

No domínio físico, a informação é o objecto sobre o qual incidem as actividades, económicas, culturais, sociais, políticas, militares, criminosas, terroristas, entre outras.

A informação, envolvida no contexto, é transformada em conhecimento e depois, quando toma a compreensão situacional, em sabedoria. É hoje um activo organizacional que integra o capital intelectual. A informação, é a nova arma que torna as organizações competitivas, tornando-se especialmente relevante em contexto de conflito. As novas tecnologias de informação e comunicação (NTIC) e as sociedades centradas em rede possuem maiores capacidades para competir pela posse de cada vez mais informação. No entanto, esta competitividade pode facilmente cair em comportamentos ilícitos, em face dos meios ou processos que utiliza. (José Dinis, 2005).

Se se compreender a guerra como um produto da sua era, verificamos que poderia surgir um conceito de guerra decorrente da “Era da Informação”. Esta opinião foi exposta por Alvin Toffler (1980), que preconiza que as guerras ocorridas ao longo das várias épocas históricas caracterizam-se pelas descobertas tecnológicas revolucionárias que causam “vagas” de mudanças sócio-económicas. A primeira vaga, a “Agrária”, caracterizou-se pelo cultivo da terra e pela domesticação de animais e em consequência as guerras ocorridas nesse período, tinham a sua causa na terra, vista como forma de obter riqueza (período de 1861 a 1865, em que ocorreu a guerra civil americana). A segunda vaga, a “Industrial”, foi caracterizada pela mecanização, produção em larga

escala e pela divisão do trabalho, pelo que a guerra seria personificada pelas armas de destruição massiva, as nucleares, químicas e biológicas (período de 1914 a 1991, em que ocorreram a I e II Guerras Mundiais, a guerra do Vietnam, a guerra do Golfo, guerra do Panamá, guerra do Kosovo e guerra do Iraque). Por último, a terceira vaga, a da "Informação", caracteriza-se pela digitalização e utilização dos computadores e tecnologias de informação. Neste novo tipo de guerra, o objectivo é levar à rendição do adversário, ou restringir a sua acção, afectando componentes sensíveis das suas infra-estruturas de informação (período de 1989 a 2003, havendo sobreposição com a "era industrial" em que ocorreram a guerra do Kosovo e guerra do Iraque). (José Dinis, 2005).

De facto, a *Internet* tem vindo, a ser uma espécie de campo de batalha digital. *Hackers*, *crakers*, grupos criminosos[17], e Estados, "combatem" entre si, nesse espaço.

Diferentes serviços e infra-estruturas, essenciais para o regular funcionamento de qualquer país, onde se incluem empresas, os particulares e as instituições governamentais, possuem uma grande dependência da Infra-estrutura de Informação Nacional (IIN). Todas estas infra-estruturas críticas detêm dependências horizontais e/ou verticais, formando assim, cadeias de infra-estruturas vitais. Um ataque a esta cadeia de inter-dependências pode gerar um "efeito de dominó", com consequências imprevisíveis. Só com uma percepção global das interdependências de uma infra-estrutura será possível discernir quais as necessárias medidas a tomar para prevenir este efeito. (Viegas Nunes, 2004).

Paralelamente, o ritmo acelerado da evolução das tecnologias de informação e comunicação (TIC) faz com que as empresas fornecedoras dos programas informáticos e equipamentos, abreviem a sua comercialização, muitas vezes sem os testarem devidamente. Este facto traduz-se na existência de novas vulnerabilidades estruturais e funcionais nas redes e nos sistemas de informação que agregam as Infra-estruturas Críticas Nacionais. Os efeitos decorrentes dos cortes de energia eléctrica que ocorreram em 2003 nos EUA, Canadá e Reino Unido, que permitiram o acesso às infra-estruturas críticas

[17] Associados a Estados, sem que a estes possa ser atribuído um envolvimento directo.

destes países, devido ao efeito do *worm Blaster*, originaram uma nova tomada de consciência. (Viegas Nunes, 2004).

Todas as nossas infra-estruturas críticas nacionais têm uma dependência estrutural relativamente à Rede Eléctrica Nacional (REN) e uma dependência funcional relativamente à Infra-estrutura de Informação Nacional.

Os resultados possíveis de um ataque à Infra-estrutura de Informação Nacional poderão ser os seguintes:

- Perda de tempo para resolver o problema;
- Diminuição da produtividade das organizações;
- Prejuízos financeiros avultados resultantes da perda de credibilidade ou de oportunidade de mercado das empresas afectadas;
- Falência de empresas;
- Instabilidade e caos social;
- Paralisia do sistema de transportes;
- Limitações à acção das Forças Armadas e forças de segurança;
- Descredibilização do Governo e da Administração do Estado;
- Perda de vidas humanas. (Viegas Nunes, 2004).

Em suma, as sociedades actuais estão organizadas em rede num mundo globalizado, onde a *Internet* e o ciberespaço são as dimensões onde se interage. A globalização e as tecnologias de informação, tornaram países e regiões, interdependentes.

O surgimento do quinto domínio, o ciberespaço, tornou possível a utilização do espectro electromagnético e o uso exponencial da tecnologia, tornando mais fácil a criação, armazenamento, modificação, troca e exploração da informação. Com a tecnologia os conceitos de espaço e de tempo foram restringidos, a *Internet* mudou o campo de actuação para o ciberespaço e é agora neste espaço, que interagem as redes, numa confluência de todas as dimensões sociais, económicas, políticas e militares.

A assimetria de forças existente entre um actor individual provido de um computador e um Estado com capacidades militares convencionais, constitui uma ameaça, uma vez que é possível ao primeiro lançar um ciberataque com capacidades disruptivas e até destrutivas às infra-estruturas críticas de um país.

Os novos actores não estatais, onde se incluem os ciberterroristas, podem agora ter um papel projectado ao nível internacional, passando a ter estes igualmente um novo instrumento de poder, o que traz problemas ao nível da governação e da política. Os próprios Estados utilizam estes actores não estatais para efectuar ciberataques, problema acrescido pelo facto de o ciberpoder dos países, estar em grande parte, no sector privado. É por isso essencial a cooperação destes actores não estatais, sobretudo em questões de defesa.

De alguma forma, as manifestações terroristas modificaram-se com o surgimento das novas tecnologias. As operações psicológicas e políticas e a subversão de Estados, organizações e movimentos internacionais são particularidades do contexto estratégico dos dias de hoje, ou seja, o ambiente das sociedades actuais é de "violência dissimulada".

Agora com o ciberespaço, os centros de poder habituais já não estão apenas ao alcance dos Estados, sendo agora os privados a controlar a informação, logo têm a capacidade acrescida de controlar todas as dimensões da vida.

Tendo em consideração o espectro dos conflitos e o grau de violência e interacção envolvidos, o ciberterrorismo constitui o penúltimo escalão anterior ao da ciberguerra, embora seja consensual a ideia de que não podemos considerar a ocorrência de qualquer ciberataque terrorista até aos dias de hoje, porque nenhum dos ciberataques ocorridos produziu sentimento de terror, foi orientado por motivações políticas e sociais, nem provocou danos significativos.

Todavia, é indiscutível que a *Internet* veio exponenciar a possibilidade da concretização de um ciberataque terrorista, alargou o número de alvos possíveis, revolucionou o modo como os governos e actores não estatais orientam as suas operações, havendo agora a possibilidade de agirem transnacionalmente num mundo virtual a coberto do anonimato, de uma forma fácil e a custos diminutos.

O uso da *Internet* não tem sido regulado pela maioria dos Estados, o que leva a que os utilizadores mal intencionados sintam uma liberdade a coberto do anonimato, havendo muitos autores que se referem a ela como "*Wild Wild West*".

Os tipos de armas que podem ser utilizadas com fins terroristas são as convencionais, as lógicas e as comportamentais e podem possuir capacidade letal.

Os terroristas agora organizam-se de uma forma horizontal e não vertical (hierarquicamente), porque a *Internet* permite a descentralização da liderança, o que torna difícil as operações de contra-terrorismo. Já não é possível atacar o centro gravitacional, removê-lo e vigiar o grupo até o mesmo se desintegrar. Ao remover uma célula não se pode prever onde vai nascer a seguinte e quem será o seu líder.

Acresce que os terroristas aprendem rápido com os erros, adaptam-se facilmente e disseminam, sem dificuldade, as práticas para combater as tácticas dos serviços de informações e de segurança. Todavia, é possível monitorizar fóruns, por exemplo, e determinar tendências, instalar infiltrados para colocar desinformação ou criar dúvidas na confiança entre terroristas.

Esta ameaça, a concretizar-se constituiria um facto gravíssimo relativamente à segurança interna, pelos efeitos de terror e insegurança que teriam ao nível social e ainda pelos prejuízos económicos que provocaria.

Capítulo III - O desafio para a segurança

"A História ensinou-nos: nunca subestimar a quantia de dinheiro, tempo, e esforço que alguém despende para frustrar um sistema de segurança. É sempre melhor esperar o pior. Considera que os teus adversários são melhor do que são. Presume que a ciência e a tecnologia em breve serão capazes de realizar coisas que não podem ainda. Dá a ti mesmo uma margem de erro. Dá a ti mesmo mais segurança do que aquela que necessitas hoje. Quando o inesperado acontecer, vais ficar feliz por tê-lo feito".

Bruce Schneier

3.1 – O conceito de cibersegurança

Vasta literatura diz-nos que a cibersegurança entrou para o debate público nos anos 80 e o discurso à sua volta tem sido articulado pelos governos, empresas do sector, instituições públicas, especialistas, técnicos,

meios de comunicação e organizações internacionais essencialmente, fazendo a ligação entre a segurança dos computadores e a segurança interna dos Estados. Contudo, não existe uma definição consensual de cibersegurança a nível internacional.

As referências sistemáticas às vulnerabilidades das infra-estruturas críticas, a retórica exagerada à volta do facto de um ciberataque como uma ciberarma ter equivalência aos efeitos das armas de destruição massiva e a eminência de um "*Pearl Harbor* digital" por parte dos Estados Unidos da América, arrastou o tema para a esfera popular, suscitando todo o tipo de discursos, o que leva público a uma concepção errada das ciberameaças.

No que toca à segurança dos computadores e das redes, a segurança tem sido definida com base em três objectivos ou propriedades: disponibilidade, integridade e confidencialidade. Disponibilidade, significa a garantia de acesso à informação por aqueles que estão autorizados. Integridade, visa a protecção da informação contra modificações ou eliminações não autorizadas. Confidencialidade, consiste na prevenção contra divulgação não autorizada. (José Dinis, 2005).

Quanto a estes objectivos, o escopo é a protecção dos computadores e dos seus utilizadores contra ataques e ameaças de ataque.

Helen Nissembaum (2005), no que diz respeito à vulnerabilidade dos computadores e redes de computadores em caso de ataque, distingue duas concepções de segurança, que coexistem em simultâneo:

- A segurança dos computadores e redes de computadores, baseada na vertente das ciências computacionais e engenharia;
- A cibersegurança, mais recente, baseada nas preocupações das agências de segurança governamentais e detentores de propriedade intelectual.

Quanto à primeira entende a autora que, a segurança dos computadores e redes de computadores, os seus objectivos principais são garantir: acessibilidade, integridade e confidencialidade. As ameaças relativamente a estes objectivos serão três:

- Ataques que tornam os sistemas, informações e redes indisponíveis para os utilizadores (DDoS, vírus, *worms*, etc.), que desactivam sistemas ou parte deles;

- Ataques que ameaçam a integridade da informação ou sistemas e redes de dados, que corrompem, destroem arquivos, etc;

- Ataques que ameaçam a confidencialidade das informações e comunicações (intercepção de e-mails, acesso não autorizado a sistemas e dados, *spyware*, etc).

Relativamente à segunda, a cibersegurança propriamente dita, considera que as principais ameaças serão três:

- Uso de computadores ligados em rede ou comunicações por organizações revolucionárias, como por exemplo, *websites* de grupos de ódio racial, cibercrime, pornografia infantil e uso da *Internet* para fins terroristas.

- Ataque de infra-estruturas críticas (serviços públicos, banca, governos, meios de comunicação, etc.), uma vez que os sistemas críticos são cada vez mais dependentes da informação em sistemas de rede, por isso mais vulneráveis a ataques à rede. Os quais, podem vir de organizações terroristas internacionais, ou nações hostis que pretendem envolver-se numa ciberguerra, por exemplo.

- Ataques ao sistema de informações que podem ir desde a sua incapacidade até à debilitação.

Estas diferenças de terminologias e conceitos têm consequências ao nível da sua regulamentação e concepção. Os países que já definiram uma estratégia para a cibersegurança evidenciam ter conceitos diferentes.

Apesar de tudo, a *Internet* tem mostrado uma "…capacidade extraordinária de penetração, "resiliência", e até de subversão política, ao garantir fluxos regulares e imparáveis de informação…". (Armando Marques Guedes, 2007).

Em Portugal, segundo Alexandre Caldas[18], a cibersegurança parece ter sido assumida como uma questão estratégica e entendida numa visão lata que:

[18] Disponível: http://www.ceger.gov.pt/INDEX_PHP/PT/SEGURANCA/NOTICIAS/70_ENC.HTM, sítio do Centro de Gestão da Rede Informática do Governo e publicado na revista Segurança e Defesa, nº 16, Janeiro de 2011.

"…cobre todas as dimensões de segurança que afectam o designado "ciberespaço" ou espaço cibernético. Se entendermos o ciberespaço como todo o espaço ou "território" que integra as redes electrónicas ou de comunicação que constituem a infra-estrutura sobre a qual são criados, tratados, armazenados e distribuídos fluxos de informação, então a "cibersegurança" deve de igual modo ser entendida como a "segurança" deste mesmo espaço cibernético".

Na União Europeia, de acordo com dados de 2012, da *European Network Information Security Agency* (ENISA)[19], apenas dez países definiram uma estratégia de cibersegurança, onde não se inclui Portugal, uma vez que ainda se encontra na fase de estudo da proposta, de acordo com o Gabinete Nacional de Segurança[20], destes países, a Inglaterra releva significativamente na sua estratégia o ciberterrorismo como constituindo uma ameaça.

Parece haver consenso na essência do que respeita ao conceito de cibersegurança, uma vez que na maioria das estratégias são referidas as preocupações com confidencialidade, acessibilidade e integridade. No entanto, as estratégias de cibersegurança criadas colocam o seu enfoque no reforço dos mercados internos de cada país, o que impede uma perspectiva de segurança interna e afasta o envolvimento militar. (Helen Nissembaum 2005).

3.2 - A cibersegurança e a segurança interna

De acordo com o Relatório "A Sociedade da Informação em Portugal"[21], relativo ao ano de 2010, da Agência para a Sociedade do Conhecimento (UMIC), a utilização das tecnologias de informação e *Internet* pelos particulares, empresas e administração pública tem crescido, o que tem como consequência uma maior vulnerabilidade a potenciais ameaças.

A cibersegurança vai para além da segurança dos computadores e das redes de computadores (Helen Nissembaum, 2005), porque afecta pessoas, empresas e o Estado (mecanismos decisórios de governação).

[19] Disponível: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide.
[20] Disponível: http://www.gns.gov.pt/gns/pt/ciberseguranca/.
[21] Disponível: http://www.rcc.gov.pt/SiteCollectionDocuments/A_SI_em_PT_doc_Maio2010.pdf.

Em Portugal a segurança foi consagrada como um direito constitucional, estando consagrado no Artigo 27º/1: "Todos têm direito à liberdade e à segurança", sendo considerada no Capítulo I, relativo as Direitos, Liberdades e Garantias Pessoais.

A Lei de Segurança Interna (Lei 53/2008 de 29 de Agosto), diz-nos no Artigo 1º que a segurança interna é "…a actividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir a criminalidade…".

No mesmo Titulo II, no Artigo 37º/1 e 2, consagra-se a liberdade de expressão e de informação e o impedimento à sua restrição:

"1. Todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, pela imagem ou por qualquer outro meio, bem como o direito de informar, de se informar e de ser informados, sem impedimentos nem discriminações.

2. O exercício destes direitos não pode ser impedido ou limitado por qualquer tipo ou forma de censura".

Daqui decorre a obrigatoriedade do Estado em garantir a segurança dos cidadãos e da informação, dada a dependência dos particulares, empresas e do Estado relativamente às tecnologias de informação e à informação propriamente dita, bem como assegurar a liberdade de expressão.

De acordo com o Relatório Anual de Segurança Interna de 2011, das ameaças globais à segurança interna constam as ciberameaças. No entanto, a garantia da nossa segurança tem que ser balanceada com a protecção dos nossos direitos liberdades e garantias, protegidos na Constituição da República Portuguesa (CRP) e demais legislação.

O Artigo 26º/1 da CRP, diz-nos que o direito à reserva da intimidade da vida privada é um direito fundamental, de carácter pessoal. Deste modo, está incluído nos direitos da personalidade, estatuídos no Artigo 80º do Código Civil (CC). Este direito contém duas vertentes: o direito de impedir que estranhos acedam a informações sobre a vida privada e familiar e o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outros (cfr. Gomes Canotilho e Vital Moreira, 2007).

Estas duas dimensões reflectem-se no direito ao sigilo das comunicações, estabelecido no Artigo 34º/1 e 4 da CRP: "…o sigilo da

correspondência e dos outros meios de comunicação privada…" e "É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de procedimento criminal." Há assim, uma proibição de acesso não autorizado de terceiros aos conteúdos de todas as comunicações.

A protecção de dados pessoais é regulada pela Lei nº 67/98, de 26 de Outubro (Lei da Protecção de Dados Pessoais), que transpôs para a ordem interna a Directiva nº 95/46/CE, de 24-10-1995 e pela Lei nº 68/98, de 28 de Outubro, que regula o tratamento de dados pessoais e a protecção da privacidade no sector das telecomunicações, que transpôs para a ordem interna a Directiva 97/66/CE, de 15-12-1997.

Igualmente importante é a Convenção do Conselho da Europa para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, que foi aprovada pela Resolução da Assembleia da República nº 23/93, cujo objectivo e finalidade estão consagrados no seu Artigo 1º: "A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito ("protecção dos dados")."

Relativamente à Convenção Europeia dos Direitos do Homem (CEDH), no seu Artigo 8º/2, tenta demarcar um equilíbrio entre a protecção do direito à reserva da intimidade da vida privada com os interesses públicos, que com ele podem entrar em conflito. Esta regra estatui restrições às interferências das autoridades públicas: a legalidade (a vigilância só pode ser feita se houver legislação que a preveja), a democraticidade (as razões invocadas têm que estar de acordo com os princípios democráticos) e por fim a proporcionalidade (a necessidade apenas se justifica para que se protejam a segurança nacional, a segurança pública, defesa da ordem, bem-estar económico do país prevenção das infracções penais, protecção da saúde ou da moral, protecção dos direitos e das liberdades de terceiros, ou seja, o interesse público).

O que nos foi possível sobretudo avaliar, depois das conferências e seminários a que assistimos, Portugal não possui uma estratégia de

cibersegurança. No entanto, o nosso país tem sido alvo de ciberataques, provenientes sobretudo da China, Rússia e Brasil. O facto de a segurança das nossas infra-estruturas críticas estar nas mãos das empresas privadas, aumenta as preocupações, uma vez que o seu enfoque está no lucro e não na segurança e provavelmente boa parte dos seus accionistas são estrangeiros provenientes de países com interesses antagónicos aos nacionais. Para além disso, a cibersegurança está dependente de inúmeros intervenientes com diferentes necessidades e funções, que vão desde o utilizador de comunicações públicas e serviços, ao fornecedor de serviços de *Internet*, que permite o acesso à infra-estrutura e manipulação da mesma.

Os responsáveis pela segurança das infra-estruturas devem, por isso, ter a obrigação de testar sistematicamente a sua resiliência a ataques. Uma estratégia nacional de cibersegurança deve assim, ter em consideração todos os envolvidos, criar condições para a cooperação e coordenação entre eles. A responsabilização cabe a todos e não só a quem faz parte do sector. Todas estas dimensões foram referidas nas conferências e seminários a que assistimos.

Para Viegas Nunes (2004), quando se analisam os riscos associados à Infra-estrutura de Informação Nacional, deve ter-se em consideração que estes riscos, resultam da conjugação de três factores:

- Recursos a proteger (isto é, os alvos potenciais dos ataques);
- Detecção das vulnerabilidades da Infra-estrutura de Informação;
- Ameaças que, depois de exploradas as vulnerabilidades, podem afectar os recursos a proteger.

Assim, para este autor, para proteger a Infra-estrutura de Informação é necessário que seja criado um sistema que tenha por objectivo implementar a segurança e atenuar os impactos de quaisquer ciberataques, ou se possível eliminá-los e para tal, é necessário, pelo menos:

- Proceder ao levantamento de um *Computer Emergence Response Team* (CERT) nacional[22];
- Implementar programas adequados de educação e treino;

[22] Portugal detém um CERT, no seio da Fundação para a Computação Científica Nacional (FCCN), entidade actualmente em extinção. Esse CERT é fruto de uma iniciativa privada, apoiada financeiramente em parceria público-privada, e embora nos representasse junto da ENISA, não é verdadeiramente uma entidade oficial.

- Desenvolver mecanismos de segurança e redundância da Infra-estrutura de Informação;
- Desenvolver regimes de cooperação e actuação internacional na área da protecção da Infra-estrutura de Informação.

Uma estratégia de cibersegurança deve, no essencial, ser pensada na perspectiva da segurança interna e deve conjuntamente, de uma forma articulada, tornar possível a cooperação entre serviços de informações, forças policiais, instituições judiciais, militares e privados, promover a cooperação internacional, capacitar as autoridades competentes de modo a abrangerem todo o espectro de ciberameaças e de utilizadores, desde os utilizadores individuais às infra-estruturas críticas, responder de forma imediata a todos os riscos e ameaças, tornar a *Internet* um lugar de reunião e uma ferramenta de acesso à informação, no estrito respeito pelos direitos, liberdades e garantias dos cidadãos, ganhar a confiança dos cidadãos para que estes colaborem, combater e prevenir o cibercrime e impedir que ocorram ciberataques terroristas.

De acordo com a Resolução do Conselho de Ministros nº 42/2012, está prevista a definição e implementação de uma Estratégia Nacional de Segurança da Informação (ENSI), que envolve a "criação, instalação e operacionalização" de um Centro Nacional de Cibersegurança. No entanto, este diploma apenas constituiu a Comissão Instaladora do Centro Nacional de Cibersegurança, ficando este, na dependência do Primeiro-Ministro não estando especificado como funcionará em termos operacionais ou como se articulará com outros organismos existentes ligados à cibersegurança. No sítio do Gabinete Nacional de Segurança[23], estão lançadas as bases de uma estratégia. Haverá várias entidades a envolver prevendo-se, segundo Lino Santos (2011) as seguintes: o Centro de Gestão da Rede Informática do Governo, a Agência Para a Modernização Administrativa, a Agência Para a Sociedade do Conhecimento, o Gabinete Nacional de Segurança, o Sistema de Segurança Interna, o Sistema de Informações da República Portuguesa, o Conselho Nacional de Planeamento Civil de Emergência, a Autoridade

[23] Disponível: http://www.gns.gov.pt/gns/pt/.

Nacional de Comunicações, a Fundação Para a Computação Científica Nacional e a Policia Judiciária. (José Santos, 2011).

3.3 - O papel da União Europeia, OSCE, Conselho da Europa, OTAN e ONU relativamente à cibersegurança

União Europeia

A União Europeia, à qual Portugal pertence, tem tido um papel muito menos activo do que julga. Limitou-se até agora a adoptar vários textos, entre os quais podem destacar-se:

- Uma estratégia chamada "i2010" ("Uma Sociedade da Informação para o crescimento e o emprego"), instituído através de uma comunicação da Comissão Europeia em 2005 (COM (2005) 229 final);
- Em 2006, uma Comunicação da Comissão Europeia designada "Uma estratégia para uma sociedade da informação segura - Diálogo, parcerias e capacitação" (COM (2006) 251 final), que inclui uma apreciação comparativa das políticas nacionais sobre a segurança da rede e da informação, mas não forneceu qualquer acção concreta;
- A Comunicação da Comissão Europeia em 2009 sobre a "protecção de infra-estruturas críticas de informação" (COM (2009) 149 final), que define as prioridades na área de sistemas de segurança da informação, com um plano de acção com várias medidas, como por exemplo a criação de um fórum intercâmbio europeu público-privado;
- A Comunicação da Comissão Europeia em 2010, denominada "Uma Agenda Digital para a Europa" (COM (2010) 245 final), que aborda todas as questões relacionadas com o desenvolvimento da sociedade da informação na Europa e reafirma a necessidade de implementação rápida e eficaz de um plano de acção da União Europeia para a protecção de infra-estruturas críticas da informação;

Ainda em 2010, o Conselho Europeu apresentou uma Estratégia de Segurança Interna Europeia. Porém, a Estratégia apenas pretendeu reconhecer ameaças comuns, colocou o enfoque na cooperação entre os Estados-membros e as instituições e nomeou cinco prioridades:

- Desmantelar as redes internacionais de criminalidade;
- Prevenir o terrorismo e responder à radicalização e ao recrutamento;
- Reforçar os níveis de segurança para os cidadãos e as empresas no ciberespaço;
- Reforçar a segurança através da gestão de fronteiras; e
- Reforçar a capacidade de resistência da Europa às crises e catástrofes.

A comunicação da Comissão Europeia (COM (2011) 163 final) sobre a "protecção de infra-estruturas críticas de informação" em 2011, que incorpora e amplia as cinco áreas de comunicação de 2009 e introduz novas propostas, tais como a criação de um grupo de trabalho conjunto da União Europeia com os Estados Unidos da América no âmbito da cibersegurança e cibercrime.

Em 2012 numa Comunicação Comissão ao Conselho e ao Parlamento (COM (2012) final), no âmbito da luta contra a cibercriminalidade digital é proposta a criação de um Centro Europeu da Criminalidade, fazendo referência às infra-estruturas críticas e sistemas de informação da União.

Estes documentos estabelecem objectivos muito gerais, mas sem iniciativas concretas.

Ao nível da luta contra a cibercriminalidade, por exemplo, foi adoptada em 24 de Fevereiro de 2005, uma decisão-quadro relativa a ataques contra sistemas de informação (Decisão-Quadro 2005/222/JAI do Conselho).

Em 8 de Dezembro de 2008, foi adoptada uma directiva sobre a protecção das infra-estruturas críticas, mas limitada às áreas da energia e transportes (Directiva 2008/114/CE do Conselho).

Em Novembro de 2009, foi aprovada a Directiva-Quadro 2009/136/CE: "Pacote das Telecomunicações" que regulamenta a alteração das comunicações electrónicas. No Artigo 13º, é dito que as operadoras de telecomunicações são obrigadas a notificar as autoridades nacionais competentes sobre qualquer violação de segurança ou perda de integridade, que tiverem um impacto significativo no funcionamento das redes ou serviços. Esta Directiva introduz a obrigatoriedade da implementação de medidas mínimas de segurança por parte dos operadores e determina que as autoridades nacionais são responsáveis por garantir que os operadores

cumprem essas obrigações. Esta Directiva foi transposta para o direito interno através da Lei 46/2012, de 29 de Agosto[24].

Relativamente à aplicação da "cláusula de defesa mútua" (Artigo 42º, nº 7, do Tratado da União Europeia), contida no Tratado de Lisboa, em caso de ciberataque contra um Estado membro, não existe consenso entre os vinte e sete países membros, tendo o Parlamento Europeu emanado a Resolução 2012/2223 (INI), em 22 de Novembro de 2012, versando sobre a sua dimensão política e operacional e onde consta:

> "11. Recorda aos Estados-Membros a sua inequívoca obrigação de prestar ajuda e assistência por todos os meios ao seu alcance se um Estado-Membro for alvo de agressão armada no seu território; sublinha que, embora uma agressão em grande escala contra um Estado-Membro pareça improvável num futuro próximo, a defesa territorial tradicional e a defesa contra novas ameaças devem continuar a ser uma prioridade; recorda também que o Tratado estipula que os compromissos e a cooperação na área da defesa mútua devem ser compatíveis com os compromissos assumidos no âmbito da NATO, que, para os Estados que desta são membros, continua a ser a base da sua defesa colectiva e o fórum para a implementação da mesma;
>
> 12. Realça simultaneamente, e por ser igualmente importante, a necessidade de preparação para situações que envolvam Estados-Membros da UE que não pertencem à NATO ou territórios de Estados-Membros da UE fora da área do Atlântico Norte que, por conseguinte, não são abrangidas pelo Tratado de Washington, ou para situações em que não seja alcançado um acordo sobre uma ação coletiva no seio da NATO; salienta igualmente, neste contexto, a necessidade de recorrer às capacidades da NATO, como previsto no Acordo «Berlim Mais»;
>
> 13. Considera que mesmo os ataques não armados, como, por exemplo, os ciberataques contra infraestruturas críticas, lançados com o objetivo de causar graves danos e perturbação num Estado-Membro e identificados como sendo provenientes de uma entidade externa, podem ser abrangidos pela cláusula, caso a segurança do Estado-Membro em causa seja significativamente ameaçada pelas consequências do ataque, no pleno respeito pelo princípio da

[24] Na parte que altera a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, procedendo à primeira alteração à Lei n.º 41/2004, de 18 de agosto, e à segunda alteração ao Decreto-Lei n.º 7/2004, de 7 de Janeiro.

proporcionalidade; Em geral, apesar da adopção de vários documentos ou planos de acção, pela União Europeia e pela Comissão Europeia, não parece haver uma medida importante relacionada com sistemas de segurança informações."

Em geral, apesar da adopção de vários documentos ou planos de acção pela União Europeia e pela Comissão Europeia, não parece haver uma medida importante relacionada com segurança da informação e das redes e sistemas de informação.

Assim, podemos concluir que são três as lacunas essenciais:

- Não existe uma estratégia real global do ciberespaço a nível europeu. Há no âmbito da Comissão Europeia, uma competição entre os diferentes ramos para controlar as questões que envolvem a cibersegurança na União Europeia;
- Não existe coordenação entre a União Europeia e a Comissão Europeia em matérias como a política externa, política de segurança e defesa comum;
- Há uma falta de eficácia, pois a União Europeia ainda não parece capaz de proteger as suas próprias redes e sistemas de informação.

Embora a União Europeia tenha um CERT ("*Computer Emergency Response Team*") desde 2011, incumbido de prever e responder a ataques cibernéticos contra redes ou sistemas das instituições europeias, agências ou outros órgãos ligados a ela, ainda está longe de oferecer protecção para todas as redes e sistemas da União Europeia.

A União Europeia tem, no entanto, um instrumento especial para segurança das redes e da informação, a Agência Europeia para a Segurança da Informação (ENISA), criada em Março de 2004 (pelo Regulamento (EC) Nº 460/2004 do Parlamento Europeu e do Conselho) à qual foram conferidas as seguintes missões:

- Aconselhar e assistir a Comissão Europeia e os Estados-Membros sobre a segurança dos sistemas de informação, por meio de "guias de boas práticas", por exemplo;

- Apoiar os Estados-Membros e instituições europeias no desenvolvimento de capacidades para responder às ameaças à segurança dos sistemas de informação;
- Encorajar a cooperação entre os Estados-Membros, através de exercícios conjuntos ou outros mecanismos.

De entre as acções tomadas por este organismo, podem destacar-se a publicação de relatórios com recomendações concretas, por exemplo, em sistemas de controlo industrial SCADA, cibersegurança e ciberameaças[25]. Foram realizados exercícios liderados pela ENISA, como por exemplo, o "*Cyber Europe 2010"*[26], no âmbito da protecção das infra-estruturas críticas de informação, o "*Cyber Atlantic 2011*"[27], em matéria de cooperação da União Europeia com os Estados Unidos da América e o "*Cyber Europe 2012*"[28], que incidiu sobre confiança e cooperação, similarmente ao exercício de 2010.

O mandato da ENISA foi prorrogado até Setembro de 2013[29] e uma proposta de regulamento que altera e prorroga o mandato da agência está em discussão a nível europeu[30].

OSCE

A Acção da *Organization for Security and Co-operation in Europe* (OSCE) relativamente à cibersegurança é mais recente e insere-se no âmbito da promoção e estabelecimento de medidas de confiança no ciberespaço entre os países, especialmente com a Rússia.

Tem considerado a perspectiva do ciberterrorismo, tendo em 2002 criado a *Action Against Terrorism Unit* (ATU)[31].

---

[25] Como é o caso do "*ENISA Threat Landscape*", disponível: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape.
[26] Disponível: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report.
[27] Disponível: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-atlantic/cyber-atlantic-2011.
[28] Disponível: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012.
[29] Conforme o Regulamento 580/201 do Parlamento Europeu e do Conselho, disponível: http://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1.
[30] Conforme informação disponível no sítio da Autoridade Nacional de Comunicações (ANACOM): http://www.anacom.pt/mobile/render.jsp?contentId=1086410&showAll=1.
[31] Disponível: http://www.osce.org/atu/13578.

Porém, a denotada falta de experiência prática em segurança cibernética deve fazer com que se mantenha como um fórum de intercâmbio entre Estados.

Conselho da Europa

A Convenção de Budapeste[32], conhecida como a Convenção sobre o Cibercrime, foi assinada em 23 de Novembro de 2001, no âmbito do Conselho da Europa, coloca o seu enfoque na luta contra o cibercrime e é o primeiro tratado internacional que define crimes cometidos através da *Internet* e outras redes informáticas. Centra-se nas infracções relacionadas com direitos de autor, burla, pornografia infantil, e delitos relacionados com a segurança das redes, mas também contém poderes para executar procedimentos, como a busca de redes de computadores e interceptação.

Foi ratificada por Portugal e outros países da União Europeia, bem como por vários países não-membros do Conselho da Europa, como os Estados Unidos, contudo não foi assinada pela Rússia e China[33].

Esta Convenção é referida de uma forma geral como um instrumento para responder às questões do cibercrime, sendo inclusivamente recomendada aos países membros da ONU[34], contudo não foca o problema do específico ciberterrorismo.

OTAN

A questão da cibernética chamou a atenção da OTAN na Cimeira de Praga em 2002. A OTAN foi a primeira organização a proteger seus próprios sistemas de informação e comunicações. Para tal implementou o órgão *NATO Computer Incident Response Capability* (NCIRC)[35], responsável pela prestação de segurança cibernética técnica e operacional de todas as redes, sistemas de informação e de comunicação da Aliança Atlântica, sendo ainda responsável pelo tratamento de incidentes, centralizando-os e coordenando-os, de modo a evitar duplicações de capacidades.

---

[32] Disponível: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
[33] Carta de Assinaturas e Ratificações disponível: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.
[34] Conforme o 12th UN Congress on Crime Prevention and Criminal Justice-Committee II-2nd & 3rd Meetings, disponível: http://www.un.org/News/Press/docs/2010/soccp349.doc.htm.
[35] Disponível: http://www.ncirc.nato.int/index.htm.

Depois dos ataques à Estónia em 2007, a OTAN foi obrigada a repensar o seu papel como aliança defensiva, caso ocorra um ataque contra um de seus membros.

Na Cimeira de Bucareste em 2008[36], foi salientada a necessidade dos países protegerem os seus sistemas de informação críticos, articulando responsabilidades e partilhando as melhores práticas para desenvolver capacidades para apoiar os países membros no combate contra ataques cibernéticos.

É então criado em 2008 o *Cyber Defence Management Authority* (CDMA)[37], que é dirigido pelo *Cyber Defence Management Board*, este integra os líderes políticos, militares, operacionais e técnicos com responsabilidades na ciberdefesa da OTAN.

Em 2010, na Cimeira da OTAN em Lisboa, as ciberameaças foram contempladas no novo conceito estratégico:

> "*Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses,economies and potentially also transportation and supply networks and other critical infrastructure;*
> *they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks*"[38].

Mantém-se a garantia de assistência mútua entre os Estados signatários caso ocorra uma agressão externa, de acordo com o Artigo 5º do Tratado do Atlântico Norte:

> "*NATO members will always assist each other against attack, in accordance with Article 5 of the Washington Treaty That commitment remains firm and*

[36] Bucharest Summit Declaration: http://www.nato.int/cps/en/natolive/official_texts_8443.htm?mode=pressrelease.
[37] Idem.
[38] Disponível: http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

binding NATO will deter and defend against any threat of aggression, and against emerging security challenges where they threaten the fundamental security of individual Allies or the Alliance as a whole".

Em 2011, a OTAN aprovou um conceito para ciberdefesa[39], cujo escopo essencial é o aumento da segurança dos sistemas de informação da Aliança, de modo a ter sempre os níveis de ameaça actualizados, com recurso ao aperfeiçoamento dos padrões e procedimentos de segurança e à gestão mais centralizada.

A OTAN tem realizado exercícios. O "*Crisis Management Exercise"* (CMX) e a "*NATO Cyber Coalition 2011*"[40], testaram, em momentos distintos, a capacidade cibernética, técnica e operacional de defesa da Aliança. Foi criada uma crise fictícia, com a simulação de ciberataques em larga escala à OTAN e a infra-estruturas críticas, em que participaram vinte e três membros e seis parceiros da OTAN, pertencentes ao sector académico, privado e organizações internacionais.

No entanto, a própria OTAN foi alvo de ataques por parte dos *Anonymous*, denotando, ainda assim, vulnerabilidades.

Na última Cimeira da OTAN em 2012, em Chicago, os Chefes de Estado e de Governo dos países membros da OTAN, reafirmaram o objectivo de obter a plena capacidade operacional na resposta a incidentes para o final do ano. Nesta Cimeira o ponto 49 foi dedicado à ciberdefesa:

"*Cyber attacks continue to increase significantly in number and evolve in sophistication and complexity. We reaffirm the cyber defence commitments made at the Lisbon Summit. Following Lisbon, last year we adopted a Cyber Defence Concept, Policy, and Action Plan, which are now being implemented"*….

"*We will develop further our ability to prevent, detect, defend against, and recover from cyber attacks. To address the cyber security threats and to improve our common security, we are committed to engage with relevant partner nations on a case-by-case basis and with international*

[39] Disponível: http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.
[40] Conforme: http://www.nato.int/cps/en/natolive/news_91115.htm?mode=pressrelease.

organisations, inter alia the EU, as agreed, the Council of Europe, the UN and the OSCE, in order to increase concrete cooperation. We will also take full advantage of the expertise offered by the Cooperative Cyber Defence Centre of Excellence in Estonia."[41]

A OTAN deve assim determinar qual a postura a tomar para responder a ciberataques contra os Estados-Membros. Relativamente a esta questão há a considerar por exemplo:

- Se pode invocar-se o Artigo 5º do Tratado de Washington em caso de ataque cibernético. Este artigo foi concebido como um mecanismo através do qual os Estados Unidos seriam obrigados a acorrer em auxílio dos seus aliados europeus.
- Se um ciberataque pode ser equiparado a um acto de guerra;
- Como identificar o agressor;
- Se podem ser usados conjuntamente ataques militares convencionais, ou apenas cibernéticos.

Em 2008, foi instituído o *Cooperative Cyber Defence Centre*, em Tallinn na Estónia. Este organismo foi reconhecido pela OTAN como Centro de Excelência, está focado na ciberdefesa, e no âmbito dos seus trabalhos foram recentemente publicados: "*The Tallinn Manual on the International Law Applicable to Cyber Warfare*"[42], resultante do trabalho de vários especialistas, que se debruçaram sobre o *jus ad bellum* (legislação internacional que incide sobre o recurso à força pelos Estados) e o *jus in bello* (que regula os conflitos armados), editado pelo Professor Michael N. Schmitt, do *U.S. Naval War College*, e ainda, o "*National Cyber Security Framework Manual*"[43], editado pelo Consultor Senior Alexander Klimburg, do *Austrian Institute for International Affairs*, que foca a componente da cibersegurança na segurança interna, onde é considera a possibilidade da ocorrência de ciberataques terroristas. O *Tallinn Manual* não é um documento oficial da OTAN nem do Centro de Excelência, mas expressa a convergência das opiniões de um grupo de especialistas

[41] Disponível: http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease.
[42] Disponível: https://www.ccdcoe.org/249.html.
[43] Disponível: http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

independentes, no que respeita à aplicação do direito internacional à "nova" forma de guerra.

Organização das Nações Unidas (ONU)

A acção da ONU relativamente à cibersegurança poderá ser repartida em três áreas principais: a político-militar (ciberguerra), a económica (cibercrime) e a *Internet Governance Forum* (IGF) (governança mais ampla da *Internet*).

Em 1998, aquando do crescimento exponencial da *Internet*, foi introduzido o primeiro projecto de resolução no contexto da segurança internacional, pelo governo russo na Assembleia Geral (A/RES/53/70), sobre os desenvolvimentos nas telecomunicações e informação, o que demonstrou uma preocupação com a segurança internacional, perante a possibilidade da ocorrerem ataques a nível transnacional, no âmbito do cibercrime, do ciberterrorismo e da ciberguerra.

A ONU tem discutido os princípios que demarcarão a não proliferação de ciberarmas, de modo a limitar a exploração militar do ciberespaço.

Mais recentemente, há um desenvolvimento, relativamente aos governos da Rússia, China, Tajiquistão e Uzbequistão, que propuseram um Código Internacional de Conduta para a segurança de informação, em 14 de Setembro de 2011, a ser considerado na próxima sessão da Assembleia Geral da ONU (A/66/359, ver Anexo)[44].

No início de 2010, numa reunião da ONU, um grupo de especialistas governamentais dos Estados Unidos da América, Rússia e China, declaram as ameaças existentes e potenciais na área de segurança da informação, as mais sérias do século XXI (A/65/201)[45]. No entanto, já tinha sido criado um primeiro grupo em 2004, que não encontrou qualquer consenso (A/60/202)[46]. Ao que parece houve um total de cinco grupos de peritos governamentais em questões relacionadas com o ciberespaço.

[44] Disponível: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement.
[45] Disponível: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement.
[46] Disponível: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/453/63/PDF/N0545363.pdf?OpenElement.

Pelo que se observa, o envolvimento do Conselho de Segurança da ONU tem sido direccionado para o *Working Group on Countering the Use of the Internet for Terrorist Purposes*[47] que complementa a *Counter-Terrorism Implementation Task Force* (CTITF). Todavia, na sua Resolução relativa à Geórgia, não refere o aspecto cibernético e quanto à Estónia e Irão não houve resoluções.

Em 2010 a sessão de abertura do Economic and Social Council (ECOSOC) intitulou-se: "*Cyber security: emerging threats and Challenges*"[48].

A Assembleia Geral apenas tem tido uma série de actividades, discussões e projectos sobre as normas que irão reger o comportamento dos Estados membros, mas não existem medidas concretas.

A *International Telecommunication Union* (ITU)[49], uma agência especializada da ONU em telecomunicações, no que toca à cibersegurança, aparentemente divide-se em três áreas de trabalho:

- Combate ao cibercrime: ITU e UNODC (*United Nations Office on Drugs and Crime*);
- Capacitação: ITU, UNIDIR (*United Nations Institute for Disarmament Research*) e UNICRI (*United Nations Interregional crime and Justice Research Institute*);
- Protecção à Criança Online: ITU, UNICEF (The United Nations Children´s Fund), UNICRI, o UNODC.

A Agenda Global para a Cibersegurança apenas inclui recomendações, por exemplo a utilização da Convenção do Cibercrime.

Será, difícil obter consensos uma vez que esta organização é composta por quase duzentos países, podendo assim, a sua dimensão constituir a sua fraqueza.

Podemos concluir que, apesar de não existir uma concepção de cibersegurança ao nível internacional, afigura-se um entendimento relativamente à sua concepção, sendo referida a óptica da confidencialidade, acessibilidade e integridade, na maioria das estratégias de cibersegurança. Apesar disto, as estratégias concentram-se no fortalecimento dos mercados

[47] Disponível: http://www.un.org/terrorism/internet.
[48] Disponível: http://www.un.org/en/ecosoc/julyhls/pdf10/cyber_security_statement.pdf.
[49] Conforme: http://www.itu.int/en/about/Pages/whatwedo.aspx.

internos de cada país, obstando uma visão de segurança interna no desenho das estratégias e desvia o envolvimento dos militares.

Portugal não possui uma estratégia de cibersegurança, embora já tenha desenvolvido importantes iniciativas ad-*hoc*. Contudo, sendo agora a informação digital, o Estado está obrigado a garantir a sua segurança. “A quantidade de informação e de conhecimento apresentam cada vez mais valor, no tipo de sociedade actual referida aos países mais desenvolvidos tecnologicamente”. (José Dinis, 2005).

A não existência de uma estratégia de cibersegurança nacional, bem como de legislação correspondente, faz com que Portugal seja apenas um seguidor das estratégias de outros países. O enquadramento normativo deve de algum modo, contemplar a utilização conflitual da informação, as responsabilidades e atribuições das Forças Armadas e das Forças de Segurança, de forma a garantir a segurança nacional no ciberespaço.

No entanto, esta estratégia não deve ser desenhada numa perspectiva apenas securitária, mas sim ter também em conta os interesses nacionais, sociais, a necessidade de modernização e promoção do desenvolvimento nacional.

Os conceitos de segurança terão que ser reconsiderados, pois a conjuntura estratégica presente é de conflito e o terrorismo é transnacional e de carácter assimétrico. A noção e o escopo da cibersegurança terão que ter em consideração que um ataque individual não é o mesmo que um ataque a uma infra-estrutura crítica, muito menos se o ataque for multidireccionado de modo a ter um efeito dominó.

Uma estratégia de cibersegurança deve ser pensada na óptica da segurança interna, possibilitar a coordenação e colaboração entre todos os interessados.

As organizações da União Europeia, OSCE, Conselho da Europa, OTAN e ONU, não têm tido o papel desejado a nível da cibersegurança na prevenção contra o ciberterrorismo. Apenas a Convenção do Cibercrime, foi o documento criado no âmbito do Conselho da Europa que tem um papel mais preponderante, sendo inclusivamente recomendado pela OTAN, na sua Agenda Global para a Cibersegurança.

A criação do *The Tallinn Manual on the International Law Applicable to Cyber Warfare,* e o *National Cyber Security Framework Manual,* já constituem importantes textos de apoio. No entanto, este facto sugere que dada a inadequação da legislação para responder às ciberameaças, esta legislação está a evoluir para a área dos conflitos cibernéticos. Quanto aos outros órgãos, podemos concluir, portanto, que o seu papel é residual.

Capítulo IV – Enquadramento legislativo do terrorismo

"Os problemas não podem ser resolvidos ao mesmo nível da consciência que os criou." Albert Einstein

4.1 – Quadro normativo geral do Direito Internacional relativo às convenções multilaterais

Abordaremos o quadro convencional internacional no âmbito do combate ao terrorismo, no entanto, não de uma forma exaustiva, apenas procurando relevar algumas características dos vários acordos existentes.

Existem doze acordos de alcance internacional, todos eles ratificados por Portugal:

- Convenção de Tóquio: Convenção Referente às Infracções e a Certos Outros Actos Cometidos a Bordo de Aeronaves, assinada em Tóquio, em 14 de Setembro de 1963,[50] foi produzida no âmbito da Organização da Aviação Civil Internacional (*International Civil Aviation Organization* (ICAO)), tendo sido aprovada pelo Decreto-Lei nº 45904, de 5 de Setembro de 1964. Esta é a convenção mais antiga, é multilateral geral, ainda vigora e trata da questão do terrorismo na perspectiva do direito internacional.

O intento principal deste acordo é a regulação dos actos ilícitos cometidos a bordo de aeronaves, quando as mesmas não se encontrem no Estado da sua origem e outras infracções que, não consistindo em infracções de acordo com o direito desse Estado, "possam pôr ou ponham em perigo a segurança da aeronave, ou das pessoas ou bens, ou que ponham em perigo a boa ordem e a disciplina a bordo", de acordo com o Artigo 1º, nº 1 e 2.

[50] Disponível: http://www2.icao.int/en/leb/List%20of%20Parties/Tokyo_EN.pdf.

Esta Convenção não menciona actos que possam ser qualificados como actos terroristas ou praticados por terroristas, antes qualifica esses comportamentos como “infracções”.

- Convenção de Haia: Convenção para a Repressão da Captura Ilícita de Aeronaves, assinada em Haia, em 16 de Dezembro de 1970[51], foi também executada no âmbito da ICAO, tendo sido aprovada através do Decreto nº 386/72, de 12 de Outubro de 1972.

O alcance desta convenção é idêntico ao da Convenção de Tóquio, mas a diferença reside no facto de visar a repressão penal contra os actos cometidos a bordo de aeronaves.

- Convenção de Montreal: Convenção para a Supressão de Actos Ilícitos contra a Segurança da Aviação Civil, assinada em 23 de Setembro de 1971,[52] similarmente elaborada no âmbito da ICAO, foi aprovada pelo Decreto nº 451/72, de 14 de Novembro de 1972.

O âmbito desta convenção é análogo ao das duas anteriores, contudo, os ilícitos estendem-se a outros actos e não somente à captura de aeronaves.

- Convenção sobre Prevenção e Repressão de Crimes contra Pessoas gozando de Protecção Internacional, incluindo os Agentes Diplomáticos: adoptada em Nova Iorque, em 14 de Dezembro de 1973,[53] aprovada pela Assembleia da República através da Resolução nº 20/94, de 5 de Maio.

Contém uma reserva no Artigo 2 º: “Portugal não extradita por facto punível com pena de morte ou com pena de prisão perpétua segundo a lei do Estado requerente nem por infracção a que corresponda medida de segurança com carácter perpétuo”.

Esta convenção visou essencialmente dois objectivos: a criação de um sistema de cooperação e troca de informações de modo a prevenir e evitar homicídios, raptos ou atentados contra pessoas que gozem do direito de protecção internacional e ainda, adoptar normas de carácter repressivo que

[51] Disponível: http://www2.icao.int/en/leb/List%20of%20Parties/Hague_EN.pdf.
[52] Disponível: http://www2.icao.int/en/leb/List%20of%20Parties/Mtl71_EN.pdf.
[53] Disponível: http://untreaty.un.org/cod/avl/pdf/ha/cppcipp/cppcipp_e.pdf.

obrigam os Estados a adoptar normas sancionatórias, bem como, instrumentos que garantam a aplicação dessas penas.

- Convenção Internacional contra a Tomada de Reféns: assinada em Nova Iorque, em 17 de Dezembro de 1979,[54] foi aprovada pela Assembleia da República através da Resolução nº 3/84, de 8 de Fevereiro.

A organização deste texto é idêntica à da Convenção anterior e similarmente são adoptadas medidas destinadas a prevenir a tomada de reféns e normas penais para repressão penal destes actos.

- Convenção sobre a Protecção Física de Materiais Nucleares: assinada em Viena e Nova Iorque, em 26 de Março de 1980,[55] foi aprovada pela Assembleia da República através da Resolução nº 7/90, de 15 de Março.

Esta convenção não foca directamente o terrorismo ou actos terroristas, mas sim a segurança na utilização, importação, exportação e transporte de materiais nucleares, de acordo com o que está contido nos Artigos 3º, 4º e 5º.

- Protocolo para a Repressão de Actos Ilícitos de Violência nos Aeroportos ao Serviço da Aviação Civil Internacional: complementar relativamente à Convenção de Montreal, foi assinado em Montreal, em 24 de Fevereiro de 1988,[56] igualmente no âmbito da ICAO, foi aprovado pela Assembleia da República através da Resolução nº 32/98, de 17 de Junho.

As alterações fundamentais que apresenta dizem respeito ao melhoramento da noção de infracção penal, englobando as agressões contra pessoas ou instalações e aeronaves em aeroportos.

- Convenção para a Supressão de Certos Actos Ilícitos contra a Segurança da Navegação Marítima: assinada em Roma, em 10 de Março de 1988,[57] foi realizada no âmbito da Organização Marítima Internacional, tendo sido

[54] Disponível: http://www.unodc.org/documents/treaties/Special/1979%20International%20Convention%20against%20the%20Taking%20of%20Hostages.pdf.
[55] Disponível: http://www.iaea.org/Publications/Documents/Infcircs/Others/inf274r1.shtml.
[56] Disponível: http://www.icao.int/secretariat/legal/List%20of%20Parties/VIA_EN.pdf.
[57] Disponível: http://treaties.un.org/doc/db/Terrorism/Conv8-english.pdf.

aprovada pela Assembleia da República através da Resolução nº 51/94 de 12 de Agosto.

Esta convenção não respeita directamente a actos de terrorismo, no entanto estão comtemplados nas sanções penais previstas. Por exemplo, refere quem "destrua um navio, ou cause avaria ao mesmo", de acordo com o que nos diz o Artigo 5º.

- Protocolo Adicional para a Supressão de Actos Ilícitos contra a Segurança das Plataformas Fixas Localizadas na Plataforma Continental: assinado em Roma, em 10 de Março de 1988,[58] foi aprovado e ratificado na mesma data da Convenção para a Supressão de Certos Actos Ilícitos contra a Segurança da Navegação Marítima e foi igualmente realizado no âmbito da Organização Marítima Internacional.

Este acordo distende normas da Convenção para a Supressão de Certos Actos Ilícitos contra a Segurança da Navegação Marítima às infracções aqui previstas, que sejam levadas a cabo contra plataformas fixas.

- Convenção sobre a Marcação dos Explosivos de Plástico para Efeitos de Detecção: foi assinada em Montreal, em 1 de Março de 1991,[59] também no âmbito da ICAO, foi aprovada dez anos depois, pela Assembleia da República através da Resolução nº 52/2002 de 2 de Agosto.

Somente indirectamente abarca actos relativos ao terrorismo. Visou essencialmente proibir o fabrico de explosivos não marcados, conforme o Artigo II, permitindo que aqui se integrem comportamentos que nada têm a ver com a prática de actos terrorismo.

- Convenção Internacional para a Repressão de Atentados Terroristas à Bomba: assinada em Nova Iorque, em 15 de Dezembro de 1997,[60] foi adoptada pela Assembleia Geral da ONU em 15 de Dezembro de 1997 e aprovada pela Assembleia da República através da Resolução nº 40//2001, de 25 de Junho.

[58] Disponível: http://treaties.un.org/doc/db/Terrorism/Conv9-english.pdf.
[59] Disponível: http://legacy.icao.int/icao/en/leb/MEX.pdf.
[60] Disponível: http://www.un.org/law/cod/terroris.htm.

Esta convenção já se refere directamente a actos terroristas, contudo não regula os atentados terroristas, mas apenas as agressões efectuadas por meio de bombas.

Visa a prevenção e repressão de comportamentos, configurando como crime determinados actos.

Menciona já as infra-estruturas, dando a sua noção no Artigo 1º, nº 2: "O termo «infra-estruturas» designa qualquer instalação pública ou privada que providencie ou distribua serviços de utilidade pública, tais como água, esgotos, energia, combustível ou comunicações". O Artigo 2º, nº 1, criminaliza os comportamentos de quem cometer:

> *"…an offence within the meaning of this Convention if that person unlawfully and intentionally delivers, places, discharges or detonates an explosive or other lethal device in, into or against a place of public use, a State or government facility, a public transportation system or an infrastructure facility:*
> *(a) with the intent to cause death or serious bodily injury; or*
> *(b) with the intent to cause extensive destruction of such a place, facility or system, where such destruction results in or is likely to result in major economic loss.*"

- Convenção Internacional para a Eliminação do Financiamento do Terrorismo: assinada em Nova Iorque, em 9 de Dezembro de 1999,[61] foi adoptada pela Assembleia Geral da ONU em 9 de Dezembro de 1999, tendo a Assembleia da República aprovado esta convenção através da Resolução nº 51/2002 de 2 de Agosto.

Esta convenção incide directamente no combate ao terrorismo, mas apenas no que diz respeito ao financiamento de organizações terroristas. De acordo com o Artigo 2º, nº 3, a infracção que se proíbe é a obtenção de financiamento para uma organização que desenvolva acções terroristas, mesmo que o financiamento em causa seja posteriormente utilizado directamente para a prossecução dos fins ilícitos.

São puníveis: a tentativa, as condutas que contribuam para a obtenção dos financiamentos, a cumplicidade na obtenção dos financiamentos, a

[61] Disponível: http://www.un.org/law/cod/finterr.htm.

organização ou o incitamento de terceiros à prática das infracções previstas, conforme os nºs 4 e 5 do Artigo 2º.

No Artigo 8º, estabelecem-se normas para a identificação e apreensão de fundos utilizados para os propósitos comtemplados. Estes fundos e meios financeiros podem ser aplicados numa compensação concedida por danos sofridos pelas vítimas de actos terroristas.

De acordo com o Artigo 18º, institui-se a obrigatoriedade de proibição de actividades de organizações ou pessoas que encorajem, instiguem ou organizem actos conformáveis com as infracções da convenção, no território dos Estados que dela fazem parte.

Conjuntamente determina-se a adopção de acções que obriguem à utilização de mecanismos para a detecção de contas bancárias ou transacções suspeitas por instituições financeiras. Não se estabelece a obrigatoriedade de comunicar às autoridades certas transacções que, pela sua complexidade, configurem infracções de acordo com o estipulado na convenção, mas apenas a possibilidade de criar essa obrigatoriedade. Igualmente se contempla como possibilidade a obrigação das instituições financeiras preservarem os registos das transacções realizadas por um período de cinco anos.

Ao nível das Nações Unidas, as resoluções do Conselho de Segurança no âmbito das "medidas para eliminar o terrorismo internacional", a Resolução 1269 (1999) e a Resolução 1368 (2001), comprovavam que não tem sido possível obter consenso, para uma resposta global ao terrorismo. Acresce que o carácter ad hoc do Comité criado por esta resolução e o facto de o escopo do Conselho de Segurança ser a manutenção da paz e segurança internacionais, de acordo com o que nos diz o Capítulo VII da Carta das Nações Unidas, a nova comissão parece ter assim, poderes limitados.

Após os ataques do 11 de Setembro e no seguimento da Resolução do Conselho de Segurança 1373 (2001) de 28 de Setembro,[62] onde se reafirmam as Resoluções 1269 (1999) e a Resolução 1368 (2001), foi decidido o estabelecimento de um Comité contra o terrorismo (*Counter-Terrorism Committee*), com o objectivo de certificar a aplicação da Resolução 1373

[62] Disponível: http://www.un.org/News/Press/docs/2001/sc7158.doc.htm.

(2001). Após esta, foi ainda emanada a Resolução 1377 (2001) de 12 de Novembro,[63] na qual é feito um apelo a todos os países para que reforcem os seus intentos na eliminação do terrorismo internacional.

A Resolução 1373 (2001), institui vários princípios na luta contra o terrorismo relativamente ao financiamento, controlo de armas, troca de informações, criminalização de actos terroristas, cooperação judiciária e controlo policial.

No Relatório "*A more secure world: our shared responsability",* de 2004,[64] que coloca o seu enfoque na regulamentação convencional do terrorismo, é referido que muitos Estados não ratificaram as convenções e muitos outros igualmente não adoptaram as medidas constantes das mesmas, que os meios empregues na luta contra o financiamento de organizações terroristas são desadequados, sugere-se que os Estados-membros procedam à ratificação das convenções adoptadas, inclusivamente as oito recomendações da OCDE, em relação ao financiamento de organizações terroristas. Mas, principalmente, é mencionado que um dos problemas principais é a dificuldade em chegar a uma noção de terrorismo que possibilite a concordância entre os Estados, sendo considerado forçoso a obtenção de acordo.

As recomendações deste relatório quanto à obtenção de uma noção de terrorismo deverão incluir:

- O reconhecimento de que o uso da força por um Estado contra alvos civis seja regulado pela Convenção de Genebra e outros instrumentos internacionais e pode constituir um crime de guerra ou um crime contra a humanidade;
- O reconhecimento dos actos previstos nas doze convenções referidas como actos terroristas e crimes, de acordo com o direito internacional, bem como, a proibição do terrorismo em tempo de guerra de acordo com a Convenção de Genebra e os seus protocolos;
- Uma referência às definições que constam na Convenção Internacional para a Eliminação do Financiamento do Terrorismo e da Resolução do Conselho de Segurança nº 1566 (2004)[65];

[63] Disponível: http://www.un.org/News/Press/docs/2001/sc7207.doc.htm.
[64] Disponível: http://www.un.org/secureworld/report.pdf.
[65] Disponível: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/542/82/PDF/N0454282.pdf?OpenElement.

- O terrorismo deverá ser definido da seguinte forma:

"…*any action, in addition to actions already specified by the existing conventions on aspects of terrorism, the Geneva Conventions and Security Council resolution 1566 (2004), that is intended to cause death or serious bodily harm to civilians or non-combatants, when the purpose of such an act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act*".

Deve nesta altura dizer-se que, a viagem legislativa internacional com o objectivo de combater o terrorismo iniciou-se em 1937, quando a Liga das Nações tentou definir e tipificar o terrorismo. Contudo, o projecto não foi aprovado. (Alex P. Schmid, 2011).

A primeira Convenção adoptada a nível internacional surge em 1963, vinte e seis anos após a proposta da Liga das Nações. Contudo, apenas em 1997, sessenta anos depois, há referência explícita do termo terrorismo no título da Convenção Internacional para a Repressão de Atentados Terroristas à Bomba.

Nenhum destes textos adoptou uma definição de terrorismo, tendo sido elaborados sem que exista uma definição académica ou legal de terrorismo consensual ao nível internacional.

Pode nesta altura dizer-se, setenta e cinco anos depois, que continua a discussão sobre o combate ao terrorismo, sem que a comunidade internacional detenha uma noção de terrorismo.

Relativamente ao ciberterrorismo, quanto à obtenção de legislação ao nível internacional, parece-nos que a viagem também será longa. Não se vê assim, como se pode obter resultados no combate ao fenómeno do ciberterrorismo.

Não existe uma convenção global sobre o terrorismo que unifique todos estes textos, de modo a eliminar as suas lacunas.

As Nações Unidas possuem um Centro de Prevenção do Crime Internacional (*Centre for International Crime Prevention*), sedeado em Viena,

cujo mandato inclui o combate ao terrorismo, porém ao que tudo indica tem estado inactivo.

A Interpol, apesar de ter criado um Grupo Misto Especializado para a luta contra o terrorismo, parece também não possuir grandes capacidades, nem ter obtido grandes resultados.

4.2 - Quadro normativo regional

Organização para a Segurança e Cooperação na Europa (OSCE)

No âmbito desta organização, existe a:

- Carta da OSCE sobre Prevenção e Combate ao Terrorismo[66] que foi adoptada em reunião do Conselho de Ministros, em 6 e 7 de Dezembro de 2002. Consiste numa declaração de um grupo amplo de Estados europeus, na sequência dos atentados de 11 de Setembro de 2001. Neste documento é referido principalmente que:

  - Se condenam todos os tipos de terrorismo;
  - Se rejeita a identificação do terrorismo com qualquer tipo de nacionalidade ou religião;
  - Há necessidade de concertação e cooperação entre os Estados;
  - O terrorismo, a assistência ao terrorismo e os respectivos financiamentos, planeamento ou incitamento são contrários ao direito internacional;
  - É preciso proteger os direitos fundamentais e, em especial, o direito à vida das potenciais vítimas de actos terroristas;
  - Serão tomadas medidas ajustadas para negar asilo político a quem tenha participado, planeado ou financiado actos qualificáveis como terrorismo;
  - As convenções das Nações Unidas e as resoluções do Conselho de Segurança, em especial, a Resolução 1373 (2001) consideram-se os mecanismos legais principais ao nível internacional, no âmbito da luta contra o terrorismo;

[66] Disponível: http://www.osce.org/odihr/16609.

- É fundamental o controlo das armas, o desarmamento e a não-proliferação na diminuição do risco de actos terroristas.

Outros textos relevantes são a Decisão sobre o Combate ao Terrorismo[67] e o Plano de Acção de Bucareste Para o Combate ao Terrorismo[68], adoptados em reunião do Conselho de Ministros da OSCE, em Bucareste, em 3 e 4 de Dezembro de 2001, que versam essencialmente sobre acções a tomar com a finalidade de determinar um objectivo geral para as medidas a serem levadas a cabo pelos Estados-Membros no combate ao terrorismo.

Conselho da Europa

No campo de actuação desta organização, foi assinada a:

- Convenção Europeia para a Supressão do Terrorismo: assinada em Estrasburgo, em 27 de Janeiro de 1977,[69] tendo sido aprovada, quatro anos após, pela Assembleia da República pela Lei nº 19/81 de 18 de Agosto de 1981, e após ratificada.

Foi feita uma reserva no Artigo 2º, na qual é dito que Portugal não aceitará a extradição como Estado requisitado quando as infracções sejam punidas com a pena de morte ou com penas ou medidas de segurança privativas da liberdade com carácter perpétuo no Estado requisitante.

Não refere em que consiste um acto de terrorista. No entanto, menciona que os Estados-participantes admitem que as infracções previstas no seu Artigo 1º não são consideradas infracções de carácter político no caso de extradição. Este Artigo 1º elenca em seis alíneas, actos e infracções já constantes da Convenção de Haia, na Convenção para a Repressão de Actos Ilícitos Dirigidos contra a Segurança da Aviação Civil e outras como por exemplo "…um ataque contra a vida, a integridade física ou a liberdade das pessoas que gozem de protecção internacional, inclusive os agentes diplomáticos", incluindo a tentativa e a participação.

[67] Disponível: http://www.osce.org/mc/22645.
[68] Disponível: http://www.osce.org/atu/42524.
[69] Disponível: http://conventions.coe.int/Treaty/en/Treaties/Html/090.htm.

- Convenção da Organização dos Estados Americanos para a Prevenção e a Punição de Actos de Terrorismo sob a Forma de Crimes contra as Pessoas e Extorsão que Sejam de Relevância Internacional: assinada em Washington, em 2 de Fevereiro de 1971[70].

De acordo com o Artigo 1º, este acordo teve como objectivo instituir uma obrigação geral de cooperação entre os Estados-partes, de modo a possibilitar a prevenção e punição de actos de terrorismo, tais como raptos, assassinato e outros atentados à vida ou à integridade pessoal. Os destinatários destas medidas são aqueles que são vítimas de actos terroristas, mas somente aqueles a quem um Estado tenha a obrigação de conceder protecção especial, ao abrigo do direito internacional.

Ainda no âmbito da Organização dos Estados Americanos, existem dois documentos:

- Declaração de Lima para Prevenção, Combate e Eliminação do Terrorismo[71]: assinada na reunião de Lima da Conferência Inter-Americana Especializada sobre Terrorismo, em 26 de Abril de 1996. Sendo esta apenas uma declaração de várias intenções, com enfoque na vertente de crescimento sustentado.
- Compromisso de Mar del Plata[72], aprovado na reunião de 23 e 24 de Novembro de 1998 da II Conferência Inter-Americana Especializada sobre Terrorismo. Este texto também consiste numa declaração de intenções similar ao anterior.

- Convenção da Associação do Sul da Ásia para a Cooperação Regional (SAARC) sobre a Supressão do Terrorismo, adoptada em Kathmandu, em 4 de Novembro de 1987[73].

Tem como objectivo essencialmente, agilizar a cooperação através da regulação dos pedidos de extradição entre Estados contratantes.

- Convenção Árabe sobre a Supressão do Terrorismo: assinada no Cairo, em 22 de Abril de 1998[74].

[70] Disponível: http://treaties.un.org/doc/db/Terrorism/english-18-7.pdf.
[71] Disponível: http://www.oas.org/juridico/english/Docu6.htm.
[72] Disponível: http://www.oas.org/juridico/english/docu1.htm.
[73] Disponível: http://www.saarc-sec.org/areaofcooperation/detail.php?activity_id=21.
[74] Disponível: http://www.al-bab.com/arab/docs/league/terrorism98.htm.

Foi o primeiro instrumento de combate ao terrorismo realizado pelos Estados-membros da Liga Árabe, possui uma definição de terrorismo no Artigo 1º, nº 2:

> "*Any act or threat of violence, whatever its motives or purposes, that occurs in the advancement of an individual or collective criminal agenda and seeking to sow panic among people, causing fear by harming them, or placing their lives, liberty or security in danger, or seeking to cause damage to the environment or to public or private installations or property or to occupying or seizing them, or seeking to jeopardize a national resources*".

Ainda define, no nº 3, do Artigo 1º:

> "*Terrorist offence: Any offence or attempted offence committed in furtherance of a terrorist objective in any of the Contracting States, or against their nationals, property or interests, that is punishable by their domestic law. The offences stipulated in the following conventions, except where conventions have not been ratified by Contracting States or where offences have been excluded by their legislation, shall also be regarded as terrorist offences*..." fazendo referência, quanto a estas ofensas, às incluídas em seis instrumentos internacionais, entre os quais as Convenções de Tóquio, Haia e Montreal".

Estabelece medidas preventivas e repressivas, no Artigo 3º e contempla a cooperação entre Estados e a troca de informações, entre outros aspectos.

- Convenção da Organização da Conferência Islâmica sobre o Combate ao Terrorismo Internacional: adoptada na capital de Burkina Faso, Ouagadougou, em 1 de Julho de 1999[75].

Esta Convenção define terrorismo no Artigo 1º, nº 2:

> "*Terrorism" means any act of violence or threat thereof notwithstanding its motives or intentions perpetrated to carry out an individual or collective criminal plan with the aim of terrorizing people or threatening to harm them or imperiling their lives, honor, freedoms, security or rights or exposing the environment or*

[75] Disponível: http://www.oicun.org/7/38/.

any facility or public or private property to hazards or occupying or seizing them, or endangering a national resource, or international facilities, or threatening the stability, territorial integrity, political unity or sovereignty of independent States".

No nº 3 do mesmo Artigo, define crime terrorista:

"*Terrorist Crime" means any crime executed, started or participated in to realize a terrorist objective in any of the Contracting States or against its nationals, assets or interests or foreign facilities and nationals residing in its territory punishable by its internal law*".

Por fim, no nº 4 é dito que os crimes constantes de determinadas convenções, entre as quais a Convenção de Haia e Montreal, são considerados crimes terroristas, ressalvando aqueles que não são considerados como tal nas suas legislações internas, excluindo ainda os Estados que não ratificaram as convenções mencionadas.

No Artigo 3º, são enumeradas uma série de medidas de prevenção e repressão na luta contra o terrorismo.

- A Convenção da Organização dos Estados Africanos sobre a Prevenção e o Combate ao Terrorismo, assinada em Argel, em 14 de Julho de 1999[76].

Inclui uma definição de acto terrorista no Artigo 1º, nº 3:

"Terrorist act" means:

(a) any act which is a violation of the criminal laws of a State Party and which may endanger the life, physical integrity or freedom of, or cause serious injury or death to, any person, any number or group of persons or causes or may cause damage to public or private property, natural resources, environmental or cultural heritage and is calculated or intended to:

(i) intimidate, put in fear, force, coerce or induce any government, body, institution, the general public or any segment thereof, to do or abstain from doing any act, or to adopt or abandon a particular standpoint, or to act according to certain principles; or

(ii) disrupt any public service, the delivery of any essential service to the public

[76] Disponível: http://treaties.un.org/doc/db/Terrorism/OAU-english.pdf.

or to create a public emergency; or

(iii) create general insurrection in a State;

(b) any promotion, sponsoring, contribution to, command, aid, incitement, encouragement, attempt, threat, conspiracy, organizing, or procurement of any person, with the intent to commit any act referred to in paragraph (a) (i) to (iii). acordo com certos princípios; ou (ii) romper qualquer serviço público, a entrega de qualquer serviço essencial ao público ou criar uma emergência pública; ou (iii) criar uma insurreição geral em um Estado. (b) Qualquer promoção, patrocínio, contribuição, comando, ajuda, incitação, encorajamento, tentativa, ameaça, conspiração, organização ou aliciamento de qualquer pessoa com o intuito de cometer qualquer ato referido nos parágrafos (i) e (iii)".

No Artigo 2º criminalizam-se os actos terroristas praticados pelos Estados-partes.

No Artigo 4º e seguintes são instituídas normas sobre cooperação.

No Artigo 6º é estabelecida a respectiva competência para o julgamento de actos terroristas.

A extradição é contemplada no Artigo 8º e seguintes, bem como se regula a investigação criminal, fora do território do Estado onde essa investigação se realiza, no Artigo 14º e seguintes.

- Tratado para Cooperação entre os Estados-Membros da Comunidade de Estados Independentes (CEI) no Combate ao Terrorismo, assinado em Minsk, em 4 de Junho de 1999[77].

Este Tratado integra as definições de terrorismo e terrorismo tecnológico no Artigo 1º:

"*Terrorism" - an illegal act punishable under criminal law committed for the purpose of undermining public safety, influencing decision-making by the authorities or terrorizing the population, and taking the form of: Violence or the threat of violence against natural or juridical persons;*

Destroying (damaging) or threatening to destroy (damage) property and other material objects so as to endanger people's lives;

[77] Disponível: http://treaties.un.org/doc/db/Terrorism/csi-english.pdf.

Causing substantial harm to property or the occurrence of other consequences dangerous to society;

Threatening the life of a statesman or public figure for the purpose of putting an end to his State or other public activity or in revenge for such activity;

Attacking a representative of a foreign State or an internationally protected staff member of an international organization, as well as the business premises or vehicles of internationally protected persons;

Other acts classified as terrorist under the national legislation of the Parties or under universally recognized international legal instruments aimed at combating terrorism;

"*Technological terrorism" - the use or threat of the use of nuclear, radiological, chemical or bacteriological (biological) weapons or their components, pathogenic micro-organisms, radioactive substances or other substances harmful to human health, including the seizure, putting out of operation or destruction of nuclear, chemical or other facilities posing an increased technological and environmental danger and the utility systems of towns and other inhabited localities, if these acts are committed for the purpose of undermining public safety, terrorizing the population or influencing the decisions of the authorities in order to achieve political, mercenary or any other ends, as well as attempts to commit one of the crimes listed above for the same purposes and leading, financing or acting as the instigator, accessory or accomplice of a person who commits or attempts to commit such a crime;*

"Facilities posing an increased technological and environmental danger" - enterprises, installations, plant and other facilities whose inoperability may lead to loss of human life, the impairment of human health, pollution of the environment or destabilization of the situation in a given region or a given State as a whole;

Define normas relativas à cooperação e troca de informações na luta contra o terrorismo.

A novidade deste acordo está nos Artigos 12º a 15º, onde é regulada a transposição de fronteiras por forças anti-terroristas entre os Estados-Membros.

4.3 – Legislação da União Europeia

Ao nível da União Europeia existem dois instrumentos principais, no plano da luta contra o terrorismo:

- Decisão-Quadro 2002/475/JAI, do Conselho, de 13 de Junho de 2002[78].

No Artigo 1º é adoptada uma noção de actos terroristas:

> "…aqueles que pela sua natureza ou pelo contexto em que forem cometidos, sejam susceptíveis de afectar gravemente um país ou uma organização internacional, quando o seu autor os pratique com o objectivo de intimidar gravemente uma população" ou "constranger indevidamente os poderes públicos, ou uma organização internacional, a praticar ou a abster-se de praticar qualquer acto, ou destabilizar gravemente ou destruir as estruturas fundamentais políticas, constitucionais, económicas ou sociais de um país, ou de uma organização internacional".

As várias alíneas deste artigo 1º aludem, depois, aos vários comportamentos que, enquadrados com a definição referida, configuram actos terroristas.

O principal objectivo deste texto é a criminalização das condutas previstas, não obstante seja referido o termo "infracção".

- Posição Comum 2001/931/PESC, do Conselho, de 27 de Dezembro de 2001,[79] respeitante à aplicação de medidas específicas de combate ao terrorismo.

Este texto visa a concretização das medidas previstas na Resolução do Conselho de Segurança da Organização das Nações Unidas 1373 (2001). Pretende-se a elaboração de uma lista de pessoas, grupos e entidades envolvidos em actos terroristas, de modo a poder aplicar-se medidas de congelamento de fundos e activos financeiros no âmbito da luta contra o

[78] Disponível: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:164:0003:0007:PT:PDF.
[79] Disponível: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:344:0093:0096:PT:PDF.

financiamento do terrorismo. Esta lista será revista regularmente, pelo menos, de seis em seis meses, de acordo com o estipulado no Artigo 6º/1.

Nesta Posição Comum, as "pessoas, grupos e entidades envolvidas em actos terroristas" são aquelas:

> "…que pratiquem ou tentem praticar actos terroristas, neles participem ou os facilitem;" "grupos e entidades directa ou indirectamente possuídas ou controladas por essas pessoas; e pessoas, grupos e entidades que actuem em nome ou sob a orientação dessas pessoas,
> grupos e entidades, incluindo fundos obtidos a partir de bens directa ou indirectamente possuídos ou controlados por essas pessoas e por pessoas, grupos e entidades a elas associadas, ou provenientes desses bens."

Quanto ao "acto terrorista" é considerado:

> "…um acto intencional que, dada a sua natureza ou o seu contexto, possa causar sérios danos a um país ou a uma organização internacional, definido como infracção na legislação nacional e cometido com o intuito de:…", sendo as intenções descritas em três números e onze alíneas.

4.4 - Direito interno

No que respeita à prevenção e combate do terrorismo na legislação interna, foi apenas em 2003 que se aprovou a Lei nº 52/2003, de 22 de Agosto,[80] a chamada Lei de Combate ao Terrorismo, na sequência da mencionada aprovação da Decisão-Quadro 2002/475/JAI, do Conselho, de 13 de Junho de 2002.

Com a aprovação da Lei de Combate ao Terrorismo, foram revogados os Artigos 300º e 301º do Código Penal, passando assim, estranhamente, a estar consagrada numa lei avulsa, a tipificação do crime de terrorismo.

A acrescer, no Artigo 7º deste diploma, é dito que se aplica subsidiariamente o disposto no Código Penal "e respectiva legislação

[80] Disponível: http://www.dre.pt/pdf1sdip/2003/08/193A00/53985400.PDF.

complementar". Contudo, esta mesma Lei é "legislação complementar", o que não invalida que ainda seja criada mais legislação avulsa.

A Lei nº 52/2003, de 22 de Agosto, contém onze artigos e separa quatro conceitos, nas epígrafes dos artigos 2º, 3º, 4º e 5º: "organizações terroristas", "outras organizações terroristas", "terrorismo" e "terrorismo internacional".

Verifica-se nesta Lei um agravamento das molduras penais, excepto quanto aos actos preparatórios da constituição da organização terrorista, que manteve a pena de prisão de um a oito anos.

Desaparece o crime de "sabotagem", apenas se referindo no Artigo 2º, nº 1, d): "actos que destruam ou que impossibilitem o funcionamento ou desviem dos seus fins normais, definitiva ou temporariamente, total ou parcialmente, meios ou vias de comunicação, instalações de serviços públicos ou destinadas ao abastecimento e satisfação das necessidades vitais da população".

No Artigo 8.º, consagra-se a aplicação da lei interna, caso ocorram actos cometidos fora do território nacional.

No Artigo 9º é alterado o Artigo 1º, nº 2, a) do Código de Processo Penal, em que se estatui uma remissão para a Lei nº 52/2003, de 22 de Agosto, no entanto, apenas remete para os Artigos 2º e 3º. Assim, os Artigos 4º e 5º que também estabelecem punições ao terrorismo ficam fora da remissão.

As alterações mais relevantes residem na destrinça entre terrorismo interno e internacional, nos Artigos 4º e 5º e a responsabilização penal das pessoas colectivas, prevista no Artigo 6º.

Faz referência, tal como os Artigos 300º e 301º do Código Penal ao uso de energia nuclear, armas de fogo, explosivos, entre outros, porém acrescenta as armas químicas e biológicas.

Foi estabelecida a punição da pessoa colectiva com um mínimo de apenas 500 Euros, de acordo com o Artigo 6º, nº 5, porém esta Lei não especifica quem devem ser consideradas como "pessoas colectivas ou equiparadas".

Embora seja possível dizer que o legislador visou aperfeiçoar o combate ao terrorismo, tanto internamente como transnacionalmente, é provável que

com esta Lei nº 52/2003, de 22 de Agosto, não esteja garantida uma tipificação legal de terrorismo de uma forma que não haja espaço para dúvidas.

Deve, portanto, concluir-se, que ao nível regional foi possível definir terrorismo em três acordos, assinados antes do 11 de Setembro de 2001, são eles:

- A Convenção da Organização da Conferência Islâmica sobre o Combate ao Terrorismo Internacional;
- A Convenção Árabe sobre a Supressão do Terrorismo;
- O Tratado para Cooperação entre os Estados-Membros da Comunidade de Estados Independentes (CEI) no Combate ao Terrorismo.

Quanto à Convenção da Organização dos Estados Africanos sobre a Prevenção e o Combate ao Terrorismo, a mesma definiu acto terrorista.

No entanto, a legislação internacional deveria convergir com a regional.

Relativamente ao direito da União Europeia, embora exista uma Posição Comum desde 2001, que tem o objectivo de materializar as medidas previstas na Resolução 1373 (2001) do Conselho de Segurança da ONU, relativamente à definição de terrorismo e acto terrorista, o combate ao terrorismo não teve as consequências desejadas pois a ameaça do terrorismo continua a ser "…uma das maiores ameaças à nossa subsistência".

Quanto ao direito interno, a colocação da regulação do terrorismo foi realizada através de uma lei avulsa, ao que parece insuficiente e ineficaz para dar resposta caso haja um ataque terrorista e não contemplou o fenómeno do ciberterrorismo, à semelhança de outros Estados.

Todos estes factos tornam fácil a percepção de que no "Ocidente" a legislação é contraditória, insuficiente, logo ineficaz, permitindo um campo de actuação cómodo para a prática terrorista.

Capítulo V – Conclusões

O que significa ciberterrorismo?

Tendo em consideração as noções de Mark Pollitt (1997), do *National Infrastructure Protection Center* (2003) e de Dorothy Denning (2001), da sua junção resultam as seguintes características:

- Ataque criminoso premeditado contra informações, dados, sistemas e programas de computadores;
- Intenções políticas, económicas, religiosas ou ideológicas;
- Ataque levado a cabo por meio de computadores;
- O resultado é a violência, ofensas físicas, morte ou destruição de propriedade, incluindo as infra-estruturas críticas desde que suficientemente grave e não apenas uma disrupção de serviços não essenciais;
- Contra alvos não combatentes, por grupos regionais ou locais, ou agentes clandestinos;
- Gerar medo ou terror com o objectivo de coagir um governo a alterar as suas políticas.

O ciberterrorismo, consiste assim numa ameaça, que de acordo com Bonnie Adkins (2001) e Michael Ronczkowski (2011) pode evoluir, e numa escalada de conflito, coloca-se no patamar imediatamente anterior a uma ciberguerra.

A diferenciação entre terrorismo e ciberterrorismo justifica-se?

O terrorismo possui um campo de estudos autónomo, porém a não existência de acordo ao nível internacional quanto às concepções académica e legal, impede em consequência um consenso quanto à própria noção de ciberterrorismo.

Os terroristas possuem uma nova ferramenta de poder, mas os próprios Estados utilizam estes actores não estatais para efectuar ciberataques, assim, as demonstrações terroristas alteraram-se com o surgimento das novas tecnologias, as operações psicológicas e políticas e a subversão de Estados, organizações e movimentos internacionais constituem as singularidades do contexto estratégico actual. Hoje, os núcleos de poder tradicionais já são

também acessíveis a grupos privados e é inegável que a Internet veio exponenciar a possibilidade da concretização de um ciberataque terrorista, bem como veio permitir a descentralização da liderança das organizações terroristas. Os terroristas fazem assim, uso da dependência das sociedades desenvolvidas relativamente ao ciberespaço.

As armas cibernéticas similarmente às utilizadas em conflitos tradicionais com armas de fogo, podem possuir capacidade letal. É o caso das armas lógicas, que visam atacar a lógica operacional dos sistemas de informação, introduzindo atrasos ou procedimentos indesejados no seu funcionamento, através de vírus informáticos, bombas lógicas, *Back Doors* e *Trap Doors*, *Worms*, cavalos de Tróia, *virtual sit-ins* e *blockades*, *e-mail bombs* ou DDoD's. Estes tipos de armas permitem desligar e destruir sistemas de transmissão de dados e *hardware*.

Contudo, o fenómeno do ciberterrorismo na sua essência consistiu na transposição das práticas terroristas para o quinto espaço de actuação, o ciberespaço. Não deixou por isso, de se considerar terrorismo. Os alvos, as motivações e os objectivos essenciais são os mesmos: vítimas inocentes, motivações políticas ou ideológicas com o intuito de provocar medo ou terror. Embora não tenha ainda ocorrido um ciberataque terrorista, é inegável que a probabilidade do surgimento desse tipo de ataques já não é tão remota, depois dos vírus *Blaster* do surgimento do *worm Stuxnet*.

Poderemos assim dizer, que não se justifica a diferenciação do ciberterrorismo para um campo autónomo do terrorismo.

Concretizou-se algum ciberataque terrorista ou suspeita-se da sua preparação?

De acordo com vasta literatura parece ser consensual que até aos dias de hoje não ocorreu nenhum ciberataque terrorista. Embora a Estónia tenha equiparado o ataque que sofreu em 2007, a um ataque terrorista, não foi considerado como tal, não havendo qualquer pronúncia sobre esta questão pelo Conselho de Segurança das Nações Unidas.

Relativamente ao "*Pearl Harbor* digital", que é referido sistematicamente por vários autores e pelos meios de comunicação dos Estados Unidos da

América, constituem referências a ataques hipotéticos, o que leva a que as ciberameaças não sejam avaliadas de uma forma realista, de modo a conduzir a soluções práticas. De acordo com Dorothy Denning (2012), apesar de haver referência num fórum *jihadista*, o *al-Shamukh*, a ataques contra sistemas SCADA, e apesar do *Stuxnet* ter possibilitado uma previsão do que poderá eventualmente acontecer, não considera a ameaça eminente, uma vez que ao que parece, a curto prazo, não haverá no campo do terrorismo, capacidade nem meios para levar a cabo ciberataques arrasadores.

Que medidas tomar para enfrentar o fenómeno?

O que a seguir expomos são apenas propostas genéricas. No entanto, se levadas a cabo de uma forma integrada e coordenada, englobando e analisando as especificidades dos aspectos relativos ao combate ao ciberterrorismo, poderão constituir um contributo a eventuais alterações normativas.

Embora haja entendimento relativamente à concepção de cibersegurança, uma vez que é mencionada na perspectiva da confidencialidade, acessibilidade e integridade da informação e dos sistemas de informação, na maioria das estratégias de cibersegurança existentes, estas mesmas estratégias, colocam o seu enfoque na consolidação dos mercados internos de cada país, não contemplando a segurança interna no seu delineamento. Como se verificou, Portugal não possui uma estratégia de cibersegurança, embora já tenham ocorrido iniciativas ad hoc e evidencia sinais do caminho para uma estratégia dispersa, não integrada, nem coordenada.

De acordo com o que percepcionamos, há insuficiência de legislação para responder às ciberameaças, no entanto, já há uma evolução para a área dos ciberconflitos.

Relativamente aos órgãos que poderiam ter um papel relevante para obtenção de acordos ao nível internacional, a União Europeia, a OSCE, o Conselho da Europa, a OTAN e a ONU, a sua acção é diminuta[81].

[81] Embora variável. Quanto a este ponto, ver, por todos, o trabalho de Armando Marques Guedes, intitulado "*The new geopolitical coordinates of cyberspace*", in Revista Militar, 2503/2504: 825-849, Lisboa, 2010.

O enquadramento normativo deverá assim, ser feito também numa perspectiva de segurança interna e defesa nacional e não somente económica, deve contemplar o ciberterrorismo, o contexto de conflitualidade da informação, o contexto assimétrico internacional, a transnacionalidade do terrorismo, as infra-estruturas críticas, quais as responsabilidades e atribuições das Forças Armadas e das Forças de Segurança, por forma a acautelar a coordenação e colaboração de todos os interessados e de forma a garantir a segurança nacional no ciberespaço. Contudo, tendo sempre em conta os interesses nacionais, sociais, a salvaguarda dos direitos, liberdades e garantias, a necessidade de modernização e promoção do desenvolvimento nacional, ou seja, não se limitar a uma visão securitária.

A cooperação das Forças Armada será uma ajuda valiosíssima, uma vez que possuem capital humano e capacidades. Deve delimitar-se muito bem o seu campo de intervenção.

O ciberterrorismo não deve ser separado do campo normativo do terrorismo.

Os requisitos técnicos devem ser aumentados, de modo a evitar eficazmente um eventual ataque cibernético.

Por último, a consciencialização para uma cultura de cibersegurança e para a consciencialização das ciberameaças, baseada na confiança e colaboração mútua entre Estado e cidadãos, poderá ser uma boa resposta a um combate sério e eficaz ao fenómeno do ciberterrorismo.

Em conclusão, o terrorismo pela sua complexidade e transnacionalidade tem sido estudado como um campo independente. No entanto, há setenta e cinco anos que a comunidade internacional não consegue obter consenso quanto à sua concepção, académica ou legal, tipologias, já para não mencionar quanto às motivações, actores, entre outros aspectos. Esta inexistência de concordância, vai permitindo a tortura, escravidão, genocídio, entre outras práticas, uma vez que não havendo cooperação ao nível internacional não é possível um combate eficaz ao fenómeno. A cooperação internacional é fundamental, uma vez que o fenómeno do terrorismo é transnacional, logo, a resposta tem que ser global.

O terrorismo tenderá a ser liderado, como tem acontecido pelo menos nos últimos quinze anos, pelo terrorismo religioso islâmico e esta ameaça, encaminha-nos para a chamada *4th generation warfare*. (Armando Marques Guedes, 2007).

Apesar dos estudos do terrorismo surgirem no âmbito da segurança nacional e interna, após os ataques de 11 de Setembro de 2001, não há ainda uma resposta global ao fenómeno do terrorismo, mas os nossos direitos, liberdades e garantias vão paulatinamente sendo restringidos em nome da segurança. As consequências da morte de Bin Laden ainda não se fizeram sentir.

Perspectivamos que teremos surpresas, dado o contexto actual global de crise financeira, económica e social, que estão a agravar as já existentes desigualdades na distribuição da riqueza, injustiça social, crescimento populacional e degradação ambiental. Todos estes factores são propulsores de violência e poderão "…finalmente despertar uma cólera apocalíptica com que o terrorismo global massacra inocentes…". (Adriano Moreira, 2011).

O Estado já não é o único detentor do uso exclusivo da força, bem como já não consegue há muito prover às necessidades básicas das suas populações. "Um Estado-nação impotente ou insuficientemente capacitado é pouco atraente."..."progressivamente reduzido às suas funções de uma esquadra de polícia…". (Zygmunt Bauman, 2009).

As sociedades actuais estruturadas em rede e globalizadas tornaram países e regiões, interdependentes. Esta globalização "…que, em relação à Europa, parece mais a definição de um ponto final na excepcionalidade, do que uma plataforma de arranque para a liderança de novos horizontes." (Adriano Moreira, 2011).

O ciberespaço e a Internet alteraram a configuração dos actores e a magnitude dos riscos. Os terroristas exploram agora este novo campo de forças assimétrico e os próprios Estados utilizam estes actores não estatais para efectuar ciberataques. O "*Wild Wild West*", é hoje um campo de batalha onde podem ser usadas armas cibernéticas com capacidade letal, por particulares e por Estados.

As infra-estruturas críticas digitais, vitais à subsistência de qualquer país, estão assim, vulneráveis a um qualquer ataque cibernético. A avaliação das

ameaças e a prevenção tem sido impossibilitada por divergências burocráticas. São sempre necessários estudos que demoram o tempo suficiente para que uma ameaça desapareça e surja outra.

A cultura institucional não tem permitido a cooperação entre forças de segurança, serviços de informação e militares. Contudo, este problema é denotado em todos os países, mas ao que parece também não tem solução.

A incapacidade de pensar estrategicamente fora dos parâmetros ocidentais, parece ter assolado o Ocidente, o que constitui uma desvantagem relativamente ao terrorismo.

A preocupação dos Estados devia ser a agregação dos seus cidadãos, mas ao contrário, o que se observa é a promoção da desunião. Não é possível assim, construir quaisquer estratégias ou políticas que tenham eficácia.

Todos estes aspectos, reflectem-se na quantidade enorme de legislação e acordos internacionais, tornando o quadro normativo num avolumado de diplomas que já demonstraram ser inadequados e ineficazes.

Nem a existência de uma "*Unrestricted Warfare*" mobilizou e agilizou uma resposta capaz ao ciberterrorismo, tendo já passado treze anos.

A viagem irá continuar e o caminho será ao que tudo indica, o mesmo.

Lista de definições

Backdoors: portas dos fundos, são programas de retorno a um computador comprometido, através de serviços criados ou modificados para este fim. Geralmente um atacante tenta garantir uma forma de voltar a um computador comprometido sem necessitar recorrer aos métodos utilizados na concretização da invasão. Na maioria dos casos, o propósito do atacante é poder regressar ao computador comprometido sem ser notado. (José Dinis, 2005).

Botnets: grupo de *bots* (diminutivo de robots), significa um conjunto de computadores comprometidos onde o *software* malicioso permanece em execução, sendo este normalmente instalado por meio de *downloads* que exploram as vulnerabilidades do navegador *web*, via *worms*, cavalos de Tróia (*Trojans*) ou *backdoors* com o objectivo de obter o controlo da máquina. (Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Ciberespaço: termo que resulta da união da palavra “cibernética”, a ciência que estuda os mecanismos de comunicação e de controlo nos organismos vivos e nas máquinas, e “espaço”. Foi utilizado pela primeira vez por um escritor de obras de ficção científica, o canadiano William Gibson no livro “*Neuromencer*”, em 1984 e passou depois a ser utilizado para descrever o espaço virtual relacionado com a *Internet*. Constitui o conjunto de todos os computadores, servidores, cabos de fibra óptica, redes de computadores e sistemas de computadores. (José Dinis, 2005 e Franklin D.Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Cracker: indivíduo que entra sem autorização num sistema ou rede de computadores para causar ameaça ou dano, normalmente confundido com um *hacker.* É um tipo de pirata informático. (José Dinis, 2005).

DDoS: *distributed denial-of-service*, é uma forma de sabotagem que consiste na sobrecarga de sítios da *Internet*, serviços ou sistemas, com milhares de solicitações por segundo até provocar a sua paralisação. Estas solicitações são executadas por vários computadores infectados que apenas aguardam a

ordem para execução. (José Dinis, 2005 e Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Cyberwar: refere-se à condução ou à preparação de operações de acordo com os princípios da era da informação, com objectivos disruptivos ou destrutivos de informação ou sistemas de comunicação. Baseia-se no conhecimento da cultura militar do adversário, ao mesmo tempo que se tem a noção da própria cultura, de modo a conhecer tudo sobre o mesmo, ou seja, obter a superioridade da informação, principalmente se existir assimetria. Envolve diversas tecnologias, recolha de informação, processamento e sua disseminação. (John Arquilla e David Ronfeldt, 2001, 2012).

Defacement: ataques realizados com o objectivo de modificar a página de um sítio na *Internet*. (Franklin D.Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Guerra de informação: conflito cujo objectivo é o domínio da informação, para a obtenção de ganhos políticos ou militares, contra infra-estruturas, sistemas de tecnologias de informação e informação, privada ou pública, através de técnicas para atacar ou influenciar operações. Existe mesmo nos tempos de paz e não é declarada. Este conceito atravessa as noções de *netwar* (focada nos conflitos irregulares, onde se inclui o terror, o crime, e o activismo social) *e ciberwar* (com ênfase no domínio militar), tendo estas sido apresentados em 1996 e 1993, respectivamente, pelos autores John Aquilla e David Ronfeldt.
(José Dinis, 2005, Viegas Nunes, 2011 e John Arquilla e David Ronfeldt, 2001).

Hacker: indivíduo que entra sem autorização num sistema ou rede de computadores, mas sem objectivos maliciosos, normalmente movidos pelo desafio, conhecimento e gosto pelo que fazem e normalmente são confundidos com *crackers*. É outro tipo de pirata informático. (José Dinis, 2005).

Hacktivismo: termo que deriva da conjugação da palavra *hacker* e *acktivism* (activismo), sendo geralmente concebido como manipulação de informação digital, motivado pelas mudanças sociais ou políticas. Os alvos são pessoas com poder de decisão ou vítimas inocentes. Os métodos utilizados são os

defacements ou os *DDoS.* É considerado uma desobediência civil, semelhante ao activismo regular. (Franklin D.Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Hardware: refere-se aos componentes físicos internos, ou sejam, o disco duro, placa mãe, microprocessador, circuitos, cabos, etc. e também aos periféricos, como a impressora, por exemplo. Pode ser básico, se integrar os dispositivos necessários para iniciar o funcionamento de um computador ou complementar, se abranger os dispositivos que realizam funções específicas. (*BusinessDictionary*, 2012)

Internet: *INTERconnected NETworks*. A "rede das redes", que interliga redes locais (*LAN- Local Area Network*), redes de área alargada (*WAN – Wide Area Network*) e redes metropolitanas (*MAN – Metropolitan Area Network*). (José Dinis, 2005).

Jihad: existem três interpretações no Islão: na interpretação pessoal significa luta pela purificação da alma contra as influências demoníacas. Na interpretação verbal significa busca da justiça através das palavras e acções não violentas. Na interpretação física significa uso da força física para protecção dos muçulmanos contra a opressão e transgressão dos inimigos de Allah, o Islão e os muçulmanos. (*Religious Tolerance*, 2012).

Mujahedin: aquele que leva a cabo a *jihad*. (Religious Tolerance, 2012).

Netwar: tem uma natureza dualista, pois integra os conflitos perpetrados por terroristas, criminosos e extremistas etno-nacionalistas e conflitos levados a cabo por activistas da sociedade civil (ocorre entre nações e sociedades, governos, governo e actores não estatais, empresas, entre outros). É uma forma de conflito na medida em que os intervenientes estão organizados numa estrutura em rede, com muitos grupos sem líder, mas com a capacidade de se agregarem rapidamente para lançarem ataques. É uma nova forma de conflito e crime, com muitos poucos traços dos conflitos militares convencionais e os seus participantes partilham as mesmas doutrinas, estratégias e tecnologias da

era da informação, cujo objectivo é a tentativa de corromper, danificar, modificar o que uma determinada população pensa acerca de si mesma e do mundo que a cerca. (John Arquilla e David Ronfeldt, 2001, 2012).

SCADA (*supervisory control and data acquisition):* supervisão de controlo e aquisição de dados, é um programa que colecta informações em tempo real para controle de processo de equipamentos e pode ser utilizado em infra-estruturas de telecomunicações, petróleo, gás, água, etc. Por exemplo, este sistema reúne informações, sobre a localização de uma fuga e determina qual a sua importância, organiza e processa as informações, entre outras capacidades. Pode ser monitorizado através de um computador portátil e tecnologias relacionadas com a *Internet,* embora a maioria das instalações que usam esta tecnologia, não estejam ligadas à *Internet,* os postos de manutenção que as supervisionam usam tecnologia semelhante à *Internet* e são por vezes ligadas a esta, o que pode ser uma forma de se obter uma *backdoor*, criando assim vulnerabilidades. (Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Spamming: envio de mensagens não solicitadas, normalmente enviadas por um número enorme de *e-mails.* (José Dinis, 2005).

Spyware: programas introduzidos em computadores, sem conhecimento ou consentimento, para recolha de informação dos utilizadores desses computadores, permitindo que terceiros saibam qual a configuração do sistema, hábitos de navegação na *Web*, furto de informação, documentos, senhas de acesso ou números de contas bancárias, por exemplo. É utilizado por determinadas empresas e criminosos. (Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz, 2009).

Trojan horse – programa não autorizado contido num programa legítimo que despois de instalado realiza funções que o utilizador desconhece. Geralmente espera que ocorra um evento no computador, uma data por exemplo, para se activar. Não se replica nem se autocopia. Podem constituir um vírus ou um

programa de controlo remoto, que dá acesso completo ao computador da vítima. (Robert. W. Taylor, Tory j. Caeti, D. Kall Loper e outros, 2006).

Worms: programa que se reproduz automaticamente, através do envio de cópias de si mesmo a outros computadores, de modo a infectá-los. Executa-se através da exploração de vulnerabilidades ou falhas de *software* instalado. Danificam o desempenho de redes e podem ocupar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que consegue propagar. (José Dinis, 2005).

BIBLIOGRAFIA

ARQUILLA, John e RONFELDT, David – Networks and Netwars: The Future of Terror, Crime and Militancy, RAND, National Defense Research Institut, 2001.

BAUMAN, Zygmunt – Comunidade, A busca por segurança no mundo actual, Ed. Jorge Zhar, 2003.

BAUMAN, Zygmunt – Globalização: As consequências humanas, Trad. Marcus Penchel, Ed. Jorge Zahar, 1999.

BAUMAN, Zygmunt – A Sociedade Individualizada, Jorge Zahar Editor Ltda., Rio de Janeiro, 2009.

BAUMAN, Zygmunt – Tempos Líquidos, Jorge Zahar Editor Ltda., Rio de Janeiro, 2007.

BOLLIER, David – The Rise of Netpolitik, How de Internet is Changing International Politics and Diplomacy, Ed. The Aspen Institut, 2003.

CANOTILHO, Gomes e MOREIRA, Vital, Constituição da República Portuguesa Anotada, Ed. Coimbra Editora, 2007.

DIAS, Carlos Manuel Mendes - Geopolítica: teorização clássica e ensinamentos, Prefácio Edições, Lisboa, 2005.

DINIS, José, Guerra de Informação: Perspectivas de Segurança e Competitividade, Ed. Sílabo, 2005

GUEDES, Armando Marques – Ligações Perigosas: Conectividade, Coordenação e Aprendizagem em Redes Terroristas, Almedina, Coimbra, 2007.

GIDDENS, Anthony – As consequências da modernidade, Trad. Editorial Presença, Lisboa, 2000.

GOUVEIA, Bacelar – Direito Internacional Público – Textos Fundamentais, Ed. Coimbra Editora, 2003.

HORGAN, John and Kurt Braddock - Terrorism studies: a reader, Routledge, 2012.

KARATZOGIANNI, Athina - Cyber Conflict and Global Politics, Routledge, 2009.

KLIMBURG, Alexander - National Cyber Security Framework Manual, Ed. Alexander Klimburg, NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia, 201.
http://www.ccdcoe.org/369.html (consultado em 14-12-12).

KRAMER, Franklin D., Stuart H. Starr and Larry K. Wentz – Cyberpower and National Security, Center for Technology and National Security Policy, National Defense University, 2009.

LIANG, Qiao and XIANGSUI, Wang - Unrestricted Warfare, Beijing: PLA Literature and Arts Publishing House, February 1999.

LIBICKI, Martin C. - What is information warfare?, Washington, National Defense University, Institute for National Strategic Studies, 1995.

LIBICKI, Martin C. - Dominant Battlespace Knowledge, Washington, National Defense University, Institute for National Strategic Studies, 1996.

MACHADO, Jónatas E. M., Direito Internacional – Do Paradigma Clássico ao Pós -11 de Setembro, Coimbra Editora, 2003.

MARCHUETA, Maria Regina - O conceito de Fronteira na Época da Mundialização, Lisboa, Instituto da Defesa Nacional, Ed. Cosmos, 2002.

MARCHUETA, Maria Regina – Considerações sobre o fenómeno do terrorismo, Ed. Duarte Reis, 2003.

MOREIRA, Adriano – Terrorismo - coord. Adriano Moreira, Coimbra, Almedina, 2004.

MOREIRA, Adriano – Da Utopia à Fronteira da Pobreza, Imprensa Nacional Casa da Moeda, Lisboa, 2011.

RANSTORP, Magnus - Mapping Terrorism Research: State of the art, gaps and future direction, Routledge, 2007.

ROCHA, Manuel Lopes, CORREIA, Miguel Pupo, RODRIGUES, Marta Felino, ANDRADE, Miguel Almeida, AMORIM, Pedro Patrício, CARREIRO, José Henrique, CABRITA, Luís – Leis da Sociedade de Informação: Comércio Electrónico, Coimbra Editora, 2008.

RONCZKOWSKI, Michael - Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis and Investigations, CRC Press, 2011. http://books.google.pt/books?id=ROHYNssl-CsC&pg=PA231&lpg=PA231&dq=ronczkowski+spectrum+cyber+conflict&source=bl&ots=9Ppjtxrkx3&sig=bG_LOBGdPcEfjlG1OXFyzD-KRtc&hl=pt-BR&sa=X&ei=irrLUJr8Ds2FhQfH6YCQCw&redir_esc=y#v=onepage&q=ronczkowski%20spectrum%20cyber%20conflict&f=false (consultado em 10-12-2012).

SCHMID, Alex P. - The Routledge Handbook of Terrorism Research, Routledge, 2011.

SCHMID, Alex P., JONGMAN A. J. - Political Terrorism - A Research Guide to Concepts, Theories Data Bases and Literature – Amsterdam: North Holland, 1984.

SCHMID, Alex P., CRELINSTEN, Ronald D. - Western responses to terrorism, London, Frank Cass, 1993.

SHMITT, Michael N. - The Tallinn Manual on the International Law Applicable to Cyber Warfare, Gen. Ed. Michael n. Schmitt, NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia, 2012.
http://www.ccdcoe.org/249.html (consultado em 10-11-2012).

TAYLOR, Robert W., CAETI, Tory J., LOPER, D. Kall, FRITSCH, Eric J., LIEDERBACH, John – Digital Crime and Digital Terrorism, Pearson Education, Inc., Pearson Prentice Hall Upper Saddle River, 2006.

TOFFLER, Alvin - Os novos poderes, trad. Fernanda Pinto Rodrigues, Lisboa, Livros do Brasil, 1991.

TOFFLER, Alvin - The third wave, Bautan Books, 1980.
VAN CREVELD, Martin - The transformation of war, New York, The Free Press, 1991.

VERDELHO, Pedro, BRAVO, Rogério, ROCHA, Manuel Lopes – Leis do Cibercrime, Ed. Centro Atlântico, 2003.

VENÂNCIO, Pedro Dias – Lei do Cibercrime: Anotada e Comentada, Coimbra Editora, 2011.

TRABALHOS E ARTIGOS ACADÉMICOS

ADKINS, Bonnie N. – "The spectrum of cyber conflict from hacking to information warfare: what is law enforcement's role?", US Air Force, 2001.
http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA406949 (consultado em 10-09-2012).

BRITO, Jerry, WATKINS, Tate - "Loving the cyberbomb? The dangers of Inflation in Cybersecurity Policy", Mercatus Center, George Mason University", Abril, 2011.

COLLIN, Barry - “The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge”, Institute for Security and Intelligence, 11th Annual International Symposium on Criminal Justice Issues, Chicago, 1996. http://afgen.com/terrorism1.html (consultado em 11-08-2012).

DENNING, Dorothy E. – “Cyberterrorism: Testemony Before the Special Oversight Panel on Terrorism Committee on Armed Services”, Georgetown University, May, 23, 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (consultado em 21-08-2012).

DENNING, Dorothy E. – “Information Operations and Terrorism”, August, 18, 2005. http://faculty.nps.edu/dedennin/publications/io%20and%20terrorism.pdf (consultado em 10-08-2012).

DENNING, Dorothy E. – “A View of Cyberterrorism Five Years Later, in Internet Security: Hacking, Counterhacking, and Society”, K. Himma ed., 2007. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484928 (consultado em 15-11-2012).

DENNING, Dorothy E. – “Terror‟s Web: How the Internet Is Transforming Terrorism”, Handbook on Internet Crime, Willan Publishing, 2009. http://faculty.nps.edu/dedennin/publications/Denning-TerrorsWeb.pdf (consultado em 10-09-2012)

DENNING, Dorothy E. – “Cyber Conflict as an Emergent Social Phenomenon”, Information Science Reference, 2011. http://faculty.nps.edu/dedennin/publications/CyberConflict-EmergentSocial Phenomenon-final.pdf (consultado em 11-12-2012).

DENNING, Dorothy E. – “Stuxnet: What Has Changed?”, Future Internet, 2012. http://www.mdpi.com/1999-5903/4/3/672 (consultado em 15-12-2012).

GUEDES, Armando Marques - “CyberWarfare Q&A”, published as the first article in The Spoked Wheel, 25th July, 2009.
http://spokedwheel.wordpress.com (consultado em 08-12-2013).

GUEDES, Armando Marques - “The new geopolitical coordinates of cyberspace”, in Revista Militar, 2503/2504: 825-849, Lisboa, 2010.

GUEDES, Armando Marques - “Geopolitica del Ciberspazio”, Quaderni Speciali di Limes. Rivista Italiana di Geopolitica: 187-199, Roma, 2010.

HUGHES, Rex B. – “NATO and Cyber Defence: Mission Accomplished?”, US Army War College, 2009.
http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf (consultado em 20-11-2012).

KUEHL, Dan - From Cyberspace to Cyberpower: Defining the Problem, Information Resources Management College/National Defense University, U.S. Army War College, 2003.
http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCwQFjAA&url=http%3A%2F%2Fwww.carlisle.army.mil%2FDIME%2Fdocuments%2FCyber%2520Chapter%2520Kuehl%2520Final.doc&ei=l7_uUPefKYa2hAepqYC4CQ&usg=AFQjCNHYEmoa8LxYIdGhRmXyFetQy9M-bQ&bvm=bv.1357700187,d.ZG4 (consultado em 22-11-2012).

MAURER, Tim – “Cyber Norm Emergence at the United Nations - An Analysis of the UN‘s Activities Regarding Cyber-security”, Belfer Center for Science and International Affairs, Cambridge, 2011.
http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf (consultado em 11-12-2012).

NISSENBAUM, Helen. – “Where Computer Security Meets National Security”, Ethics and Information Technology, Vol. 7, Nº 2, June 2005.

NUNES, Viegas - O Impacto da Aplicação do Conceito de Network Centric Warfare nas Forças Armadas Portuguesas: Subsídios Para o Levantamento de Uma Capacidade Militar Centrada em Rede, Academia Militar, 2005.

O'HARA, Timothy – "Cyberwarfare/Cyberterrorism", USAWC Research Project, US Army War College, Pennsylvania, 2004.
http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA424310 (consultado em 11-09-2012).

POLLITT, Mark M. – "CYBERTERRORISM - Fact or Fancy?" Proceedings of the 20th National Information Systems Security Conference, 1997.
http://www.cs.georgetown.edu/~denning/infosec/pollitt.html (consultado em 10-06-2012).

ARTIGOS DE REVISTAS ESPECIALIZADAS E OUTRAS PUBLICAÇÕES PERIÓDICAS

ALMEIDA, Paulo Pereira de – "Políticas de Segurança: Visão de Futuro", in Revista Segurança e Defesa, Janeiro/Março,2009.

BESSA, João Manuel de Andrade Pinto – "As Nações Unidas e o Terrorismo", in Revista Militar, 2006.
http://www.revistamilitar.pt/modules/articles/article.php?id=159 (consultado em 23-10-2012).

BISPO, António de Jesus – "As operações militares no quadro das novas tecnologias: conceito de Network Centric Warfare (NCW)", in Revista Militar, Ano 56, nº 10, Lisboa, Outubro de 2004.

CORREIA, Armando J. Dias – "IRAQUE: Objectivos, Estratégias e Perspectivas Futuras", in Revista Militar, 2009.
http://www.revistamilitar.pt/modules/articles/article.php?id=356 (consultado em 23-10-2012).

DINIS, José - “A Guerra de Informação: Perspectivas de Segurança e Competitividade”, in Revista Militar, 2009.
http://www.revistamilitar.pt/modules/articles/article.php?id=401 (consultado em 15-07-2012).

DUARTE, Felipe Pathé – “A Trindade de Clausewitz: Uma Revisitação Dialéctica”, in Estratégia, Instituto Português da Conjuntura Estratégica, Coord. De Adriano Moreira e Pinto Ramalho, Vol. XXI, Lisboa, 2012.

EZZELDEEN, Khalil – “Jihadbokk: The evolution of online Islamist forums”, in Jane’s Intelligence Review, November 2012.

FARWELL, James P., ROHOZINSKI, Rafal – “Stuxnet and the Future of Cyber War”, International Institute for strategic Studies, Oxford University Press, in Survival, Vol. 53, nº 1, February-March 2011.

FERNANDES, Pedro Teixeira – “Utopia, Liberdade e Soberania no Ciberespaço”, in Nação e Defesa, nº 133, Instituto de Defesa Nacional, Lisboa, 2012.

FOLTZ, Andrew C. - “Stuxnet, Schmitt Analysis, and the Cyber “Use-of-Force” Debate”, in JFQ - Joint Force Quarterly, ed. Col William T. Eliason, Issue 67, 4th Quarter 2012.

GARCIA, Francisco Proença - “As Ameaças Transnacionais e a Segurança dos Estados. Subsídios para o seu estudo”, in Negócios Estrangeiros, nº 9.1, 2004.

GUEDES, Armando Marques – “CyberWarfare Q&A”, published as the first article in The Spoked Wheel, http://spokedwheel.wordpress.com/, 25th July, 2009.

GUEDES, Armando Marques - “The new geopolitical coordinates of cyberspace”, in Revista Militar, 2503/2504: 825-849, Lisboa, 2010.

GUEDES, Armando Marques - “Geopolitica del Ciberspazio”, Quaderni Speciali di Limes, in Rivista Italiana di Geopolitica: 187-199, Roma, 2010.

KLIMBURG, Alexander – “Mobilizing Cyber Power”, in Survival, Vol. 53, Nº 1, 2011.

MARTINS, Marco – “Ciberespaço: Uma Nova Realidade Para a Segurança Internacional, in Nação e Defesa, nº 133, Instituto de Defesa Nacional, Lisboa, 2012.

MASTERS, Jonathan – “Mujahadeen-e-Khalq (MEK) (aka People's Mujahedin of Iran or PMOI)”, in Council on Foreign Relations, 18 de Julho de 2012. http://www.cfr.org/iran/mujahadeen-e-khalq-mek-aka-peoples-mujahedin-iran-pmoi/p9158 (consultado em 20-12-2012).

MATIAS, Rui Manuel Fernandes Xavier - “O Exército e a Ciberdefesa”, in Planeamento Civil de Emergência, Conselho Nacional de Planeamento Civil de Emergência, nº 23, Lisboa, 2011.

MARTINS, Raúl François – “Geopolítica e Geoestratégia: Para que São e Para que Servem”, in Nação e Defesa, Nº 78, 1996.

NUNES, Viegas – “Ciberterrorismo: Aspectos de Segurança”, in Revista Militar, Nº 10, Outubro, 2004.

NUNES, Viegas – “Impacto das ciberameaças na segurança e defesa: da ciberdefesa ao levantamento da estratégia da informação nacional”, in Estratégia, Instituto Português da Conjuntura Estratégica, Vol. XX, Lisboa, 2011.

PAARLBERG, Robert L. – “Knowledge as Power”, Science, Military Dominance, and U.S. Security, International Security Center for Science and International Affairs, in Harvard University Press, Cambridge, Vol. 29, Nº 1, 2004.

RAMALHO, José Luís Pinto – “Guerra de informação - novos riscos e ameaças”, in Estratégia / Instituto de Estudos Estratégicos e Internacionais, Vol. XV, Lisboa, 2005.

RATHMELL, Andrew – “Cyber-terrorism: the shape of the future conflict?”, in RUSI Journal, London, Vol. 142, Nº 5, 1997.

SILVEIRA, João Tiago, ROMÃO, Miguel Lopes - “Regime jurídico do combate ao terrorismo: os quadros normativos internacional, comunitário e português”, in CIEJD, Lisboa, 2005.
https://infoeuropa.eurocid.pt/registo/000021565/documento/0001/ (consultado em 10-12-2012)

ARTIGOS DE JORNAIS E REVISTAS PERIÓDICAS

Breitbart
“Oh No You Didn't: Mossad Agents Claim Obama Lying About Stuxnet”, Joel B. Pollak, 10 de Junho de 2012.
http://www.breitbart.com/Big-Peace/2012/06/10/Oh-No-You-Didnt-Mossad-Agents-Claim-Obama-Lying-About-Stuxnet (consultado em 05 de Novembro de 2012).

Time Tech
“Report: Obama, Israel Behind Stuxnet Worm and Accelerated Iran cyberattacks”, Matt Peckham, 01 de Junho de 2012 (consultado em 05-11-2012).
http://techland.time.com/2012/06/01/report-obama-israel-behind-stuxnet-worm-and-accelerated-iran-cyberattacks/ (consultado em 05 de Novembro de 2012).

The New York Times
“Iranian Dissidents Convince U.S. to Drop Terror Label”, Scott Shane, 21 de Setembro de 2012.

http://www.nytimes.com/2012/09/22/world/middleeast/iranian-opposition-group-mek-wins-removal-from-us-terrorist-list.html?pagewanted=all&_r=1& (consultado em 10-12-2012).

SÍTIOS DE INTERNET CONSULTADOS

Agência Para a Sociedade do Conhecimento
http://www.umic.pt (consultado em 10-11-2012)

ANPC - Autoridade Nacional de Protecção Civil
http://www.prociv.pt (consultado em 17-05-2012)

APDSI – Associação Promoção Desenvolvimento Sociedade Informação
http://www.apdsi.pt/ (consultado em 17-05-2012)

Bitdefender
http://www.bitdefender.pt (consultado em 17-05-2012)

BusinessDictionary
http://www.businessdictionary.com (consultado em 20-12-2012)

Center for Democracy and Technology
https://www.cdt.org (consultado em 23-05-2012)

Centro de Gestão da Rede Informática do Governo
http://www.ceger.gov.pt (consultado em 20-11-2012)

CCRP - Command and Control Research Program
www.dodccrp.org (consultado em 30-04-2012)

CNSS - Committee on National Security Systems
http://www.cnss.gov (consultado em 17-05-2012)

Council of Europe Cybercrime
http://www.coe.int (consultado em 10-10-2012)

DoD - Department of Defense Cyber Crime Center
http://www.dc3.mil/ (consultado em 16-05-2012)

Eur-Lex
http://eur-lex.europa.eu (consultado em 17-05-2012)

Europa Press Releases - RAPID
http://europa.eu/rapid (consultado em 23-05-2012)

European Parliament
http://www.europarl.europa.eu (consultado em 21-09-2012)

European Council
http://www.assembly.coe.int (consultado em 21-09-2012)

Federation of American Scientists
http://www.fas.org (consultado em 17-05-2012)

Forward Edge (U.S. Department of Homeland Security)
http://www.defense.gov (consultado em 16-05-2012)

Gabinete de Documentação e Direito Comparado
http://www.gddc.pt (consultado em 10-12-2012)

Gabinete Nacional de Segurança
http://www.gns.gov.pt (consultado em 20-11-2012)

Global Research – Centre For research on Globalization
"CYBER TERRORISM": US-supported Terrorist Group MEK Plants Stuxnet Virus Malware to Disable Iran's Nuclear Facilities", Nile Bowie, 16 Abril 2012.

http://www.globalresearch.ca/cyber-terrorism-us-supported-terrorist-group-mek-plants-stuxnet-virus-malware-to-disable-iran-s-nuclear-facilities/30353 (consultado em 21-12-2012)

Homeland Security News Wire
www.homelandsecuritynewswire.com (consultado em 16-05-2012)

Infoeuropa biblioteca
https://infoeuropa.eurocid.pt (consultado em 15-12-2012)

International Terrorism and Security Research
http://www.terrorism-research.com (consultado em 21-09-2012)

Internet World Stats
http://www.internetworldstats.com (consultado em 16-05-2012)

Interpol
http://www.interpol.int/es (consultado em 15-12-2012)

ISN – International Relations and Security Network
http://www.isn.ethz.ch (consultado em 20-02-2012)

IWS - The Information Warfare Site
http://www.iwar.org.uk (consultado em 30-04-2012)

JTIC - Joint Interoperability Test Command
http://jitc.fhu.disa.mil (consultado em 16-12-2012)

Microsoft – Centro de Protecção e Segurança
http://www.microsoft.com (consultado em 17-12-2012)

New York University
http://www.nyu.edu (consultado em 10-12-2012)

NATO
http://www.nato.int (consultado em 17-12-2012)

NCIRC - Nato Computer Incident Response Capability
http://www.ncirc.nato.int (consultado em 30-12-2012)

OSCE – Organization for Security and Co-operation in Europe Permanent Council
http://www.osce.org (consultado em 30-12-2012)

OECD - Organization for Economic Co-operation and Development
www.oecd.org (consultado em 30-12-2012)

Parlamento Europeu
http://www.europarl.europa.eu (consultado em 18-12-2012)

Perspectives on terrorism
http://www.terrorismanalysts.com (consultado em 30-12-2012)

Procuradoria Geral Distrital de Lisboa
http://www.pgdlisboa.pt/pgdl/leis/lei_main.php (consultado em 22-12-2012)

RAND CORPORATION
http://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1218.pdf (consultado em 23-05-2012)

Religious Tolerance
http://www.religioustolerance.org/isl_jihad.htm (consultado em 22-12-2012)

Small Arms Survey
http://www.smallarmssurvey.org (consultado em 30-12-2012)

UCLA International Institute
http://www.international.ucla.edu (consultado em 30-12-2012)

Sénat
http://www.senat.fr (consultado em 12-12-2012)

The Foundry
“Stuxnet Revelation Continues Obama Administration Trend of Classified Leaks”, Steven Bucci, 01 de Junho de 2012. http://blog.heritage.org/2012/06/01/stuxnet-revelation-continues-obama-administration-trend-of-classified-leaks/ (consultado em 11 de Novembro de 2012)

Threat Post
http://threatpost.com/en_us/blogs/eugene-kaspersky-conficker-could-have-been-much-worse-052209 (consultado em 30-12-2012)

UN - United Nations
http://www.un.org (consultado em 30-12-2012)

UNODOC – United Nations Office for Drugs and Crime
http://www.unodc.org (consultado em 16-12-2012)

UNIDIR – United Nations Institute for Disarmament Research
http://unidir.org (consultado em 30-12-2012)

U. S. Department of Defense
www.defense.gov (consultado em 16-12-2012)

U. S. Department of State
http://www.state.gov (consultado em 21-12-2012)

U. S. Srategic Cybercommand
http://www.stratcom.mil/factsheets/cyber_command/ (consultado em 23-12-2012)

Wired
http://www.wired.com/threatlevel/2010/01/operation-aurora/ (consultado em 01-12-2012)

Worldmapper
http://www.worldmapper.org (consultado em 16-12-2012)

www.al-bab.com
http://www.al-bab.com/arab/docs/league/terrorism98.htm (consultado em 22-11-2012)

CONFERÊNCIAS E SEMINÁRIOS

Ciberespaço: Espaço mediático, virtual e global, Academia das Ciências de Lisboa, 2012.

Seminário de Inteligência: Os Intelligence Fusion Centers no combate ao terrorismo, Instituto Superior de Ciências Sociais e Políticas, 2012.

Seminário: Segurança e Gestão do Risco, Instituto de Estudos Superiores Militares, 2012.

Conferência: Que NATO para o século XXI, Instituo de Defesa Nacional, 2012.

Conferência: O Desafio da Cibersegurança, OSCOT – Observatório de Segurança e Criminalidade Organizada, Centro Cultural de Belém, 2012.

Seminário: Informação e Conflito, Academia das Ciências de Lisboa, 2012.

Conferência - Percepções Estratégicas Sobre o Ciberespaço: A Cooperação Internacional e a Segurança Nacional, Instituto da Defesa Nacional, 2011.

TESES CONSULTADAS

NUNES, Viegas – Análise da Conflitualidade da Informação na sociedade em Rede: Um Enquadramento para a Concepção e Implementação de um Modelo de Estratégia da Informação Nacional, Madrid, 2009. (Tese de Doutoramento).

SANTOS, José - Contributos para uma melhor governação da cibersegurança em Portugal, Faculdade de Direito da Universidade Nova de Lisboa, 2011. (Tese de Mestrado).