

CIBERTERRORISMO<sup>1</sup>:  
A NOVA FORMA DE CRIME DO SÉC. XXI  
COMO COMBATÊ-LA?

*Eng. Gonçalo Batista*  
*Carlos Ribeiro<sup>(\*)</sup>*  
*Tenente Coronel TM (Eng)*  
*TEN GNR Feliciano Amaral*  
*Tenente GNR*

*“Terrorismo e Internet, uma relação cada vez mais estreita e perigosa.”*

Fonte: Ernestina Herrera de Noble, *Directora do Clarin.com, 18 de Junho de 2002.*

## 1. Introdução

Ao longo da história foram travadas várias guerras, nas quais a tecnologia teve um papel decisivo, quer ao nível do armamento e da organização, quer das técnicas de combate utilizadas. Constata-se que os exércitos tecnologicamente melhor apetrechados e que inovaram os seus dispositivos, obtiveram vantagens consideráveis sobre os seus adversários. Alvin e Heidi Toffler, nas suas obras “*A Terceira Vaga*” e “*Guerra e Anti-Guerra*”, defendem que, ao longo dos tempos, ocorreram várias descobertas tecnológicas revolucionárias causadoras de mudanças socio-económicas. A primeira destas revoluções foi a Revolução Agrária, caracterizada pelo cultivo da terra, pela domesticação dos animais e pelas lutas pelo controlo e disputa da terra e dos recursos; a segunda foi a Revolução Industrial, centrada na mecanização, na produção em larga escala e na divisão do trabalho; finalmente, a terceira designada por Revolução da Informação e do Conhecimento, caracteriza-se pela digitalização e desenvolvimento das tecnologias de informação.

Face à crescente digitalização, abrangendo todos os sectores de actividade estatais, desde o político ao económico, passando pelos sectores sociais, a Internet e as

---

<sup>1</sup> Este artigo é um extracto de um trabalho realizado pelos autores em Maio de 2003, enquanto alunos do Curso de Pós-Graduação em Guerra de Informação/*Competitive Intelligence* realizado na Academia Militar, para a disciplina de Relações Internacionais e Globalização leccionada pelo Maj Inf Doutor Francisco Proença Garcia.

<sup>\*</sup> Docente na Academia Militar das disciplinas de Controlo, Tática de Transmissões e Transmissões e Guerra Electrónica; Director dos Cursos de Transmissões da Academia Militar e membro efectivo do CINAMIL (Centro de Investigação da Academia Militar).

redes de computadores adquiriram uma grande importância, principalmente nos países industrializados e nos países em vias de desenvolvimento. A Internet é constituída por uma rede de comunicações transnacional que permite a troca de informação, aquisição de bens e serviços, etc. No entanto, apresenta algumas vulnerabilidades, nomeadamente, os acessos fraudulentos a determinados serviços web, onde estão depositadas informações vitais para as empresas, com o objectivo de roubar essa informação ou simplesmente destruí-la por prazer.

Nos últimos anos temos assistido a uma "*revolução*" das comunicações, ainda em curso, que vai disponibilizar novas formas de acesso à Internet, nomeadamente o *wireless* (acesso sem fios), que nos fornecerá, por certo, novos benefícios, mas que também, implicará novas vulnerabilidades na utilização desta rede global. As auto-estradas da informação são hoje em dia uma realidade ligando todos os povos e tornando o mundo, como disse Marshall McLuhan, numa "*Aldeia Global*" com um ponto comum: o Ciberespaço.

Devido à Globalização, qualquer acontecimento no canto mais recôndito do mundo, tem consequências efectivas ao nível mundial, nas vertentes política, económica, de segurança e defesa, entre outras. Deste modo, com o desenvolvimento da Internet, surgiram novos conceitos que fazem os clichés dos telejornais e as manchetes dos jornais, tais como: Guerra da Informação, Ciberguerra, Ciberterrorismo e Cibersegurança, que estão a revolucionar a "*arte da guerra*", o combate ao banditismo e ao crime organizado. Actualmente, as múltiplas formas de crime são mais difusas e difíceis de detectar, devido à sua rápida evolução e à utilização do Ciberespaço, que proporcionou, por um lado, novas oportunidades e, por outro, novas vulnerabilidades.

As acções terroristas são muito antigas. Ao longo da história foram utilizadas essencialmente por dois tipos de actores: *governos*, com o objectivo de domínio; e *grupos insatisfeitos*, com a finalidade de derrubar governos. No entanto, a palavra "*Terrorismo*" só foi utilizada pela primeira vez na Conferência de Bruxelas para a Unificação do Direito Penal, em 1931 e desde então, este conceito generalizou-se e, embora não exista uma definição consensual <sup>2</sup>, é actualmente utilizado para

---

<sup>2</sup> Entre 1936 e a actualidade foram utilizadas mais de 110 definições distintas de Terrorismo. No entanto, decidimos adoptar a definição da cadeira de Relações Internacionais e Globalização, do curso de Pós-Graduação em Guerra de Informação/Competitive Intelligence que decorreu na Academia Militar em 2003 e cujo docente foi o Maj Inf/Doutor Francisco Proença Garcia.

Assim, define-se **Terrorismo** como a "*sistemática utilização da violência sobre pessoas e bens, para fins políticos provocando sentimentos de medo e de insegurança, e um inevitável clima de terror*".

designar a violência criminosa e indiscriminada, perpetuada por organizações e indivíduos armados.

*“Depois dos atentados de 11 de Setembro, nos EUA, o terrorismo deixou de ser um fenómeno de natureza nacional ou regional, como o IRA ou a ETA. Passou para uma escala internacional, adquirindo uma categoria transnacional.”*<sup>3</sup> No entanto, *“apesar da ocorrência de anteriores atentados terroristas de carácter internacional, os acontecimentos de 11 de Setembro superaram aqueles na dimensão da tragédia, na carga política simbólica que lhes foi imprimida, nos seus efeitos e consequências globais.”*<sup>4</sup>

Com o aparecimento e conseqüente desenvolvimento das novas tecnologias, os grupos terroristas descobriram um novo espaço alternativo para a prossecução dos seus objectivos criminosos, que vão desde a simples propaganda, passando pelo recrutamento de voluntários para a sua causa, até à utilização do ciberespaço para executarem os seus ataques digitais sobre os vários tipos de instituições (políticas, de defesa e económicas), causando prejuízos de milhões de dólares todos os anos. É neste cenário que surge o novo conceito de Ciberterrorismo, fruto da convergência entre ciberespaço e terrorismo ou mais explicitamente, utilização do ciberespaço para fins terroristas. Este conceito começou a ser apontado com maior ênfase após os atentados de 11 de Setembro nos Estados Unidos da América (EUA).

Á medida que a Internet se vai desenvolvendo e fornecendo novos tipos de serviços e facilidades, colocam-se também novos desafios e problemas que carecem de resolução: é o caso da segurança dos dados nos servidores e utilizadores ligados à world wide web; também designada por Cibersegurança. Os Estados estão actualmente a concentrar esforços para complementar a segurança física e lógica das redes de computadores, com medidas legislativas e outras para evitar ataques terroristas aos seus centros nevrálgicos.

Podemos justificar o tema deste artigo, o ciberterrorismo; pela sua actualidade, transnacionalidade e devido aos danos causados pelos seus ataques, porque julgamos que esta nova forma de crime vai assumir um papel de destaque no dealbar deste novo século.

---

<sup>3</sup> Maria Regina Marchueta, *“Considerações sobre o fenómeno terrorismo”*, Outubro de 2002, no prelo.

<sup>4</sup> Idem, *Ibidem*.

## 2. Internet

Nos anos 60 foi desenvolvida, pelo Departamento de Defesa dos EUA, a antecessora da Internet, que na altura se designou por ARPANET (Advanced Research Project Agency Network); no entanto, esta rede só começou a ser utilizada intensivamente durante os anos 70, quando os computadores das organizações militares e das universidades foram interligados através da rede telefónica. No início dos anos 90, a Internet constituía já uma plataforma internacional e registava mais de sete milhões de utilizadores em todo o mundo; contudo, foi nesta década que se assistiu ao crescimento desenfreado, não só do número de utilizadores, como dos conteúdos disponíveis e das tecnologias utilizadas para acesso a esta rede de comunicação global. Na década de 90, este sistema tornou-se tão complexo que é impossível determinar quem o domina e ainda hoje, não se conhecem todas as acções mal intencionadas que se podem realizar sobre os computadores ligados a esta plataforma tecnológica.

A Internet permite-nos pesquisar informação em bases de dados, importar ficheiros e aplicações, enviar correio electrónico, etc. O mundo da informação a que se tem acesso é tão vasto que muitas das teses de mestrado e de doutoramento feitas nos últimos anos, foram buscar parte da sua informação à Internet. Ligar-se à Internet significa ter a possibilidade de aceder a milhões de computadores (servidores) espalhados pelo mundo. Como alguém disse um dia, “o seu disco rígido passa a ser o mundo inteiro”<sup>5</sup>. Através do correio electrónico, pode-se comunicar com inúmeros utilizadores em qualquer parte do globo terrestre. Tais recursos facilitam decisivamente a comunicação das empresas e dos profissionais liberais com seus clientes e com o público em geral, 24 horas por dia, 7 dias por semana. Um site na *Web* é uma autêntica vitrine virtual, quer seja para acções de propaganda institucional, quer para a obtenção de informações sobre produtos e serviços ou para a sua comercialização.

Como inconvenientes à utilização da Internet podemos referir os seguintes:

- Desigualdade de acesso (*diferença social*); nem todas as classes sociais tem acesso à Net;
- A grande variedade de informação pode causar dispersão por falta de objectividade;

---

<sup>5</sup> “Vantagens da Internet !”, [http://www.terravista.pt/Meco/7435/vantagens\\_internet.htm](http://www.terravista.pt/Meco/7435/vantagens_internet.htm).

- Criação de uma linguagem simbólica;
- A Internet cria vício nos utilizadores;
- Problemas técnicos de acesso;
- Utilização da Internet para fraude ou crime, de que são exemplo: a pedofilia, prostituição, tráfico de droga e inúmeras actividades criminosas.

O terrorismo e a Internet relacionam-se de duas formas distintas: por um lado, a Internet transformou-se num fórum para os grupos terroristas difundirem as suas mensagens de ódio e de violência e para comunicarem uns com os outros e com os seus simpatizantes; por outro lado, os indivíduos e os grupos ensaiaram ataques às redes de computadores, incluindo aqueles que se encontram ligadas à "Net" – acção que se designa por Ciberterrorismo.

### 3. Ciberterrorismo

A "Revolução" da Informação alterou profundamente as estruturas organizacionais, a natureza e a estratégia dos conflitos. Esta mesma "revolução" da informação e do conhecimento, actualmente em curso, gerou novos conceitos e novas ameaças globais para a sociedade, como é o caso do Ciberterrorismo que iremos desenvolver seguidamente.

#### a. *Definição e Objectivos*

Com o advento das novas tecnologias, especialmente com a extensão e com o alcance da Internet obtido ultimamente, os grupos terroristas descobriram um novo espaço alternativo para levar adiante os seus ataques, dando lugar a um novo tipo de actividade criminosa designada por **Ciberterrorismo**. Este conceito foi utilizado pela primeira vez por Barry Collin<sup>6</sup>, investigador no "Institute for Security and Intelligence", na década de 80, para se referir à convergência do ciberespaço e do terrorismo, mas só a partir do ataque terrorista às Torres Gémeas do World Trade Center (11SET01), o "FBI divulgou inúmeros alertas sobre a responsabilidade e gravidade do ciberterrorismo"<sup>7</sup>, e foi também nesta altura, que se intensificaram os ataques ciberterroristas, dos quais resultaram prejuízos avultados.

---

<sup>6</sup> Barry Collin, "The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge", <http://afgen.com/terrorism1.html>, March 1997, págs. 15-18.

<sup>7</sup> Paulo Perez, "Terror nos EUA - Ameaça do Ciberterrorismo se torna realidade" <http://www.novomilenio.inf.br/ano01/0110d008.htm>.

A Internet é uma rede desterritorializada e transnacional que permite atacar potências geograficamente longínquas. Por isso, a tecnologia informática deve permitir uma comunicação rápida, ampla e barata, proporcionando um aumento na quantidade de informação disponível para todos os cidadãos. De acordo com Mark Pollitt, **Ciberterrorismo** “*é o ataque premeditado contra informações, dados, sistemas e programas de computadores, com intenções políticas, económicas, religiosas ou ideológicas resultando em violência contra alvos não combatentes de organizações ou agentes clandestinos*”<sup>8</sup>. Esses ataques realizados por “*hackers*”<sup>9</sup>, ao serviço de organizações criminosas ou de estados subversivos, têm como intenção causar danos graves, tais como: perdas de vidas (por ex.: devido à intrusão de “*hackers*” nos sistemas de controlo de tráfego aéreo, provocando colisões de aviões), prejuízos económicos, cortes de energia eléctrica ou água. Este tipo de terrorismo tem como objectivo desestabilizar política, ideológica ou financeiramente um grupo, organização ou governo, utilizando a Internet para perpetrarem as acções consideradas necessárias.

#### b. *Os Actores do Ciberterrorismo*

Quem é que são os ciberterroristas? São grupos terroristas já existentes ou são novas organizações criminosas?

Embora existam alguns grupos ciberterroristas “*puros*”, a grande maioria deriva de grupos terroristas já reconhecidos. Por isso, na era da informação, as organizações terroristas que não tenham acesso à televisão ou às estações de rádio, podem facilmente difundir as suas mensagens através da Internet.

Actualmente, podem realizar acções ciberterroristas os seguintes **tipos de actores**:

- Hackers – amadores ou profissionais;
- Grupos Criminosos (nos quais se inserem, entre outros, os grupos terroristas);
- “*Sub-estados*” (pretendentes a Estados, Movimentos de Libertação ou Regiões), motivados por objectivos políticos.

---

<sup>8</sup> Mark M. Pollitt, “*CYBERTERRORISM - Fact or Fancy?*”, Proceedings of the 20th National Information Systems Security Conference, <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>, October 1997, pags. 285-289.

<sup>9</sup> Indivíduos com conhecimentos técnicos que utilizam os computadores e a Internet para fins ilegais ou mesmo criminosos, com a ajuda de software especial.

Os actores do terrorismo convencional (*Talibans*, ETA; IRA, etc.) podem contratar “*hackers*” ou recorrer à conversão de alguns “*hackers*” às suas ideologias, para exercer esta nova forma de violência: O Ciberterrorismo. No entanto, nem sempre é fácil ao grupo terrorista recrutar, no seu próprio seio, “*hackers*” e treiná-los, porque não possuem as infra-estruturas necessárias (alguns grupos, não têm sequer computadores em grandes quantidades, como por ex.: no caso do Afeganistão); parece mais aceitável a primeira alternativa, ou seja, contratá-los para perpetrarem os seus ataques a alvos específicos. Num dos seus estudos, Sarah Gordon, pesquisadora da IBM, diz que o perfil dos “*hackers*”<sup>10</sup> tem mudado com o tempo. Na segunda metade dos anos 90, predominavam jovens estudantes do sexo masculino e a maioria abandonava completamente essas actividades irregulares quando ingressava no mercado de trabalho; nos últimos anos, o nível técnico e a média de idades subiram; muitos são programadores de grande habilidade, com idades compreendidas entre os 20 e os 35 anos.



### c. *Tipos de Armas Utilizadas*

“O ciberterrorismo encontrou um novo cenário bélico, fazendo parecer obsoletas as armas utilizadas nas guerras convencionais, dado que o terrorista é um inimigo, muitas vezes sem rosto e sem fronteiras, tendo encontrado na Internet as facilidades e possibilidades que essa oferece”<sup>11</sup>. Portanto, a Internet é utilizada como arma pelos ciberterroristas para exercerem acções em prol das respectivas causas, demonstrando assim que acompanham o desenvolvimento das novas tecnologias e que delas retiram proveito. Assim, as **armas utilizadas** podem incluir os seguintes tipos:

- Armas do tipo Convencional;
- Armas Lógicas;
- Armas Comportamentais.

<sup>10</sup> Utilizam pseudónimos como “*Dark Avenger*”, “*Randomizer*” ou “*Aristotle*”.

<sup>11</sup> Pastor Sérgio Garcia, “*Terrorismo Digital*”, 27Jun01, <http://www.sigueme.com.ar/Editorial/Terrorismo%20Digital.htm>.

As **Armas do Tipo Convencional** (ou de destruição física) têm por objectivo atacar, essencialmente, as estruturas físicas dos suportes da informação impedindo a utilização de determinados serviços utilizando para o efeito:

- **Bombas de Impulso Electromagnético** – estes dispositivos geram impulsos electromagnéticos que actuam como uma onda de choque do mesmo tipo, provocando danos no alvo semelhantes aos efeitos das descargas eléctricas dos relâmpagos;
- **Munições de Radiofrequência (RF)** – estas armas podem ser activadas por sinais de rádio e podem adaptar-se a granadas de mão, granadas de morteiro ou de artilharia;
- **Dispositivos Electromagnéticos Transitórios – TED's** (“*Transient Electromagnetic Device*”) para realizarem a monitorização TEMPEST<sup>12</sup>.

Algumas destas armas representam um grande perigo, porque podem realizar ataques indetectáveis a grande distância e a vítima pode não se aperceber que está a ser atacada. Não existem medidas disponíveis para proteger um alvo potencial de um ataque; por isso, as armas RF e os TED's apresentam as seguintes vantagens face às armas convencionais:

- Têm baixo custo e são resistentes ao tempo;
- Têm capacidade para atacar instantaneamente alvos únicos ou alvos múltiplos;
- Não são letais para os seres humanos, desde que devidamente ajustadas.

Com as **Armas Lógicas** pretende-se atacar a lógica operacional dos sistemas de informação, introduzindo atrasos ou comportamentos indesejados no seu funcionamento. De acordo com a NSA (*National Security Agency*) dos EUA, os “*hackers*” utilizam as seguintes técnicas para efectuarem os ataques: envio de **Vírus Informáticos** (que podem ser introduzidos num computador e destruir programas); **Bombas Lógicas** (que se instalam nos sistemas operativos dos computadores e permanecem em hibernação até receberem um sinal específico que os acciona e que vai despoletar a destruição dos sistemas hospedeiros - “*host systems*”); “**Worms**” (vírus que se propagam

---

<sup>12</sup> TEMPEST (*Transient ElectroMagnetic Pulse Emanation Standard*) é o nome de código para as actividades de monitorização e defesa dos conteúdos dos computadores a ataques externos, embora o computador não estivesse ligado em rede. Em 1985, Van Eck mostrou que existiam semelhanças entre os PC e as emissões de rádio e TV; utilizando uma antena direccional e um bom amplificador de sinal conseguia-se vigiar as emissões radiadas.

de forma independente e destroiem os sistemas operativos); **Cavalos de Tróia** (proporcionam a entrada de intrusos sem serem percebidos; apesar de aparentemente inofensivos quando são activados têm um elevado poder destrutivo); **“Back Doors”** e **“Trap Doors”** (são mecanismos construídos dentro de um sistema para acesso à sua informação num momento posterior à sua instalação); **“Virtual Sit-Ins”** e **“Blockades”** (bloqueio do acesso ao equipamento); **“e-mail Bombs”**; **Ataques de Recusa de Serviço** (*“Denial of Service Attacks”*<sup>13</sup>), entre outros mecanismos que permitem desligar e destruir sistemas de transmissão de dados e hardware.

Esta é a esfera típica de actuação dos ciberterroristas e o objectivo deste tipo de armas é, numa primeira fase, instalar-se no sistema e, posteriormente, desactivá-lo. *“Ciberterroristas com elevados conhecimentos de programação e nenhuma ética vêm produzindo vírus cada vez mais sofisticados. Trata-se de uma guerra em que o inimigo é oculto, não tem objectivos claros, excepto a destruição, e atira-a mesmo contra uma multidão de inocentes”*<sup>14</sup> e só em 1999, os vírus informáticos causaram prejuízos de 12,1 biliões de dólares em todo o mundo. Ao **nível Comportamental** ou **Semântico**, utilizam-se armas que visam destruir a confiança que os utilizadores depositam nos sistemas de informação e na rede que os suporta, bem como influenciar a interpretação da informação que neles circula. A este nível, os ciberterroristas utilizam, essencialmente, a decepção e a guerra psicológica, que também são vulgarmente utilizadas ao nível do terrorismo convencional.

#### d. *Os Alvos Preferenciais dos Ciberterroristas*

Actualmente, a Internet oferece um espaço para que as organizações terroristas, de qualquer parte do mundo, actuem em qualquer ponto do planeta desde que exista conectividade com o possível alvo. A Internet não respeita divisões políticas ou geográficas<sup>15</sup>.

---

<sup>13</sup> Através deste tipo de ataque podem *“capturar-se”* computadores e utilizá-los para enviar quantidades excessivas de *“e-mails”* para o sistema ou servidor alvo; este sistema, depois de ficar completamente dominado, bloqueia.

<sup>14</sup> Maurício Grego, Julho 2000 *“Ciberterrorismo, - Programadores com muita habilidade e nenhuma ética criam virus cada vez mais devastadores. Há uma saída?”*, Revista Info Exame. <http://www.modulo.com.br/emprea3/noticias/habilidade.htm>.

<sup>15</sup> Alguns *hackers* uniram-se em prol da causa terrorista de Bin Laden no Afeganistão; existem também dados sobre a ataques ciberterroristas durante o conflito no Kosovo; no Iraque; a luta dos Zapatistas Mexicanos; conflito sobre os direitos humanos na China entre outros.

Como é que os ciberterroristas cumprem a sua missão?

O ciberterrorista está, normalmente, ao serviço de um grupo terrorista com objectivos bem definidos; por isso, vai fazer incidir a sua acção sobre populações alvo, onde se incluem as pessoas, as instituições políticas e sociais, as infra-estruturas económicas, etc. Deste modo, podemos classificar as acções ciberterroristas em três tipos distintos:

- Obtenção de informação, comunicações, lavagem de dinheiro e propaganda;
- Destruição física e lógica da informação e dos respectivos sistemas de informação;
- Roubar informação e dados sensíveis ou simplesmente alterar essa informação.

O roubo de informação é uma das actividades mais aliciantes para os ciberterroristas.

Existem já vários registos deste tipo de crime, especialmente nos EUA: *“por exemplo, entre Janeiro e Maio de 1999 um ataque conseguiu roubar documentos classificados com códigos navais e informação sobre sistemas de mísseis. O Pentágono sabe que um ataque cibernético de carácter bélico aos centros de informação militares e políticos do país inutilizaria os sistemas de decisão política e de resposta militar e, por isso, deixaria o país desprotegido ante qualquer agressão.”*<sup>16</sup>



Os grupos ciberterroristas utilizam a Internet para, por um lado, atacar as redes informáticas que gerem sistemas essenciais de um país, por outro, porque esta plataforma lhes garante, entre outras vantagens, o anonimato. Deste modo, podem atacar qualquer alvo situado em qualquer país, a partir de qualquer parte do mundo, sem arriscar a sua integridade física, utilizando um simples computador e um modem. Estes ataques disseminados através da rede podem ter motivações políticas, históricas e até religiosas.

Os ciberterroristas podem aceder a grandes servidores em qualquer parte do mundo e usá-los em ataques coordenados. Os seus objectivos podem ser a

---

<sup>16</sup> Laura Levy, *“Ciberterrorismo, lo que faltaba”*, <http://www.3pontos.com>.

economia de um país ou as condições de vida da população. A finalidade principal dos ataques ciberterroristas não é atacar as componentes físicas das infra-estruturas, mas sim, os programas de gestão e controlo dos serviços essenciais, provocando a sua paralização ou até a sua destruição. Nestes programas de gestão incluem-se estruturas tais como: redes de distribuição de energia eléctrica, de água potável e de gás; redes dos sistemas hospitalares; redes de controlo de tráfego aéreo e ferroviário; redes de emergência (polícia, bombeiros, etc.); redes bancárias e financeiras; redes de comunicações e sistemas de radiodifusão; redes governamentais; redes militares e das Forças de Segurança; sistemas estratégicos de defesa; instalações militares; centrais de energia e bases de dados com informação estratégica. Este uso bélico da rede, indica a entrada numa nova etapa no sistema militar, no qual se utiliza a rede como meio de acesso para destruir sistemas informáticos nevrálgicos do inimigo. Actualmente, os ciberterroristas mundiais elegeram os EUA e as empresas multinacionais como alvos preferenciais. Assim, executam ataques com objectivos políticos, militares<sup>17</sup>, económicos e religiosos, tendo a sua incidência aumentado consideravelmente a partir dos atentados de 11 de Setembro de 2001. *“Os seus objectivos são especialmente simbólicos e altamente mortíferos, procurando a sua repercussão e multiplicação pelos meios de comunicação social, cuja omnipresença (em especial da televisão) potencia os seus efeitos, provocando pânico generalizado, e originando respostas em todos os campos de intervenção estratégica, com os correspondentes custos. Pior do que tudo, abalam a economia do mundo desenvolvido e corroem os principais alicerces das sociedades democráticas, limitando a liberdade dos seus cidadãos, pela obsessão securitária que é criada, não só nas pessoas enquanto tais, mas principalmente nos responsáveis políticos.”*<sup>18</sup>

#### **e. O Ciberterrorismo e a Guerra de Informação**

Para a consecução dos seus objectivos, os Ciberterroristas utilizam com grande frequência a Guerra de Informação<sup>19</sup>. Como os Países Desenvolvidos

<sup>17</sup> Durante os conflitos do Kosovo e do Golfo, diversos sites dos EUA e da NATO foram atacados por *hackers* mundiais.

<sup>18</sup> General José Loureiro dos Santos, *“A Idade Imperial – A Nova Era - Reflexões sobre Estratégia III”*, pág. 98.

<sup>19</sup> *“O conjunto de acções que visam preservar a integridade dos nossos sistemas de informação, evitando a sua exploração, corrupção ou destruição, por parte de adversários e, simultaneamente, executar acções que permitam explorar, corromper ou destruir os sistemas de informação dos adversários, obtendo-se assim vantagem de informação, no âmbito político, económico ou militar”*.

dependem cada vez mais dos sistemas de informação e das comunicações, os seus principais sistemas de suporte, nomeadamente os sistemas financeiros, saúde, comunicações, segurança e defesa, entre outros, são geridos por sistemas informáticos cada vez mais complexos. Por isso, através da Guerra de Informação, os ciberterroristas executam ataques aos computadores, quer os individuais quer os que estão ligados à rede.

Tendo por base o tipo de acção a desenvolver, existem duas formas distintas de Guerra de Informação: Guerra de Informação Ofensiva, muito utilizada pelos ciberterroristas e a Guerra de Informação Defensiva (relacionada com a segurança e integridade da informação e dos sistemas de informação).

A **Guerra de Informação Ofensiva** inclui todas as acções que permitam a intrusão nos sistemas de informação dos adversários, alterando-lhes os sistemas para produzir determinadas acções, ou provocando a sua degradação progressiva até à sua inutilização. Estas acções são orientadas essencialmente para três níveis distintos:

- Nível Físico;
- Nível de Informação ou Estrutural;
- Nível Comportamental ou Semântico.

Referimos já anteriormente os tipos de armas utilizados e respectivos efeitos, por isso, vamos apenas abordar a importância da Decepção e da Guerra Psicológica no âmbito da Guerra de Informação.

A **Decepção** pode ser desencadeada através de múltiplas formas (mensagens, “sitios”, correio electrónico, acções físicas, panfletos, media, etc.) com a finalidade de ocultar, destruir ou falsificar informação. Por sua vez, a **Guerra Psicológica** pretende afectar a mente humana através do medo, da afectação lógica e de outros processos mentais, para levar o opositor a cometer erros de raciocínio.

A Guerra de Informação pode desenrolar-se em três **níveis de acção**: “*Hackers*”, Ciberguerra e “*Netwar*” ou Guerra em Rede.

No nível mais elementar e ao mesmo tempo constituindo a ameaça mais frequente, incluem-se os **Piratas Electrónicos** (Hackers e Ciberterroristas); no entanto, é também a este nível que é mais difícil distinguir a simples intrusão na rede, da agressão premeditada.

No segundo nível, surge a **Ciberguerra**, que tem por objectivo invadir os sistemas do adversário, para roubar ou corromper informação ou no limite,

para inutilizar a informação e os respectivos sistemas. De acordo com Arquilla e Ronfeldt, a Ciberguerra é utilizada para “*conduzir operações militares de acordo com determinados princípios da informação*”<sup>20</sup>. Por sua vez, Rathmell refere que “*os conflitos inter-estaduais ou transnacionais que envolvem Sub-estados ou quase-Estados, têm aumentado à medida que as redes dos países industrializados se tornam mais complexas e, conseqüentemente, aumentam também as vulnerabilidades das mesmas redes que se constituem como alvo remunerador*”. A diferença relativamente aos Hackers é que os ataques não são isolados e têm por objectivo interferir ou destruir os sistemas de informação do inimigo, país ou organização.

O terceiro nível é o mais complexo e designa-se por “*Netwar*” ou Guerra em Rede. Nos seus objectivos estão incluídos não só ataques aos sistemas de informação, como também, a interrupção de todos os serviços de um país e a difusão de mensagens destinadas a confundir e a gerar o pânico na opinião pública. Não se trata apenas de danificar o sistema operativo do computador ou da rede, mas também, afectar a informação neles contida. A “*Netwar*” pode também ser utilizada pelos governos para combater grupos dissidentes, terroristas ou associações criminosas (droga, crime organizado, prostituição, pedofilia, etc.).

No limite, a Guerra de Informação Ofensiva pode provocar a inoperacionalidade de todos os sistemas vitais de comando e controlo de uma força ou de um estado.

Na Guerra de Informação Ofensiva incluem-se igualmente as acções de difusão de propaganda, utilizando os media e outras acções de cariz sociológico como: o **activismo** (utilização da Internet em prol de determinada causa) e o **hacktivismo** (acção destrutiva dos hackers em prol de determinada causa, incluindo a manipulação e destruição de informação e dos respectivos sistemas).

#### f. *Utilização da Internet em proveito do Terrorismo Convencional*

O terrorismo é um fenómeno cada vez mais internacional e, para o efeito, muito têm contribuído os seguintes aspectos: as comunicações globais; a transferência electrónica de dados; a utilização da Internet para fins propagandísticos, o recrutamento, a troca de tácticas, a aquisição de armas

---

<sup>20</sup> Toby Blyth, “*Cyberterrorism and Private Corporations*”, 11<sup>th</sup> Annual International Symposium on Criminal Justice ISSUES, pág. 15, <http://afgen.com/terrorism1.html>.

e o movimento de fundos financeiros. “É o caso do *Jihad News* (216.180.224.51), *Kavkaz.org*, *Chechen.org/kavkaz* (ligado a uma facção extrema da guerrilha chechena, e em certa medida oposto a), *Azzam Pub.* ([www.azzam.com](http://www.azzam.com)), *waaqiah.com*, *maktabah.net*, *Jihadunspun.net*, *jusplus.net*, *islamic-news.co.uk*, *supportersofshariah.co.uk*, <http://www.202.43.163.180/~acom/afghan/>, e <http://www.66.132.29.71>, etc.”<sup>21</sup>

Por seu lado, os países procuram acentuar o nível de segurança ante uma rede que abre muitas janelas e que pode afectar desde as suas economias, até às suas centrais eléctricas e nucleares, unidades militares, bases de dados com informação estratégica e outros alvos remuneradores para os terroristas. Num mundo globalizado, com uma rede global, começam também agora a aparecer os problemas globais que afectam toda a rede e poderão causar prejuízos de milhões de dólares. Afinal, quais são as vantagens que o ciberespaço tem para oferecer ao terrorismo convencional?

- (1) Anonimato – não há exposição física do atacante e, caso a operação se transforme num fracasso, o ciberterrorista pode analisar o erro, adquirir experiência e aprender como operar correctamente para ter sucesso na próxima vez, sem colocar em risco a sua localização. A proliferação dos pontos de acesso anónimos (por ex.: cibercafés), vem também contribuir para o anonimato destes terroristas do ciberespaço.
- (2) O grau de investimento é mínimo comparado com outro tipo de ataque; a sua influência pode alcançar proporções monumentais, dado que se trata de manipular os elementos tecnológicos do adversário ou pelo menos, privá-lo das suas próprias defesas.
- (3) Difusão da sua “cultura terrorista”, onde se inclui a sua história, postulados e objectivos a atingir com a sua causa.
- (4) Para fins propagandísticos, podem facilmente comunicar os seus objectivos de forma global e sem grandes encargos, tendo os seus actos, quase sempre, cobertura dos “*media*”. A CNN (Cable News Network) e as outras redes de notícias proporcionam, aos terroristas, um meio para disseminar a sua mensagem de medo e intimidação.
- (5) Obtenção de Informação sobre a tecnologia que pode ser utilizada para fins terroristas, com por exemplo: a construção de bombas de impulso

---

<sup>21</sup> Nuno Rogeiro, “O Inimigo Público – Carl Schmitt, Bin Laden e o Terrorismo Pós-Moderno”, pág.158.

- electromagnético (site: <http://www.cs.monash.edu.au/~carlo/>) ou a interferência com satélites de comunicações (site: <http://www.spectre.com>).
- (6) *Para recrutar pessoal* para as suas causas.
  - (7) *Para o comando e controlo das operações*, utilizam a rede como meio de comunicações.
  - (8) *Para administrar, financiar* e para efeitos logísticos de toda a sua actividade.
  - (9) *A transferência de fundos financeiros* – hoje é vulgar realizar depósitos através da *Net* e fazer movimentos financeiros sem necessidade de comprometer a sua identidade.

*“Os terroristas utilizam o ciberespaço para facilitarem as formas de terrorismo convencional tais como, bombardeamentos. Colocam web sites para difundirem as suas mensagens e para recrutarem defensores da causa e utilizam a internet para comunicarem e para coordenação. Assim, existem algumas indicações sobre a actuação de ciberterrorismo, ora atacam isoladamente ou em conjugação com actos físicos violentos”*<sup>22</sup>. A outra manifestação de violência através da Internet é produzida quando os grupos terroristas comunicam, utilizando mensagens de correio electrónico cifradas, através dos quais trocam dados relativos a possíveis vítimas, tais como: domicílio, itinerários realizados pelo sujeito, fotografias, etc. Recebem informação através de sites institucionais e de partidos políticos, trocam tácticas, armazenam e difundem as suas mensagens com o fim de conseguir adeptos.

Além destas vantagens, as organizações terroristas podem realizar ataques ciberterroristas conjugados com ataques convencionais (sequestro de pessoas importantes, atentados bombistas, ataques com vírus aos centros nevrálgicos de informação, etc.) causando o caos e o pânico nas cidades. O seu grau de exposição é mínimo comparado com outro tipo de ataque (não requer manuseamento de explosivos ou missões suicidas) e a sua influência pode alcançar proporções dramáticas. Encontramo-nos, por isso, ante um novo estilo de conflito para o qual dificilmente se poderá vigiar a sua extensa fronteira global.

*“O Mundo físico e o mundo virtual têm pontos comuns, os quais podem e serão usados como alvos por uma nova geração de violentos – os ciberterroristas.”*<sup>23</sup>

---

<sup>22</sup> Dorothy E. Denning, “Cyberterrorism”, <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

<sup>23</sup> Esteban Falcionelli, “Ciberterrorismo, outro de los nuevos rostros del miedo”, [http://www.forodeseguridad.com/art\\_ciberterrorismo.htm](http://www.forodeseguridad.com/art_ciberterrorismo.htm).

## 4. Cibersegurança

### a. *Generalidades*

A evolução vertiginosa da Internet, quer ao nível dos conteúdos, quer de utilizadores, não foi acompanhada pelo respectivo suporte jurídico, para normalizar o acesso e utilização desta rede mundial de informação e conhecimento, nem para regular os comportamentos anormais (utilização fraudulenta da informação e ataques aos sistemas de informação).

O termo ciberterrorismo ganhou maior impacto a partir dos atentados ao World Trade Center (WTC) de Nova Iorque, em 11 de Setembro de 2001, nos EUA. Dada a gravidade da matéria, vários governos mundiais têm debatido medidas para fiscalizar e controlar o tráfego na Internet, com o objectivo de prevenir ataques de ciberterroristas. Estas invasões criminosas têm causado inúmeros prejuízos às organizações, sendo os mais frequentes o roubo de informação confidencial e os furtos económicos, que na maioria dos casos não são comunicados, porque as instituições ou empresas têm medo de perder a confiança dos seus clientes e accionistas, bem como o receio que a sua imagem seja afectada pela divulgação dos ataques sofridos. Actualmente, as empresas estão interessadas em cooperar na luta contra o cibercrime; no entanto, as medidas a adoptar não deverão ser demasiado dispendiosas, para evitar que a Internet fique menos acessível aos utilizadores e que os custos de acesso aumentem.



Face à dependência das actividades vitais dos Estados relativamente aos sistemas de computadores e às telecomunicações, com tendência para aumentar no futuro, devem equacionar-se medidas para minimizar os ataques criminosos que visam gerar o pânico nas populações. *“Os problemas de segurança das redes e da informação são de âmbito mundial, dado que os canais de comunicação electrónica não param nas fronteiras nacionais ou europeias. É necessária uma melhor cooperação internacional nesta matéria”*<sup>24</sup>. *“No final do ano 2000, foram feitos estudos pelo governo americano sobre o real impacto que ciberataques teriam na economia global e na sociedade*

<sup>24</sup> Carlos Marçalo, “Cibersegurança europeia ganha Centro”, Jornal Expresso, semana de 21 a 27 de Fev 2003.

*como um todo. Os resultados deste estudo, que recentemente foi banido da Internet pelo próprio governo americano, especulavam a possibilidade da paralização de fabricas centrais de energia eléctrica, além de inúmeros problemas nos serviços de água e telecomunicações”<sup>25</sup>.*

Após o 11 de Setembro de 2001, a preocupação dos representantes governamentais com a defesa do ciberespaço aumentou, principalmente nos Estados Unidos. Por isso, a principal preocupação dos norte Americanos tem sido reduzir as ameaça e as vulnerabilidades a ataques orquestrados por ciberterroristas, ou por outras associações criminosas através do ciberespaço. Desde de 1980 que a Comissão Europeia tem mostrado a sua preocupação relativamente às ameaças do *hacking* e às várias formas de cibercrime; no entanto, praticamente não legislou sobre questões relacionadas com o ciberterrorismo.

A vulnerabilidade dos computadores não é igual para todos, (uns são mais vulneráveis do que outros) dependendo de vários factores, tais como: o tipo de segurança implementado, a organização ou instituição a que pertence, o país ou região onde está instalado, etc. A atractividade de determinada informação para os ciberterroristas, cibercriminosos e ciberdelinquentes é diferente, se o servidor web pertencer ao Pentágono, ao Banco de Portugal, à Sonae ou a um particular. Ela depende dos objectivos de quem realiza o ataque; por exemplo: se a finalidade for angariar fundos, é mais lucrativo tentar um ataque electrónico a uma entidade bancaria; mas se o objectivo é político, então é mais compensador realizar um ataque a uma rede governamental ou militar.

Quando se fala em segurança, uma das coisas que nos preocupa é a de manter a nossa privacidade, evitando que outras pessoas tenham acesso aos nossos dados pessoais. Será que os sistemas de segurança são uma ameaça à segurança nacional? Se a segurança na Internet é tão importante porque não desenvolve o governo esses mesmos sistemas, tornando-os compatíveis? Actualmente para aceder à Internet, basta ter um computador e um modem, ou ter acesso a estes meios e conhecer as respectivas passwords de acesso. A partir daqui, o vulgar utilizador pode ter acesso a toda a informação alojada noutros computadores, também ligados à Net. Embora a maioria dos cibernautas que aí navegam sejam bem intencionados, isto é, procuram

---

<sup>25</sup> Paulo Perez, “*Terror nos EUA - Ameaça do Ciberterrorismo se torna realidade*”, <http://www.novomilenio.inf.br/ano01/0110d008.htm>.

informação, cultura, oportunidades de negócio, laser, etc., existe uma percentagem de pessoas que utilizam o ciberespaço para a delinquência, extorsão e roubo de fundos, destruição de informação, de dados e de sistemas de informação. Assim, para evitar os efeitos nefastos originados pelo acesso à informação confidencial e à respectiva utilização de forma fraudulenta, por utilizadores não autorizados, dado que no caso das empresas de Comércio-Electrónico, isso poderia significar prejuízos de milhões de Dólares/Euros, muitas empresas começaram a desenvolver software e sistemas que permitem isolar a parte do computador ligado à Internet das outras partes do sistema.

**b. *Porque Razão são os Servidores Web Atacados?***

Uma das razões para os ataques aos Servidores *Web* é porque eles constituem um grande meio de publicidade das empresas ou de outras organizações na Internet, e por isso, um ataque bem sucedido pode ser visto por milhares de pessoas em pouco tempo. Essas acções ofensivas podem ter um objectivo ideológico, financeiro ou apenas simples vandalismo. Outra razão, relaciona-se com o comércio que se pratica na Internet; os servidores *web* contém informações financeiras, tais como os números de cartões de crédito, que são um polo de interesse para muitos criminosos. Diversas organizações utilizam tecnologia *web* para distribuir ou comunicar informação privada aos seus membros e associados, não só internamente, mas também externamente. Esta informação interessa igualmente às empresas concorrentes ou aos Estados adversários. Os servidores *web* são utilizados por pessoas tanto no interior, como no exterior da organização e fazem a ponte entre a sua rede interna e a rede externa; por isso, constituem um ponto privilegiado, dada a sua conectividade à rede, para aceder a outros computadores no interior da organização.

O problema da segurança pode sistematizar-se em três partes distintas:

- A segurança no Servidor Web;
- A segurança da informação que viaja entre o Servidor e o Browser;
- A segurança do computador do utilizador.

A segurança dos servidores Web depende de vários factores: por um lado, da segurança da máquina onde está instalado o servidor web da empresa ou instituição; por outro lado, dos conteúdos existentes no servidor e da sua maior ou menor atractividade para fins ilícitos. O que se entende por servidor

seguro? Este conceito depende do agente social em questão. Para os utilizadores, é o servidor que salvaguarda a informação pessoal que lhe é transmitida, que mantenha a sua privacidade, que não permita ao seu *browser* o *download* de vírus e outros programas perigosos para o seu computador. No entanto, para os vendedores, um servidor web seguro, é um programa que implementa alguns protocolos de criptografia, por forma a que a informação transferida entre um servidor e o *browser* não seja visualizada por quem não esteja autorizado.

Existem várias formas para a proteger a informação que transita na rede:

- Proteger fisicamente a rede para evitar o acesso por utilizadores não autorizados;
- Esconder a informação a transmitir no meio de informação aparentemente sem interesse;
- Encriptar a informação tornando-a apenas visualizável por quem possuir a chave correcta.

É impossível proteger toda a rede. Em consequência, a 2.<sup>a</sup> forma referenciada só resulta se a pessoa da qual se pretende esconder a informação, não conhece como a essa vai escondida; deste modo a única opção viável é a encriptação. Em termos gerais, os problemas de segurança mais comuns estão relacionados com os *browsers web*. À medida que estes problemas vão sendo corrigidos, devido à evolução tecnológica, surgem outros nas novas versões dos *browsers*. Para além disso, existem problemas relacionados com as linguagens de programação e ambientes de trabalho que foram introduzidos para tornar a Internet e os seus conteúdos mais atractivos.

### c. *Segurança dos Servidores Web e dos Utilizadores*

Uma das formas mais comuns de proteger as empresas ou instituições de ataques criminosos ou fraudulentos, é a criação de *firewalls*, para separar a Internet do servidor interno (Intranet). Estas *firewalls* deixam passar algumas ligações e bloqueiam a passagem a outras. A sua configuração é feita de modo a que as ligações externas passem por determinados pontos da rede bem monitorizados. No entanto, após a sua



implementação, é necessário continuar a manter a vigilância, dado que este sistema também pode falhar, bem como estar sempre a par das actualizações efectuadas pelos fabricantes. Existem sistemas já desenvolvidos para fazer a monitorização continua das redes internas e dos respectivos acessos, quer internos, quer externos.

Ao nível do utilizador, a forma de identificação mais usada são as passwords, mas estas podem ser esquecidas, interceptadas, comunicadas e, para as validar, o computador tem de ter um ficheiro contendo todas as *passwords*. Existem contudo outras formas de identificação, como por exemplo: uso de testemunhos que autorizam quem os possua; contudo, estes são vulneráveis ao roubo e podem ser facilmente copiados; utilização da informação biológica da pessoa (impressões digitais, imagens da retina, informação contida no ADN, etc.); utilização de assinaturas digitais, etc.

#### d. *Criptografia na Web*

A melhor solução que existe actualmente no mercado para transmitir dados de uma forma segura é realizar a sua encriptação, ou seja, utilizar os métodos da criptografia <sup>26</sup>. Este método é muito seguro e mesmo que um intruso intercepte as comunicações entre o emissor e o destinatário, só consegue aceder aos dados quem possuir a chave para descriptar o *ciphertext*; caso contrário, a informação não lhe serve para nada.

A Criptografia desempenha um papel fundamental na segurança da informação que circula na Web, especificamente na:

- Confidencialidade, garantindo que só o destinatário da mensagem tem a chave; por isso, os intrusos que observarem a mensagem não poderão decifrá-la;
- Autenticação, através do uso dos certificados digitais é possível ter a certeza de quem envia e recebe a mensagem, obtendo-se a autenticação;
- Integridade, obtida pela autenticação da mensagem garantindo a sua inviolabilidade;

O acesso à tecnologia é livre; assim, tanto têm acesso pessoas conscientes e bem

---

<sup>26</sup> A *criptografia* permite que a informação seja enviada numa forma segura, garantindo que só o destinatário é capaz de a visualizar. O princípio básico da criptografia é o seguinte: a mensagem antes de ser enviada (*plaintext*) é codificada usando algoritmos de criptografia (*encriptação*); depois de encriptada (*ciphertext*), a mensagem é transmitida e, só no destinatário, convertida (*desencriptação*). Este processo só é possível conhecendo-se a chave.

intencionadas, como pessoas sem escrúpulos. Deste modo “*parece que o uso da criptografia se converteu numa ferramenta de trabalho para os grupos extremistas que utilizam a rede para trocar informação encriptada com o objectivo de preparar atentados, realizar intercâmbios de informação: imagens e mapas, notícias financeiras, desportos, chats ou páginas pornográficas, que são distribuídos graças ao emprego de portais populares da Internet. São dados que viajam pela rede encriptados com programas e que tornam quase impossível a operação de decifrar uma mensagem se não possuímos a respectiva chave*”<sup>27</sup>.

#### e. **Guerra de Informação Defensiva**

A **Guerra de Informação Defensiva** inclui todas as medidas que garantam a protecção da informação e dos nossos sistemas de informação a ataques, quer internos, quer externos. Nestas operações incluem-se acções de prevenção, de dissuasão, de alerta, de detecção do ataque, de preparação para a emergência, de contra-ataque e de recuperação da área afectada.

As medidas de protecção da informação compreendem:

- A segurança das radiações, evitando-se que a informação contida numa radiação electromagnética seja interceptada e posteriormente utilizada;
- A segurança física e electrónica, concebida para garantir que só terão acesso à informação as pessoas devidamente autorizadas;
- A segurança criptográfica e a sobrevivência das comunicações, garantindo um nível de desempenho mínimo, mesmo quando sujeitas a ataques.

A Guerra de Informação Defensiva inclui acções no âmbito estratégico, de segurança operacional e de segurança técnica. Ao **nível estratégico** definem-se as “políticas” de emprego das armas de informação, possíveis formas de retaliação, publicação de legislação punitiva para este tipo de crime, etc. Incluem-se aqui os sistemas de monitorização de correio electrónico, como o “*Carnivore*”<sup>28</sup> utilizado pelo FBI e sistemas para detectar todas as formas de comunicações electrónicas, como o “*Echelon*”<sup>29</sup>. Na **segurança operacional**

<sup>27</sup> Juan J. Sánchez “*Ciberterrorismo – La Amenaza Fantasma*”, BIT 136, Nov-Dec 2002.

<sup>28</sup> É um tipo de software utilizado pelo FBI para “*monitorizar*” e-mails, acessos a sites, downloads de arquivos e grupos de discussão (Chats) considerados suspeitos. No entanto, se as mensagens estiverem encriptadas, já é mais difícil ou até impossível, nos casos de chaves mais complexas.

<sup>29</sup> É uma rede de vigilância global das telecomunicações que é utilizada para benefício político dos países membros (EUA, Canadá, Reino Unido, Austrália e Nova Zelândia), bem como para proveito das respectivas empresas e para espionagem comercial. Esta rede é formada por 120 satélites com capacidade para interceptar e decifrar 189 milhões de mensagens electrónicas por hora.

englobam-se as medidas de segurança física, nomeadamente, sistemas de controlo de acessos, para proteger pessoal, material e *software*. Ao nível da **segurança técnica**, pretende-se negar o acesso indevido à informação e aos sistemas de informação através da utilização de *passwords*, chaves digitais, introdução de *firewalls* nos servidores, etc.

#### f. *Situação actual dos EUA*

Devido à sofisticação dos *hackers*, que tem vindo a aumentar e à sua capacidade de realizarem ataques inesperados a instituições ou empresas específicas, os EUA estabeleceram uma “*Estratégia Nacional para Segurança do Ciberespaço*” (“*National Strategy to Secure Cyberspace*”), articulada com a “*National Strategy for Homeland Security*”, para evitar que aqueles ataques degenerem em situações de caos e de pânico generalizado ou que destruam informações e sistemas de informação importantes, traduzindo-se em prejuízos de milhões de dólares.



Os objectivos definidos para esta estratégia de segurança do ciberespaço são os seguintes:

- Prevenir ciberataques contra infra-estruturas americanas críticas;
- Reduzir a vulnerabilidade nacional aos ciberataques;
- Minimizar danos e ganhar tempo antes da ocorrência de ciberataques.

A primeira medida adoptada foi estabelecer, por níveis, os tipos de ameaças com origem no ciberespaço e tipificar os actores desta nova forma de crime organizado. Com base nesta classificação, pretende-se implementar as medidas mais aconselhadas para combate à ciberdelinquência, ciberfraude, cibercrime, ciberterrorismo, etc.

Esta classificação está agrupada em cinco níveis, sendo o quinto nível o mais importante, porque envolve riscos ao nível global. A gestão e as acções a adoptar são particularmente complexas, dado que existem vários grupos de actores; a saber:

- **Nível 1 – O Utilizador e o Pequeno Negócio** – a este nível, os actores não fazem parte de infra-estruturas críticas, mas podem ser controlados remotamente para se iniciarem ataques a outros níveis.

- **Nível 2 – A Grande Empresa** – os ataques a estas empresas são muito comuns e muitas delas fazem parte de infra-estruturas críticas; consequentemente, devem estabelecer-se "políticas" de segurança restritivas, para evitar ataques à informação ou aos sistemas de informação, para fins ilícitos ou no mínimo, atenuar os efeitos nefastos dos referidos ataques.
- **Nível 3 – Sectores Críticos/Infra-estruturas** – os ataques a áreas específicas de determinados sectores críticos, como as redes de gestão e controlo da distribuição de água ou electricidade, podem criar vulnerabilidades que afectarão todo sector e terão implicações ao nível dos utentes do serviço, materializadas por cortes na distribuição de água e electricidade, aumentos e diminuições na facturação, prejudicando o consumidor ou a empresa. Por isso, há necessidade de conjugar esforços no âmbito da segurança dos sectores críticos, por forma a reduzir as suas vulnerabilidades parciais e globais.
- **Nível 4 – Valores e Vulnerabilidades Nacionais** – nalgumas áreas, a segurança não depende unicamente das empresas, nem a sua resolução pode ser um acto isolado. Há determinados assuntos-chave na utilização da Internet, tais como, a formação e a certificação, que deverão ser realizados pelo Estado, dado que são de interesse nacional.
- **Nível 5 – Global** – o ciberespaço é constituído por uma rede mundial de computadores que partilha standards internacionais e que permitem a operacionalidade e inter-conectividade entre os computadores, acedendo ao vasto “*planeta*” da informação que disponibiliza. Devido à globalização, os problemas que afectam um país ou continente terão repercussões noutras partes do mundo. Por isso, só através da cooperação e partilha de informação sobre actividades ilícitas, ao nível mundial, será mais fácil isolar ou capturar os cibercriminosos.

As recomendações e medidas aconselhadas pela Entidade de Segurança Nacional dos EUA para os diversos grupos de actores (empresas/organizações, população, etc.), foram agrupadas de acordo com o seu grau de importância, em cinco prioridades:

- 1.<sup>a</sup>: Sistema de segurança para o ciberespaço nacional;
- 2.<sup>a</sup>: Segurança do ciberespaço e programas para redução das ameaças e vulnerabilidades;
- 3.<sup>a</sup>: Ciberespaço nacional e programas de treino;

- 4.<sup>a</sup>: Segurança do ciberespaço governamental;
- 5.<sup>a</sup>: Segurança nacional e cooperação internacional para a segurança do ciberespaço.

No quadro que se segue, apresentamos as medidas e recomendações da “Estratégia Nacional de Segurança para o Ciberespaço” dos EUA, por prioridades:

Prioridade	Medidas e Recomendações
1. <sup>a</sup>	<ol style="list-style-type: none"> <li>1. Estabelecer uma arquitetura pública-privada para responder aos ataques ao nível nacional.</li> <li>2. Fornecer as vulnerabilidades de acesso, para o desenvolvimento e análise de táticas e estratégias de ciberataques.</li> <li>3. Incentivar o desenvolvimento do sector privado para fiscalizar o ciberespaço.</li> <li>4. Difundir avisos e informação com medidas para evitar ciberataques e para coordenação de crises no ciberespaço.</li> <li>5. Aumentar a capacidade para a gestão de crises nacionais.</li> <li>6. Coordenar, num plano nacional de contingência, o processo de participação no desenvolvimento.</li> <li>7. Treinar um plano contínuo para sistemas federais.</li> <li>8. Aumentar a troca de informações relativa a ataques, ameaças e vulnerabilidades.</li> </ol>
2. <sup>a</sup>	<ol style="list-style-type: none"> <li>1. Evitar esforços para prevenir ciberataques.</li> <li>2. Criar uma base de dados de vulnerabilidades para melhor compreender as ameaças do ciberespaço.</li> <li>3. Criar mecanismos de segurança na Internet tais como o “<i>routing</i>” (reencaminhamento de circuitos) e melhoria de protocolos.</li> <li>4. Aumentar a utilização de sistemas de controlo digital/supervisão na aquisição da informação.</li> <li>5. Reduzir e corrigir as vulnerabilidades do software.</li> <li>6. Compreender a interdependência das estruturas e aumentar a segurança física dos ciberistemas e dos sistemas de telecomunicações.</li> <li>7. Agendar a investigação e desenvolvimento de cibersegurança.</li> <li>8. Acesso a sistemas de segurança de emergência.</li> </ol>
3. <sup>a</sup>	<ol style="list-style-type: none"> <li>1. Promover a campanha de informação nacional para todos os americanos.</li> <li>2. Criar planos de educação adequados para apoio às necessidades de cibersegurança.</li> <li>3. Aumentar a eficácia dos treinos do programa cibersegurança actual.</li> <li>4. Promover um apoio coordenado para reconhecimento de certificados de cibersegurança.</li> </ol>

Prioridade	Medidas e Recomendações
4. <sup>a</sup>	<ol style="list-style-type: none"> <li>1. Testar continuamente as ameaças e vulnerabilidades aos ciberistemas federais.</li> <li>2. Autenticar e manter actualizada a relação de utilizadores autorizados com acesso aos sistemas federais.</li> <li>3. Garantir a segurança das redes locais, sem fios.</li> <li>4. Aumentar a segurança do outsourcing do governo.</li> <li>5. Promover a utilização de programas e tecnologias de segurança de informação pelos estados e governos locais, partilhando a informação e análise com outras entidades a considerar.</li> </ol>
5. <sup>a</sup>	<ol style="list-style-type: none"> <li>1. Desenvolver esforços no âmbito da contra-informação.</li> <li>2. Aumentar a intensidade da resposta a ataques do ciberespaço.</li> <li>3. Aumentar a coordenação e a resposta a ataques dentro da comunidade de segurança dos Estados Unidos.</li> <li>4. Trabalhar com a indústria e com organizações internacionais para facilitar o diálogo e as alianças neste combate.</li> <li>5. Criar vigilantes de redes nacionais e internacionais para detectar ciberataques.</li> <li>6. Encorajar outras nações a aceder à convenção do Conselho da Europa sobre as leis e procedimentos do ciberterrorismo.</li> </ol>

#### ***g. Situação actual da União Europeia***

A União Europeia (UE), apesar da iniciativa da *e-europe*, em Dezembro de 1999, para garantir o acesso às novas tecnologias digitais e beneficiar das vantagens competitivas da Sociedade da Informação, tem ainda um longo caminho a percorrer na direcção da segurança dos sistemas de informação e redes de suporte. A UE adoptou medidas para: combater conteúdos ilegais e perigosos na Internet; proteger propriedade intelectual e os dados pessoais; promover o comércio electrónico e o uso de assinaturas electrónicas e para garantir a segurança das transacções. No entanto, ficaram ainda de fora as medidas contra o ciberterrorismo ou pelo menos, medidas de igual importância às desenvolvidas pelos EUA.

Em Junho de 2000, na reunião do Conselho Europeu realizado em Santa Maria da Feira, foi adoptado um plano de acção para o *e-europe*, que deveria ter sido implementado até ao fim de 2002, cujos pontos principais eram a segurança da rede e a luta contra o cibercrime.

Tendo por base o plano de acção sobre o cibercrime e ciberterrorismo, aprovado em Junho de 2000, o Conselho da Europa considerou quatro categorias

de ofensas criminosas. Os tópicos principais, endereçados por legislação, no que concerne a crimes relacionados com computadores na UE, ou em Estados Membros, são:

- Ofensa de privacidade: alguns países adoptaram leis criminais contra a recolha, guarda, modificação e difusão ilegal de dados pessoais. Os países da UE, aprovaram duas directivas para a protecção da privacidade da informação pessoal; assim o artigo 24 da Directiva 95/46/EC obriga os membros a adoptar todas as medidas adequadas para garantir a implementação das directivas orientadoras, incluindo sanções a impor em caso de infracção das leis nacionais. Os direitos fundamentais à privacidade e à protecção da informação ainda foram incluídos nos capítulos dos direitos humanos da UE.
- Conteúdos relacionados com ofensas: a difusão, especialmente via Internet, de pornografia, em particular, de pornografia infantil, declarações racistas e informação a incitar à violência, levanta questões sobre a extensão destes actos e sobre a legislação criminal a adoptar. Para a UE, os conteúdos anteriormente referidos, são proibidos, quer on-line, quer off-line. Por isso, os autores ou fornecedores de conteúdos podem ser levados a tribunal. A responsabilidade dos fornecedores de serviços intermédios (redes ou servidores usados para a transmissão de informação ou para guardar parte da informação) é controlada pela directiva do comércio electrónico.
- Crimes económicos, acesso não autorizado e sabotagem: muitos países têm adoptado leis relativas a crimes de computadores, utilizados para fins económicos e definiram uma nova ofensiva para penalizarem quem tente aceder a computadores, sem que para tal esteja autorizado (por ex.: hacking, sabotagem de computadores, dissiminação de vírus, espionagem, falsificação e fraude por computador). O objecto do crime é muitas vezes intangível, de que é exemplo o acesso directo aos programas de computadores para realizarem depósitos de dinheiro nos bancos. Actualmente, a UE não dispõe de instrumentos para vigiar este tipo de actividade ilegal. Relativamente à prevenção, a recente regulamentação adoptada para a comercialização de produtos e serviços, contribuiu significativamente para liberalizar a utilização dos produtos encriptados.
- Ofensas à propriedade intelectual: foram adoptadas as duas directivas, para a protecção legal de programas de computadores e bases de dados. O Conselho da Europa adoptou uma posição comum para protecção dos direitos de autor cuja violação será punida, não só nos aspectos relacionados

com os direitos, mas também, com as medidas tecnológicas desenhadas para proteger os produtos ou serviços.

A Internet tornou-se um veículo muito importante em termos comerciais, havendo, assim, necessidade de adoptar regras e procedimentos para evitar os assaltos informáticos.

A UE criou a Agência Europeia para a Segurança das Redes e da Informação, cujo objectivo é funcionar como centro de competências para aconselhamento dos governos dos Estados membros e das instituições europeias em matérias relacionadas com a cibersegurança.

As medidas e tecnologias propostas para garantir a segurança das infra-estruturas da informação na UE são as seguintes:

- Garantir a segurança das infra-estruturas e dos computadores através da utilização de chaves públicas e do desenvolvimento de protocolos seguros.
- Garantir a segurança de ambientes públicos e privados através de *software* específico, *firewalls*, programas antivírus, sistemas de gestão de direitos electrónicos e encriptação.
- Garantir a segurança de utilizadores autorizados, a utilização de *Smart Cards*, identificação biométrica e assinatura electrónica.
- A criação de uma polícia especial que garanta a segurança dos sistemas de informação.
- Melhorar a cooperação entre a indústria, as organizações e as autoridades, para a protecção dos respectivos dados.
- Fomentar a iniciativa das comunidades e indústria, relativamente à segurança dos produtos.
- A Comissão Europeia reconhece que há necessidade de acompanhar o diálogo entre utilizadores e indústria, implementando para o efeito legislação específica.
- Criação de unidades especializadas com capacidade de resposta rápida aos pedidos de informação com suspeitas de ataques. Os formatos comuns para a troca dessa informação deverão ser definidos por especialistas do G-8.
- Nos casos mais complicados, pode actuar para aplicar as leis nacionais e internacionais e para receber todas as queixas sobre utilizadores ilegais da Internet.
- Aprovar e desenvolver computadores com técnicas específicas para investigar e detectar a utilização desses meios para cometer crimes de qualquer tipo.
- Actuar como um centro de informação e de partilha de experiências na área do cibercrime.

Os Estados membros deverão aproximar as respectivas legislações nacionais, da legislação actualmente existente na UE, no que diz respeito ao *hacking*, ataques aos serviços e pornografia infantil. Esta aproximação de procedimentos legislativos irá garantir, por um lado, maior protecção às vítimas, e por outro, vai reforçar o poder das agências para investigar os ataques cometidos contra os respectivos países e actuar em cooperação com outros estados membros.

Na Europa existe um princípio geral de confidencialidade das comunicações; por isso, é ilegal realizar escutas, a menos que estejam autorizadas. Para combater os ataques aos computadores é necessário um esforço contínuo na prevenção e no treino de pessoal especializado, incluindo polícias. Deste modo, a UE deverá disponibilizar, no futuro uma base de dados sobre crimes cometidos através dos computadores.

Tendo como objectivo a criação de regras/ferramentas comuns entre a polícia e a justiça, sobre crimes de computador, deve implementar-se o reforço da lei, disponibilizando às autoridades judiciais, informação e arquivos para análise e avaliação.

#### h. *Futuro*

O ciberespaço é composto por centenas de milhares de computadores interligados através de servidores, *routers*, *switches* e cabos de fibra óptica, que constituem o sistema nervoso central da nossa sociedade.

Os Estados não conseguem garantir a segurança total da rede; como tal, devem contribuir activamente para a segurança dos sectores críticos implementando medidas que contribuam para reduzir a sua vulnerabilidade aos ataques indesejados, criando fóruns, apoiados pelos EUA e UE, para reforçar a cooperação das agências de segurança, com fornecedores de serviços Internet, operadores de telecomunicações, organizações civis, associações de consumidores e autoridades de protecção de dados. Estes fóruns deverão ter em atenção as seguintes áreas:

- Desenvolvimento da cooperação entre a indústria e os governos.
- Desenvolver formatos normalizados para solicitar informação à indústria e para aumentar o reforço da lei na Internet, quando se comunica com fornecedores de serviços.



- Encorajar o desenvolvimento e implementação de códigos de conduta, na partilha de informação entre a indústria e o governo.
- Encorajar a troca de informação sobre crimes graves, particularmente entre a indústria e agências de segurança.
- Incentivar o cumprimento da lei, durante a fase de desenvolvimento de novas tecnologias.
- Promover o desenvolvimento de mecanismos de gestão de crises para prevenir, identificar e lidar com ameaças ou distúrbios sobre infra-estruturas de informações.
- Encorajar a cooperação, nos termos da lei, entre a indústria e os utilizadores de serviços.

Através da adopção destas medidas, espera-se aumentar a segurança dos computadores onde estão alojados sistemas de informação, tornando mais seguras as transacções de informação e as operações comerciais, entre as pessoas e as instituições. Os custos relativos à implementação das medidas de segurança são significativamente inferiores aos prejuízos causados pelos ataques dos ciberterroristas.

*“A Internet tornou-se demasiado valiosa para deixar de ser utilizada, mas também muito arriscada de utilizar sem o perigo de algum utilizador mal intencionado entrar fortuitamente no nosso PC ou mesmo na nossa LAN”<sup>30</sup>.*

## 5. Conclusões

Vivemos hoje na Era da Informação e do Conhecimento, caracterizada pela digitalização dos vários sectores de actividade dos Estados e pelo desenvolvimento de Tecnologias de Informação. A Internet e o desenvolvimento das comunicações, por um lado, vieram acelerar todo este processo, criando novas necessidades de informação, partilha de conhecimento independentemente da distância física entre os interlocutores, criação de novos serviços que permitam realizar determinadas funções sem sairmos de casa (por ex.: Comércio-electrónico, Homebanking, etc.); por outro lado, criaram novas vulnerabilidades: quaisquer acontecimentos, especialmente os económicos, têm hoje repercussões à escala mundial, acrescentando ao facto deste meio poder ser utilizado de forma fraudulenta ou criminosa, de acordo com os interesses dos diversos actores (por ex.: Ciberterrorismo, Guerra da Informação, etc.).

---

<sup>30</sup> Capitão Tm (Eng) Viegas Nunes, *“Impacto da Novas Tecnologias no Meio Militar: A Guerra de Informação”*, Revista Militar, pág. 11.

Um dos subprodutos da globalização da “*Sociedade da Informação*” é o ciberterrorismo, que consiste na utilização do ciberespaço para fins terroristas. O conceito do ciberterrorismo teve a sua génese nos anos 80, com o advento dos primeiros ataques de *hackers*, isolados e não coordenados, aos sistemas de informações militares dos EUA (Pentágono). Mas, foi só após os acontecimentos de 11 de Setembro de 2001, que a actividade dos ciberterroristas se intensificou, de forma coordenada e com fins pré-estabelecidos.

Os grupos terroristas utilizam a Internet para atacarem os sistemas nevrálgicos de controlo da informação dos serviços públicos e privados, podendo a sua utilização estruturar-se em dois aspectos básicos: o primeiro, para apoio à sua actividade terrorista no concerne ao recrutamento de pessoal, transferências de fundos financeiros, propaganda, obtenção de informação e para comunicação e controlo das *acções* terroristas; o segundo, para *acções* de ciberterrorismo, materializadas pelos ataques aos sistemas nevrálgicos de controlo da informação, públicos ou privados, com o objectivo de roubar, manipular ou até mesmo destruir a informação e os sistemas de informação, causando o descrédito desses sistemas aos olhos da população.

Os principais actores do ciberterrorismo são os *hackers* (amadores ou profissionais ao serviço de determinado grupo terrorista), os grupos criminosos e os “*Quase-estados*”, cada qual com os seus objectivos e motivações. Nas suas *acções* poderão utilizar Armas do tipo Convencional para realizarem a destruição física dos sistemas de informação e respectivas infra-estruturas; Armas Lógicas que visam a destruição lógica dos computadores e sistemas de informação ou Armas Comportamentais para destruírem a confiança que os utilizadores depositam nos sistemas de informação.

As aspirações humanas visam essencialmente a Segurança, a Prosperidade e o Bem-Estar das pessoas da comunidade ou Estado. No entanto, a maior parte dos Estados é incapaz de garantir, isoladamente, a segurança do seu território e das populações. Actualmente, face às novas ameaças, as fronteiras e as medidas defensivas, por mais vastas e aperfeiçoadas que estejam, não constituem barreiras eficazes contra a intrusão; ou seja, não há Estados invulneráveis. Agora não nos devemos preocupar apenas em proteger as fronteiras, os aeroportos ou as centrais de energia eléctrica, mas também, os sistemas informáticos que controlam estas infra-estruturas de armazenamento de informação estratégica. Deste modo, na actual “*Sociedade da Informação*”, existem bons e maus aldeãos (Cibercriminosos), havendo necessidade de proteger os sistemas de informação destes últimos,

através da implementação um conjunto de normas que regulamentem a utilização da Internet e de legislar no sentido de aplicar sanções aos prevaricadores. Para o efeito, ao nível dos sistemas, é necessário implementar medidas, procedimentos e atitudes para proteger a informação dos *Servidores Web*, garantir a sua segurança durante os processos de transferência e, finalmente, garantir a segurança dos utilizadores, implementado *firewalls*, *passwords*, assinaturas digitais, etc. Presentemente, uma das formas mais seguras para transmitir dados ou informação sem interferências externas, é obtida através da criptografia.

No âmbito da segurança da informação, recorre-se à Guerra de Informação Defensiva para garantir a protecção dos sistemas de informação contra ataques internos ou externos. Assim, ao nível estratégico, foram adoptadas pelos Estados mais desenvolvidos, formas de monitorizar o correio electrónico (“*Carnivore*”) e para detectar todos os tipos de comunicações electrónicas (“*Echelon*”), com o objectivo de reduzir as potenciais ameaças criminosas sobre os sistemas nevrálgicos de informação.

Face ás actuais ameaças com origem no ciberespaço, os EUA adoptaram uma “*Estratégia Nacional para a Segurança do Ciberespaço*” evitando que os ataques ciberespaciais destruam informação ou sistemas de informação importantes. Esta estratégia definiu como objectivos a prevenção contra os ciberataques, a redução das vulnerabilidades e a minimização de danos. Por isso, definiram-se cinco níveis de actores, de acordo com os riscos de ataque: o utilizador e o pequeno negócio; a grande empresa; os sectores críticos e as infra-estruturas; os valores e vulnerabilidades nacionais e o nível global. Para fazer face a estas ameaças, esta estratégia aconselha vários tipos de medidas estruturadas em cinco níveis, de acordo com os diversos grupos ou actores a proteger.

Ao nível da UE, embora já exista legislação específica para os crimes relacionados com computadores, onde se incluem as ofensas de privacidade, de conteúdos e propriedade intelectual, os crimes económicos, o acesso não autorizado e a sabotagem, ainda não foram adoptadas medidas específicas contra o ciberterrorismo. No entanto, a recente criação de um fórum de discussão e de aconselhamento dos Estados Membros, relativamente à cibersegurança – Agência de Cibersegurança – constitui um passo importante para a sensibilização dos políticos e da população em geral sobre estas matérias.

Actualmente, utiliza-se a tecnologia para combater as próprias inovações tecnológicas, por esta razão, os Estados em geral e os cidadãos, em particular, deverão desenvolver ferramentas para evitar que os ciberataques provoquem o

caos nas sociedades, ficando esta à mercê dos “marginais” electrónicos. Assim, devemos envidar todos os esforços ao nosso alcance para evitar que se concretize a afirmação de Arquilla e Ronfeldt:

*“Amanhã os terroristas provocarão mais danos apenas com um teclado do que com uma bomba”<sup>31</sup>.*

---

<sup>31</sup> Dorothy E. Denning, “Activism, Hacktivism and Cyberterrorism: The Internet as a tools for Influencing Foreigner Policy”, in “Networks and Netwars”, John Arquilla e David Ronfeldt.

## BIBLIOGRAFIA

### 1. LIVROS

- ARQUILLA**, John e **RONFELDT**, David, 2001, “*Networks and Netwars*”, National Defence Research Institute, RAND, Pittsburgh, EUA.
- BISPO**, António de Jesus, 2002, “*A Sociedade da Informação e a Segurança Nacional*”, Instituto Português da Conjuntura Estratégica, Lisboa.
- Joint Pub (JP)** 3-13, Outubro de 1998, “*Joint Doctrine for Implementations Operations*”, EUA.
- LOUREIRO DOS SANTOS**, General José A., Fevereiro de 2001, “*A Idade Imperial – A Nova Era – Reflexões sobre Estratégia III*”, Publicações Europa-América, 3ª Edição.
- MARCHUETA**, Maria R., “*Considerações sobre o fenómeno terrorismo*”, Lisboa, Outubro de 2002, no prelo.
- ROGEIRO**, Nuno, Fevereiro 2001, “*O Inimigo Público – Carl Schmitt, Bin Laden e o Terrorismo Pós-Moderno*”, Gradiva, 1.ª edição.
- TOFFLER**, Alvin e Toffler Heidi, 1995, “*War and anti-War: Survival at the Dawn of the 21 Century*”, New York, Warner Books.

### 2. ARTIGOS DIVERSOS

- AGUILA-COLLANTES**, Juan J. Sánchez, 2002, “*Ciberterrorismo – La Amenaza Fantasma*”, Revista BIT n.º 136, Novembro - Dezembro 2002.
- AUTOR DESCONHECIDO**, “*Criada a Agência de Cibersegurança*”, Jornal de Noticias, 20 de Abril de 2003.
- BISPO**, António de Jesus, 1997, “*Guerra de Informação*”, Revista Militar, nº 49, Vol II, Agosto – Setembro de 1997, págs 707 a 728.
- CRONIN**, B. e **CRAWFORD**, H., “*Information Warfare: Its Application in the Military and civilian Context*”, School of Library and Information Science Indiana University, Indiana, EUA.
- GARCIA**, Maj Inf/Doutor Francisco Proença, 2003, Apontamentos de cadeira “*Relações Internacionais e Globalização*”, curso de Pós-Graduação de Guerra de Informação/Competitive Intelligence, Academia Militar.

**MARÇALO**, Carlos, 2003, “*Cibersegurança europeia ganha Centro*”, Jornal Expresso, semana de 21 a 27 de Fevereiro de 2003.

**NUNES**, Cap Tm (Eng) Paulo F. Viegas, 13 de Setembro de 1999, “*Impacto das Novas Tecnologias no Meio Militar: Guerra de Informação*”, III Congresso Internacional da Imprensa Militar, IAEM.

**NUNES**, Cap Tm (Eng) Paulo F. Viegas, 2001, “*Sociedade da Informação, Globalização e Guerra de Informação*”, Jornal do Exército, Abril de 2001.

### 3. INTERNET

#### **Internet – Vantagens desvantagens (11Mai03):**

**AUTOR DESCONHECIDO**, “*Vantagens da Internet!*”, vantagens\_internet.htm»  
[http://www.terravista.pt/Meco/7435/vantagens\\_internet.htm](http://www.terravista.pt/Meco/7435/vantagens_internet.htm).

#### **Ciberterrorismo (02Mai03):**

**ARQUILLA**, John e **RONFELDT**, D, “Cyberwar and Netwar: New Modes, Old Concepts, of Conflict”, <http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/cyberwar.html>.

**BLYTH**, Toby, “*Cyberterrorism and Private Corporations*”, 11<sup>th</sup> Annual International Symposium on Criminal Justice ISSUES, pág. 15, <http://afgen.com/terrorism1.html>.

**BORLAND**, John, “*Analyzing The Threat Of Cyberterrorism*”, <http://content.techweb.com/wire/story/TWB19980923S0016>.

**CARRION**, José Granados, 2001, “*Ciberguerra*” Conferencia Internacional “La Seguridad Europea en el Siglo XXI, Universidade de Granada, 5-9 de Novembro de 2001”, <http://www.ugr.es/~ceas/Desafios%20emergentes/3.pdf>.

**COLIN**, Barry, “*CyberTerrorism - From Virtual Darkness: New Weapons in a Timeless Battle*”, <http://www.nici.org/Research/Pubs/98-5.htm>.

**COLIN**, Barry, Março de 1997, “*The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge*”, 11<sup>th</sup> Annual International Symposium on Criminal Justice Issues, Institute for Security and Intelligence, págs. 15-18, <http://afgen.com/terrorism1.html>.

**DENNING**, Dorothy E, “*Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*”, <http://www.terrorism.com/documents/denning-infoterrorism.html>.

- DENNING**, Dorothy E., Maio de 2000, “*Cyberterrorism*”, Georgetown University, <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.
- DENNING**, Dorothy E., “*Hiding Crimes in Cyberspace*”, <http://cryptome.org/hiding-db.htm>.
- FALCIONELLI**, Esteban – “*Ciberterrorismo, outro de los nuevos rostros del miedo*”, [http://www.forodeseguridad.com/art\\_ciberterrosirmo.htm](http://www.forodeseguridad.com/art_ciberterrosirmo.htm).
- GARCÍA**, Noelia, 2001, “*El ciberterrorismo expande las fronteras de la violencia*”, <http://orbita.starmedia.com/~norma-duval/prensa/ciberviolencia.htm>.
- GARCIA**, Pastor Sérgio, 27 Junho de 2001, “*Terrorismo Digital*”, <http://www.siguemec.com.ar/Editorial/Terrorismo20Digital.htm>.
- GREGO**, Maurício, Julho de 2000, “*Ciberterrorismo - Programadores muita habilidade e nenhuma ética criam vírus cada vez mais devastadores. Há uma saída?*”. Revista Info Exame, <http://www.modulo.com.br/empresa3/noticias/habilidade.html>.
- KIRKHOPE**, “*Terrorism: Motivations and Causes*”, <http://www.terrorism.com/modules.php?op=modload&name=News&file=article&sid=5693&mode=thread>.
- KRASAVIN**, Serge, 27 de Julho de 2000, “*What is Cyber-terrorism?*”, <http://www.sans.org/rr/infowar/cyberterrorism.htm>.
- LEVY**, Laura, 24 de Setembro de 2001, “*Ciberterrorismo, lo que faltaba*”, <http://www.3pontos.com>.
- LOPES**, Bruno, “*Terrorismo na Rede*”, <http://jbon-line.terra.com.br/jb/online/internet/linkse/2001/09/onlin-tlin20010924001.html>.
- MACKO**, Steve, “*The Cyber Terrorists...*”, ENN Editor, <http://www.emergency.com/cybrterr.htm>.
- NOBLE**, Ermestina Herrera, 2002, “*Terrorismo e Internet: Una relación cada vez más estrecha y peligrosa*”, Clarim.com Produzido na Internet , 18 de Julho de 2002, <http://listas.ecuanex.net.ec/pipermail/politicas-lac/2002-june/000491.html>.
- OVERHOLT**, Matt e Professor Brenner, “*Cyber-Terrorism*”, <http://cybercrimes.net/Terrorism/overview/page1.html>.

**PEREZ**, Paulo, “*Terror nos EUA - Ameaça do Ciberterrorismo se torna realidade*” <http://www.novomilenio.inf.br/ano01/0110d008.htm>.

**POLLITT**, Mark M., October 1997, “*Cyberterrorism - Fact or Fancy?*”, Proceedings of the 20th National Information Systems Security Conference, págs. 285-289, <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>.

### **Guerra de Informação (03May03):**

**ALBERTS**, Dr David S, Agosto de 1996, “*Defensive Information Warfare*”, Director of Advanced Concepts, Technologies, and Information Strategies (ACTIS), National Defense University, NDU Press Book, <http://www.fas.org/irp/threat/cyber/docs/diw/index.html>.

**LEWIS**, Brian, “*Information Warfare*”, <http://www.fas.org/irp/eprint/snyder/infowarfare.htm>.

**SHAHAR**, Yael, ICT, “*Information Warfare: The Perfect Terrorist Weapon*”. <http://www.ict.org.il/articles/infowar.htm>.

### **Cibersegurança (06May03):**

**AAVV**, Fevereiro de 2003, “*The National Strategy To Secure Cyberspace*”, <http://www.whitehouse.gov/pcipb/>.

**KELLY**, Jessica, 2000, “*European Commission to set up pan-European cybercrime forum*”, <http://www.cnn.com/2000/TECH/computing/12/07/ec.cybercrime.forum.idg/index.html>.