Ciberterrorismo: Aspectos de Segurança

Tenente-coronel
Paulo Fernando Viegas Nunes

Introdução

O crescimento sustentado da Internet, favorecendo a percepção de que vivemos numa "aldeia global", fez surgir o ciberespaço[1] como um novo espaço virtual de interacção económica, social e cultural. As sociedades industriais, especialmente as que vivem num sistema de mercado livre e aberto, apresentam uma grande dependência relativamente às redes e sistemas de informação que estão na base do seu processo de geração de riqueza e de bem-estar social.

A existência de um autêntico "calcanhar de Aquiles electrónico" e o receio de um ataque terrorista, tem vindo a gerar uma profunda reflexão em torno do facto de 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 Harbour digital".

As ameaças e os riscos associados aos desafios que a Sociedade de Informação, Comunicação e Conhecimento encerra, não podem ser ignorados ou negligenciados. Nesse sentido, atentos ao tema central desta Conferência, procuraremos avaliar uma das linhas de acção emergentes do terrorismo pós-moderno: o ciberterrorismo.

O aprofundamento de uma cultura de segurança e a tomada de consciência colectiva das sociedades, relativamente à importância do desenvolvimento de políticas e estratégias cooperativas, levam os Estados a desenvolver sistemas e processos de combate a todas as formas de terrorismo. Nesse sentido, procura-se também apresentar uma reflexão sobre as principais envolventes de um sistema de ciberdefesa que, garantindo um alerta precoce, permita antecipar e, se possível, evitar a ocorrência de ciberataques.

Vulnerabilidade Estratégica do Ciberespaço e o Ciberterrorismo

A utilização do ciberespaço como vector privilegiado de condução de acções terroristas, tem vindo a assumir uma importância crescente para as sociedades ocidentais, obrigando os estados a rever os fundamentos das suas estratégias de segurança e defesa. No entanto, a utilização de uma nova arma ou de uma inovação tecnológica para a criação de uma vulnerabilidade estratégica não poderá ser considerada como inovadora.

Para além da incontornável referência aos princípios da guerra assimétrica e aos fundamentos do pensamento estratégico de Sun Tzu, constata-se que já na 1ª Guerra Mundial, alguns pensadores europeus como Giulio Douhet[2] e Hugh Trenchard[3] defendiam ser possível afectar a capacidade inimiga para conduzir a guerra, através do lançamento de ataques aéreos contra as suas infra-estruturas críticas, normalmente situadas em áreas distantes da linha da frente. No decurso da 2ª Guerra Mundial, estas teorias foram também levadas à prática através da condução de bombardeamentos estratégicos destinados a destruir as centrais eléctricas, os centros industriais e os sistemas de transportes que suportavam o esforço de guerra inimigo.

De acordo com a teoria desenvolvida por Alvin e Heide Toffler (1995, 1997), a era industrial deu lugar à era da informação. Face às bases em que se fundamentam a natureza e as relações de poder, os recursos-alvo a atingir deixaram de ser as instalações fabris e as matérias-primas, passando os recursos intangíveis (a informação) a constituir o alvo privilegiado desses ataques.

No actual ambiente de informação, um ciberataque (ataque de informação) poderá assim ser considerado de nível estratégico se o seu impacto for tão importante que afecte (ou possa vir a afectar) a capacidade de um Estado assegurar as suas funções vitais (segurança e bem-estar da sua população). Dentro deste contexto, tendo por base os seus efeitos, também as armas da guerra baseada na informação (Guerra de Informação[4]), poderão ser consideradas como armas de "disrupção massiva" (Libicki, 1996; Morris, 1995), apresentando a sua utilização um enquadramento estratégico semelhante ao das Armas de Destruição Maciça (ADM). Devido à incerteza das consequências e ao potencial impacto de um ciberataque nas populações civis e na sociedade em geral, os Estados terão inevitavelmente de realizar uma avaliação dos riscos decorrentes da utilização de armas de informação por parte de actores hostis, nomeadamente por parte de grupos terroristas.

Os fundamentos associados ao lançamento de ciberataques, apresentam assim grandes semelhanças com os princípios do bombardeamento estratégico, permitindo-nos este paralelismo uma melhor percepção da forma como os ataques às infra-estruturas críticas de um Estado afectam a sua sociedade.
Pelas suas directas implicações na condução da Política e da Estratégia dos diversos Países, estes terão de garantir a defesa e a protecção da sua Infra-estrutura de Informação Nacional. Só através da adopção das necessárias contra-medidas será possível fazer face à ocorrência de eventuais ataques de ciberterrorismo.

No entanto, importa avaliar qual o impacto actual deste tipo de ataques e qual a probabilidade de ocorrência de acções de ciberterrorismo num futuro próximo.

Dentro deste contexto, assume também particular importância analisar a forma como os Estados e a comunidade internacional poderão, de forma integrada e concertada, desenvolver políticas e implementar estratégias de prevenção e combate às ameaças emergentes no ciberespaço.

Ciberterrorismo: Definição e Enquadramento Conceptual

Sendo o terrorismo entendido pela sociedade como um fenómeno aleatório, normalmente incompreensível e incontrolável, constata-se que os seus efeitos são normalmente catastróficos e afectam muitos inocentes. Independentemente das motivações políticas que estiverem na sua origem, os atentados terroristas pretendem sempre provocar o terror e o medo, aí residindo a raiz do seu impacto e poder.

A acelerada evolução tecnológica, postulada por Gordan Moore[5], fez crescer a utilização de sistemas computacionais, deles dependendo os sistemas de comunicações, o controlo da rede eléctrica nacional, os sistemas bancários, o controlo de tráfego aéreo ou mesmo o sistema nacional de emergência médica.

Associado à progressiva consciência desta dependência, foi crescendo o receio de que, fruto de deficiências estruturais ou ataques de vírus e de hackers[6], deixasse de ser possível controlar os computadores que gerem as infra-estruturas críticas nacionais.

A Internet, encarada como uma "rede de redes", a partir da qual é possível aceder a todos os computadores a ela ligados, veio adensar este temor, surgindo a ideia de que será possível controlar o mundo a partir de um único computador.

A utilização do ciberespaço para a condução de acções terroristas (ciberterrorismo), combina a desconfiança e os receios associados às novas tecnologias com o medo da vitimação aleatória e violenta que caracteriza um ataque terrorista.

A dificuldade em objectivar as diversas formas que um ataque deste tipo pode assumir, aliada à falta de informação sobre o seu real poder disruptivo e impacto social, leva muitos autores a minimizar os seus efeitos (Lewis, 2002), ou até mesmo a questionar a sua existência.

Uma análise sumária da grande quantidade de informação disponível na Internet e em numerosos trabalhos e artigos publicados sobre este tema, revela que muitas vezes se confunde o fenómeno do ciberterrorismo com actividades ligadas ao cibercrime. Mais uma vez, esta situação deve-se ao facto de não existirem definições claras internacionalmente reconhecidas destes dois fenómenos, conforme refere Michael Mates (2001), citando um manual das Nações Unidas sobre as actividades criminosas

relacionadas com a utilização das Tecnologias de Informação.

Face a esta situação, considera-se importante apresentar algumas das definições existentes, para que seja possível deduzir e objectivar o conceito que nos propomos clarificar.

O National Infrastructure Protection Center (NSSC, 2003), organismo responsável pela implementação dos mecanismos de protecção das infra-estruturas governamentais dos EUA, define 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."

Por seu turno, Dorothy Denning, Professora Universitária, especialista em segurança informática e autora de diversas obras (1999, 2000, 2001), afirma que o ciberterrorismo resulta da convergência entre ciberespaço e terrorismo, considerando que este conceito se refere a "ataques criminosos e a ameaças de ataques contra computadores, redes e informação armazenada no seu interior, quando realizados com o objectivo de intimidar ou coagir um governo ou a sua população, procurando atingir objectivos políticos. Para que possa ser qualificado como ciberterrorista, um ataque deverá resultar em violência contra pessoas ou propriedade ou, pelo menos, causar danos suficientes para poder gerar medo."

De acordo com estas definições, para que um ciberataque possa ser considerado como ciberterrorismo, este terá que satisfazer dois critérios: apresentar uma motivação política e um resultado destrutivo fisicamente visível. No entanto, ainda que alguns destes ataques apresentem uma forte motivação política, não existem registos conhecidos de que os ciberataques lançados através de computadores tenham, por si só, destruído infra-estruturas ou originado a perda de vidas humanas.

Uma abordagem pragmática e objectiva, permite verificar que um ciberataque poderá provocar prejuízos financeiros elevados, algum transtorno ou mesmo instabilidade social mas não apresenta um efeito destrutivo directo. A realidade, parece assim indicar que este tipo de ameaças se coloca essencialmente ao nível da destruição de dados e informação crítica, não de infra-estruturas físicas.

Utilização da Internet pelo Terrorismo Transnacional

A Internet tem vindo a constituir um autêntico campo de batalha digital sendo palco de acções de retaliação entre hackers associados a diversos países e actores estratégicos como Israel e a Palestina, Taiwan e a China, Paquistão e a Índia ou Estados Unidos e a China[7].

Ainda que estas actividades não configurem um envolvimento directo de organizações terroristas, já em Fevereiro de 1998 existiam indícios de que algumas organizações

extremistas islâmicas estavam a procurar desenvolver uma rede de hackers[8], tanto para apoiar as suas actividades correntes como para preparar o lançamento de futuros ataques de Guerra de Informação (Denning, 1999).

Em Abril de 2002, a administração norte-americana, identificou a presença na Internet de 33 grupos terroristas (Conway, 2002). De acordo com a lista dos sites das organizações terroristas publicitada (Anexo), constata-se a dificuldade em precisar o endereço electrónico das suas páginas, ainda que essa presença tenha sido registada.

Como meio aberto de interacção digital, a Internet tem vindo a ser utilizada extensivamente por grupos terroristas tanto para difusão das suas mensagens políticas como para a coordenação das suas acções, nomeadamente, das actividades associadas a ataques terroristas tradicionais.

A realização de ciberataques oferece algumas vantagens sobre os tradicionais ataques bombistas, evitando a utilização de explosivos ou de missões suicidas, ao mesmo tempo que garante a possibilidade de um terrorista, munido apenas de um computador e de uma ligação à Internet, poder remotamente, de forma anónima e mais económica, atacar as redes e os sistemas informáticos de um determinado País.

Avaliação da Ciberameaça

A emergência de um modelo de interacção social baseado no ciberespaço, fez surgir novas "ferramentas" tecnológicas de baixo custo e fácil acesso que, quando exploradas por actores mal intencionados, lhes permitem desenvolver actividades não desejáveis.

Estas ciberameaças (Denning, 1999; NSSC, 2003), podem assumir a forma de intervenção social ("Ciber-activismo", "Ciber-hacktivismo", "Ciber-vandalismo" ou "Ciber-graffiti"), a forma de acções criminosas (Hacking, Cracking, "Cibercrime" ou "Ciberterrorismo") ou mesmo a forma de actos de guerra ("Ciberguerra", Guerra de Comando e Controlo ou Guerra Electrónica).

Dentro deste contexto, tendo por base os princípios que orientam a gestão do risco que este tipo de actividades inevitavelmente envolve para os Estados, julga-se importante definir também a sua probabilidade de ocorrência. Como facto mais saliente, a observação dos dados contidos na Tabela 1, revela que os ciberataques de natureza criminosa ou terrorista são os que apresentam uma maior probabilidade relativa de ocorrência.

Independentemente de acreditarmos ou não na iminência de um ciberataque de motivação terrorista, não podemos ignorar que a sua ocorrência poderá provocar um efeito disruptivo na nossa sociedade. Assim, a avaliação da ameaça terá forçosamente que passar por uma análise tanto da sua probabilidade de ocorrência como da sua severidade ou grau de disrupção.

Não é possível comparar um ataque do tipo "negação de serviço"[9], como o que afectou em 2002 os sites da Amazon e da Ebay, com um ataque que, afectando as infra-estruturas críticas de um Estado, provoque mortes e produza o caos social. No entanto, de forma diversa, ambos podem ter consequências catastróficas produzindo prejuízos financeiros extremamente elevados.

Esta é a convicção do Governo dos EUA que, receando um ciberataque terrorista, incluiu um programa de cibersegurança na sua Estratégia Nacional de Segurança Interna (*National Homeland Security Strategy*).

Fonte: Erbschloe (2001)

Actividades de Guerra de Informação		Probabilidade de Ocorrência	Observações
Ofensivas	Destrutivas (foco alargado)	Moderada	Circunscrita a poucos Países.
	De Contenção	Idem	Idem.
Defensiva	Destrutivas (foco alargado)	Reduzida	Custa biliões e requer uma coligação de Países.
	De Contenção	Moderada	Circunscrita a poucos Países.
	Preventivas	Moderada	Os EUA já iniciaram esta estratégia em resultado dos Ataques de 11Set01.
Terroristas	De Contenção	Elevada	Vários grupos terroristas.
	Preventivas	Idem	Idem.
Criminosas	Contínuas	Muito Elevada	Actividades subversivas.
	Aleatórias	Elevada	Organizações Criminosas.
	Amadoras	Moderada	Pequenos Grupos ou Actores Individuais.

Fonte: Erbschloe (2001)

Tabela 1 - Probabilidade de Ocorrência das Acções de Guerra de Informação

Os governos e os media têm vindo a dedicar uma atenção crescente ao aparecimento, quase que diário, de vírus informáticos e de ataques conduzidos por hackers a redes de computadores. Paradoxalmente, este facto poderá aumentar substancialmente a probabilidade do lançamento de ataques de ciberterrorismo, uma vez que esta situação favorece a sua mediatização.

A realidade, parece indicar que esta probalidade aumenta também substancialmente se este ciberataque for lançado com o objectivo de facilitar e ampliar os efeitos de um ataque terrorista convencional. Neste contexto, considera-se que o ataque terrorista de 11 de Março de 2004, para além da destruição de vidas e das composições ferroviárias que se dirigiam para a estação de Atocha, afectou também significativamente o resultado das eleições legislativas espanholas.

Não será possível ignorar que a convocação das inúmeras manifestações que ocorreram em Madrid (12 e 13 de Março), foi realizada pela Internet e através do envio de mensagens de telemóvel (SMS), configurando uma actividade de ciberactivismo. Também os meios de comunicação social de diversos Países receberam mensagens destinadas a desacreditar o governo espanhol, fazendo perceber que estas actividades concertadas poderiam ter sido cuidadosamente planeadas e articuladas de forma a maximizar os efeitos do ataque terrorista de 11 de Março. Apesar deste tipo de incidentes ter fortes motivações políticas e sociais, a questão relevante que importa clarificar é a de avaliar se eles poderão, ou não, produzir um "terror colectivo" ou danos suficientemente elevados, de forma a poderem ser classificados como ciberterrorismo.

Numa tentativa de sistematizar os dados disponíveis e perspectivar a possibilidade de algumas organizações terroristas conduzirem actividades de ciberterrorismo, o Centro de Estudos do Terrorismo e de Guerra Irregular, da Naval Postgraduate School, definiu três níveis de capacidade ciberterrorista[10]:
- Simples/Não estruturado: descrevendo a "capacidade da organização para conduzir acções básicas de hacking contra sistemas individuais, utilizando ferramentas desenvolvidas por terceiros. A organização possui um fraco nível de análise de alvos, comando e controlo e capacidade de aprendizagem."
- Avançado/Estruturado: caracterizando a "capacidade da organização para conduzir ataques mais sofisticados contra múltiplos sistemas ou redes e, possivelmente, modificar ou criar ferramentas básicas de hacking. A organização possui uma análise de alvos elementar, comando e controlo e capacidade de aprendizagem."
- Complexo/Coordenado: materializando a possibilidade da organização poder "conduzir ataques coordenados, susceptíveis de provocar uma disrupção massiva contra defesas integradas e heterogéneas (incluindo criptografia). A organização reúne as competências necessárias para criar sofisticadas ferramentas de hacking, revelando uma eficiente análise de alvos, comando e controlo e capacidade de aprendizagem."

As conclusões deste trabalho, apontam para o facto de o custo de entrada associado ao desenvolvimento de acções mais disruptivas que as básicas e tradicionais actividades de hacking ser geralmente muito alto e que falta, à generalidade das organizações e grupos terroristas, o capital humano e a capacidade para montar uma operação de ciberterrorismo com alguma relevância. O tempo estimado para um grupo terrorista levantar uma capacidade de ciberterrorismo de raiz, até atingir o nível avançado/estruturado, é de 2-4 anos e para atingir o nível complexo/coordenado de 6-10 anos. No entanto, este tempo poderá ser significativamente reduzido se for seguido um processo de outsourcing, como alguns dados recentemente recolhidos parecem indicar

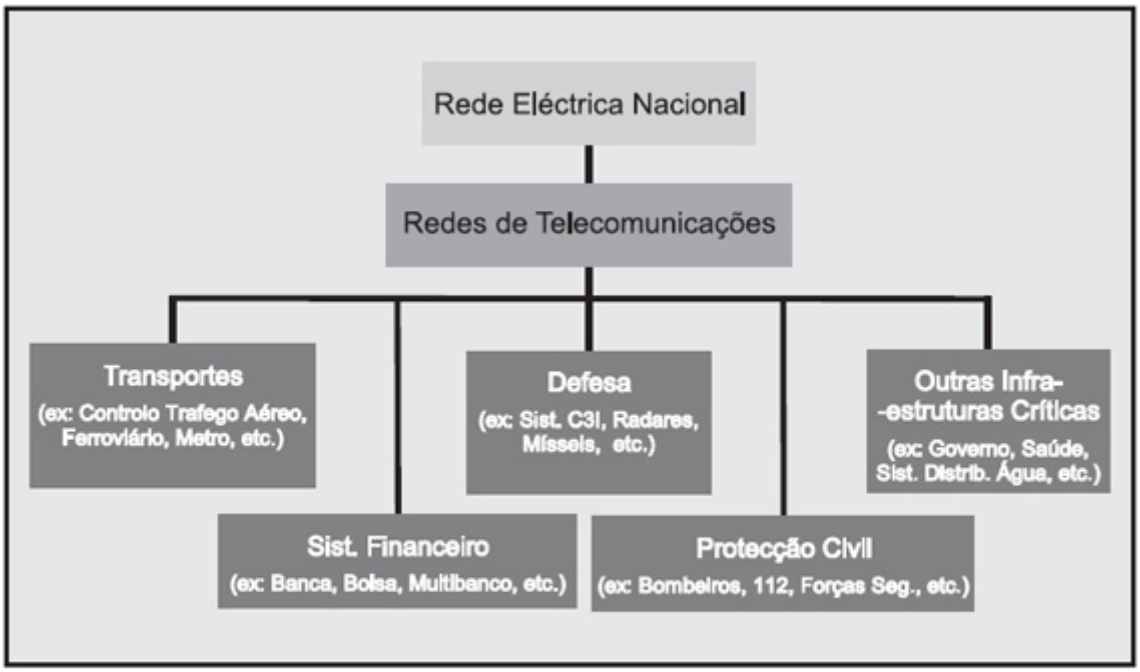
(Denning, 2000).

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

Análise das Vulnerabilidades da Infra-estrutura de Informação Nacional

A nossa sociedade possui um conjunto de Infra-estruturas Críticas[11] info-centradas que, fruto de uma cadeia de interacções funcionais, dependem da Infra-estrutura de Informação Nacional (IIN). Esta interdependência assumiu especial importância e evidência na passagem do último milénio, em que um problema informático (*Bug* do ano 2000), obrigou à realização de testes exaustivos a todas as infra-estruturas que utilizassem processadores. A percepção dos efeitos negativos, resultantes dos cortes prolongados de energia eléctrica recentemente ocorridos nos EUA, Canadá[12] e no Reino Unido[13], que conduziram a uma indisponibilidade prolongada das Infra-estruturas Críticas destes Países, devido à acção do vírus informático *Blaster*[14], constituem também um motivo de reflexão.

Temos assim que enfrentar a existência de uma pirâmide formada por sistemas tecnológicos agregados, difíceis de testar em condições limite, cujo comportamento se revela também difícil de simular e que, pela sua natureza complexa, revela pontos fracos passíveis de ser explorados por actores hostis.



Fonte: Adaptado de Major-General Pinto Ramalho (2003) e Eng Sousa Cardoso (2003).

Figura 1 – Modelo de Interdependência das Infra-Estruturas Críticas Nacionais

Um ataque à IIN poderá ter como resultado: uma perda de tempo para resolver o problema gerado, um decréscimo de produtividade das organizações, prejuízos financeiros avultados decorrentes da perda de credibilidade ou de oportunidade de mercado das empresas afectadas, a falência de empresas, a criação de condições de instabilidade e caos social, a paralisia do sistema de transportes, a criação de limitações ao funcionamento dos Sistemas C3I[15] e à acção das Forças Armadas e de Segurança, a descredibilização do Governo e da Administração do Estado e, eventualmente, a perda de vidas humanas.

A preocupação que os Governos de diversos países como os EUA (NSHS, 2002; NSPPCIKA, 2003), a Austrália (Cobb, 1999) e a Holanda (Luiijf, 2002), têm vindo a demonstrar com a Segurança da sua Infra-estrutura de Informação, revela a importância crescente que a análise das vulnerabilidades destas infra-estruturas assume, face à manifestação de novas ameaças.

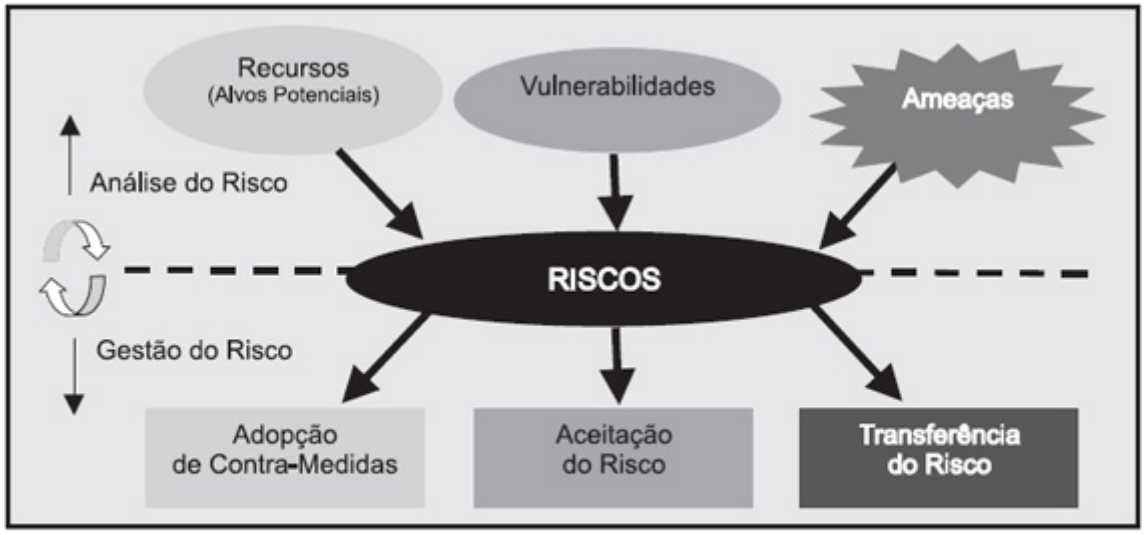
Como é possível constatar, todas as infra-estruturas críticas nacionais apresentam uma dependência estrutural relativamente à Rede Eléctrica Nacional (REN) e uma dependência funcional relativamente à IlN (Figura 1). Dentro deste contexto, importa agora analisar o risco associado a estas duas infra-estruturas para, dentro do quadro definido para o presente estudo, procurarmos determinar qual o potencial impacto de um ataque ciberterrorista na IIN, perspectivando a adopção das necessárias contra-medidas.

Modelo de Análise e Gestão do Risco

Quando analisamos o risco associado à Infra-estrutura de Informação Nacional, temos que ter em atenção que este resulta do efeito conjugado de três factores importantes: dos recursos a proteger (alvos potenciais), da detecção das vulnerabilidades da infra-estrutura de informação e das ameaças que, explorando essas vulnerabilidades, podem afectar os recursos que pretendemos proteger.

A dimensão do risco, está intimamente ligada ao valor/dependência que um actor apresenta face ao recurso (informação) e às consequências negativas que a sua não disponibilidade pode implicar para a sua actividade. Os recursos de informação são considerados tanto mais críticos quanto maior for o grau de dependência existente sobre eles. As medidas de segurança a adoptar, devem ser proporcionais ao impacto negativo previsto para a sua não disponibilidade ou funcionamento correcto. De acordo com o Tenente-General Jesus Bispo (2002), é possível determinar o risco através de métodos qualitativos/quantitativos que permitam realizar a sua avaliação[16] com base no valor da ameaça esperada, na vulnerabilidade avaliada/determinada, no valor da medida de salvaguarda adoptada para o minimizar e no valor do impacto previsto para o ataque/ameaça na infra-estrutura de informação.

Avaliado o risco, após a análise realizada, este pode ser gerido de diversas formas, nomeadamente, através da sua redução (adopção de contra-medidas), manutenção (aceitação do risco) ou transferência para terceiros. A escolha associada a cada uma destas três opções está, naturalmente, intimamente relacionada com o valor que atribuímos ao recurso a proteger. Quanto mais crítico for um recurso, maior será a necessidade de assegurarmos a adopção das contra-medidas necessárias para reduzir o risco que se lhe encontra associado. Procura-se assim garantir a disponibilidade do recurso e evitar a possível ruptura da infra-estrutura crítica, mesmo quando em presença de um cibertaque de natureza terrorista.



Fonte: Adaptado de Eng Sousa Cardoso (2003).

Figura 2 – Modelo de Análise e Gestão do Risco de uma Infra-estrutura Crítica

Face à necessidade de garantir a segurança e a protecção contínua da IIN, os Estados têm que encarar esta necessidade como um processo contínuo e sistémico (ver Figura 2). Assim, associada à necessidade de realização de uma contínua análise do risco, todos os Países terão também que assegurar permanentemente a sua gestão.

Esta preocupação, tem obrigado os Estados a uma constante revisão das suas políticas e conceitos de segurança nacional. A título de exemplo, refere-se que o conceito de *Homeland Security* (NSHS, 2002) foi deduzido pelos EUA com base na revisão dos princípios que orientam a protecção e segurança do seu território[17], resultando de um profundo trabalho de levantamento das infra-estruturas críticas e dos seus recursos-chave.

Conscientes de que alguns desses recursos podem ser alvos de ciberataques, os EUA realizaram, em 1997, uma avaliação dos riscos associados ao sistema de produção e transporte de energia eléctrica, obtendo desta forma a confirmação de que a sua rede eléctrica nacional apresentava diversos pontos fracos (SCRS, 2002). Alguns elementos da rede dependiam de sistemas de Supervisão, de Controlo e de Aquisição de Dados

(SCADA)[18] não protegidos, que podiam ser acedidos através de sistemas ligados a redes informáticas locais não integradas na estrutura do sistema. Noutros casos, foi também identificada a possibilidade de controlar, à distância, os sistemas SCADA não protegidos através da rede telefónica, comprometendo o funcionamento de todo o sistema. Concluiu-se assim que todos os recursos necessários ao correcto funcionamento das infra-estruturas críticas, ligados a uma rede de comunicações, constituiam potenciais alvos de um ciberataque.

Actualmente, surgem novos desafios internos e externos ao Estado que, pela sua natureza, poderão condicionar a segurança da sua Infra-estrutura de Informação Crítica. Se no plano interno, os problemas que se colocam são essencialmente ao nível da gestão da interligação de diversos sistemas, no plano externo existem alguns problemas tanto ao nível legal como da cooperação internacional.

Face a esta situação, começa a crescer a percepção na comunidade internacional de que este tipo de ameaças obriga a respostas concertadas e articuladas no âmbito da ciberdefesa, nomeadamente, quando se pretende garantir a segurança das infra-estruturas críticas dos diversos Estados, protegendo-as contra a ocorrência de ciberataques.

A adopção, pela Assembleia-Geral das Nações Unidas, da Resolução Nº 53/70 de Dezembro de 1998, reflecte já uma preocupação com a segurança internacional, face à emergência de fenómenos de natureza global e transnacional como o cibercrime, o ciberterrorismo e até a ciberguerra.

Também a União Europeia, procurando assegurar o desenvolvimento comunitário, sustentado numa economia baseada na informação e no conhecimento, tem vindo a revelar preocupações de segurança na construção de uma "e-Europe"[19].

Ciberdefesa da Infra-estrutura de Informação Nacional

Tendo por base a consecução do objectivo nacional de garantir a Protecção da IIN, torna-se necessário levantar uma organização/estrutura que implemente a segurança dessa infra-estrutura e permita garantir a sua ciberdefesa.

Dentro deste âmbito, após uma análise do espectro da ameaça[20], é necessário estabelecer normas de segurança para as infra-estruturas de informação governamentais e recomendar também a adopção de normas de segurança para as infra-estruturas críticas privadas.

Revela-se também particularmente importante o levantamento de um *Computer Emergence Response Team (CERT)* Nacional, a implementação de programas adequados de educação e treino, o financiamento do desenvolvimento de mecanismos de segurança e redundância das infra-estruturas de informação e o desenvolvimento de regimes de

cooperação e actuação internacional na área da Protecção da IIN.

Considera-se que a filosofia a seguir, na implementação do conceito de Protecção da Infra-estrutura Crítica de Informação, se deverá articular de acordo com uma perspectiva de gestão do risco: Protecção, Detecção e Reacção. Dentro deste contexto, assumem particular importância (Nunes, 2003):
- A clarificação e actualização permanente dos dados estatísticos referentes a incidentes ligados às TIC;
- A definição de uma Infra-estrutura de Informação Crítica Mínima, sobre a qual devam incidir prioritariamente as actividades de segurança da informação;
- A existência de um sistema de "*helpdesk*" que, em tempo-real, possua a capacidade de resposta a incidentes/ataques (CERT Governamental);
- A definição clara das responsabilidades na resolução dos problemas;
- A clarificação do apoio a prestar pelos Serviços de Informações Nacionais à condução das Operações de Informação, nomeadamente, no que se refere à obtenção de informações sobre a ameaça, recursos e sistemas de informação adversários;
- A definição da orientação a seguir no levantamento da estrutura organizacional a adoptar (uma nova organização ou uma nova função atribuída a uma organização já existente?).

De acordo com alguns especialistas nacionais (Cardoso, 2003), a implementação de um Sistema de Ciberdefesa, deverá passar pela criação de um CERT Nacional tutelado pelas Forças Armadas. No entanto, face à interdependência das Infra-estruturas de Informação Nacionais e à necessidade de uma elevada coordenação de esforços, considera-se mais ajustado que a tutela deste órgão seja atribuída a um Órgão/Organização directamente dependente do Primeiro-Ministro. Os CERT sectoriais, que apoiam os diversos Ministérios e as entidades e instituições nacionais, seriam por sua vez ligados ao CERT Nacional para garantir uma permanente avaliação das ameaças e o relato de incidentes ocorridos nas Infra-estruturas de Informação Nacionais.

O Sistema de Ciberdefesa Nacional poderia assim ser estruturado com base num *Network Operations Center* (NOC) e numa rede de CERTs que constituiriam uma Rede de Alerta e Relato Nacional (RARN) de acidentes ocorridos nas redes e sistemas de informação dos diversos sectores ou áreas críticas[21]. A existência de uma RARN obrigaria as diversas entidades da rede a relatar os acidentes e, após a sua análise e compilação, permitiria implementar um plano de recuperação (*Disaster Recovery*) da IIN. Dentro deste âmbito, deverá ser levantada um Infra-estrutura de Informação Crítica Mínima Nacional[22]. Para assegurar uma auditoria externa e a execução de testes permanentes deveriam também ser constituídas equipas especializadas (*Red Teams*). Tanto a operação da RARN como a condução de Operações de Informação exigem a mobilização de competências específicas, impondo a formação de um Corpo de Especialistas Civis e Militares ("info-corpo") especialmente vocacionado para estas áreas.

Conscientes que a resposta genética, aqui sugerida, reflecte alterações importantes ao nível das estruturas, doutrinas e orientação das políticas do Estado, considera-se

imprescindível o levantamento de um quadro legal e institucional que, permitindo assegurar tanto a condução de Operações de Informação (civis e militares) como a implementação de uma eficaz política de segurança da informação, crie as condições necessárias para garantir a Protecção da Infra-estrutura de Informação Crítica Nacional contra ciberataques.

Conclusão

Face ao elevado número de interacções e mesmo de sobreposições que as infra-estruturas de informação apresentam, o ciberespaço impõe uma forte interdependência entre a construção de uma rede global como a Internet e as diversas Infra-estruturas de Informação Nacionais, onde as fronteiras geográficas têm cada vez menos relevância. Este facto, impõe a necessidade de assegurar a sua protecção e defesa, nomeadamente, face à emergência de "novas ameaças" no ciberespaço, em que pontuam as acções terroristas e a criminalidade transnacional.

Estamos perante uma situação paradigmática da relação bem-estar/desenvolvimento e segurança das sociedades. Trata-se de uma área em que o ritmo da implementação de processos e mecanismos de segurança dificilmente acompanha a dinâmica das vulnerabilidades, materializando uma área privilegiada de "guerra assimétrica".

O ciberterrorismo, tem como maior condicionante o facto de apresentar um impacto menor na opinião pública que as tradicionais formas de terrorismo. A menos que um ciberataque permita provocar, de per si, um forte efeito psicológico, caracterizado pela existência de baixas e um grau de destruição física significativo, este tipo de ataques continuará a desempenhar o papel de "ataque secundário". Um ciberataque, poderá assim ser lançado para criar as condições ideais e para maximizar os efeitos de um ataque terrorista tradicional.

Constatando-se que o ciberterrorismo não parece constituir uma ameaça iminente, não será possível ignorar que os grupos terroristas utilizam o ciberespaço para facilitar a condução dos tradicionais ataques bombistas. As organizações terroristas utilizam a Internet para difundir as suas mensagens, para recrutar apoiantes, para comunicar e para coordenar a actuação das suas células.

O levantamento de um sistema de ciberdefesa, capaz de fornecer o alerta precoce, de permitir a rápida recuperação e a eliminação da origem de ciberataques assume um papel determinante para a protecção das infra-estruturas críticas nacionais.

A persecução violenta de objectivos políticos utilizando exclusivamente meios electrónicos, não se coloca actualmente mas não poderá deixar de ser perspectivada no futuro, sob pena de se vir a comprometer a segurança e a própria Defesa Nacional.

Bibliografia

BISPO, Jesus (2002). *A Sociedade de Informação e a Segurança Nacional*, Instituto Português da Conjuntura Estratégica, Lisboa.
CARDOSO, Sousa (2003). "*Guerra no Ciberespaço: Um Novo Método de Conflito*", Conferência proferida na Academia Militar ao Curso de Pós-Graduação em Guerra de Informação/Competitive Intelligence (não publicada), 26 de Julho.
COM, (2002). *Comunicação da Comissão ao Conselho, Parlamento Europeu, Comité Económico e Social e Comité das Regiões, Segurança da Informação e das Redes: Uma proposta para uma Abordagem Política Europeia*, Bruxelas, http://europa.eu.int//informationsociety/_/eeurope/news_library//pdf_files/netsec_en.pdf, 07-01-2003 / 23H45.
CONWAY, Maura, (2002). *Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet*, First Monday, volume 7, number 11 (Novembro), disponível por via electrónica em http://firstmonday.org/issues/issue7_11/conway/index.html.
DENNING, Dorothy E., (1999). *"Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy"*, Washington D.C., disponível por via electrónica em http://www.nautilus.org/info-policy/workshop/papers/denning.htm.
DENNING, Dorothy E., (2000). *Testemunho perante a Special Oversight Panel on Terrorism Committee on Armed Services da U.S House of Representatives* (23 Maio), disponível em http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.
DENNING, Dorothy E., (2001). *"Is Cyber Terror Next?"*, U.S. Social Science Research Council (New York), disponível em http://www.ssrc.org/sept11/essays/denning.htm.
DMDM, (2002). *Directiva Ministerial de Defesa Militar*, MDN, Janeiro.
DOUHET, Giulio, (1942). *The Command of the Air,* tradução de Dino Ferrari (nova reimpressão, Washington, D.C.: Office of the Air Force History, 1983).
FM 100-6, (1996). *Information Operations*, Documento Doutrinário do Exército dos EUA, 27 de Agosto. Disponível em: http://www.jya.com/fm100/fm100-6.htm**,** 15-09-2003 /10H50.
LEWIS, James (2002). *"Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats"*, Artigo do Center for Strategic and International Studies (CSIS), Washington D.C., Dezembro.
LIBICKI, Martin (1995). "*What is Information Warfare?*", National Defense University Press, Washington D.C.
LUIIJF, Ir. et al (2003). "*In Bits and Pieces*", Estudo sobre a vulnerabilidade da Infra-estrutura de Informação e Comunicações da Holanda e as suas consequências para a Sociedade da Informação, em INFODROME, http://www.infodrome.nl/, 02-09-2003 / 15H35.
MATES, Michael, (2001). "*Technology and Terrorism*". QG NATO/Bruxelas, disponível em http://www.tbmm.gov.tr/natopa/raporlar/bilim%20ve%20teknoloji/AU%20121%20STC%20Terrorism.htm
MORRIS, Chris et al., (1995). "*Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos*", *Airpower Journal*, Primavera, disponível em http://www.cdsar.af.mil/air-chronicles.html, 18-05-2003 /19H34.
NSHS, (2002). *National Strategy for Homeland Security*, Definição da Estratégia Nacional de Segurança do território dos Estados Unidos da América, em White House Office of Homeland Security, disponível em suporte electrónico em

http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf, 03-09-2003 / 09H47.
NSPPCIKA, (2003). *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Definição da Estratégia Nacional para a Protecção Física de Infra-estruturas Críticas e Recursos-Chave dos Estados Unidos da América, em White House Office of Homeland Security, disponível em suporte electrónico em http://www.whitehouse.gov/pcipb/physical_strategy.pdf, 03-09-2003 / 09H57.
NSSC, (2003). *National Strategy to Secure Cyberspace*, Definição da Estratégia Nacional de Segurança do Ciberespaço dos Estados Unidos da América, em White House Office of Homeland Security, disponível em suporte electrónico em http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf, 03-09-2003 / 09H50.
NUNES, Paulo (2001). *"Sociedade de Informação, Globalização e Guerra de Informação"*, em Jornal do Exército, Lisboa, Abril.
NUNES, Paulo (2003). *"A Conflitualidade da Informação: da Guerra de Informação à Estratégia da Informação"*, Trabalho de Investigação Individual do Curso de Estado Maior 2002-04, IAEM.
PÚBLICO, (2003). *"O Susto: Apagão deixa Sul de Londres uma hora às escuras"*, em Jornal Público (29-08-2003), p. 24.
RAMALHO, Pinto (2003). *"A Direcção Geral de Política de Defesa Nacional"*, Conferência proferida no Instituto de Altos Estudos Militares ao Curso de Estado-Maior (não publicada), 24 de Junho.
RAMOS, João (2003). *"Lei de Moore Contra-Ataca"*, em 2º Caderno: Suplemento Economia e Internacional do Semanário EXPRESSO (08-03-2003), p.17.
SCRS, (2002). "*Rapport Nº 2001/11: Opérations d'Information*", Perspectives, Publication du Service Canadien du Renseignement de Sécurité, Documento Doutrinário do Canadá, 06 Maio.
TOFFLER, Alvin (1991). *The Third Wave*, New York Bantam Books, New York.
TOFFLER, Alvin e TOFFLER, Heidi (1995). *War and anti-War: Survival at the Dawn of the 21 Century*, New York, Warner Books.

Anexo – Presença de Organizações Terroristas na Internet (30 Abril 2002)

Organização	URL	Idioma (s)
Organização Abu Nidal	N/D	N/D
Grupo Abu Sayyaf	N/D	N/D
Brigada dos Mártires de Al-Aqsa	N/D	N/D
Grupo Islâmico Armado (GIA)	N/D	N/D
Asbat al-Ansar	N/D	N/D
Seita da Verdade Suprema (Aum)	http://www.aleph.to/index_e.html http://www.aleph.to	Inglês Japonês
Exército de Libertação do País Basco (ETA)	http://www.contrast.org/mirrors/ehj/ /index.html http://www.batasuna.org/	Inglês Basco
Al-Gama'a al-Islamiyya (Grupo Islâmico)	http://www.azzam.com	Inglês
Hamas	http://www.palestine-info.com/hamas	Árabe/Inglês
Harakat ul-Mujahidin (HUM)	http://www.ummah.net.pk/harkat/	Árabe/Inglês
Hizbollah	http://www.hizbollah.org	Árabe/Inglês
Movimento Islâmico do Uzbequistão	N/D	N/D
Jaish-e-Mohammed	N/D	N/D
Al-Jihad (Jihad Islâmica Egípcia)	N/D	N/D
Kahane Chai	http://www.kahane.org	Inglês
Partido dos Trabalhadores do Curdistão (PKK)	http://www.pkk.org/index.html	Curdo
Lashkar-e-Tayyiba	http://www.markazdawa.org.pk/	ÁrabeInglês
Tigres de Libertação de Tamil Eelam	http://www.eelamweb.com/	Inglês
Organização Mujahedin-e Khalq	http://www.iran-e-azad.org/english/index.html	Inglês
Exército de Libertação Nacional da Colômbia	http://www.eln-voces.com/	Espanhol
Jihad Islâmica Palestiniana	http://www.entifada.net/	Árabe
Frente de Libertação da Palestina	N/D	N/D
Frente Popular para a Libertação da Palestina	http://www.pflp-pal.org/main.html	Inglês
Frente Popular para a Libertação da Palestina – Comando Geral	N/D	N/D
Al-Qaida	http://www.alneda.com	Árabe
IRA	N/D	N/D
Forças Armadas Revolucionárias da Colômbia (FARC)	http://www.farc-ep.org/	Inglês/Espanhol/Português/ /Italiano/Alemão/Russo
Nuclei Revolucionário	N/D	N/D
Organização Revolucionária 17 Novembro	N/D	N/D
Partido/Frente Revolucionária Popular	http://www.ozgurluk.org	Inglês
Grupo Salafista para a Evocação e Combate	N/D	N/D
Sendero Luminoso	http://www.csrp.org/	EspanholInglês
Forças Unidas de Auto-Defesa da Colombia	http://colombia-libre.org/colombialibre/pp.asp	Espanhol

Fonte: Conway (2002), disponível em http://www.firstmonday.dk/issues/issue7_11/conway/.

* O texto que aqui se apresenta, constituiu a base para a intervenção do autor na Lisbon Conference on Defence and Security, subordinada ao tema "Terrorism as a Global Threat: Models and Defence Strategies", que teve lugar no Instituto da Defesa Nacional entre 01-02 Julho 2004.

** Major de Transmissões (Eng). Sócio Efectivo da Revista Militar.

_____

1 Entende-se o ciberespaço como o conjunto de computadores, redes, programas e dados que materializam a infra-estrutura de informação.

2 No rescaldo da I Grande Guerra, o General Douhet sugeria já que a solução para obter a victória em futuros conflitos, teria de passar pela exploração de uma superioridade tecnologica antes que o oponente podesse responder: "A Victória sorri aqueles que anteciparem as alterações dos princípios de condução da guerra, não aos que aguardam para se poderem adaptar às alterações que entretanto vierem a ocorrer" (Douhet, 1942, p.30). Ainda que alguns responsáveis pelo planeamento militar contemporâneo tenham ignorado os principios enunciados por Giulio Douhet, o seu contributo para o estudo do fenómeno da guerra tem sido notório na introdução dos seus ensinamentos nas bases do planeamento da estratégia militar dos Estados Unidos ao longo dos últimos anos.

3 O Major-General Trenchard assumiu o comando da Força Aérea do Reino Unido durante a I Guerra Mundial. Tendo ajudado a fundar a Royal Air Force, conseguiu que esta fosse considerada um Ramo independente das Forças Armadas em Junho de 1918. Trenchard, foi um ferveroso defensor do bombardeamento estratégico, organizando diversos ataques aéreos aos caminhos-de-ferro e centros industriais da Alemanha.

4 De acordo com a definição apresentada no FM 100-6 (1996, p.GL-8), a Guerra de Informação pode ser entendida como o conjunto das "acções desenvolvidas para obter a superioridade de informação, afectando a informação, processos baseados em informação, sistemas de informação e redes de computadores de um adversário enquanto se defendem os nossos sistemas afins".

5 De acordo com a Lei de Moore, formulada em 1965, as capacidades de armazenamento e de processamento de informação duplicam em cada 18 meses. Recentemente, Gordan Moore confirmou publicamente este facto, referindo que não prevê que o seu axioma possa vir a ser violado até 2013 (Ramos, 2003).

6 Os hackers, também designados por "piratas informáticos", são pessoas que, em regra, possuem maior conhecimento técnico que os amadores. Estes indivíduos apresentam também um conhecimento mais ou menos profundo dos processos utilizados e reflectem a intenção de violar, de uma forma ou de outra a segurança ou as defesas do sistema alvo dos seus ataques. A ameaça que os hackers materializam, pode apresentar uma grande diversidade de motivações, variando entre aqueles que são simplesmente curiosos e aqueles que cometem actos de vandalismo. Este último grupo é normalmente designado por crackers.

7 Contrariamente aos restantes "conflitos electrónicos" latentes, conduzidos permanentemente por hackers profissionais conotados com cada um dos Estados referidos, os incidentes registados entre os EUA e a China podem ser analisados de uma forma quase discreta no tempo. Este tipo de ataques conheceu uma expressão muito significativa em 1999 quando, durante o conflito do Kosovo, aeronaves norte-americanas

bombardearam acidentalmente a Embaixada chinesa em Belgrado.Também em 2000, em sequência do choque de uma aeronave dos Estados Unidos, com um MIG chinês, se registou uma autêntica "batalha electrónica" entre hackers chineses e norte-americanos tendo como alvos privilegiados os sites de empresas e organizações governamentais dos dois países.

8 De acordo com o testemunho de Clark Staten, Director Executivo do Emergency Response & Research Institute de Chigago, proferido em 24 de Fevereiro de 1998, perante o Subcommittee on Technology, Terrorism and Government Information do U.S. Senate Judiciary Committee.

9 Este tipo de ataques também conhecido por Denial of Service (DoS), procura atingir o site ou recurso alvo através de um envio ininterrupto de pedidos ao servidor de forma a comprometer a sua disponibilidade e a evitar desta forma a sua utilização.

10 A classificação que aqui se apresenta, consta de um relatório designado por "Cyberterror: Prospects and Implications", elaborado em Agosto de 1999, por esta organização (Denning, 2000).

11 Cf. definição apresentada na Directiva Ministerial de Defesa Militar de 2002.

12 No dia 15 de Agosto de 2003, os EUA e o Canadá sofreram um corte de energia de grande dimensão que, para além de importantes centros urbanos destes países, deixou a cidade de Nova Iorque sem energia eléctrica durante quase 36 horas, bloqueando os sistemas de telecomunicações, o centro financeiro da maior praça económica do mundo, o sistema de metropolitano, os sistemas de informação da rede de abastecimento de águas, serviços públicos, hospitais e a maior parte dos sistemas de suporte à vida diária de cerca de 50 milhões de pessoas.

13 A Zona Sul e Sudeste de Londres, no dia 28 de Agosto de 2003, ficou cerca de 6 horas privada de energia devido a uma falha registada no seu sistema de abastecimento eléctrico. Apesar de a EDF Energy, empresa responsável pelo abastecimento eléctrico, ter referido que o tempo de interrupção foi de apenas 1 hora, admitiu que este corte de energia tornou inoperacional 60 por cento da rede de metro de Londres, provocou engarrafamentos caóticos devido ao não funcionamento dos semáforos e afectou a rede ferroviária uma vez que não foi possível recorrer a geradores porque a falha era de grande dimensão (Público, 2003).

14 Conforme refere em entrevista o Eng Sousa Cardoso, na sua qualidade de Especialista na área da Segurança da Informação, Chairman do Grupo de Trabalho sobre "Fraud Control and Network Security" do ETNO, Consultor Superior para a Qualidade e Segurança na Direcção de Wholesale Internacional da PT Comunicações.

15 Acrónimo utilizado para designar os Sistemas de Comando, Controlo, Comunicações e Informações.

16 A quantificação do risco poderá ser realizada através da seguinte expressão: R = (A.V / Ms).I, onde: R é o valor do risco, A é o valor da ameaça, V é o valor da vulnerabilidade, Ms é o valor da medida de salvaguarda e I é o valor do impacto previsto (Bispo, 2002).

17 Este conceito reflecte o esforço dos EUA na prevenção da ocorrência de ataques terroristas no interior do seu território, procurando reduzir as vulnerabilidades nacionais e minimizando o seu impacto social, através da rápida recuperação dos efeitos produzidos por este tipo de acções.

18 Os sistemas SCADA constituem uma aplicação lógica utilizada para recolher os dados à distância em tempo-real, efectuando o seu tratamento de forma a controlar um

determinado equipamento. Combinando componentes informáticos (hardware) e lógicos (software), este tipo de sistemas emite mensagens de alerta sempre que as condições de operação do sistema em que se encontram inseridos apresentam riscos de funcionamento. São normalmente utilizados em centrais eléctricas, em refinarias de petróleo e de gás, nas redes de telecomunicações, nas redes de transportes e nas centrais que controlam o sistema de distribuição de água.

19 Este conceito, encontra-se vertido no plano de acção "e-Europe 2005" cuja finalidade é a de promover a utilização das novas tecnologias, garantir o seu acesso a todos os cidadãos e empresas e conseguir uma Internet "mais rápida, barata e segura" (COM, 2002, p.1).

20 Encontra-se actualmente em desenvolvimento no INETI um ambiente de simulação e análise de vulnerabilidades das infra-estruturas de informação que, com base no espectro da ameaça, permite identificar os potenciais problemas de segurança dessas infra-estruturas.

21 As áreas funcionais críticas a envolver neste sistema poderiam ser as definidas na DMDM (2002), envolvendo nomeadamente, as seguintes áreas: Intranet do Governo (Administração Pública), Sector das Telecomunicações, área da Defesa e das Forças de Segurança, Rede Eléctrica Nacional, Transportes (ANA, REFER, etc.), Serviço Nacional de Bombeiros e Protecção Civil (Bombeiros, 112, etc.), Sistema Interbancário de Serviços (SIBS), PETROGAL e Sistemas de Trunking (Gestão de Tráfego com base em GPS).

22 O Sistema Integrado das Redes de Emergência e Segurança de Portugal (SIRESP), poderá constituir uma primeira aproximação a uma Infra-estrutura de Informação Crítica Nacional, assegurando a satisfação das necessidades de comunicações das Forças Armadas e de Segurança e dos serviços de emergência nacionais. Esta rede poderá garantir, em caso de emergência, a centralização do comando e da coordenação nacional.