As TIC Para Um Mundo Mais Seguro

Junho 2009

Patrocinadores:

Novabase

indra

apdsi

associação para a promoção e desenvolvimento da sociedade da informação

Coordenador	Mário do Carmo Durão
Relatores	Mário do Carmo Durão José M. Gomes Almeida
Grupo de Trabalho	Ana Paula Simões António Horta Lobo Fernanda Trigo Jorge Gonçalves Silva José M. Gomes Almeida José Santos Coelho Luísa Narciso Manuel Borges Gonçalves Manuel Rio e Carvalho Mário do Carmo Durão Sérgio de Sá Sérgio Sá Vanda Gonçalves Vitorino Cruz
Publicação	Junho de 2009
Actividade nº	1077


apdsi
associação para a
promoção e desenvolvimento
da sociedade da informação

INDÍCE

I. INTRODUÇÃO

A APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação, incluiu no seu Plano de Actividades de 2008, a realização do Estudo "As TIC[1] para um Mundo mais seguro" definido do seguinte modo:

> *O Mundo está a entrar numa nova Era evidenciando-se alguns sinais que fazem adivinhar mudanças radicais no equilíbrio de forças que suporta a teia global de relações internacionais, conduzindo a um novo capítulo da História.*
> *Actualmente qualquer cenário associado à sociedade moderna decorre de mudanças que se iniciaram com o 11 de Setembro de 2001, o qual constituiu a pedra de toque para uma tentativa de mudança do sistema mundial e que se revela mais premente à medida que se vão conjugando outros aspectos societários.*
> *É um facto que poderes que historicamente se concentravam (tecnologia, informação, e comércio) para dar poder a um Estado, estão hoje espalhados pelo mundo. O desenvolvimento tecnológico e científico é um factor que contribui de forma decisiva para a mudança que se aproxima, sendo a tecnologia, na sua generalidade, um dos factores que mais alteram o pensamento estratégico.*
> *Pretende-se com este estudo reflectir sobre o papel que as TIC, como parte importante do conjunto das tecnologias modernas, podem desempenhar na sociedade, nomeadamente influenciando a segurança - dos cidadãos e da sociedade no seu todo, sem descurar a protecção dos direitos, liberdades e garantias fundamentais*

Perante a abrangência do tema proposto pela APDSI e na impossibilidade de o mesmo poder ser tratado na sua globalidade, o Grupo de Estudo, decidiu estruturar o Relatório Final da seguinte forma:

- O primeiro capítulo é a "Introdução", onde se definem o âmbito do Estudo, as directrizes do trabalho, a estrutura do Relatório Final e uma breve descrição dos capítulos seguintes.

  Importa salientar, que o tema proposto para este Estudo, conduz-nos ao relacionamento de duas temáticas distintas que são, as TIC e a segurança do Mundo.
- No segundo capítulo, designado "Um Mundo Seguro?", são abordados alguns temas relacionados com a segurança do Mundo, nomeadamente e de forma genérica, a *segurança do Mundo actual e as*

[1] Tecnologias da Informação e da Comunicação

dimensões dessa segurança, a globalização e as ameaças à segurança, sendo dado particular ênfase às *ameaças transnacionais* e *assimétricas*.

Neste capítulo são ainda focadas *as questões da segurança, dos riscos e das ameaças*, numa perspectiva teórica (teoria da segurança), para melhor compreensão de alguns conceitos utilizados ao longo do Estudo.

- Analisadas as questões da segurança, ou da insegurança, do Mundo actual, o terceiro capítulo, intitulado "As TIC no Mundo actual**",** enquadra o tema da segurança da informação e analisa a importância das TIC na sociedade actual: a sua influência, a presença constante, os impactes, os desafios, os novos paradigmas.
  Pela sua importância no Mundo actual, pelo seu carácter global e pela forma como tem vindo a alterar os nossos padrões de vida em sociedade, a Internet merece uma referência especial neste capítulo, visto que muitos dos problemas de segurança que se colocam actualmente, são originados, potenciados, veiculados ou mesmo resolvidos através da utilização da Internet.
  Estes dois capítulos, de cariz mais teórico, constituem a primeira parte do Estudo, promovendo o enquadramento e o levantamento das situações, no diz respeito às TIC e à segurança do Mundo.
- O quarto capítulo, designado "As TIC para um Mundo mais seguro**"** é o capítulo fundamental do trabalho e corresponde à segunda parte do Estudo. É neste capítulo que é feita a ligação das TIC com a problemática da segurança, analisando-se também vários temas específicos que relacionam as TIC com a segurança do Mundo actual e onde são propostas/sugeridas linhas de acção.
  Ao longo do capítulo, procuram-se obter com a clareza possível, respostas para questões como: *As TIC contribuem para o incremento dos riscos e das ameaças para a segurança do Mundo?* ou, pelo contrário**,** *as TIC podem diminuir ou mesmo eliminar, esses riscos e ameaças?* Num caso ou no outro, ou mesmo em ambos, *de que forma é que as TIC poderão influenciar a segurança do Mundo?*
  Na sua globalidade, o capítulo promove uma abordagem que considera o relacionamento das TIC com a segurança do Mundo, nas perspectivas dos indivíduos, das organizações e dos Estados, procurando enquadrar os vários temas específicos, no âmbito de cada uma ou das várias perspectivas e, dentro destas, segundo várias dimensões (societária, jurídica, económica, tecnológica, etc.).
- O Estudo termina com um capítulo de Conclusões e outro de Recomendações, relativamente ao tema proposto pela APDSI.

Com a preocupação de facilitar a leitura do texto, recorremos naturalmente a termos que são tipicamente utilizados em ambientes especializados em segurança. Para o facto, contamos antecipadamente com a compreensão do leitor.

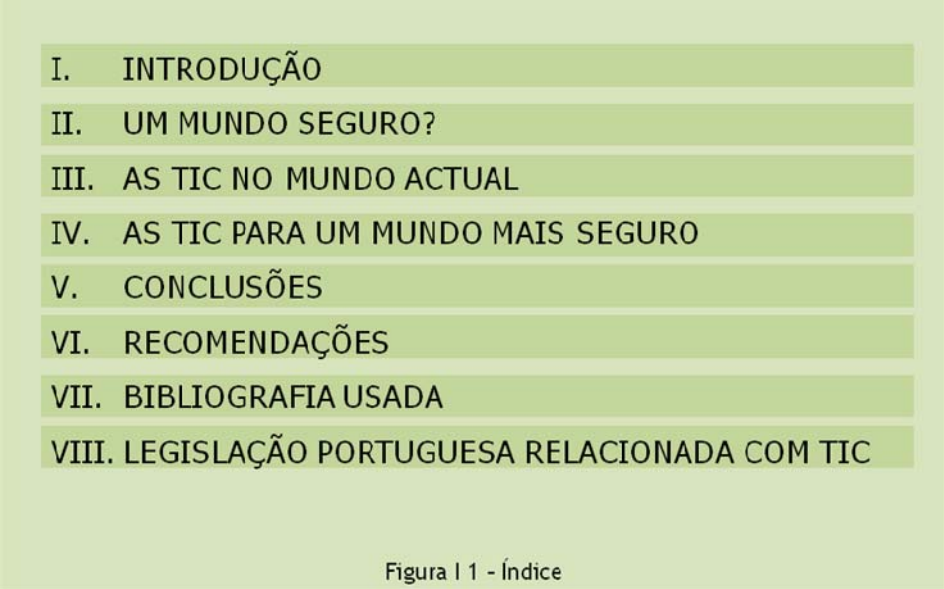

Figura I 1 - Índice


apdsi
associação para a
promoção e desenvolvimento
da sociedade da informação

II. UM MUNDO SEGURO?

A. A SEGURANÇA

No presente capítulo, serão abordados, ainda que de forma genérica, alguns temas relacionados com a segurança do Mundo actual. A abordagem de questões relacionadas com a segurança é sempre difícil sem recorrermos à terminologia mais comummente usada nos meios que lhe estão directamente relacionados.

Como acontece com praticamente qualquer outro tema, se quisermos entendê-lo bem no sentido de aprendermos as várias facetas do fenómeno e quais as acções que são aconselháveis ou mesmo obrigatórias adoptar no futuro, conforme a nossa responsabilidade individual (cívica, política, empresarial, etc.) precisamos de observar e pensar em várias esferas temáticas que se intersectam.

O título desta secção traz-nos facilmente à memória histórias que povoaram o imaginário da nossa juventude, e que ainda hoje servem para nos entreterem e para nos fazer pensar.

É óbvio, por exemplo, que as acções de espionagem não se restringem exclusivamente às páginas dos livros de Ian Fleming ou de Le Carré, ou mesmo aos *blockbusters* de Hollywood.
Em muitos filmes de *cowboys* os ladrões eram retratados de forma algo padronizada: eram altos, muitas vezes estrangeiros, frequentemente simpáticos, usavam vestes negras e transportavam grandes revólveres. Cavalgavam cavalos lustrosos em cidades do interior e saqueavam os bancos locais.

Já os modernos ladrões de bancos são muito mais parecidos com colegas nossos, e apresentam-se tão bem vestidos como nós. Em vez de transportarem armas de fogo e roubarem centenas de euros ou de dólares em moedas e notas, desenvolvem esquemas manipulativos complexos e roubam milhões de euros ou de dólares.

Esses esquemas são fundamentalmente baseados em informações que os ladrões copiam de locais normalmente disponíveis no ciberespaço ou que estão em trânsito dentro dele. É claro que o acesso indevido a informação de outrem poderá servir para uma multiplicidade de fins, sempre para obter informação sensível que possa ser utilizada em desfavor do seu legítimo dono, nomeadamente: para a realização de fraudes financeiras; para a preparação e execução de actividades terroristas; para a gestão estratégica e táctica em domínios militares; etc.

O facto das esferas de influência em que vivemos hoje se expandirem em crescendo, coloca-nos frequentemente perante situações de anormalidade social, política e económica.

Já nenhuma sociedade está "orgulhosamente só". Estamos afirmativamente inseridos numa comunidade que é cada vez mais global, e partilhamos com os outros membros dessa comunidade o que ela traz de bem e de mal.

Antes de entrarmos nas secções seguintes, é conveniente clarificar alguns conceitos fundamentais, designadamente a definição do próprio termo **segurança**, o qual tanto é usado para referir o estado de "estar a salvo" [2] como a condição de "ser protegido contra perigos ou perdas"[3].

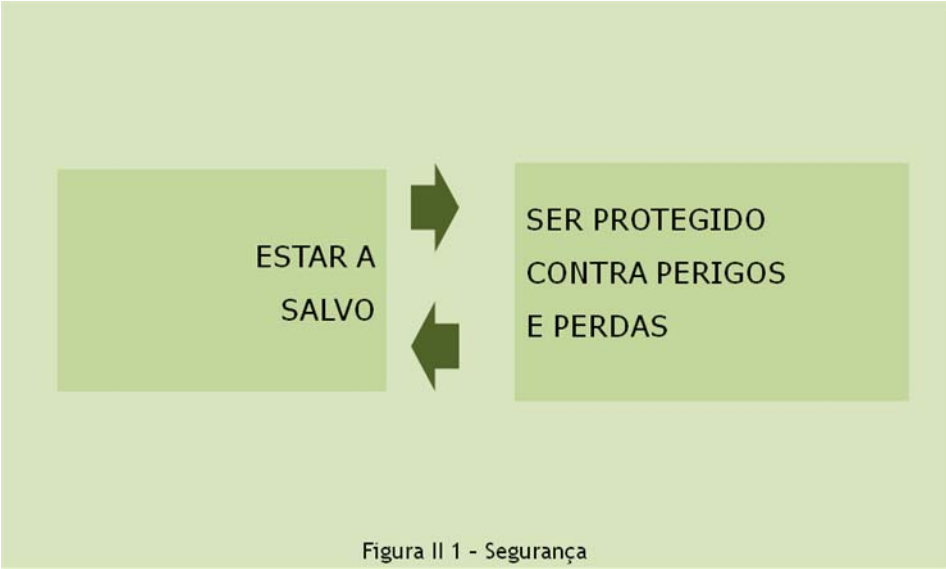

Figura II 1 - Segurança

A primeira definição, corresponde à condição de ser protegido contra falhas, danos, erros, acidentes, ou acontecimentos de outro tipo que possam ser considerados como indesejáveis, quer sejam físicos, sociais, espirituais, financeiros, políticos, emocionais, ocupacionais, psicológicos, educacionais ou outros.

Isso pode tomar a forma de ser protegido do acontecimento ou da exposição a qualquer coisa que cause perdas económicas ou de saúde. Pode incluir ainda a protecção de pessoas ou de propriedades.

Esta segurança pode ser limitada em relação a alguma garantia ou a um *standard* para assegurar a qualidade e a função não prejudicial de um objecto ou organização.

[2] *Safety*

[3] *Security*

Já relativamente à segunda definição, ela é comummente interpretada como sendo similar à anterior. Existe, no entanto, uma diferença entre as duas, que consiste na ênfase que é acrescentada na segunda relativamente a ser-se protegido de perigos originários do exterior.

Existe um outro conjunto de conceitos, igualmente associados à segurança, que importa clarificar. São estes, os conceitos de **suspeita**, **ameaça** e **risco**. Genericamente:

Suspeita É uma indicação baseada em métodos de operação conhecidos (ou previstos) como sendo próprios de terroristas ou de criminosos que poderão conduzir à crença de que uma situação observada (pessoas e/ou objectos) possui o potencial para ameaçar um determinado ambiente e/ou os seus habitantes;

Ameaça É uma suspeita que não foi refutada e por conseguinte, indica a possibilidade de uma situação perigosa poder ocorrer

Risco É a possibilidade de uma situação perigosa ocorrer, baseada na ocorrência da mesma situação no passado

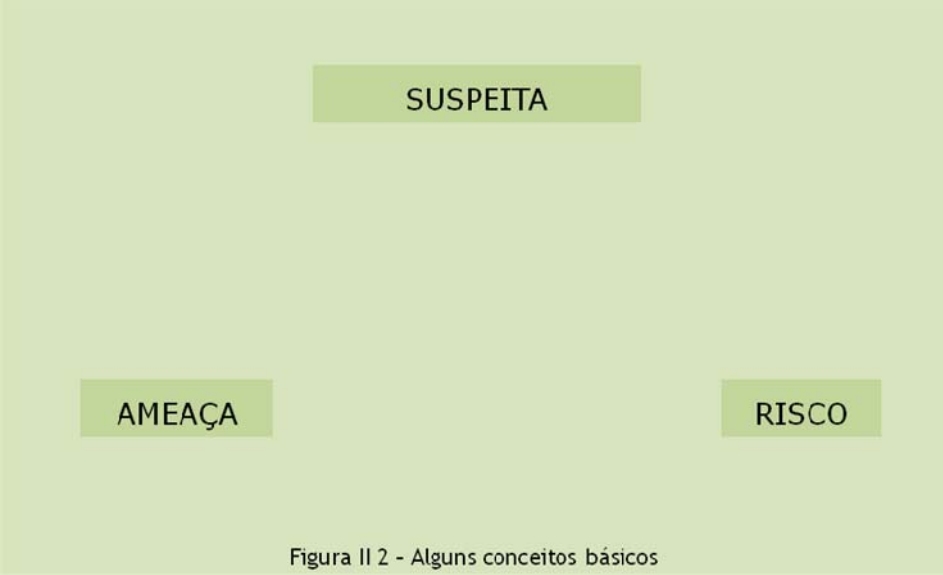

Figura II 2 - Alguns conceitos básicos

É importante diferenciar entre ameaça e suspeita. A própria definição de suspeita, potencia uma situação em que a suspeita é abundante. No entanto, na esmagadora maioria dos casos, após análise da situação, a suspeita é refutada e a situação revela-se como sendo uma situação que não virá a transformar-se em ameaça.

Um outro conceito relacionado com a segurança e que importa considerar, é o conceito de **vulnerabilidade** que poderemos definir como sendo "uma fraqueza num qualquer sistema que pode potencialmente ser explorada por uma ameaça".

Centrando-nos no tema do Estudo, é importante afirmar que quando o alvo da nossa preocupação é a segurança da informação, temos que construir e implementar esquemas e medidas que garantam a confidencialidade, autenticidade, integridade e disponibilidade dessa informação, protegendo quer os equipamentos quer os meios de comunicação.

Simplesmente, temos de assumir uma de duas atitudes – estar desligado ou estar ligado – em que a primeira, corresponde a uma situação de isolamento e onde o nível de segurança é efectivamente muito grande, e a segunda, corresponde a uma situação sujeita a riscos que temos de saber gerir.

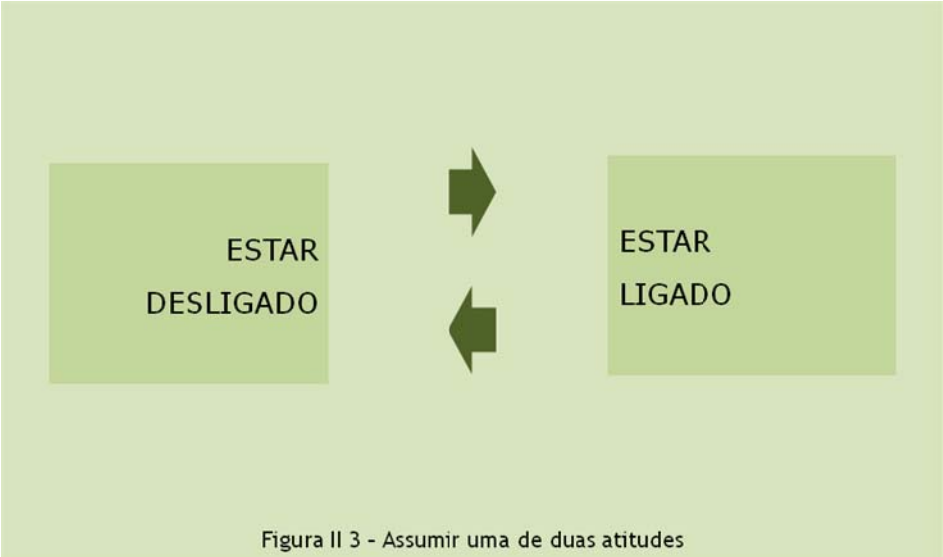

Figura II 3 - Assumir uma de duas atitudes

B. A SEGURANÇA DO MUNDO ACTUAL

Passados em revista alguns conceitos fundamentais da segurança, vejamos agora a segurança do Mundo actual, profundamente marcado pela globalização e pelas novas ameaças.

No actual contexto internacional, o ambiente estratégico caracteriza-se pela incerteza, imprevisibilidade, complexidade e volatilidade, o que implica um conceito de segurança adaptado a novas fronteiras (económica, cultural, interesses) para além das tradicionais fronteiras política e geográfica e alargado a

domínios como a política, a economia, o ambiente, a educação, a cultura, a ciência e a saúde [Garcia, 20071].

Neste contexto, a segurança também se alterou, passando da previsibilidade para uma segurança orientada para riscos diversos, mais difusos na forma, na origem, no espaço e nos actores, fazendo aumentar as condições para a eclosão de conflitos [Garcia, 20071].

Existe um sentimento generalizado de insegurança à escala mundial, perante um conjunto de novas ameaças, que surgem como de natureza global e transnacional e em relação às quais, as opiniões públicas, mantêm a desconfiança quanto à capacidade dos Estados e das estruturas internacionais, para as combater e poderem garantir a segurança das populações.

A segurança transformou-se, assim, numa obsessão à escala mundial, com repercussões na vida interna de muitos países, dada a forte ligação existente entre segurança e desenvolvimento. Os vários conflitos político-militares não só destroem as infra-estruturas materiais, sociais e humanas, como encorajam a criminalidade, impedem o desenvolvimento e obrigam muitos países a cair no ciclo infernal conflito-insegurança-pobreza [Costa, 20051]

Segundo o Embaixador Francisco Seixas da Costa num artigo publicado na Revista Militar [Costa, 20051], a segurança internacional e as ameaças que sobre ela impendem, pode ser considerada segundo várias dimensões. Resumidamente e de acordo com o citado artigo, serão de considerar:

Segurança democrática	Sendo a democracia uma realidade numa minoria de países, existe um grupo de ameaças que se situa no que poderemos designar por atentados à segurança democrática dos Estados. Neste sentido é importante notar que todos os factores que afectem os Direitos Humanos e as liberdades fundamentais, os valores da Democracia ou os princípios do Estado de Direito, são sempre elementos que afectam a segurança dos cidadãos e podem contribuir para a disrupção da estabilidade política e social. A questão do respeito pelos Direitos Humanos é hoje central na avaliação dos Estados.
Segurança económica, social e ambiental	Um segundo grupo de questões que afectam a segurança internacional, prende-se com os factores económicos, sociais e ambientais. A desigualdade económica, as flagrantes injustiças sociais e os ambientes de pobreza e exclusão, são factores da maior importância, na criação de potenciais riscos para a segurança internacional. A SIDA, a malária ou a tuberculose continuam a ser factores de risco a nível internacional, assim como os problemas económicos ligados às questões do desenvolvimento sustentável, da poluição e do não tratamento dos lixos, da gestão dos recursos hídricos ou o problema dos riscos e dos resíduos nucleares.
Segurança político-militar	Um outro grupo de ameaças, prende-se com a persistência de factores associados a riscos de natureza político-militar. A este respeito importa considerar as armas convencionais e todos os problemas associados ao seu controlo pelos Estados e ao tráfico ilícito não esquecendo as questões específicas das SALW[4] e dos MANPADS[5]. Ainda relativamente às armas

[4] *Small Arms and Light Weapons*

[5] *Man-Portable Air Defense Systems*

convencionais será de referir o seu acesso a mãos nãoestatais naquilo que alguns qualificam como a "privatização da guerra".

Num outro nível, não podem deixar de ser consideradas as armas de destruição massiva que vão desde as armas químicas e biológicas ao armamento nuclear tradicional.

Conflitos regionais

Estes conflitos constituem sérias ameaças à segurança das regiões onde se inserem e por vezes chegam a ter impacto em equilíbrios políticos bastante distantes das suas fronteiras. Convém notar que estes conflitos são originários ou potenciam facilmente o extremismo, a violência sectária e, muitas vezes, acabam por arruinar as limitadas capacidades dos novos Estados para se organizarem enquanto entidades internacionais, conduzindo, por vezes, ao fenómeno dos chamados "Estados falhados".

Combate à criminalidade

Muitas vezes associada aos conflitos, surge uma outra ameaça importante nos nossos dias: o crime organizado. Nas últimas décadas, temos assistido ao crescimento do tráfico de drogas mas, igualmente, de diamantes e produtos raros. O tráfico de seres humanos, a exploração de redes de emigração ilegal e mais recentemente, a pirataria marítima à escala internacional, também têm vindo a crescer.

Combate ao terrorismo

O terrorismo é considerado hoje a mais importante causa de instabilidade a nível mundial. Apesar não ter sido possível até hoje, encontrar um consenso internacional quanto à definição de terrorismo, é indispensável e urgente encontrar formas sérias de o combater. Uma das dificuldades reside no seu carácter assimétrico: o terrorismo actua com uma desproporção de meios e sem regras enquanto os Estados são obrigados a reagir de acordo com padrões legais. Outra dificuldade, reside nas raízes do terrorismo e nas causas sociais, económicas e políticas que estão na sua origem e nas fontes de injustiças, que são terreno fértil para o seu desenvolvimento, e as quais é absolutamente necessário atacar.

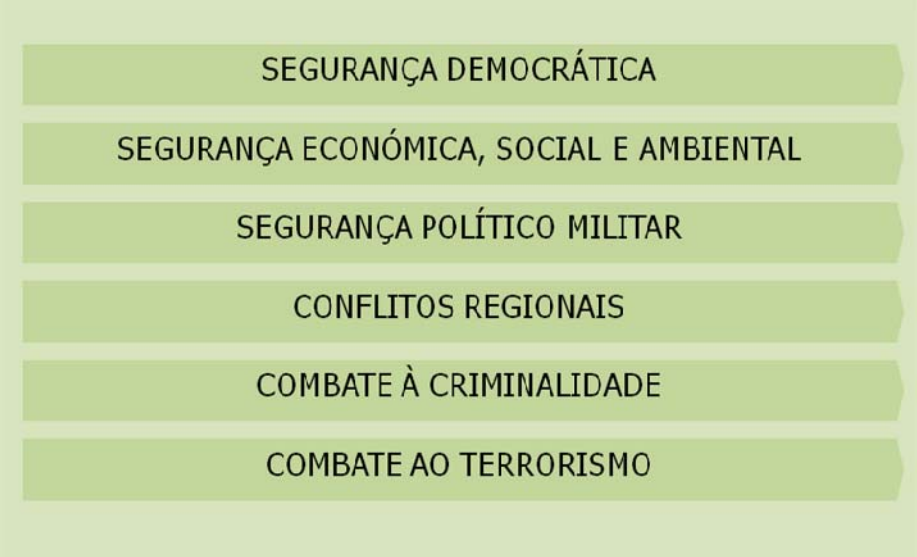

Figura II 4 - Dimensões da segurança internacional e as ameaças que sobre ela impendem

C. A GLOBALIZAÇÃO

A globalização facilita de algum modo a produção de efeitos mais ou menos desastrosos, normalmente associados a riscos que já há muito são enfrentados pelas sociedades, com maior ou menor consciência:

Caos climático e degradação ambiental	Este risco é consequência da uma sociedade de consumo despreocupada com a crescente produção de resíduos e sem soluções para a sua reciclagem.
Pobreza	Este risco é hoje em dia maior do que há alguns anos atrás pois as pessoas passaram a poder comparar com facilidade o seu bem-estar económico (ou a falta dele...) com o dos outros.
Geopolítica e energia	O grande desequilíbrio entre o uso da energia pelo Ocidente e pelo mundo em vias de desenvolvimento, assim como as implicações globais do recurso intenso a combustíveis não renováveis, sobre o ambiente e sobre a própria economia global, terá uma importância política crescente. Encontramos um exemplo muito recente de alguns destes riscos no comportamento dos mercados do Petróleo e no forte impacto que esse comportamento tem tido na economia mundial.
Crime organizado e terrorismo	Segundo os especialistas em segurança existe uma relação entre o que designam por "estados falhados", o crime organizado e o terrorismo. O elevado lucro do crime organizado constitui uma forte motivação para o crime. Por outro lado, o terrorismo pode multiplicar o efeito dos seus atentados se recorrer a novas tecnologias. Por exemplo, um terrorista armado com uma nano tecnologia é muito mais destruidor do que um terrorista armado com armas tradicionais.
Proliferação de tecnologias avançadas	A investigação e o desenvolvimento de novas tecnologias abrangem uma vastidão cada vez maior de áreas, nomeadamente: Biotecnologias; TIC; RFID; Nano tecnologias; Robótica; Inteligência artificial.
Carências de recursos	Precisamos de nos preocupar com as previsíveis carências de alguns recursos fundamentais para a vida humana, nomeadamente a água e o ar limpo.
Pandemias	A ameaça de pandemias como por exemplo a gripe aviaria e suína tem evidenciado a actual fragilidade do mundo relativamente a ameaças de doenças mais ou menos tradicionais. Isso resulta sobretudo de factores como o transporte global, a integração económica, o crescimento das cidades.
Sistemas financeiros e risco sistémico	A liberdade global de movimentos de capitais, de futuros, de derivados e outros produtos financeiros, potenciada pela impotência e incompetência das autoridades reguladoras dos países está associada a riscos também com impacto intenso e extenso. A crise que quase todo o mundo está a atravessar hoje, constitui um exemplo bem real deste tipo de risco.
Transhumanismo e ética	O progresso em determinadas tecnologias emergentes poderá facilitar *quick wins* em áreas sociais, sobretudo nos países mais pobres e/ou em vias de desenvolvimento. Por exemplo, avanços nas formas de intercomunicação e de meios de apoio à educação constituirão grandes vantagens, assim os governos os queiram e consigam promover e usar.

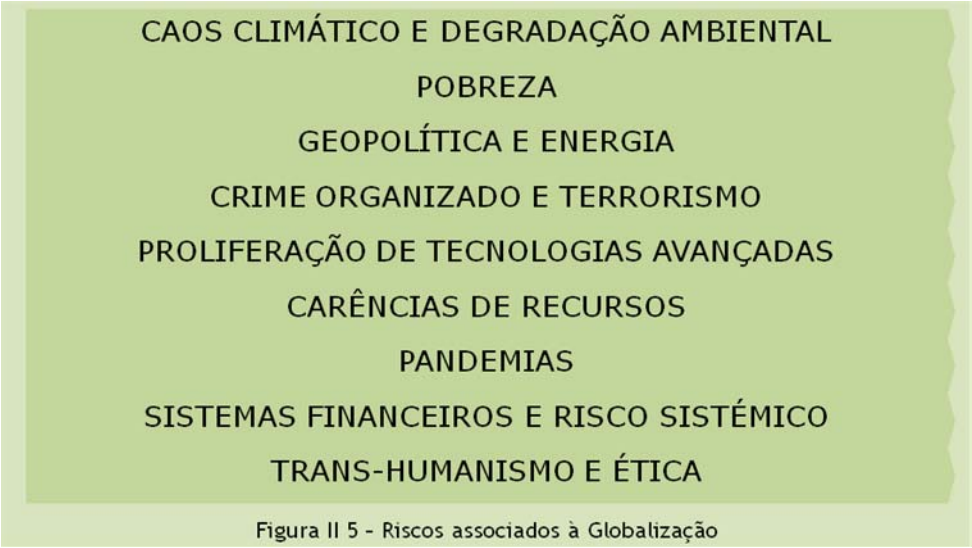

Figura II 5 - Riscos associados à Globalização

D. AS AMEAÇAS

No momento presente e nas próximas décadas, igualmente de acordo com as Nações Unidas [UN20041; p.25], o Mundo precisa de se preocupar com seis tipos de ameaças:

- Ameaças económicas e sociais.

  (Incluindo pobreza, doenças infecciosas e degradação ambiental.)

- Conflitos entre Estados.
- Conflitos internos.

  (Incluindo guerras civis, genocídios e outras atrocidades em grande escala.)

- Armas nucleares, radiológicas, químicas e biológicas.
- Terrorismo.
- Crime organizado transnacional.

Figura II 6 - Ameaças para o Mundo

Por outro lado, a Estratégia Europeia em Matéria de Segurança [UE20031], apresenta as seguintes ameaças principais para a União Europeia:

- O Terrorismo;
- A Proliferação das Armas de Destruição Massiva;
- Os Conflitos Regionais;
- O Fracasso dos Estados;
- A Criminalidade Organizada.

Assim, e de um modo geral, é fundamental que os cidadãos de todo e qualquer país, tenham a maior consciência possível dessas ameaças.

As novas ameaças, que hoje em dia afectam a nossa segurança, distinguem-se das tradicionais, pelo seu carácter transnacional, desterritorializado, disseminado e individualizado. O seu paradigma é genericamente não governamental, não convencional, dinâmico, não linear, com regras de empenhamento desconhecidas, com um modo de actuação e uma doutrina assimétrico e imprevisível [Steele 2002; p.5].

Figura II 7 - Ameaças para a União Europeia

A Organização para a Cooperação e Desenvolvimento Económico (OCDE) [OCDE20081] tem vindo a desenvolver um conjunto de recomendações para promover a Segurança dos Sistemas de Informação e Redes e que se baseia em 9 princípios:

- Consciência – Os participantes devem estar cientes da necessidade para a segurança dos sistemas de informação e do que podem fazer para melhorar esta segurança;
- Responsabilidade – Todos os participantes são responsáveis para a segurança dos sistemas de informação;
- Resposta – Os participantes devem cooperar e reagir rapidamente de forma a impedir, detectar e responder aos incidentes de segurança;
- Ética – Os participantes devem respeitar os interesses legítimos dos outros;
- Democracia – A segurança dos sistemas informação deve ser compatível com valores essenciais de uma sociedade democrática;
- Avaliação do Risco – Os participantes devem efectuar a avaliação de risco aos sistemas informação;
- Desenho e Implementação de Segurança – Os participantes devem incorporar a segurança como um elemento essencial dos sistemas informação;
- Gestão de Segurança – Os participantes devem adoptar uma aproximação detalhada à gestão da segurança;
- Reavaliação – Os participantes devem rever a segurança dos sistemas de informação, efectuar alterações apropriadas às políticas, às práticas e aos procedimentos de segurança.

As seguintes áreas foram identificadas como necessitando de uma atenção particular por parte dos governos e entidades envolvidas, nomeadamente:

- Protecção de Infra-estruturas Críticas;
- Autenticação Electrónica;
- *Malware* e Roubo de Identidades;
- Identidade Digital *Online;*
- Identificação por Radiofrequência *(RFID).*

A European Network and Information Security Agency (ENISA) [ENISA20091] é uma entidade que tem a missão de apoiar as instituições da União Europeia e os Estados membros a responder a potenciais problemas no domínio da Segurança da Informação.

Algumas das actividades em que a ENISA se encontra envolvida são:

- Melhorar a resiliência das redes de comunicação entre os Estados membros;
- Desenvolver modelos de cooperação entre os Estados Membros;
- Identificação de desafios de segurança emergentes na Sociedade de Informação;
- Boas práticas para a partilha de informação entre comunidades de CERTs/CSIRTs.

AS AMEAÇAS TRANSNACIONAIS

As Nações Unidas definem **ameaça transnacional,** de uma forma bastante ampla, como:

> *"(…) Any event or process that leads to large-scale death or lessening of life chances and undermines States as the basic unit of the international system is a threat to international security(…)" [UN20041; p.12]*

Consideram-se como ameaças transnacionais: o Terrorismo envolvendo Armas de Destruição Massiva[6], as ciberameaças[7] às infra-estruturas nacionais e o Crime Organizado internacional. Dada a sua natureza global, as ameaças transnacionais existem tanto na esfera doméstica como na esfera internacional.

Nos últimos 25 anos o Terrorismo tem constituído uma ameaça muito excepcional e significativa.

Sendo o tipo de ameaça mais perigoso com que o mundo actual tem que lidar, ele tem-nos forçado a repensar os actuais paradigmas da nossa sociedade.

Por outro lado, as ameaças transnacionais não estão limitadas por quaisquer fronteiras. Esse facto, complica muito o seu combate, particularmente quando há que perseguir, capturar ou combater criminosos (os quais podem esconder-se facilmente para lá de uma fronteira). É importante que exista confiança entre vizinhos e aliados de modo a permitir a realização de acções de combate para lá das fronteiras.

A era do computador, em que hoje nos encontramos, potenciou novas possibilidades, e ao mesmo tempo tornou a nossa vida mais complexa. Ela caracteriza-se por estar em permanente mudança e por evoluir com uma rapidez cada vez mais acelerada. Infelizmente essas características facilitam a desorientação da sociedade, muitas vezes com resultados negativos.

Cremos que os futuros conflitos generalizados diferirão muito dos que se verificaram no passado, caracterizando-se principalmente pelos seguintes aspectos:

[6] *Weapons od Massive Destruction* ou *WMD*

[7] Termo que adoptamos para referir ameaças ao/do/através do ciberespaço.

- Não será nítida a distinção entre soldados e civis.
- O campo de batalha não será um campo convencional, sendo em vez disso um campo resultante da convergência de tecnologias e de infra-estruturas.
- As ameaças serão mais difusas e os seus agentes serão difíceis de localizar.

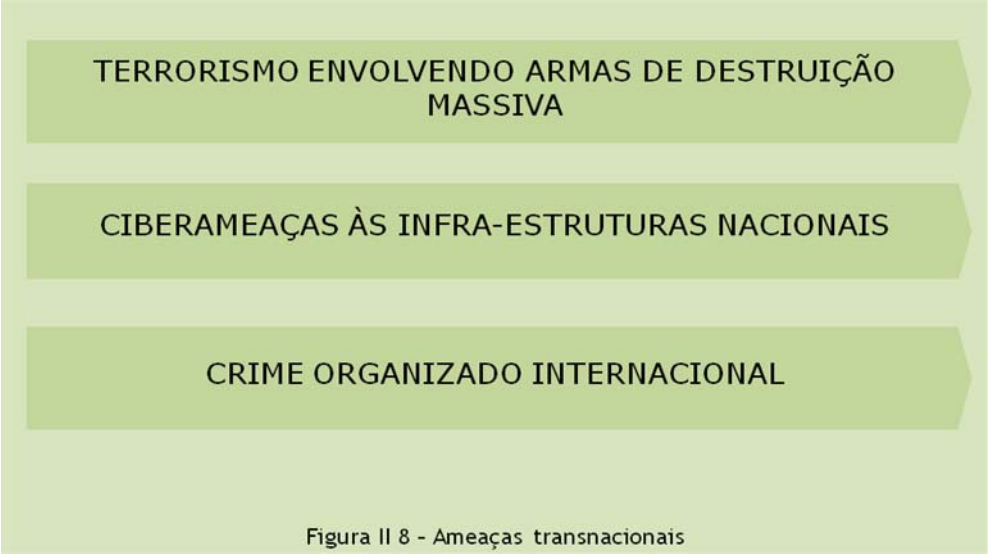

Figura II 8 - Ameaças transnacionais

AS AMEAÇAS ASSIMÉTRICAS

Na essência, qualquer ameaça que é desproporcional e que pode destruir um sistema maior e bem organizado constitui uma ameaça assimétrica.

Os ataques de 11 de Setembro de 2001[8] são exemplos de ataques assimétricos.

Outro exemplo é o cyberataque de que a Estónia foi vítima em 2007 e que paralisou toda a infra-estrutura Internet.

Na realidade, qualquer ataque que provoque disrupção sobre o nosso modo de vida, sobre a nossa sociedade, sobre a nossa economia (quer seja químico, biológico, radiológico, nuclear, digital ou mesmo o suicídio) é um ataque assimétrico.

Após o 9/11 o mundo tornou-se um lugar diferente. Por exemplo, a entrada das pessoas num país que não o seu passou a ser precedido de um ritual diferente do que acontecia antes: as pessoas passaram a precisar

[8] Por vezes referido por 9/11.

de transportar consigo meios de identificação altamente sofisticados e só interpretáveis por dispositivos de reconhecimento biométrico (de reconhecimento facial, de impressão digital, etc.).

A tecnologia passou a ser utilizada pelas mais variadas formas para controlar fronteiras e detectar criminosos e terroristas – tanto no mundo físico como no ciberespaço.

Por sua vez, as comunicações de correio electrónico e de voz são hoje em dia objecto de monitorização alargada e praticamente permanente por parte de agências de "inteligência" do mundo ocidental.

Perante a acção crescente de extremistas e do crime organizado, é importante que os países e as suas empresas colaborem activamente através da partilha de informações e de sistemas de informação destinados explicitamente a prevenir e combater as ameaças de que temos vindo a referir.

Por parte de cada cidadão (que reside permanente num país), assim como por parte de qualquer empregado de uma empresa ou outra organização, é necessário que haja meios de identificação individual. Esses meios permitem normalmente identificar uma pessoa como cidadão de um determinado país ou como colaborador de uma determinada organização, e terão quase de certeza partes com dados biométricos, facilitando o controlo e o acompanhamento dos seus movimentos – quando viajam através das fronteiras, quando se deslocam a instalações consideradas sensíveis, etc.

O crime organizado explora actualmente várias "linhas de negócio" (por exemplo: imigração ilegal; tráfico de armas; pirataria de vídeo, áudio e software; pornografia infantil; contrabando e contrafacção de bens; fraude bancária e de cartões de crédito *on-line*; etc.) que lhe rendem lucros significativos – segundo algumas estimativas na ordem de 1 a 1.5 triliões de dólares por ano.

Como já antes evidenciámos, uma guerra assimétrica pode acontecer segundo uma ou mais das seguintes cinco dimensões: terra; mar; céu; espaço exterior e ciberespaço.

O ciberespaço corresponde à quinta dimensão

As ciberameaças incluem sobretudo Guerra de informação e cibercrime.

É óbvio que estaremos perante uma situação de Guerra quando as ameaças originarem ataques com intenção de destruir ou de minar um governo legalmente constituído. Por outro lado, estaremos perante uma situação de Crime quando se verificarem ataques com motivações de ganho pessoal ou organizado.

Enquanto lidar com o Crime é uma responsabilidade de natureza policial, lidar com a Guerra é uma tarefa de militares. Frequentemente não se consegue determinar quem está na origem de uma ciberameaça, sendo impossível concluir-se se se está perante uma situação de crime ou de guerra/guerrilha.

O sector privado é proprietário e utilizador de grande parte do ciberespaço, e depende fortemente deste, tendo por isso simultaneamente uma responsabilidade e uma necessidade de defender esse mesmo ciberespaço. Contudo a cooperação no sector privado nunca foi fácil de conseguir nem é universalmente desejada.

Nesta dimensão encontra-se a nova fronteira na qual se movimentam quase livremente os extremistas e os criminosos. Passar esta fronteira tem um custo baixo, sendo também pouco significativas as possibilidades de se ser apanhado.

Para além de possibilitarem o fluxo e o tratamento da informação, as TIC são partes vitais dos sistemas de comando e de controlo das infra-estruturas críticas para a nossa sociedade.

Os serviços financeiros, a produção e o fornecimento de energia, os transportes, os serviços de emergência na saúde, os serviços de produção e distribuição da alimentação, etc., estão apoiados em sistemas de TIC. Obviamente que esses sistemas não são perfeitos, tendo cada um deles as suas vulnerabilidades, podendo assim serem alvos de ataques de *hackers*, de *malware* (*vírus*, *worms*, *hoaxes*, *trojans*, etc.), de ataques destinados a entupir a largura de banda causando engarrafamento de tráfego digital.

Encontram-se no ciberespaço diversos outros tipos de acção mal intencionada (como o furto/roubo de identidade e os esquemas de *phishing*) que fixam como alvos os bancos e os seus clientes, e que levam a efeito fraudes diversas destinadas a dar cobertura a actividades - licitas e ilícitas - por parte do crime organizado.

O espaço exterior corresponde à quarta dimensão

Não é impossível que um satélite comercial venha a ser "desviado" [9] para difundir propaganda extremista tal como aconteceu há alguns anos atrás com uma acção levada a cabo pela seita Falun Gong. Em 2002 essa seita desviou o sinal de um satélite chinês e utilizou-o para difundir a sua agenda em vez dos programas da Televisão Central da China. O que foi transmitido nesse período chegou a uma quantidade enorme de cidadãos chineses.

Qual seria o resultado se numa situação deste género fosse transmitida uma mensagem (que até poderia ser falsa) por todo um país, por extremistas pertencendo a uma fé particular, dizendo que pessoas de outra fé tinham destruído um qualquer símbolo importante para essa fé?

Não nos podemos esquecer de que há já muitos anos que a batalha pelos espíritos (e pelos corações) é uma ameaça mais ou menos latente através da exploração do enorme poder dos *media*.

[9] *Hijacked*

Os céus como terceira dimensão

O que aconteceu em 9 de Setembro de 2001 confirma que ameaças significativas podem converter-se em ataques pela utilização dos céus e usurpando os sistemas de transporte normais.

Segundo notícias que continuamos a ler nos meios de comunicação social existem informações colhidas por vários serviços de Inteligência do Leste e do Médio Oriente que sugerem que uma tragédia do tipo 9/11 pode repetir-se noutros pontos do planeta.

O mar é a segunda dimensão a ter em conta numa guerra assimétrica

Transportando os barcos comerciais a maior parte (acima de 75%) dos bens transaccionados no mundo, não custa a crer que esses barcos, os portos e outros componentes da cadeia económica marítima são alvos tentadores para ameaças assimétricas.

O recente arresto de um super petroleiro por piratas da Somália, ainda que com o fim de obter um resgate financeiro, constitui um exemplo que não deve ser ignorado.

A primeira dimensão de uma guerra assimétrica é a terra

Os inúmeros ataques de bombistas suicidas que provocaram explosões em sítios tão diferentes como: Iraque; Israel; Rússia; Quénia; Marrocos; Argélia; Turquia; Arábia Saudita; Paquistão; índia; Indonésia; Filipinas; Madrid; etc., mostram que essas tácticas desprezíveis se tornaram um fenómeno global. Para qualquer parte do mundo esse fenómeno é difícil de ser entendido e aceite pois nenhuma religião do mundo acolhe e promove ataques suicidas.

Não havendo nenhuma forma directa para se combater esta ameaça, é infelizmente necessário que as entidades públicas adoptem medidas que permitam o rastreio (sobretudo na passagem por fronteiras entre países) de actividades de suspeitos, assim como de imigrantes ilegais que usem documentos de identidade falsificados. É óbvio que, ao mesmo tempo, os estados devem implementar e aplicar medidas que protejam o cidadão relativamente a excessos na aplicação dessas mesmas medidas, no sentido de prevenir eventuais invasões da privacidade e outras influências inadequadas sobre a sua vida pessoal e social.

É de enorme importância que cada parte do Mundo compreenda a história e a tradição das outras partes, no sentido de se compreender o que conduziu as culturas e os países ao longo da sua história de modo a tornarem-se únicos no mundo de hoje.

Todos nós temos a consciência de que não há nenhuma forma perfeita de governo, assim como não há uma forma certa ou errada de viver. Para o bem da humanidade vale a pena procurar, preservar e melhorar o respeito mútuo e partilhar valores universais.

Os responsáveis pela governação dos países (no plano político e noutros) têm a responsabilidade de educar as suas populações no sentido de elas serem capazes de compreender outras pessoas e outras sociedades, o que facilitará e encorajará a evolução de indústria e de comércio, e corresponderá a uma contribuição importantíssima para a mitigação de problemas como o desemprego e a perda de auto-estima (tanto individual como colectiva).

Cremos que, em paralelo com acções destinadas a eliminar a pobreza, a aumentar os níveis de educação e de compreensão adequados à construção de um mundo composto por sociedades tolerantes quanto a religiões culturas e modos de vida, se deve procurar combater as ameaças (como o terrorismo) nas próximas décadas através de uma abordagem convergente e colaborativa, com recurso às TIC para construir infra-estruturas nacionais e internacionais que apoiem o tratamento de informação sensível, a educação da população e a gestão de conhecimento.

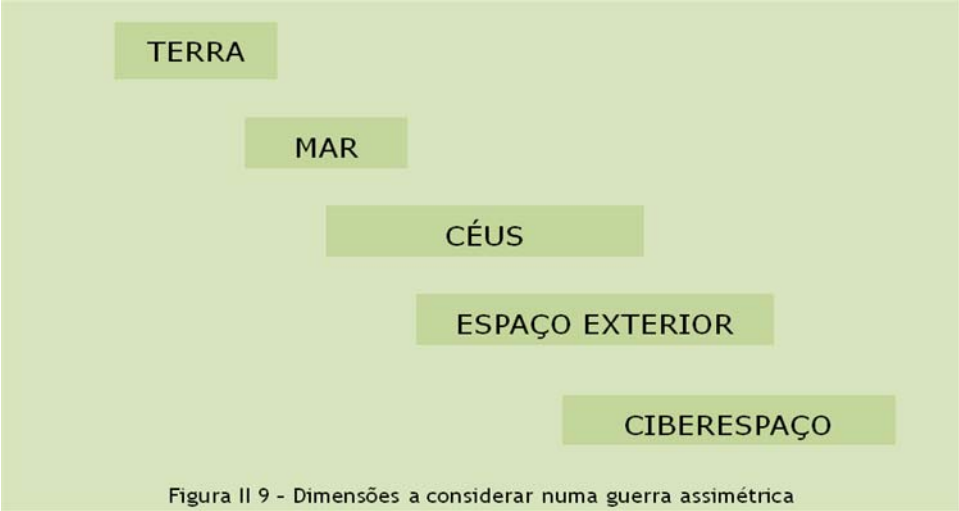

Figura II 9 - Dimensões a considerar numa guerra assimétrica

III. AS TIC NO MUNDO ACTUAL

A. IMPORTÂNCIA DA INFORMAÇÃO

É hoje consensual o reconhecimento da importância vital da informação para a vida dos Estados, das Organizações e dos Indivíduos. Esta percepção resulta da evidência clara de que a sua utilização, de forma eficaz e eficiente, potencia o aumento das capacidades de realização e postura competitiva, qualquer que seja o nível considerado, contribuindo, decisivamente, para o desfecho bem-sucedido de qualquer empreendimento a que as diferentes entidades se proponham. Este conceito está muito longe de ser novo.

Ao longo da história da humanidade e em todos os seus grandes empreendimentos, a disponibilização de informação relevante, rigorosa e atempadamente gerada, tem proporcionado um posicionamento determinante para o sucesso de empreendimentos políticos, militares, empresariais, ou de qualquer outra natureza, incluindo individuais. O advento da "Information Age", com a faculdade crescente de utilização de tecnologia para suportar a criação, partilha e utilização de informação de uma variedade de fontes, utilizando uma infra-estrutura de comunicações "omnipresente", pode ser percepcionado como uma mera evolução na jornada de desenvolvimento de cada vez mais capacidades ao longo do tempo. Ainda assim, uma evolução extraordinária!

Figura III 1 - Importância da Informação

Em 1967 Marshall McLuhan cunhou um termo que passou a ser utilizado como o paradigma desta revolução tecnológica e que, basicamente, se socorre de uma metáfora para afirmar que a tecnologia permitiria recrear o mundo à imagem de uma aldeia: a "aldeia global". Esta aldeia global é um produto das redes de comunicação estabelecidas entre computadores, possibilitando a partilha de hardware, software e informação. Entrando na rede, podemos efectuar uma reunião com pessoas geograficamente dispersas ou aceder a informação remotamente [Long20021].

Numa escala global, as redes de comunicação electrónica permitem efectuar reservas para viagens aéreas, informações sobre os impostos de um país serem processados noutro, pessoas em Antuérpia, Lisboa ou Sidney poderem negociar simultaneamente na Bolsa de Nova Iorque e noutros mercados bolsistas em todo o mundo. Esta tecnologia permite a coordenação na aquisição de produtos electrónicos Coreanos, aço Norte-americano e vidro Indonésio para produzir carros no Japão, e depois serem utilizadas para acompanhar e rastrear a venda desses carros em todo o mundo. Os jogos de sorte e azar deixaram de estar geograficamente confinados, ultrapassando barreiras fronteiriças (geográficas), jurídicas e culturais. A convergência das redes sem fios, possibilita a emergência de serviços com base na localização, como por exemplo, procurar nas redondezas um restaurante com a comida pretendida acedendo, simultaneamente, a avaliações de clientes anteriores [Long20021]. Está-se perante um tendência cada vez maior para a utilização de modelos de *Cloud Computing* - trata-se de um modelo de computação em que dados, ficheiros e aplicações residem em servidores físicos ou virtuais, acessíveis por meio de uma rede a partir de qualquer dispositivo e que podem ser partilhados (em vez de ter essas ferramentas localmente.

Figura III 2 - A "Aldeia Global"

As Tecnologias de Informação e Comunicação, cada vez mais, fazem parte integrante da colecção de recursos que se empregam, aos diversos níveis, nos mais variados ambientes, em processos de decisão ou

de criação de valor, alguns deles de elevada criticidade. Questões como a garantia da origem de determinada informação, se foi ilegitimamente alterada ou observada, ou se está disponível quando necessário, devem ser cuidadosamente acauteladas, de acordo com o valor da informação em causa, sob pena dos efeitos pretendidos poderem ser irremediavelmente comprometidos.

INFORMAÇÃO E TIC

De acordo com o Glossário da Sociedade da Informação publicado em 2007 pela APDSI [APDSI20074], a informação está enquadrada como "Dados e factos que foram organizados e comunicados de forma coerente e com significado… e a partir dos quais se podem tirar conclusões.". Esta definição de informação salienta a sua independência relativamente aos instrumentos utilizados para organizar e comunicar os dados e factos, e a sua conexão à satisfação de uma necessidade, materializada nas conclusões aludidas. Neste contexto, as tecnologias são remetidas para um papel instrumental, consideradas um recurso material que permite organizar a comunicação automatizada de "Dados e factos (...)".

Recorrendo à mesma fonte, as TIC constituem-se como a "Integração de métodos, processos de produção, hardware e software, com o objectivo de proporcionar a recolha, o processamento, a disseminação, a visualização e a utilização de informação, no interesse dos seus utilizadores.". Decorre desta abordagem, que as TIC, como outras áreas tecnológicas, possuem uma matriz teleológica, isto é, não se justificam a si mesmas, necessitam de um propósito externo que lhes proporcione o sentido para a sua realização.

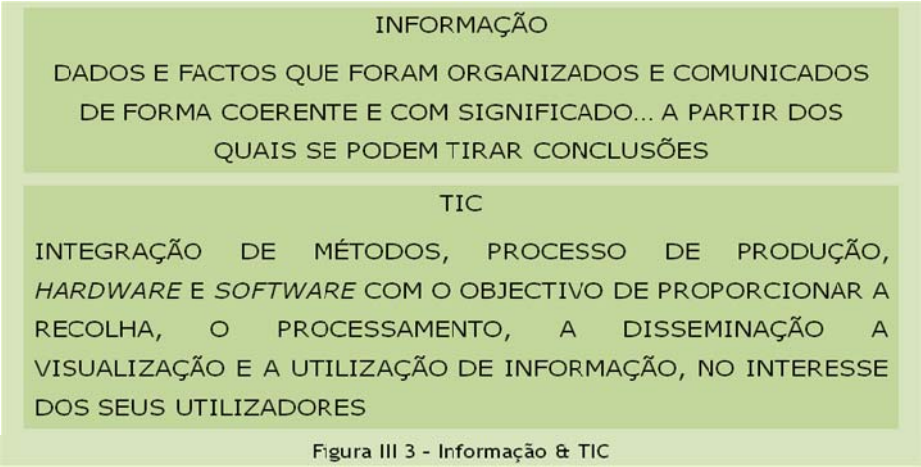

Figura III 3 - Informação & TIC

INFLUÊNCIA DAS TIC SOBRE A SOCIEDADE E DESTA SOBRE AS TIC

Quando se pretende avaliar o sentido da influência do binómio tecnologia / sociedade, é recorrente as análises desaguarem na metáfora do ovo e da galinha. De facto, é possível enumerar exemplos que evidenciam a defesa de qualquer das posições e, portanto, o mais sensato, será considerar que existe um padrão de influência mútua: por um lado, a tecnologia e as áreas do conhecimento que a suportam, constituem-se como motores de desenvolvimento das sociedades, influenciando e alterando a forma de pensar, de produzir riqueza, de nos relacionarmos, ou de nos entretermos e, por outro, a própria sociedade produz sinais relativamente aos caminhos apontados e percorridos pela tecnologia, incorporando ou rejeitando as novas propostas, encorajando ou censurando o ritmo das alterações tecnológicas.

A globalização constitui-se como um fenómeno sustentado no desenvolvimento tecnológico e com manifestações multi-dimensionais nos campos político, económico e social. O esboroamento das fronteiras geográficas e jurídicas, que permite o aumento exponencial dos fluxos mundiais de pessoas, de dinheiro, de bens e mercadorias, de ideias, de tecnologia, etc., arrastam, naturalmente, a necessidade de globalizar os fluxos de informação associados.

As TIC satisfazem esta necessidade disponibilizando, simultaneamente, a capacidade de fazer com que acontecimentos locais tenham efeitos globais, em tempo real, gerando fluxos de informação adicionais, numa dinâmica de causa e efeito à escala global. Assim, as TIC são simultaneamente um requisito e promotoras da globalização, comprimindo o tempo e o espaço, diminuindo o tempo eficaz de reacção a um determinado acontecimento, premiando, por isso, as entidades mais bem preparadas para lidar com esses fluxos de informação ciclópicos, em contextos pulverizados e menos previsíveis.

“Nos Estados Unidos, a rádio levou quarenta anos para atingir os cinquenta milhões de ouvintes. O mesmo número de pessoas usava o computador pessoal, apenas quinze anos depois da máquina ter sido inventada. Só foram precisos uns meros quatro anos, para haver cinquenta milhões de americanos que usam a Internet com regularidade” [Giddens19991]. O trecho citado ilustra a tendência de aceleração na massificação das tecnologias, que é hoje uma percepção muito forte à escala global, o que dificulta, por vezes, a sua própria compreensão. Nesta sequência, faz então algum sentido que se procurem salientar alguns aspectos mais perenes, que sustentam e viabilizam este ritmo de mudança e que providenciam uma matriz de referências mais resiliente ao tempo.

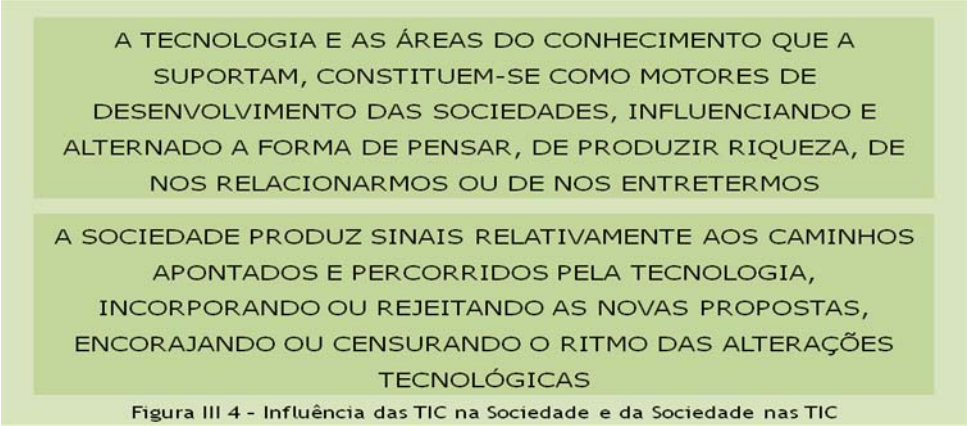

Figura III 4 - Influência das TIC na Sociedade e da Sociedade nas TIC

DA ABSTRACÇÃO À CONCRETIZAÇÃO DA INSEGURANÇA

Desde tempos imemoriais que o homem procurou explicações para fenómenos que observava na natureza, não só pela satisfação do deslumbramento (e pânico) que causavam, mas também para tirar partido desse entendimento, aproveitando para satisfazer necessidades próprias. Com a contínua acumulação de conhecimento e a complexificação das sociedades, tornou-se evidente a impossibilidade de concentrar esse conhecimento, originando, pelo contrário, uma necessidade de especialização cada vez maior[10]. Essa inevitabilidade está brilhantemente ilustrada numa alegoria sobre o conhecimento humano designada por "Powers of 10"[11], apresentada sob a forma de um pequeno filme. Mas como é que isto se relaciona com as TIC?

Como referido, a informação desempenha um papel crucial em todas as actividades humanas. Ora, as TIC providenciam o suporte para o processamento, armazenamento e transporte dessa informação, de acordo com as necessidades colocadas por um determinado domínio da actividade humana. As TIC requerem também uma especialização (na verdade, várias) e, ao mesmo tempo, é solicitada para dar resposta a diferentes tipos de interacções, em função do domínio da actividade em causa. Existe, portanto, uma necessidade real de resolver o problema de "esconder" a complexidade associada às tecnologias, da forma como elas são utilizadas. É como que se as TIC tivessem também que proporcionar as interfaces entre mundos que se regem por regras e princípios muito diferentes.

[10] A especialização origina depois custos ou dificuldades de integração, mas estas são questões e assuntos que escapam ao objecto deste trabalho.

[11] Um pequeno filme de 1997 elaborado por Charles e Ray Eames, que explora o tamanho relativo das coisas, desde a escala microscópica até à cósmica. O filme inicia a viagem com uma vista aérea de um homem num piquenique e, em saltos correspondentes à potência de 10, viaja até aos confins do universo, retornando depois para viajar em sentido contrário até ao mundo microscópico contido na mão do homem. O filme apresenta o universo como uma arena onde se manifesta, simultaneamente, a continuidade e a mudança. As formas como explicamos cada um dos níveis apresentados são, por vezes, muito diferentes, tornando impossível a sua compreensão cabal por uma única pessoa (mais informação http://powersof10.com/).

Esta faceta representa, precisamente, uma aplicação do princípio da abstracção, que preconiza a divisão de um determinado domínio complexo e vasto, em partes que se tornem compreensíveis e manejáveis, e em que cada uma delas possui os seus próprios objectos e regras de comportamento. Assim, as TIC têm que compreender os fenómenos físicos de forma a deles tirar partido para armazenar, processar e transportar informação e, ao mesmo tempo, estabelecer interfaces suficientemente simples e intuitivos de forma a não "perturbar" os diferentes domínios com a sua inerente complexidade. Sendo difícil quantificar a sua contribuição, este é um aspecto absolutamente decisivo para a espectacular penetração das TIC nos diferentes domínios da actividade humana.

Por exemplo, a pilha de protocolos TCP/IP estabelece um modelo com diversas camadas de abstracção, desde a interacção física até à interacção com uma aplicação activada por um utilizador. A implementação de diferentes camadas permite atribuir a cada uma delas a resolução de problemas muito específicos que, considerados em conjunto, seriam demasiado complexos para permitir, designadamente, a incrível escalabilidade que possibilitou a constituição da Internet, tal como a conhecemos hoje.

Ao nível do que dá corpo à entidade que conhecemos por computador, está cheio de níveis de abstracção que permitem que, em cada nível, um determinado problema seja resolvido sem que a forma como o foi seja exposto às restantes camadas. Tipicamente estas camadas são estruturadas numa hierarquia em que cada uma delas se relaciona com as adjacentes. Mesmo nas operações e / ou interacções mais simples, esta estruturação por camadas é activada, escondendo do utilizador uma complexidade da qual, tipicamente, ele não possui qualquer noção.

Esta noção de complexidade dos sistemas que suportam a manipulação da informação tem profundas implicações nas considerações sobre os riscos a que a informação está exposta e, de uma forma geral, no campo da segurança da informação. É comum dizer-se que a complexidade é inimiga da segurança, porque obscurece a compreensão das diversas interacções.

B. A SEGURANÇA DA INFORMAÇÃO E AS TIC

A segurança da informação foi, desde sempre, uma preocupação dos Estados, das Organizações e dos Indivíduos, manifestando-se a necessidade de assegurar que a informação necessária está disponível para os aliados e indisponível para os inimigos, concorrentes, ou oponentes. Muitas vezes, desta avaliação resultará um compromisso, porque os potenciais danos causados pela indisponibilidade da informação (por razões de confidencialidade) poderão ser piores do que a eventual disponibilização dessa informação aos oponentes.

A segurança da informação é uma área consideravelmente complexa que requer uma abordagem multi-dimensional. Engloba aspectos organizacionais e tecnológicos que, devidamente articulados poderão providenciar o nível de segurança da informação pretendido. Uma metáfora feliz que ilustra a necessidade de integração e complementaridade apresenta a segurança da informação como uma corrente, com o significado de que o nível global de segurança da informação está directamente relacionado com o nível do elo mais fraco dessa corrente.

ESTADOS DA INFORMAÇÃO

A informação pode estar em três estados diferentes: Em processamento; Armazenada e Em trânsito.

A satisfação das necessidades de segurança requer a adopção de procedimentos, mecanismos e tecnologias que providenciem a adequada protecção da informação, qualquer que seja o seu estado.

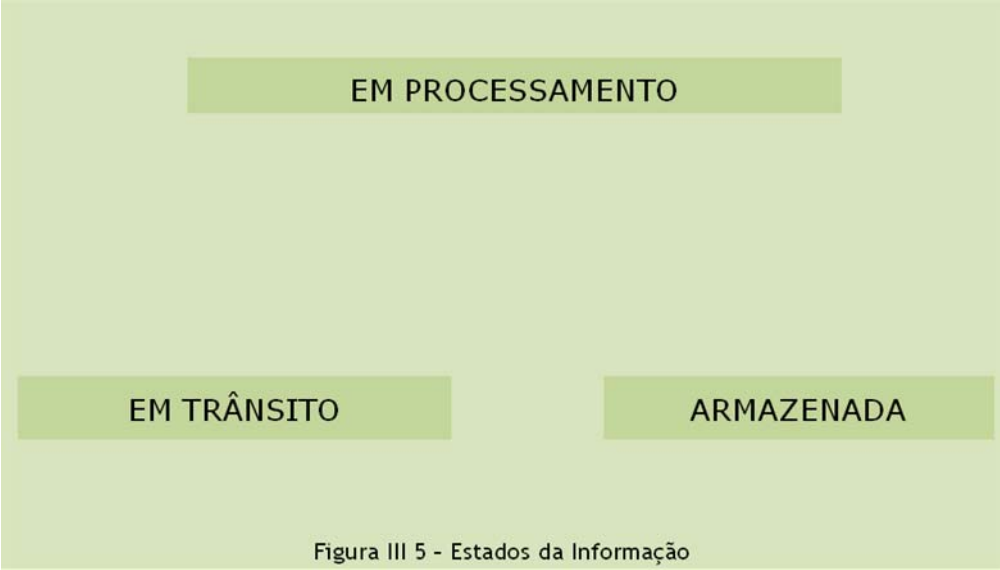

Figura III 5 - Estados da Informação

DOMÍNIOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação actua em três domínios fundamentais:

- O domínio lógico e de rede, que compreende o processamento, armazenamento e transferência de informação;
- O domínio social que está relacionado com a preocupação relativa ao conhecimento que é detido pelas pessoas e que poderá ser usado em benefício ou em prejuízo da organização;
- O domínio físico, que compreende a protecção física dos edifícios, salas de servidores, salas de terminais, controlo de acesso físico, etc.

Figura III 6 - Domínios da Segurança da Informação

DISCIPLINAS DA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

A segurança dos sistemas de informação engloba diversas disciplinas que se preocupam com aspectos específicos do universo da segurança da informação: a Segurança Física, a Segurança das Comunicações, a Segurança das Emanações[12] e a Segurança da Computação. Especificamente, sobre a COMPUSEC[13], sendo dirigida à informação armazenada e em processamento, preocupa-se com a confiabilidade do ambiente de armazenamento e processamento que pode ser influenciado pelo comportamento dos artefactos lógicos implementados, quer em *hardware*, quer em *software*. Sustenta-se na utilização de critérios de avaliação comuns que proporcionem o nível de confiabilidade pretendido. Como requisito, considera-se que para um sistema computacional proteger adequadamente a informação que processa e armazena, deverá possuir:

i) as funções de segurança adequadas; e

ii) implementadas com um nível de confiabilidade adequado.

É nesta disciplina que se enquadram os princípios preconizados pelo *Common Criteria*[14].

[12] Também conhecida por Segurança Electrónica

[13] *Computer Security*

[14] Designação anglo-saxónica livre para a norma internacional ISO/IEC 15048 na área da segurança informática. Descreve uma metodologia para especificar e implementar requisitos de segurança, e avaliar os produtos finais relativamente aos requisitos enunciados e implementação efectuada, de acordo com critérios normalizados e rigorosos.

Figura III 7 - Disciplinas da Segurança da Informação

OBJECTIVOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação enquadra-se no estabelecimento dos objectivos a atingir, tipicamente enquadrados nas seguintes áreas:

Confidencialidade Refere-se à protecção da informação contra a leitura não autorizada. Esta protecção implica o envolvimento cumulativo de duas características que podem ser enunciadas distintamente:

- por um lado, é necessária a definição de níveis de segurança, quer para os recursos (objectos ou processos), quer para as entidades (processos ou utilizadores) que pretendam aceder a esses recursos, para que possa ser permanentemente comparado e assegurado, que só acedem ao recurso em causa as entidades com um nível de segurança igual ou superior ao do recurso. Em ambientes multi-nível[15] isto implica a conjugação cumulativa de protecção contra o acesso para leitura a recursos classificados num nível superior (*no read up*), e de protecção contra o acesso para escrita a recursos classificados num domínio de segurança inferior (*no write down*);
- e, por outro lado, é necessário assegurar o acesso para leitura em função da necessidade de conhecer, agrupando a informação com características semelhantes (a definição dos termos em que o agrupamento da informação é efectuado depende do domínio em questão), e autorizando o acesso apenas às entidades que tenham o grupo de informação em questão definido no seu perfil, independentemente de terem ou não a credenciação necessária (é necessária a verificação cumulativa das duas condições).

Integridade Refere-se à protecção contra a alteração, não autorizada, intencional ou não, da informação. Em determinados cenários, designadamente no caso de informação em trânsito, é impossível assegurar que a informação não seja alterada. Nesta situação, o que se providencia são mecanismos que permitem às entidades legítimas detectar alterações não autorizadas, intencionais ou não, da informação.

[15] Um ambiente multi-nível caracteriza-se por processar, armazenar ou transmitir informação com diferentes níveis de classificação de segurança, pelo que o sistema terá que implementar mecanismos para assegurar a segregação dos diferentes domínios, assegurando que não há contaminações descendentes (fugas de informação), não autorizadas, entre os diversos domínios, o que proporcionaria uma violação da respectiva confidencialidade.

Disponibilidade Refere-se à protecção da informação que providencia a sua disponibilização em tempo útil às entidades legítimas. Relaciona-se com a tolerância à degradação do desempenho, é tipicamente caracterizada por taxas de disponibilidade e pressupõe a implementação de mecanismos contra a negação do serviço[16].

Figura III 8 - Objectivos da Segurança da Informação

Não sendo normalmente formulada como um objectivo a alcançar, as funções agregadas em torno da **Imputabilidade**[17] proporcionam funcionalidades que contribuem para que os objectivos de segurança da informação possam ser alcançados. Não se relaciona directamente com a informação, mas sim com as acções que se podem efectuar sobre a informação (por exemplo, criação, eliminação, recepção, escrita, modificação, etc.) ou sobre o sistema (*logon*, *logoff*, etc.), e com a possibilidade de rastrear e imputar essas acções às diversas entidades (processos ou utilizadores). Em sistemas com requisitos mais elevados, poderá implicar uma granularidade até ao nível do indivíduo.

A imputabilidade compreende diversas funções:

Identificação Refere-se à capacidade de identificar uma determinada entidade (utilizador ou processo).

Autenticação Refere-se à capacidade de uma entidade provar quem diz ser. Num contexto de acesso remoto a recursos informacionais, assume particular importância a garantia de que as partes em comunicação estão a comunicar com quem julgam estar, uma vez que, devido à própria natureza da comunicação, essa garantia terá que ser providenciada através de processos lógicos.

Autorização Na sequência, p.e., de um processo de *login*, depois de ultrapassada a fase de Identificação e Autenticação, refere-se ao processo de determinação dos privilégios dessa entidade, isto é, a que recursos que tem acesso e os respectivos privilégios (leitura, escrita, etc.).

Controlo de Acessos Diz respeito à forma como o acesso aos recursos do sistema são efectuados. Tipicamente são efectuados de duas maneiras:

[16] *Denial Of Service* – DOS

[17] Ou *Accountability*

- De forma discricionária, em que a própria entidade tem capacidade para determinar os privilégios de acesso aos recursos do sistema de que é "proprietário"[18];
- E de forma mandatória, em que a própria entidade não tem privilégios para determinar quem e de que forma se pode aceder aos recursos, ainda que tenham sido produzidos por si.

Autenticidade Refere-se à capacidade de provar a autoria de uma determinada informação, com aplicabilidade, p.e., na produção de informação.

Não-repúdio Refere-se à capacidade de retirar à entidade em causa a possibilidade de negar um determinado acto (p.e.: *login*, recepção de uma comunicação, leitura de um ficheiro, etc.).

Monitorização e registos (auditoria) Refere-se à capacidade para reproduzir, *a posteriori*, os acontecimentos no sistema relevantes para a segurança: quem é que teve acesso, quando, de que forma é que esse acesso foi efectuado, etc. A informação disponível nestes registos deverá também obedecer a requisitos de integridade, com um nível adequado aos requisitos da informação processada, armazenada ou transmitida.

Figura III 9 - Componentes da Imputabilidade

A imputabilidade é assim uma propriedade que providencia suporte aos objectivos enunciados para a segurança da informação, e consubstancia um modelo de requisitos que estabelece a capacidade para demonstrar a autoria de uma determinada acção, nas suas diversas variantes. Por exemplo: *login* ou parte numa comunicação (autenticação), recepção de uma informação ou impossibilidade de negar acções efectuadas (não-repúdio), ou produção de uma informação (autenticidade); a possibilidade de estabelecer factos, em tempo real ou depois da sua ocorrência (monitorização, registo e auditoria).

[18] *Owner*

C. A UTILIZAÇÃO DAS TIC NO MUNDO ACTUAL

Nos parágrafos anteriores procurou-se proporcionar uma perspectiva mais fundamental que sustenta a tecnologia e as consequências nos aspectos de segurança, o que incluiu uma elaboração sobre um modelo de segurança da informação.

Consideremos agora a forma como as TIC são utilizadas actualmente. Nesta vertente, um aspecto que ressalta imediatamente, é a presença destas tecnologias em praticamente todas as áreas de actividade, tirando partido das suas extraordinárias capacidades de armazenamento, processamento e transmissão da informação. Um outro aspecto a salientar será a transversalidade da sua utilização na globalidade do Mundo actual, com aplicações intensivas em todos os tipos de empresas, nas mais variadas áreas das Administrações Públicas e na generalidade das famílias.

Dados publicados em Dezembro de 2008, pela UMIC – Agência para a Sociedade do Conhecimento, relativamente à penetração das TIC em Portugal, num formato que se poderia designar por "As TIC em números", mostram designadamente que:

- 92%, 90% e 30% das pessoas (de 16 a 74 anos) com, respectivamente, educação superior, secundária, e de 9º ano ou inferior, utilizam computador.
- 91%, 87% e 26% das pessoas (de 16 a 74 anos) com, respectivamente, educação superior, secundária, e de 9º ano ou inferior, utilizam Internet.
- 97% e 98% dos estudantes usam, respectivamente, Internet e computador
- 39% dos agregados familiares dispõem de ligações em banda larga à Internet.
- A penetração do Serviço Telefónico Móvel na população é 137%.
- 96% das empresas têm computadores, valor que é 100% para as médias e as grandes empresas.
- 92% das empresas têm acesso à Internet, e 81% em banda larga
- Todos os Organismos da Administração Pública Central, Regional e Local dispõem de ligações à Internet,
- 92% dos Organismos da Administração Pública Central têm presença na Internet
- 99% das Câmaras Municipais tem presença na Internet.

A INTERNET

Pela sua importância no Mundo actual, pelo seu carácter global e pela forma como tem vindo a alterar os nossos padrões de vida em sociedade, a Internet merece uma referência especial neste capítulo, visto que

muitos dos problemas de segurança que se colocam actualmente, são originados, potenciados, veiculados ou mesmo resolvidos através da utilização da Internet.

A Internet**,** tal com a conhecemos, é um gigantesco conglomerado de redes de computadores, interligadas à escala mundial pelo Protocolo de Internet, que permite a transferência de dados e o acesso a todo tipo de informações e que é utilizada por cerca de 20% da população mundial.

O que constitui hoje a Internet, começou em 1969 como a ARPANET, uma rede criada pelo Departamento de Defesa dos Estados Unidos, para proteger os dados valiosos do governo, espalhando-os por várias localizações, ao invés de estarem centralizados num único servidor. De seguida, começou a ser utilizada pelas universidades, como um meio rápido de troca de informação entre os estudantes.

Contudo, a Internet como hoje a conhecemos, só se tornou possível pela contribuição do cientista Tim Berners-Lee e do CERN - Centro Europeu de Pesquisas Nucleares, que criaram a *World Wide Web* (WWW), inicialmente interligando universidades. Em Agosto de 1991, depois de criar o HTML e o HTTP, Berners-Lee publicou seu novo projecto para a *World Wide Web*, e apresentou as primeiras *páginas Web* no CERN, na Suíça. Em 1996 a palavra Internet já era de uso comum, principalmente nos países desenvolvidos, referida muitas vezes como *WWW*.

Uma das principais características da Internet são os serviços que disponibiliza e de entre os quais serão de salientar:

O correio electrónico (*e-mail*)	O envio de mensagens electrónicas (*e-mail*) de maneira análoga ao envio do correio tradicional é uma das utilizações mais populares da Internet. Mesmo hoje, com a vulgarização dos serviços de mensagens instantâneas, o *e-mail* continua a ser um importante meio de comunicação corporativa.
A *World Wide Web* (WWW)	Através de *páginas Web* organizadas em *sítios Web* e pesquisadas por *motores de busca*, milhões de utilizadores possuem acesso instantâneo a uma vasta gama de informação online. Com uma capacidade muito superior à das enciclopédias e das bibliotecas tradicionais, a Web permitiu a total descentralização da informação e dos dados e a criação de tecnologias como as páginas pessoais, os blogues e as redes sociais. A Web pode ser igualmente utilizada para o envio de correio electrónico (através de *webmail*), e para o trabalho colaborativo (como na *Wikipédia*).
O acesso remoto	A Internet permite que os utilizadores se liguem facilmente a outros computadores, a partir de qualquer localização remota, de forma segura, com autenticação e criptografia de dados, utilizando por exemplo uma Rede Virtual Privada[19] para esse propósito. Desta forma, o utilizador tem a possibilidade de acesso às suas aplicações, e-mails e outros dados independentemente do lugar em que se encontre.
O trabalho colaborativo	A grande facilidade de troca de informação e o baixo custo, tornaram o trabalho colaborativo muito mais fácil através da Internet. Os sistemas de controlo de versão gerem a colaboração entre as diversas pessoas, mantendo um histórico do trabalho e evitando que o esforço de um utilizador anule acidentalmente o esforço de outro. Os

[19] *Virtual Private Network* (*VPN*)

chats, as *redes sociais* e as *mensagens instantâneas* são tecnologias que também utilizam a Internet como meio de troca de informação e de colaboração. Outra aplicação de colaboração na Internet são os sistemas *wiki*, que utilizam a *Web* para realizar colaboração, fornecendo ferramentas como sistemas de controlo de versão e autenticação de utilizadores para a edição *online* de documentos.

Transmissão de áudio e vídeo

Vários canais de televisão na Internet oferecem transmissão de áudio e vídeo em tempo real. Outras tecnologias como o *podcast* permitem a disponibilização de ficheiros de áudio, de forma análoga à dos blogues. Com a popularização das *webcams*, é possível para qualquer pessoa tornar-se um fornecedor de conteúdos de áudio e vídeo pela Internet em tempo real. *A Voz sobre IP* é um protocolo de Internet para a comunicação por áudio bastante conveniente e fácil de ser utilizado. Essa tecnologia está a constituir-se como uma alternativa aos telefones convencionais.

Para além dos serviços, outras utilizações importantes da Internet situam-se nas áreas da educação, do lazer e do marketing.

Educação

O uso da Internet como uma nova forma de interacção no processo educativo, amplia a comunicação entre o aluno e o professor e o intercâmbio educacional e cultural. Desta forma, o acto de educar (com o auxílio da Internet) proporciona a quebra de barreiras e de fronteiras e remove o isolamento da sala de aula. Ao utilizar os computadores no processo de ensino, o mais importante, no entanto, será a forma como esses computadores vão ser utilizados em cada sala de aula no que diz respeito à originalidade, à criatividade e à inovação.

A utilização da Internet leva-nos a acreditar numa nova dimensão qualitativa para o ensino, através da qual se coloca o processo educativo voltado para a visão cooperativa e onde o uso das redes de computadores traz para a prática pedagógica um ambiente atractivo em que o aluno se torna capaz, através da auto-aprendizagem e da acção dos professores, de poder tirar proveito dessa tecnologia para a vida.

Lazer

A Internet tem-se tornado igualmente uma fonte de lazer com a criação de vários fóruns com sessões de jogos, vídeos e animações e uma grande área de *jogos multi-jogador*, criando comunidades de jogadores pelo mundo.

A indústria das *apostas* (em forma de jogos electrónicos) e a *pornografia* também tiram grande proveito da popularidade da Internet.

Marketing

A Internet, no entanto, tornou-se um grande mercado para empresas, que fazendo uso da natureza eficiente da publicidade com baixo custo, encontram na rede mundial, a forma mais rápida de difundirem em simultâneo, informação comercial para uma grande quantidade de pessoas. Com os recursos electrónicos oferecidos pela Internet, o *comércio electrónico* fica muito facilitado e as informações que um anunciante pode obter sobre o histórico de um cliente, permitem um marketing personalizado.

Ética na Internet

A facilidade de utilização da Internet e a possibilidade de acesso instantâneo a uma vasta gama de informação disponível, proveniente de pessoas com ideias e culturas muito diferentes, pode, no entanto, influenciar o desenvolvimento moral e social dos utilizadores. A utilização da rede beneficia em muito a *globalização*, mas também cria a interferência de informações entre culturas distintas, mudando a forma de pensar das pessoas e, dependendo da informação disponível, podendo mesmo acarretar uma mudança dos conceitos da sociedade.

Nem todas as informações disponíveis na Internet são verdadeiras, existindo sempre a possibilidade de utilizadores mal intencionados, ao abrigo da "*liberdade de expressão*", publicarem informações incorrectas, pouco rigorosas ou mesmo falsas, com as quais prejudicam a consistência e a credibilidade da rede.

Neste sentido, qualquer utilizador da Internet deve ter um mínimo de *ética*, e tentar,

sempre que possível, colaborar para o desenvolvimento da mesma publicando informações credíveis ou melhorando a qualidade das informações já existentes, preservando assim a integridade do conjunto.

Segurança da Internet

A utilização generalizada da Internet, contudo, e tal como se afirmou anteriormente, coloca inúmeros problemas de segurança, muitas vezes associados a práticas criminosas, problemas esses que são originados, potenciados ou veiculados pela própria Internet. Outras vezes, porém, é a Internet que fornece os meios e as práticas necessárias para a resolução de muitas questões de segurança.

Uma das práticas criminosas mais divulgada através da Internet está associada à pedofilia, envolvendo a prostituição e a divulgação de fotos pornográficas de menores. Outros dos crimes mais usuais na rede, está associado ao sistema bancário e financeiro através do envio de e-mails com pedidos de actualização dos dados bancários e de *palavras-chave* (*phishing*). Da mesma forma, e-mails referentes a listas negras ou à atribuição de falsos prémios são igualmente práticas comuns.

A abertura de ficheiros enviados como anexos deve ser sempre rodeada de alguns cuidados dado que alguns desses ficheiros com extensões do tipo ".exe", ou ".scr", poderão servir de porta de entrada para vírus de computadores, os quais poderão causar danos ou roubar informação (*spywares*). No entanto, é generalizado o consenso de que os chamados "*cookies*" são inofensivos, uma vez que o seu objectivo é obter informação estatística sobre a utilização dos sítios.

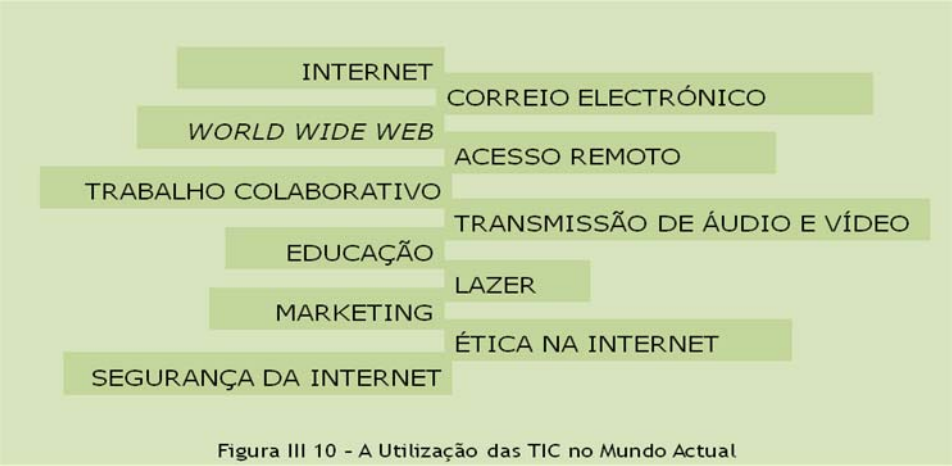

Figura III 10 - A Utilização das TIC no Mundo Actual

IV. AS TIC PARA UM MUNDO MAIS SEGURO

A. AS TECNOLOGIAS EMERGENTES

OPORTUNIDADES E RISCOS GLOBAIS

Num contexto de ameaças assimétricas, as ameaças que estão mais directamente associadas às tecnologias emergentes são aquelas que exigem uma maior atenção nos próximos decénios.

Não custa prever que essas tecnologias vão ter um papel crucial num contexto de globalização.

Os grandes desafios globais do século XXI dependem muito da abordagem que a humanidade vier a adoptar na sua forma de pensar e de agir. As inter-relações e inter-dependências de sistemas - sociais, económicos e outros – cruzar-se-ão com evoluções das tecnologias, criando novos desafios que terão que ser devidamente geridos sob pena de se verificarem desequilíbrios na dinâmica global.

Por exemplo, o domínio da Robótica – e atendendo aos avanços significativos no domínio da Inteligência Artificial – coloca-nos preocupações especiais. Ainda que não seja de todo claro, nos dias de hoje, se um robot poderá alguma vez ter a capacidade de amar, de perdoar, de ser tolerante - qualidades que estão intrinsecamente associadas ao ser humano. Os peritos em Inteligência Artificial dizem-nos que não se pode excluir quaisquer possibilidades, devendo os políticos estarem preparados para estes tipos de questões filosóficas que estão a emergir e que necessitarão, obviamente de ser objecto (com a antecipação possível) de políticas adequadas.

Por exemplo, outra tecnologia que está a ter uma expansão muito rápida é o RFID (*Radio-Frequency Identification*) que tem por objectivo a identificação automática através de sinais de rádio, acedendo e armazenando dados remotamente através de dispositivos denominados de tags RFID que podem ser colocados em bens, animais e pessoas. Dada a capacidade de utilização desta tecnologia nos mais variados domínios existem questões que têm de ser resolvidos tais como - este tipo de dispositivos podem ser “invisível” para os indivíduos, e intrusivos a médio prazo, uma vez que podem recolher e processar dados de qualquer parte e a qualquer momento.

A definição de **tecnologias emergentes** muda com o tempo. Novas tecnologias estão constantemente a emergir, quase sempre com implicações para o ser humano.

Para além da robótica e o RFID temos que ter em conta outras tecnologias, nomeadamente: a genética; a Nano tecnologia; a Inteligência Artificial; as Tecnologias de Informação e de Comunicação (dos quais se destacam nos tempos mais próximos: Autenticação Electrónica, Identidade Digital e Videovigilância).

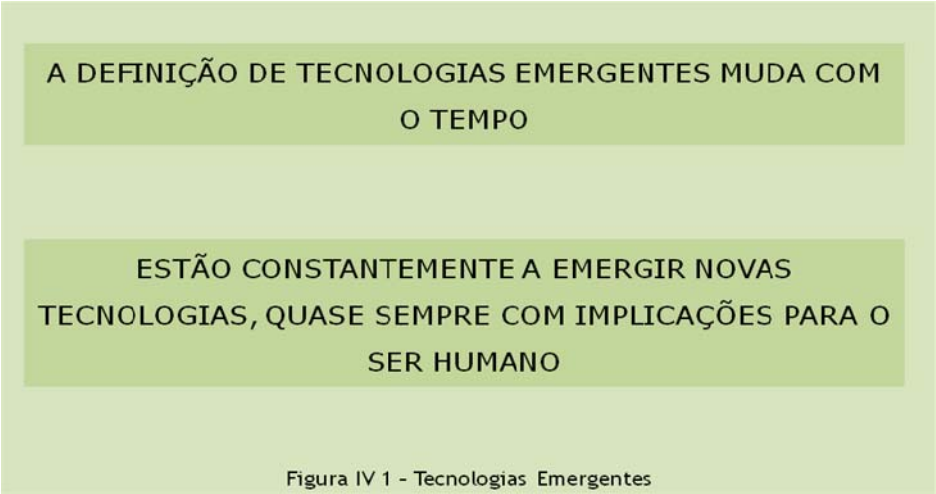

Figura IV 1 - Tecnologias Emergentes

Dependemos cada vez mais de dispositivos tecnológicos como o telefone móvel e o PDA. Se eles param de trabalhar, ainda que seja por algumas horas, temos que alterar a dinâmica do nosso pensamento e a nossa capacidade de acção e reacção. Isto corresponde claramente a uma vulnerabilidade na sociedade que estamos a construir, e que depende da vulnerabilidade dos dispositivos de TIC em causa.

Muitas das questões associadas ao uso das tecnologias justificam o desenvolvimento de uma sensibilidade especialmente orientada para a análise colectiva, a qual idealmente adicionará uma dimensão ética ao processo criativo de invenção e inovação.

O esforço de integração naturalmente associado à globalização em diversos domínios – tecnológico, económico, social, político – minimizou ou anulou barreiras comerciais e, ao mesmo tempo, fomentou a intensificação de fluxos de capitais e de produtos e soluções financeiras altamente elaboradas e com fraca sustentação.

Queiramos ou não, os políticos são agentes fundamentais de desenvolvimento ou de bloqueio das sociedades modernas. A sua própria actuação pública tem normalmente influência na forma como os cidadãos vêem as tecnologias e o seu uso para o bem comum.

Praticamente todos os políticos no mundo inteiro entendem como funciona a televisão e sabem como a usar para nos manipular. Eles sabem como usar um sorriso na televisão, como desobedecer na televisão, como manipular as nossas emoções na televisão. Ainda não se passa o mesmo com a Internet e com o ciberespaço – eles ainda não os entenderam.

De facto está a acontecer uma revolução, a qual está a mudar a forma como o panorama político é definido pelos líderes e partidos políticos actuais e ao mesmo tempo pelos líderes do futuro. A introdução de uma nova tecnologia na sociedade pode ter um impacto profundo na sua estrutura e no seu desenvolvimento.

Não são só as tecnologias que referimos atrás (TIC, RFID, Robótica, Inteligência artificial, Nano tecnologia e outras) que têm esse poder. Outras tecnologias também têm grande poder de influência, como por exemplo, a genética.

É claro que no âmbito deste trabalho queremos focar especialmente as Tecnologias de Informação e da Comunicação.

DILEMAS DA SOCIEDADE ACTUAL

A introdução de novas tecnologias é sempre acompanhada de novos desafios e oportunidades para os indivíduos e para as sociedades, colocando-os perante dilemas de natureza diversa e por vezes de difícil equilíbrio. Eis alguns deles:

GARANTIA DE LIBERDADES INDIVIDUAIS	⟷	NECESSIDADE DE VIGILÂNCIA DO INDIVÍDUO
ACESSIBILIDADE À INTERNET PARA FINS COMERCIAIS	⟷	VULNERABILIDADES
USO DE TECNOLOGIA PELOS GOVERNOS E ENTIDADES PÚBLICAS	⟷	AMEAÇAS DE CIBERTERRORISMO
DISSEMINAÇÃO DE BENS NORMAIS	⟷	DISSEMINAÇÃO DE BENS DANOSOS
DISSEMINAÇÃO DE MENSAGENS PACÍFICAS E ÉTICAS	⟷	DISSEMINAÇÃO DE MENSAGENS RADICAIS E OFENSIVAS
LIBERDADE DE EXPRESSÃO	⟷	CENSURA DE ESTADO
RÁPIDA DISSEMINAÇÃO DE INFORMAÇÃO	⟷	LONGO TEMPO DE RESPOSTA POR PARTE DOS DECISORES POLÍTICOS
TECNOLOGIA PARA COMBATER O TERRORISMO	⟷	TECNOLOGIA PARA APOIAR ACTIVIDADES TERRORISTAS

Figura IV 2 - Dilemas da Sociedade Actual

Considerando as características da Sociedade da Informação, conclui-se facilmente que todos estes dilemas se colocam também relativamente a qualquer ambiente que recorra às TIC ou em que elas próprias constituem o núcleo.

B. AS TIC E A SEGURANÇA GLOBAL

A abordagem ao tema Segurança Global incide sobre a interconectividade e a intersecção de cinco planos: económico, sociocultural, político, ambiental e militar:

No plano Político Devido à grande influência que tem o sector político na globalização, e consequentemente noutros sectores abordados neste texto, são de enorme importância os desafios de políticas, acontecimentos, acções e reacções que ocorrem neste domínio.

No plano Económico A Globalização está fortemente associada à Economia.
As primeiras indicações de uma interconectividade global podem ser encontradas na história do comércio entre nações. Com a expansão das dependências do comércio, as fronteiras políticas tradicionais do passado pareceram derreter-se e foram substituídas por novas fronteiras e por economias mais fortes.

No plano Sociocultural Os aspectos sociais e culturais fazem parte natural dos discursos sobre a globalização. O desenvolvimento social num quadro de globalização tem sido profundamente influenciado pelos avanços tecnológicos ao longo dos anos.
Numa era caracterizada por constantes trocas de informação e de notícias, a forma como as culturas evoluem em relação ao resto do mundo mudou dramaticamente desde o fim da segunda Guerra Mundial.
A introdução da televisão, do telefone e da Internet trouxe novos meios de comunicação e as mudanças sociais influenciaram a interacção entre as pessoas num âmbito internacional. A era da comunicação instantânea mudou intensamente a forma como nós vemos o nosso mundo e o nosso lugar nele.
Tudo isso alterou para sempre a forma como interagimos.

No plano da Segurança Este plano é afectado por todos os outros, recebendo impactos das decisões que são tomadas em cada uma delas. Mas simultaneamente influencia o âmago de cada uma das outras dimensões. Não há dúvida de que a segurança de uma nação, de um povo, de uma região é condicionada por decisões políticas, económicas, militares e também de política social.
Na história da globalização, vários factores e contextos contribuíram para a evolução de conceitos relacionados com Segurança. São exemplos: as duas guerras mundiais, a guerra da Coreia, o conflito do Vietname, o desenvolvimento de armas nucleares.
Os desenvolvimentos que tiveram lugar ao longo do tempo contribuíram para medidas destinadas a assegurar maior estabilidade no quadro mundial, mas contribuíram ao mesmo tempo para a instabilidade global, facilitando e potenciando reacções transnacionais.
Em paralelo foram constituídos modelos e processos destinados a conseguir a estabilização do sistema internacional, suportados e geridos por organizações especificamente criadas para o efeito: a Organização das Nações Unidas, o Fundo Monetário Internacional, o Banco Mundial, a União Europeia, a OCDE, a ENISA e outras.

No plano Militar Os avanços tecnológicos (sobretudo os dos últimos 50 anos) modernizaram a forma de "fazer guerra", relativamente ao que acontecia há centenas de anos atrás.
É de salientar o desenvolvimento da aviação, o qual tornou o mundo incrivelmente pequeno. Grandes distâncias são agora percorridas em poucas horas em vez de meses. Obviamente que tudo isso contribui para enormes mudanças no domínio militar. A I Guerra Mundial, tornou vital o controlo do ar. Em paralelo, a introdução de tanques de guerra durante esse conflito ajudou à criação de um exército moderno. Segundo os especialistas, o segundo grande ponto de viragem correspondeu à aplicação da propulsão a jacto.
Para além de todas essas evoluções tecnológicas, de processos e de métodos, o desenvolvimento da bomba de hidrogénio e o nascimento da era nuclear nos anos 40, corresponderam a avanços militares significativos.

Figura IV 3 - Planos a considerar quanto à Segurança Global

C. CONSEGUIR A SEGURANÇA DA INFORMAÇÃO

A segurança consegue-se com a adopção de medidas de diversos tipos, as quais devem incluir sem dúvida nenhuma regras e atitudes de operação.

No que se refere aos sistemas de informação, e depois de se definir o que se quer segurar ou proteger e depois de se avaliar o respectivo valor, precisamos montar defesas que sejam adequadas, nomeadamente: antivírus, modems seguros, anteparas (*firewalls)*; servidores de segurança; cifração de ficheiros e comunicação; senhas descartáveis; comunicação criptográfica.

Ao avaliarmos a importância da informação que circula ou que está hospedada numa rede, temos que cuidar da: privacidade da informação individual; confidencialidade e integridade da informação classificada; autenticidade, confidencialidade e integridade da comunicação classificada, entre

governantes ou governos; etc. A segurança da informação tem várias componentes e atributos que devem ser considerados quando se analisam os riscos potenciais.

Como já vimos na secção anterior, englobam-se em três categorias: Disponibilidade; Confidencialidade e Integridade.

Disponibilidade No comércio electrónico, é crítica a disponibilidade da informação, dos recursos do sistema aplicacional e da largura de banda.

Quando um prestador de serviços disponibiliza normalmente serviços de colocação de encomendas, ou de transferências electrónicas de fundos sobre uma rede, os seus clientes esperam ter acessos e respostas rápidas. A resposta adequada a essa expectativa dos clientes é sem dúvida uma vantagem competitiva: uma empresa pode operar 24 horas por dia, fornecer serviços e informação aos seus clientes de acordos com a sua conveniência. De facto, a conveniência torna-se uma comodidade.

Quando se tomam em consideração ameaças criminosas aos sistemas de informação, verifica-se que os chamados ataques de "negação de serviço" são simples de levar a efeito por terceiros. Através da inundação de um sistema com perguntas ou com correio electrónico falso, as aplicações podem entrar em sobrecarga e não conseguirem responder a pedidos de serviços legítimos.

Confidencialidade Este é o atributo mais familiar relativo à informação, e é o melhor compreendido pelas pessoas.

De um modo geral, a maior parte das empresas não necessita de gerir informação com o mesmo grau de exigência do que é esperável de um serviço público. De facto, a maior parte da informação com que uma empresa trabalha diariamente terá pouco valor e requer pouca protecção. Contudo, cada empresa possui informação cuja divulgação inadequada poderá ter impacto significativo: no preço das suas acções; nas suas receitas; na redução das suas vantagens competitivas; etc.

É fundamental para uma empresa que ela seja capaz de identificar os tipos de informação que são críticas para a sua operação, e que compreenda as ameaças potenciais e que implemente salvaguardas apropriadas.

Integridade O rigor e a fiabilidade da informação, dos sistemas e redes, são elementos críticos para muitas aplicações de negócio.

Os modernos modelos de comércio electrónico são baseados na confiança entre uma empresa (ainda que seja uma "empresa virtual"), os seus clientes, os seus vendedores e fornecedores, e aplicam códigos e práticas de negócio estabelecidos. Num ambiente electrónico, em rede, ambas as partes – negócio e cliente – devem confiar na infra-estrutura que suporta o intercâmbio electrónico da informação e dos serviços. Infelizmente as redes de hoje não foram desenhadas com estes níveis de confiança em mente.

Na avaliação dos riscos da operação, temos que pesar o binómio "vulnerabilidades / ameaças" e ter consciência de que: a ligação ao exterior introduz ameaças; o *software* comercial tem vulnerabilidades; um sistema falha pelo elo mais fraco. Ao mesmo tempo há que reconhecer-se que nada é 100% seguro e que o custo de um ataque é normalmente comensurável com o valor da informação ameaçada, devendo o risco aceitável ser comensurável com o valor da informação protegida.

Existem muitos tipos de ameaças que os sistemas de informação enfrentam: acidentes; erros de *software*; falhas de *hardware*; etc.

Na realidade, influências ambientais, tais como o fogo podem afectar seriamente uma operação de negócio. Cada uma dessas ameaças requer planeamento e controlo apropriado.

Também pairam sobre um largo espectro de actividades Ameaças maliciosas, desde o roubo e furto físico, até à destruição de propriedade.

Obviamente que as ameaças electrónicas maliciosas e deliberadas e, em particular, ameaças criminosas para fins fraudulentos, não são as únicas que devemos ter em conta. O perpetrador dessas ameaças criminosas pode ser uma pessoa interna ou externa à organização.

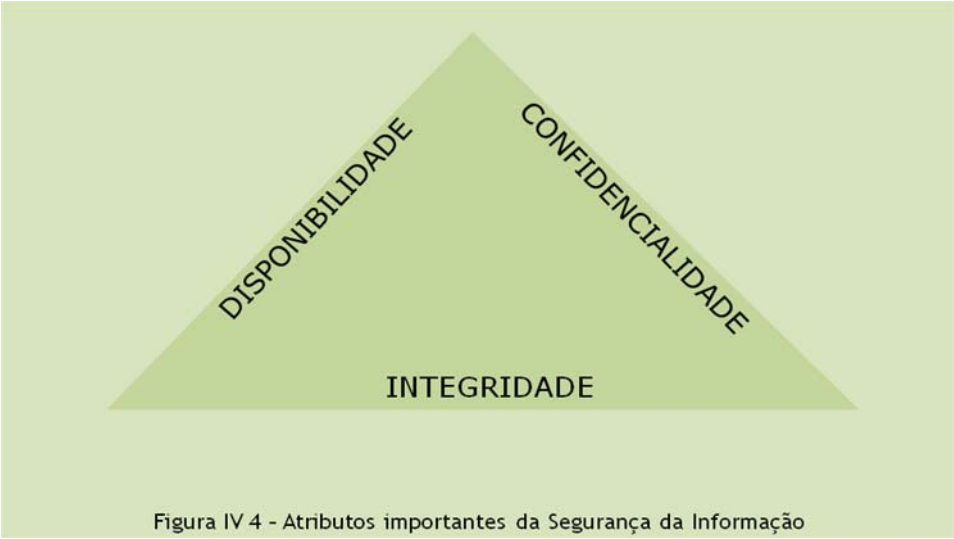

Figura IV 4 - Atributos importantes da Segurança da Informação

As ameaças a qualquer um destes atributos podem levar à disrupção da actividade de uma empresa. A importância de cada actor no conjunto das operações de uma empresa varia de indústria para indústria e de empresa para empresa.

A maior parte das empresas estão preparadas para tolerar pequenas disrupções na disponibilidade da sua informação. Igualmente, muitas empresas têm grandes quantidades de informação cuja divulgação pública terá pouco ou nenhum impacto na segurança.

Devido a essas variações, é importante que cada empresa avalie os seus requisitos particulares e faça os seus planos de acordo com isso. O primeiro passo é identificar os riscos potenciais e quais as protecções que devem ser implementadas para mitigar e controlar os riscos.

As acções podem ser concretizadas:

- Individualmente;
- Por um grupo com fracas ligações entre si;
- Por elementos criminosos organizados;
- Por empresas;
- Por estados.

Qualquer ataque contra a infra-estrutura crítica de uma actividade pode causar uma disrupção severa e pode resultar em perdas de fundos, de produtividade, de fatia de mercado, ou de reputação.

A actividade criminosa contra os sistemas de informação está a aumentar. Podemos classificar a actividade criminosa contra sistemas de informação da seguinte maneira:

Intrusão de baixo nível

Este grupo constitui um subgrupo do estereótipo *hacker*. Esses indivíduos podem evoluir do trespasse e vandalismo em linha para actividades eminentemente criminosas, tais como furto de informação, extorsão, e fraude de cartões de crédito.

Fraude para lucro

A actividade em linha deste grupo é muito variável e pode incluir *scams*, extorsão, publicidade enganosa, furto, transferência ilegal de fundos, etc. Em muitos casos os sistemas de informação são usados como uma ferramenta e não como o alvo.

Crime organizado

Não custa a crer que cada vez mais os agentes do crime organizado necessitam de compreender e de dominar o uso dos sistemas de informação para conseguirem manter o seu tradicional nível de influência e receitas.
A motivação para o crime organizado que está envolvido em alta tecnologia de TIC ultrapassa a simples fraude e extorsão, e pode incluir vigilância de forças e agentes policiais e de segurança, lavagem de dinheiro, e comunicação segura e anónima.

Um aspecto relativamente novo da actividade deste tipo de grupo é o recurso a grupos criminosos organizados da Europa de Leste e da Rússia. A situação económica de muitas organizações daquelas regiões tem facilitado o fornecimento de uma *pool* rica em recursos, os quais vão sendo explorados para diferentes tipos de actividades criminosas.

A engenharia de *hardware*, *software* e de dispositivos de controlo de acesso, assim como outros métodos e meios de alta tecnologia que podem provocar disrupção de sistemas de informação constituem áreas de preocupação.

Outra área de preocupação para muitas organizações é o aumento do uso de sistemas de informação por parte de cartéis de droga organizados.

Grupos extremistas: políticos, religiosos e outros

Ainda que estes grupos raramente tenham motivações que os levem a realizar acções fraudulentas, tem havido um aumento no uso de sistemas de informação por parte de alguns deles para perseguirem os seus fins. A maior parte desses ataques envolve furtos de informação e ataques de negação de serviço.

Espionagem industrial e sabotagem

Com a ideia de protegerem a sua reputação, só ocasionalmente reportam oficialmente casos deste tipo, razão pela qual existe um conhecimento reduzido sobre os modos de operação dos atacantes.

Espionagem internacional e Guerra de informação

As acções de espionagem, que incidem muitas vezes em empresas, preocupam as entidades públicas.
Vieram à luz do dia diversos casos em que organizações de segurança nacional de um determinado país recolheram informação económica sensível, a qual foi usada para apoiar empresas desse mesmo país em situações de concorrência. Alguns dos métodos aplicados na recolha desta informação englobaram tentativas de acesso a sistemas de informação e de comunicações.

Configurando outro tipo de acções, a imprensa de alguns países referiram haver sinais de que os seus governos e entidades públicas estarão a avaliar o potencial do uso ofensivo de sistemas de TIC para provocar disrupções nas infra-estruturas de informação de outros países. Exemplo dessa situação é o incidente do ciberataque que ocorreu em 2007 na Estónia e provocou o colapso de toda a infra-estrutura Internet. Este incidente não é isolado. Este tipo de incidentes tem vindo a acontecer em particular quando ocorrem conflitos regionais.

Terrorismo

Existem sinais de que organizações terroristas encaram cada vez mais as TIC e os sistemas de informação simultaneamente como sendo um meio e um alvo. Um dos alvos que requer atenção são as infra-estruturas críticas.

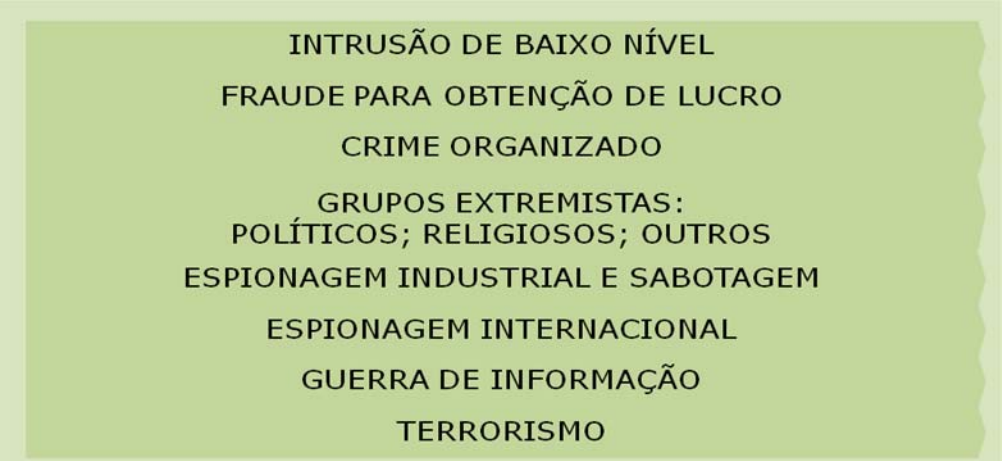

Figura IV 5 - Actividades criminosas contra os Sistemas de Informação

D. ARMADILHAS DA SOCIEDADE DE INFORMAÇÃO

O **ciberespaço** [20] é uma sociedade complexa para a qual nos faltam ainda metáforas da vida comum que guiem o nosso comportamento quando a utilizamos [Veríssimo 2002].

A **Net** tem uma envolvente tecnológica que faz muitas coisas acontecerem muitas vezes, muito rapidamente, de muito longe, a muitos participantes... e isto afecta utilizadores legítimos e ilegítimos. Por tudo isso é preciso que sejamos capazes de perseguir uma ética e uma moral relativamente à "coisa informática".

Se perguntarmos a um pirata informático se é lícito alguém invadir a casa dele só porque a porta está entreaberta, ou a chave ficou esquecida na fechadura, ele logo dirá que não! No entanto é exactamente isso que ele faz amiúde nos equipamentos e nas redes.

Mas o risco não vem só do exterior…

Se perguntarmos à maior parte das pessoas se têm algo de verdadeiramente valioso no seu computador, muitas dirão que não! Mas quantas vezes está lá esquecida e/ou não classificada informação que é sensível e/ou privada?

Importa ter-se consciência de que o individual pode por em risco o colectivo. Na realidade, se uma pessoa opera o seu computador de modo a possibilitar o risco dele ser invadido ou penetrado por um pirata, ele

[20] Muitas vezes referido de forma simplista por *The Net*.

pode estar a abrir a porta a uma penetração geral no sistema ou na rede de que faz parte. Com isto queremos dizer que se requer do utilizador:

- Formação e ética comportamental

  Adquirindo conhecimentos mínimos do sistema e de segurança individual, assim como atitude ética em relação à informação a que tem acesso.

- Cuidados e disciplina

  Seguindo de um modo geral as instruções da administração, assegurando a não transmissão a outros dos meios de autenticação e protegendo a informação individual na sua transmissão (através de autenticação e de cifra).

A nossa sociedade é tão vulnerável quanto é preciosa, tendo o mundo de hoje poucas semelhanças com o mundo de há alguns anos atrás.

Os ataques terroristas ao WTC, em Bali, em Madrid, em Londres demonstraram as vulnerabilidades na nossa sociedade e a determinação de grupos sem escrúpulos para explorar essas fraquezas.

Estas situações novas têm obrigado as organizações a repensar a forma como são salvaguardados as pessoas, as propriedades, os activos e os serviços essenciais.

Hoje requer-se uma segurança credível e efectiva em muitas e variadas áreas: nos transportes, nas finanças, na indústria, no desporto, no lazer, independentemente da sua localização.

A actuação em parceria, com objectivos envolvendo o sector público e privado é crítica para se gerar compreensão sobre os problemas e ameaças que enfrentamos e assim podermos enfrentá-los e combater.

As soluções não devem impor constrangimentos irrealistas na actividade quotidiana normal.

A segurança deve ser realista e deve procurar ser suportável.

Todos os cidadãos precisam de entender que a criação de um “mundo seguro” significa que devemos ser capazes de salvaguardar vidas, proteger estruturas e indústrias críticas e providenciar um ambiente seguro para a actividade diária normal.

Conseguir estes objectivos transcende os governos e exige novas parcerias funcionais, no sentido de promoverem uma compreensão extensa e assim dominarem os desafios da segurança.

USO DAS TIC PELO TERRORISMO

Foram confiscados no Afeganistão alguns computadores da *Al-Qaeda* que continham modelos de barragens e programas informáticos que podiam ter sido usados em ataques contra essas infra-estruturas.

Obviamente que as pessoas encarregues de fazer cumprir a lei estão condicionadas pela livre acessibilidade, versatilidade, velocidade, e carácter transnacional do ciberespaço, o qual permite uma impunidade quase total. A possibilidade de ataques terroristas com meios informáticos contra infra-estruturas críticas ou redes de informação é real.

Ainda que isso possa não ser fácil de concretizar, a possibilidade é intensamente debatida por especialistas pois ninguém pode ignorar o risco de que grupos de terroristas venham a usar TIC não somente como uma arma mas também como um alvo. Por exemplo, lançando ciberataques contra sistemas de supervisão e controlo de redes que controlam infra-estruturas sensíveis (sistemas de controlo de tráfego aéreo, fornecimento de energia eléctrica, barragens, instalações industriais, sistemas de comunicação, serviços financeiros, etc.) ou computadores contendo dados críticos.

Julgamos que actualmente essa possibilidade situa-se mais no plano do indivíduo (ainda que integrado em organizações) "*hackers e crackers*" actuando por motivos pessoais, económicos, ideológicos, ou criminosos. É claro que a actividade desses indivíduos é um produto antinatural da sociedade das TIC, e corresponde a um fenómeno preocupante e que está a aumentar.

À medida que as redes terroristas adquirem as competências necessárias, a opção por ciberataques poderá corresponder a uma escolha estratégica. Ocorreram já incidentes através das TIC, cujo alvo eram as infra-estruturas críticas, numa tentativa de atingir os seus objectivos: fatalidades em massa e/ou disrupção da economia, politica, e vida social no país alvo, quer seja independentemente ou conjugado com um ataque físico, seguido de uma grande divulgação pelos media.

EXPLORAÇÃO DE OPORTUNIDADES CRIADAS PELAS TIC

Os grupos de terroristas internacionais e de criminosos usam TIC avançadas, nomeadamente capacidades de encriptação e de "anonimato" em computadores, e contratam piratas informáticos, os quais conduzem as suas operações transnacionais sem temor de detecção.

Sabe-se que os grupos terroristas conduzem frequentemente as suas actividades criminosas pelos seus próprios meios, fazendo lavagem de dinheiro, tráfico de drogas ou de seres humanos, fraudes com cartões de crédito, venda de produtos contrafeitos, com o fim de financiarem as suas organizações.

Tal como acontece nas empresas multinacionais, os grupos terroristas capitalizam sobre as vantagens das sociedades ocidentais, explorando lacunas legislativas, fraco enquadramento legal e policial, corrupção, trabalho barato, desemprego. Eles usam a Internet para produzir documentos de identidade forjados para eles próprios, para os seus operacionais ou para as pessoas que enviam para os países ocidentais.

Os governos precisam de rever e incrementar os obstáculos legais e técnicos colocados no caminho dessas actividades em ordem, no sentido de tornar o quadro legal mais efectivo. São exemplos:

As TIC podem ser usadas pelos governos como um instrumento de contra-terrorismo e de inteligência	Em 2003 os EUA identificaram várias áreas em que o uso de TIC era crítico para a luta contra o terrorismo: prevenção, detecção, e mitigação de ataques terroristas. Numa outra frente, as TIC podem ser de uma ajuda valiosa para combater o apoio ideológico ao terrorismo.
As TIC podem ajudar na prevenção contra ataques terroristas	Antes de qualquer ataque terrorista, os serviços de inteligência apoiam-se fortemente na vigilância de comunicações electrónicas e na Internet para identificar padrões de comportamento de entre grupos ou indivíduos suspeitos. Essas técnicas foram desenvolvidas para modelação da evolução de grupos sociais nos espaços de *chat* na *Web*, *newsgroups*, e *bulletin boards*, com o objectivo específico de detecção de grupos potencialmente danosos. O progresso verificado na fusão de informação, i.e. a agregação de dados de várias origens, combinados com motores de pesquisa potentes, pode facilitar que especialistas bem equipados e bem treinados possam descobrir planos terroristas.
As TIC podem ajudar os serviços de informação a detectar ataques terroristas eminentes	A recolha e análise rápida de inteligência através de meios electrónicos podem ser críticos na detecção de ataques terroristas planeados. O falhanço da comunidade de *inteligência* dos EUA em interpretar os sinais que recebeu antes dos ataques do 11 de Setembro foi uma das principais falhas criticadas pela comissão do 9/11, tendo levado à reorganização da arquitectura dos serviços de inteligência dos EUA. Uma outra falha resultou da confiança excessiva da comunidade de inteligência sobre os sinais electrónicos de antes da invasão do Iraque, a qual foi desmontada por revelações subsequentes sobre a inexistência de armas de destruição massiva.
O uso e protecção das TIC são cruciais para mitigar e gerir as consequências de um ataque terrorista	Os primeiros a responder à emergência (bombeiros, polícia, paramédicos, outros trabalhadores de cuidados de saúde, etc.) têm que ser capazes de ter confiança na capacidade dos seus sistemas de TIC para permitir as suas comunicações, possibilitar a coordenação de acções e a partilha de informação. Para essas organizações, o desafio consiste em manter os seus sistemas actualizados e protegidos de ataques, tanto para treinar adequadamente todo o *staff* sobre como usar esses sistemas, como para partilhar boas práticas e lições aprendidas com outras organizações. O sector privado necessita também de apoio do governo para poderem aumentar a sua resiliência a ataques terroristas.
É necessário o uso de TIC para que aumente a consciência sobre riscos e para combater o apoio ideológico ao terrorismo	Os governos podem tomar vantagem sobre o vasto espectro de oportunidades oferecido pela revolução digital para aumentar o conhecimento e a consciência entre o colectivo dos cidadãos sobre os riscos terroristas. Os governos podem também procurar aliados entre os mesmos grupos alvos pelos terroristas para recrutamento ou suporte como parte da sua própria política de contra-terrorismo.

Figura IV 6 - Oportunidades criadas pelas TIC relativamente ao combate antiterrorista

E. O *CERT* COMO PARTE DA RESPOSTA A AMEAÇAS

CERT® (*Computer Emergency Response Team*), é a designação atribuída a uma entidade cuja actividade se centra, em exclusivo, na prestação de um conjunto de serviços de segurança em computadores e/ou redes informáticas. As duas características fundamentais de um CERT são: o facto de esta estrutura prestar o serviço de tratamento e resposta a incidentes de segurança e de ter um âmbito de actuação e uma autoridade claramente definidos. [21]

> O primeiro CERT que surgiu foi organizado pelo *Software Engineering Institute* (SEI), um centro de desenvolvimento suportado primariamente pelo Departamento de Defesa e pelo Departamento de Segurança Interna dos EUA assim com por outros organismos públicos americanos. Esse CERT é operado pela Universidade de Carnegie Mellon.

Em Portugal existe uma estrutura de CERT. Encontramos nas páginas do sítio Web do CERT português [CERT20091] a descrição da motivação para a sua constituição, assim como a sua missão.

> A sua missão é a seguinte:
>
> Prestar apoio a utilizadores de sistemas informáticos na resolução de incidentes de segurança, aconselhando procedimentos, analisando artefactos e coordenando acções com as entidades envolvidas.
>
> Reunir e disseminar um conjunto de informação autoritativa sobre vulnerabilidades e recomendações referentes a potenciais riscos de segurança e actividades maliciosas em curso.

[21] CERT é um nome e uma marca registada. "CERT" e "CERT *Coordination Center*" estão registados no *U.S. Patent and Trademark office* como uma marca de um serviço da *Carnegie Mellon University*.

Convém referir que o termo CERT também é usado para designar equipas comunitárias de emergência de resposta a situações de grandes desastres (*Community Emergency Response Team),* num quadro de Protecção Civil.

Receber, de fontes acreditadas, informação relacionada com novas vulnerabilidades de segurança, e actuar junto da comunidade no sentido de minimizar danos a nível Nacional.

Incentivar a criação de novos CERT em Portugal e a formação de consciência junto dos utilizadores de sistemas informáticos para a problemática da segurança informática.

O âmbito de actuação do CERT português existente à data da produção deste trabalho é coincidente com a comunidade utilizadora da RCTS - Rede Ciência, Tecnologia e Sociedade.

O funcionamento bem sucedido de um CERT depende em grande escala da informação que lhe é disponibilizada por outras organizações (por exemplo, CERTs de outros países) sobre ameaças detectadas, formas de neutralização dessas ameaças, riscos potenciais considerados mais prováveis, etc.

A divulgação pública que cada CERT assegura sobre ameaças reais ou potenciais[22], formas de as combater e acções de formação que promove é, de um modo geral, de grande utilidade para as estruturas encarregues pela segurança da informação e dos sistemas informáticos de qualquer organização. No entanto, e como acontece no caso português, o universo de destinatários normais da acção do CERT é restrito.

De acordo com [CERT20092] a acção de um CERT será mais abrangente, mais eficazmente dirigida e porventura mais útil se existirem em organizações de alguma dimensão e com responsabilidades significativas para a sociedade - entidades do sector público (central e local) e do sector privado – estruturas que tenham a responsabilidade de receber, rever e responder a incidentes de segurança sobre sistemas informáticos que tenham acontecido e sejam reportados ao CERT.

Estas estruturas, que podem tomar a forma de uma equipa formal ou de uma equipa *ad-hoc*, são designadas por *CSIRT - Computer Security Incident Response Team*.

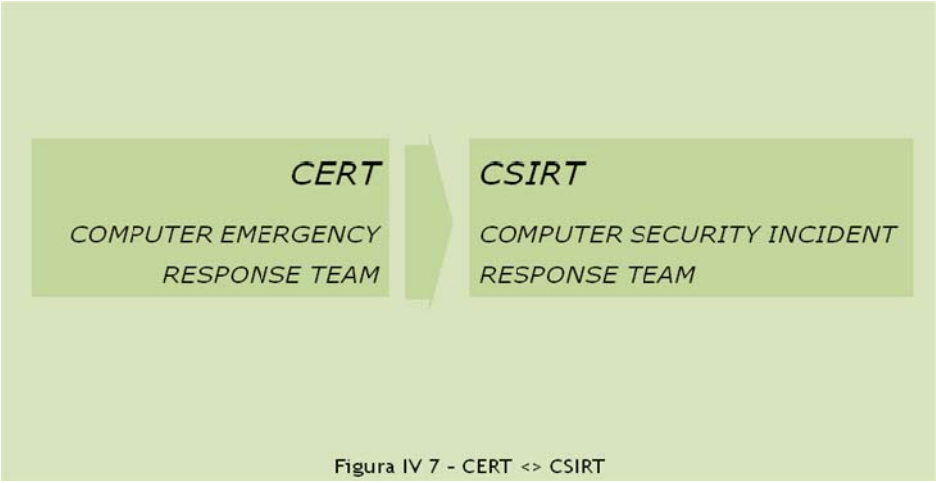

Figura IV 7 - CERT <> CSIRT

[22] Normalmente veiculada pelos seus sítios Web.

F. A PERSPECTIVA DOS INDIVÍDUOS

A PRIVACIDADE

Privacidade é uma consideração crítica na concepção de qualquer sistema de informação como por exemplo de comércio (electrónico ou de qualquer outro tipo), sobretudo porque é dado assente que as pessoas não usarão sistemas em que não confiem. Os sistemas como de identificação e de autenticação digital, videovigilância e RFID colocam novos desafios e riscos para a privacidade.

Mas o que é a **Privacidade**? Uma das definições preferidas por muitos diz que é "o direito de ser deixado sozinho"·. No entanto, e numa perspectiva moderna, pode dizer-se que é "o direito de controlar o acesso à informação sobre si próprio".

Na Sociedade da Informação, Privacidade é sobretudo o conjunto de conceitos "privacidade da informação, confidencialidade dos dados e segurança", os quais são elementos essenciais na construção de relações de confiança.

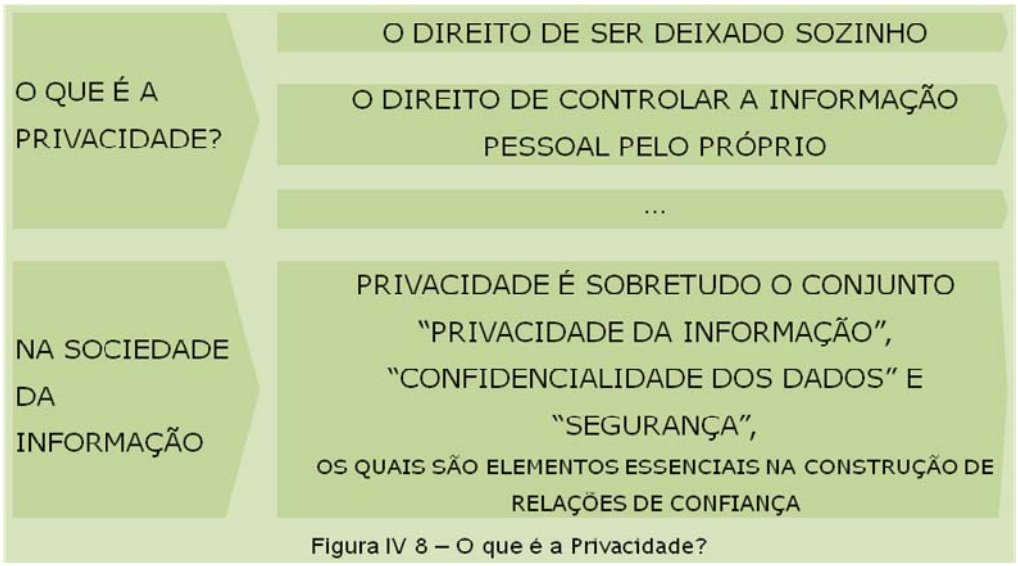

Figura IV 8 – O que é a Privacidade?

Existem hoje novas ameaças à privacidade, associadas à proliferação de repositórios electrónicos de informação mais ou menos sensível e a riscos adicionados por necessidades do comércio electrónico. Para fazer face a essas ameaças e minimizar os riscos adoptam-se soluções de segurança dos sistemas que incluem autenticação digital das partes envolvidas, cifragem de informação, boas práticas na gestão da informação.

A evolução que se tem verificado nos últimos anos no domínio da "administração pública electrónica" [23] tem correspondido a uma imersão cada vez mais alargada da Administração Pública (AP) na sociedade da informação, generalizando assim a interacção Cidadão-AP [24] à vida quotidiana.

È assim necessário que o cidadão estenda a esse relacionamento o mesmo tipo de cuidados que terá relativamente a outras redes e sistemas. Neste contexto o problema da identificação nacional tem que ser olhado pelo cidadão e pela própria AP de forma diferente.

Referem-se a seguir alguns factos reais que ilustram muito do que dissemos atrás.

O uso ilícito de dados pessoais por terceiros é um dos mais importantes e numerosos casos que se encontram hoje no ciberespaço, por exemplo:

- Ficheiros confidenciais de doentes roubados (ou copiados…) de hospitais e de gabinetes dos médicos e usados para chantagem, pressões relacionadas com o emprego, difamação, etc.
- O Primeiro-ministro de um determinado país descobriu que o seu correio electrónico foi sistematicamente lido por terceiros durante vários meses…
- Um agente dos serviços de Impostos forneceu a um cidadão dados fiscais sobre juízes e jurados …

Este tipo de casos é frequentemente facilitado pelo facto das pessoas deixarem os seus computadores sem protecção facilitado assim o acesso a dados sensíveis.

Um outro caso de ataque relativamente frequente consiste na alteração de páginas *Web*. São exemplos:

- A página de entrada da CIA foi alterada por *hackers* [25]…
- A página *Web* da Indonésia foi alterada por *hackers* apoiantes da causa timorense, os quais inseriram documentos mostrando a repressão no território…

Estas acções são facilitadas pelo facto da maior parte dos utilizadores minimizarem a segurança quando as páginas *Web* apresentam fundamentalmente funcionalidades de leitura.

Infelizmente mesmo quando elas não o são, verifica-se que são perpetradas acções ilícitas que podem ser muito gravosas para os utilizadores, por exemplo:

- Um ex-empregado sabotou uma cópia mestre de computador da Enciclopédia Britânica…
- Uma base de dados de uma empresa foi completamente apagada por um pirata informático…

[23] Em inglês referida como *e-government*.

[24] Por vezes referida como sendo do tipo *C2G*, ou seja, relação *Citizen to Government*.

[25] Piratas informáticos.

De facto, cremos que a maior parte dos perigos da segurança estará associada a situações de negação de serviço e de corrupção, levadas e a efeito por sabotagem, vingança e por motivações políticas.

Podemos concluir:

- A insegurança é possibilitada tanto pelos computadores como pelas próprias pessoas.
- No que se refere a segurança, mais vale investir do que despender.
- Quando está em causa (ainda que de forma não evidente) a protecção de informação (seja qual for o seu objecto e a forma como ela está registada) é fundamental que se aplique uma Ética adequada, que se promova a formação das pessoas e que se assegure disciplina de atitudes nos acessos ao ciberespaço.
- Temos que ter consciência de que a nossa insegurança contribui para a dos outros.
- Devemos ter consciência que por vezes o melhor segredo é o partilhado – por isso é importante que haja auditoria, que seja possível o rastreio quando se trate de organizações, e que existam integrada na cultura de segurança a possibilidade natural de responsabilização adequada de quem fura as regras e compromete a segurança.
- Temos que reconhecer que não existe segurança absoluta.

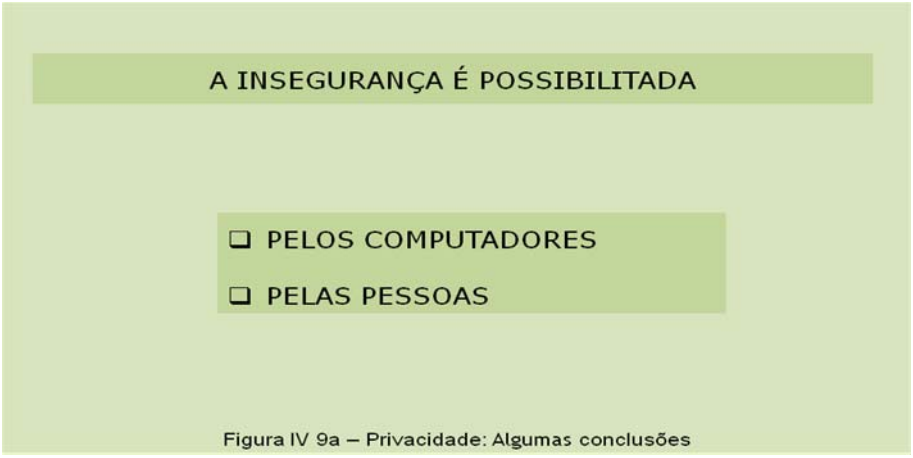

Figura IV 9a – Privacidade: Algumas conclusões

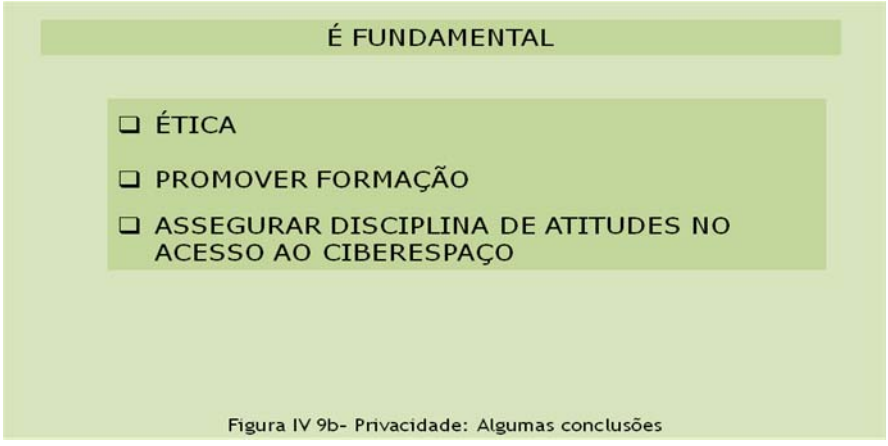

Figura IV 9b- Privacidade: Algumas conclusões

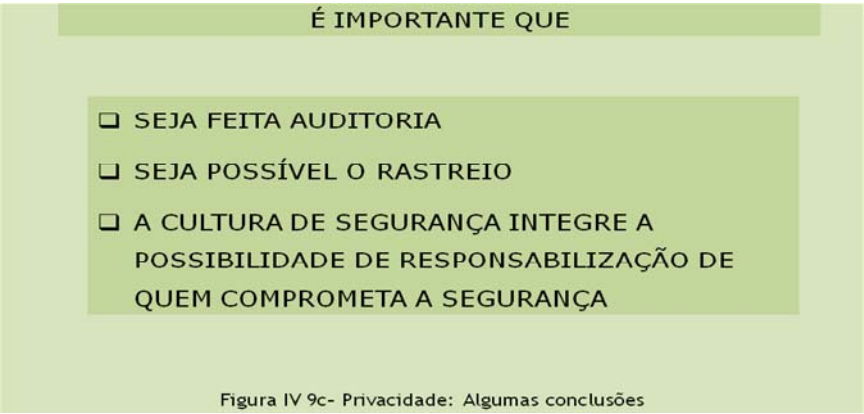

Figura IV 9c- Privacidade: Algumas conclusões

IDENTIDADE DIGITAL

Do texto "Sociedade da Informação, Sociedade (in)Segura?" incluído no livro "Sociedade da Informação – O Percurso Português" [Veríssimo, 2007], a identidade digital (ID), mais do que uma tecnologia que dá um toque moderno às sociedades, é acima de tudo uma pedra de toque do caminho para a sociedade da informação.

A opção ID deve reunir consenso em volta da confiança: introdução de tecnologias seguras e robustas; inclusão de procedimentos transparentes de verificação, teste e certificação; garantia de auditabilidade pela sociedade.

A ID deve incondicionalmente respeitar os níveis de privacidade existentes com a identidade física, ou até melhorá-los, numa demonstração incontestável das vantagens da migração para a ID.

Os cidadãos são obrigados a ter B.I., não é uma opção, portanto a evolução para o B.I. digital não pode nem deve comprometer qualquer direito dos cidadãos. Seria grave que, como cidadãos, não pudéssemos *justificadamente confiar*, isto é, ter uma certeza fundamentada que, em operações digitais feitas com o tal cartão digital, não era possível, inadvertida ou maliciosamente, aceder a, ou mesmo modificar indevidamente dados do cartão. Um cartão de ID deve ser pelo menos tão robusto quanto o antecessor físico.

As questões da robustez e da credibilidade, bem como a sua certificação por entidades independentes e da confiança dos cidadãos, são factores chave, não alienáveis, da introdução de qualquer sistema de ID. Alguns especialistas advogam que um cartão de ID deve ser ainda mais robusto do que a alternativa física, pois a velocidade a que as fraudes se processam no mundo digital e a verosimilhança delas com operações genuínas, aumenta significativamente o risco de danos de monta, materiais e pessoais. No caso de um problema, as fraudes podem atingir níveis de perfeição que as tornarão virtualmente indistinguíveis de operações verdadeiras, levando à criação de duplos digitais perfeitos, possivelmente operados por

cibercriminosos, assombrando a existência de alguns cidadãos e causando o pânico nos já "ciberófobos" tribunais.

Porque nem tudo é mau, a utilização de tecnologias digitais pode abrir-nos um mundo totalmente novo, mais seguro, mais privado, mais responsável. A utilização correcta de pseudónimos digitais, por exemplo, permitir-nos-á criar várias personalidades digitais para diversos usos, incluindo transacções comerciais, protegendo o nosso anonimato e privacidade, enquanto manterá uma ligação segura à nossa identidade real, que nos responsabilizará enquanto cidadãos, nos necessários planos financeiro, fiscal, ou jurídico.

No momento actual, o debate sobre a gestão da identidade está inevitavelmente ligado aos documentos de identificação oficiais, como é o caso do cartão do cidadão (CC) e o passaporte electrónico português (PEP), processos em que Portugal se encontra recentemente envolvido.

O estudo "Identidade Digital" elaborado por um grupo de trabalho no âmbito da APDSI, liderado por Paulo Veríssimo, produziu um conjunto de recomendações que cremos ser importante reproduzir no contexto do presente trabalho.

Considerando que:

(a) Projecção do social no digital

A esfera da identidade digital não deve retirar conteúdo à esfera da identidade social, antes afirmando-se como um super conjunto "melhor" de possibilidades para as partes interessadas (*stakeholders*).

(b) Adequação do regime juridico-legal

A esfera da identidade digital não deve levar a uma degradação das condições de credibilidade, responsabilidade e protecção que a sociedade e as suas partes interessadas hoje esperam da identidade, por via de desadequações ou vazios jurídico-legais.

(c) Compreensão e confiança no digital

A esfera da identidade digital deve assumir junto da sociedade e as suas partes interessadas um nível de compreensão e confiança semelhante à existente na esfera da identidade social, através da transparência e auditabilidade de processos e métodos subjacentes.

(d) Subordinação do tecnológico ao social

Os processos e sistemas informáticos da identidade digital devem adaptar-se aos objectivos da sociedade e as suas partes interessadas e não o contrário.

Estes princípios gerais encontram-se ameaçados pelos riscos de diversa ordem que foram acima condensados. No sentido de os prevenir e/ou mitigar, terminamos com um conjunto de recomendações específicas a pôr em prática pelas várias partes interessadas, com especial relevância para as instituições do Estado, como catalisadores de processos que poderão então ser seguidos por empresas, associações cívicas, cidadãos:

(e) Sociedade

Promover a educação das partes interessadas, dos cidadãos às empresas.

Promover uma cultura de exigência por parte do cidadão relativamente aos serviços de que é utente, garantindo a existência de instituições sancionatórias confiáveis.

Garantir a transparência, certificação e auditabilidade dos sistemas e processos.

Garantir a posse da sua ID (*empowerment*) pelas partes interessadas, no funcionamento dos sistemas e processos.

Figura IV 10 - Privacidade: Algumas recomendações - Sociedade

(f) Legislação

Promover urgentemente a modernização da lei do crime informático.

Promover prontamente a adequação das leis relacionadas com a identidade e identificação.

Garantir a imputabilidade/responsabilização de qualquer agente público perante consequências negativas resultantes de incompetência ou simples negligência na concepção, projecto, concretização e/ou exploração de processos.

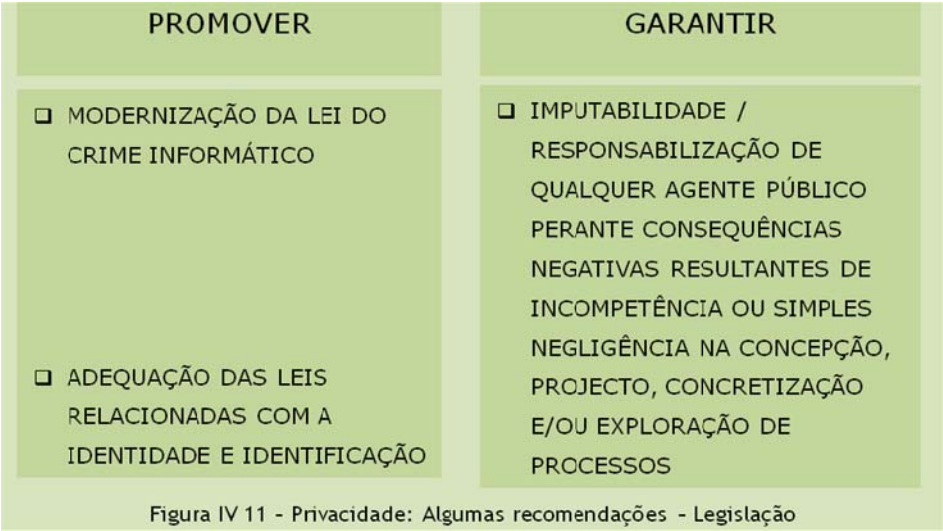

Figura IV 11 - Privacidade: Algumas recomendações - Legislação

(g) Polícias/Tribunais

Sensibilizar e promover a formação da administração, polícias e magistratura, para as questões da sociedade da informação no geral e para os aspectos da Identidade Digital em particular.

Criar meios, predominantemente de natureza tecnológica, que garantam a eficácia das polícias e dos tribunais na esfera digital.

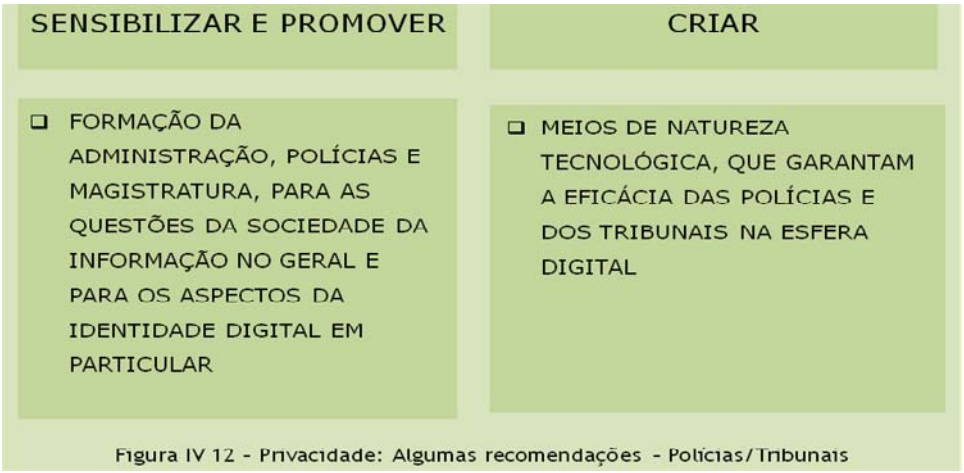

Figura IV 12 - Privacidade: Algumas recomendações - Polícias/Tribunais

(h) Segurança

Definir claramente as propriedades técnicas de segurança necessárias aos sistemas e processos da Identidade Digital (identificação, autenticação, assinatura, delegação, etc.) e os procedimentos conducentes à sua imposição (especificação, teste, validação, certificação, auditoria, etc.).

Assegurar que os direitos de privacidade das partes interessadas não são prejudicados pela transição para a ID.

Promover uma cultura generalizada de segurança na Administração Pública, e assegurar que ela é aplicada de forma sustentada a todo o universo dos seus sistemas informáticos.

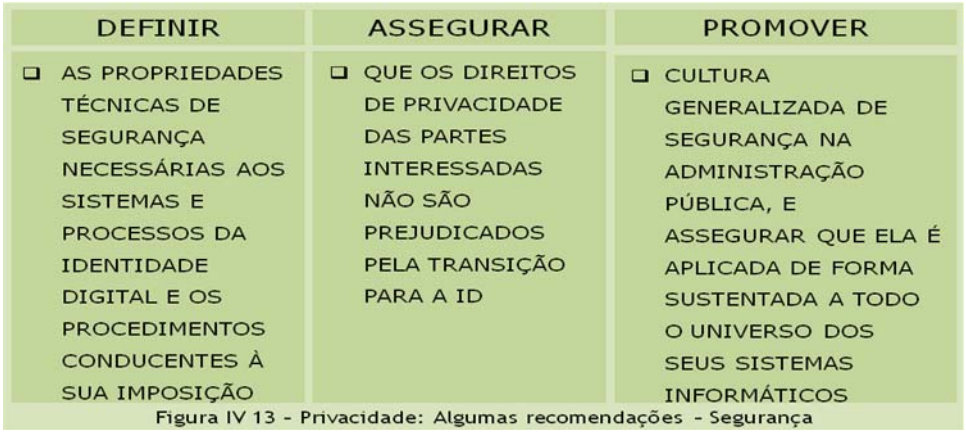

Figura IV 13 - Privacidade: Algumas recomendações - Segurança

(i) Tecnologia

Definir, regulamentar e controlar, por parte do Estado, a introdução das tecnologias mais adequadas ao objectivo de servir a ID, nomeadamente visando as propriedades técnicas de segurança e de robustez dos sistemas.

Definir, regulamentar e controlar, por parte do Estado, a execução dos procedimentos (especificação, teste, validação, certificação, auditoria, etc.) conducentes à imposição das propriedades técnicas de segurança e comprovação da robustez dos sistemas.

Garantir um nível de auditabilidade pela sociedade que contribua para a sua confiança no funcionamento do sistema.

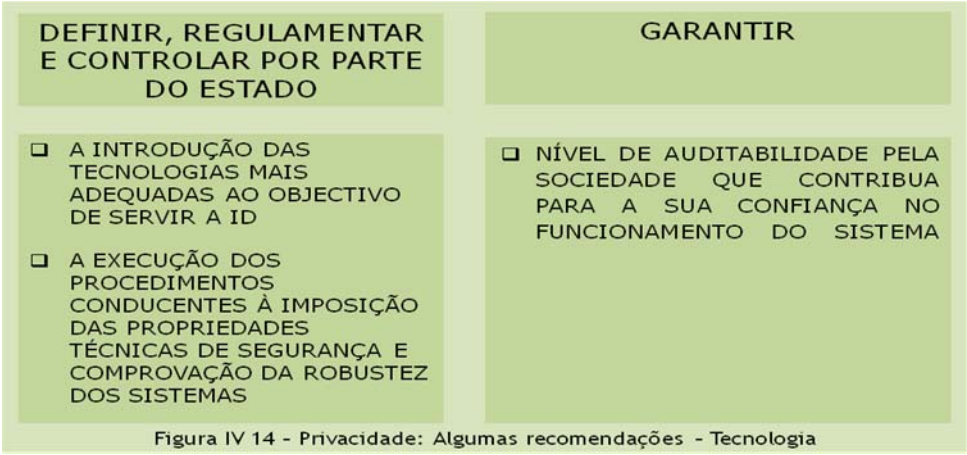

Figura IV 14 - Privacidade: Algumas recomendações - Tecnologia

A ENGENHARIA SOCIAL

Todos os dias, milhões de internautas são persuadidos a entrar em *sites* que servem apenas para espalhar o caos virtual.

> Um dos exemplos mais conhecidos é o da mensagem que avisa, em tom de cumplicidade: "Você está a ser traído". Junto, há um endereço no qual, supostamente, podem ser vistas as fotos que comprovam a traição – mas que na verdade instala um vírus no computador da vítima. Existem até variações sobre o tema: "Verifique as suas finanças", "Você recebeu um cartão virtual" e até a propaganda de um aparelho capaz de aumentar os genitais masculinos são casos famosos. O grande problema é que, hoje, essas mensagens não servem apenas para destruir discos rígidos. Agora, os ataques do cibercrime têm uma finalidade muito mais onerosa: roubar informações e, se possível, o dinheiro da vítima. Isso ocorre graças aos chamados *spywares*, ou "softwares espiões". Esses programas capturam tudo o que é gravado e digitado num computador, desde um simples relatório até senhas de banco. O material recolhido é automaticamente enviado para um criminoso qualquer, que a seguir aproveita para realizar operações bancárias, fazer compras e até burlar outros utilizadores noutros computadores. O detalhe macabro é que é a própria vítima quem instala o espião em sua máquina. Nesse caso, não há antivírus que possa impedir o contágio.

No dia-a-dia, é fácil identificar os hábitos capazes de tornar uma empresa vulnerável à espionagem virtual. Abrir anexos de *e-mails* suspeitos, anotar ou compartilhar senhas e até o simples ato de navegar por um site desconhecido são vias abertas para os *spywares*. Só em Novembro de 2005, a associação internacional de combate a fraudes electrónicas *Anti-Phishing Working Group* detectou 16,8 mil tipos diferentes de *phishing* – como são conhecidas as mensagens que motivam o internauta a adoptar comportamentos que o prejudicam, sem que ele se aperceba que os está a cometer. É quase o dobro do registado no mesmo período do ano anterior.

"As acções de segurança passam pelo tripé Tecnologia, Processos e Pessoas. Destes três elos, o mais fraco é o que se refere às Pessoas".

> Os próprios *hackers* reconhecem que não é difícil obter "ajuda" do utilizador para invadir uma rede. "É preciso convencê-lo a *clicar* no *link* que descarrega o vírus para dentro da máquina. E a melhor maneira de fazer isso é instigando a curiosidade".

Figura IV 15 - Tripé que apoia as acções de segurança

"No passado, os *hackers* queriam ficar famosos com as invasões de redes e sistemas de terceiros. Ultimamente, no entanto, a intenção é obter proveitos financeiros". Uma pesquisa realizada pela empresa Symantec ajuda a vislumbrar essa mudança de comportamento. No primeiro semestre de 2004, quase 54% dos vírus detectados por aquela empresa tinham a função de capturar informações confidenciais. Um ano depois, o índice havia crescido para 75%.

O primeiro passo para afugentar os *softwares* espiões é fazer o óbvio: manter antivírus e protecções de rede actualizados constantemente. As mais novas actualizações já são capazes de detectar quando o internauta está navegando nas águas mais perigosas da rede. Também é possível recorrer a programas que têm a função específica de eliminar *spywares*.

De resto, é necessário definir regras e procedimentos entre os próprios funcionários – para que eles próprios saibam como manter as informações da empresa a salvo. Afinal, não há tecnologia capaz de evitar a falha humana. Apesar de todos os avanços na área da segurança de informação, cerca de 80% das invasões realizadas em redes corporativas ainda contam com a participação directa ou indirecta de funcionários ou ex-funcionários. "Existe muita preocupação com o investimento em equipamentos. Mas isso não garante 100% de segurança.

Tudo dependerá sempre da acção das pessoas envolvidas".

Até mesmo os *blogs* podem indicar formas de violar o conteúdo sigiloso de uma empresa. "Alguns funcionários fazem relatos do quotidiano da empresa e, involuntariamente, acabam revelando brechas para quem deseja ter acesso às informações".

A pior notícia é que nem os mais chorudos investimentos serão suficientes para conter a expansão do cibercrime nos próximos anos. Pelo contrário: na medida em que surgem novas tecnologias, também cresce o raio de acção dos *hackers*.

Um próximo alvo dos ataques, por sinal, situa-se num ambiente ainda relativamente novo: o da telefonia IP (ou VoIP). "No VoIP, a voz é transmitida pela Internet em formato de dados. Sendo assim, ela está exposta a todas as vulnerabilidades de um ficheiro que é transmitido pela rede". Caso a empresa não tenha mecanismos de criptografia para proteger a rede, as conversas travadas pelos funcionários podem ser interceptadas como se fossem um simples *e-mail*. No entanto, as ferramentas de VoIP disponibilizadas pelas grandes empresas já vêm com os devidos dispositivos de segurança – o que torna essa tecnologia quase intransponível.

A telefonia móvel também deverá entrar na lista dos *hackers*. Actualmente, existem vírus capazes de fazer estragos em aparelhos mais antigos. A verdadeira preocupação, porém, é quanto à integridade das empresas que utilizam o telemóvel como meio de transmissão de dados – prática que já é bastante comum sobretudo no sector de serviços. Os especialistas não têm dúvidas de que os *hackers* acabarão por descobrir uma maneira de copiar ou apagar as informações que saem dos aparelhos. É uma questão de tempo. "No futuro, os telefones móveis funcionarão como atalho para a inclusão digital de quem não pode comprar um computador. Nesse momento, o celular dará acesso a dados cada vez mais valiosos e, por isso, será atacado.

Junto com os celulares, todas as tecnologias que visam a dar mobilidade às empresas correm algum risco. É o caso dos PDAs e *notebooks*. Não é preciso ser-se perito em informática para roubar dados desses aparelhos - basta ter o equipamento certo. "Hoje, é mais fácil roubar a informação fisicamente do que virtualmente. Com uma *pen-drive* do tamanho de uma moeda, por exemplo, é possível descarregar uma infinidade de informações em poucos segundos".

SEGURANÇA DOS UTILIZADORES

As protecções que actualmente conseguimos activar relativamente aos conteúdos disponíveis na *World Wide Web*, em que muitos desses conteúdos estão associados a potenciais acções nefastas (mais activas ou mais adormecidas) apresentam riscos que têm que ser adequadamente geridos.

Os riscos, que exercem influência nefasta sobre o utilizador (que é, na maior parte dos casos, facilmente influenciável em termos comportamentais), apresentam diferentes tipos de impacto, são potenciados através dos sistemas informáticos e de outros sistemas que ele utiliza para chegar aos conteúdos,

As crescentes ameaças actuais relacionadas com a WWW e a exploração instantânea de qualquer vulnerabilidade, por parte de autores de *software* "mal intencionado", evidenciam o facto de que não é suficiente para as organizações e para os indivíduos protegerem o seu correio electrónico e os sistemas terminais. Eles necessitam de agir rapidamente no sentido de garantir que a navegação na Internet não coloca ameaças à segurança das TIC, aos recursos da rede ou à produtividade das pessoas. Para além de boas práticas de prevenção, nomeadamente através da aplicação rigorosa de *patches* ao *software* e ao *firmware* e promovendo e realizando a educação e formação dos utilizadores particularmente sobre os riscos associados às simples acções de *browsing*, é vital que as organizações implementem soluções de protecção que se orientem para os três pilares principais da protecção *web*:

1. Filtragem baseada na reputação
2. Filtragem por antecipação de ameaças, em tempo real
3. Filtragem baseada em conteúdos

Os filtros "baseados na reputação" constituem a primeira componente crítica da luta contra ameaças baseadas na WWW.

Eles fazem a sua prevenção através de catálogos de sítios web que são conhecidos por hospedarem software pernicioso ou outro conteúdo indesejável, filtrando e classificando os URLs como bons ou maus com base na sua reputação e que são uma forma já estabelecida e razoavelmente provada para uma protecção adequada contra ameaças já conhecidas e localizadas na *web*.

Da mesma maneira que eles asseguram uma prevenção básica, ajudam a optimizar a performance da rede e a produtividade dos utilizadores através do bloqueio de acesso ilegal ou inadequado a conteúdos que não são críticos para as necessidades do indivíduo ou da organização.
Por outro lado, esses filtros são facilmente contornados pelos criminosos – que, obviamente, conhecem-nos e sabem como eles actuam – hospedando o seu *software* malicioso em sitos legítimos e recém criados. O tráfego oriundo desses sítios não é bloqueado e o *software* malicioso, quer seja novo ou velho, acaba por ser introduzido em casa ou na organização.

No caso da filtragem por antecipação de ameaças em tempo real, todo o tráfego *web* passa através de um dispositivo (normalmente *software*) de *scanning* destinado a identificar o *software* malicioso – não só o que é conhecido como também o que está a emergir. Sempre que um utilizador acede a um sítio *web*, independentemente da sua reputação, o tráfego é varrido por um motor que analisa e detecta o *software* malicioso, usando uma combinação de tecnologias baseadas em assinaturas e em comportamentos.
A filtragem por conteúdos é aplicada através de *software* que é parametrizado para bloquear conteúdos previamente tipificados e inclui normalmente a alimentação e actualização de uma base de dados de

termos e frases que faz com que o *software* bloqueie o acesso sempre que algum desses termos ou frases sejam detectados numa página de um sítio *web*. Existem algumas versões de *software* deste género que procuram termos e outros elementos visuais e/ou estruturais (constantes da base de dados) dentro de imagens na forma digital.

Figura IV 16 - Filtragens para protecção Web

A educação dos utilizadores como medida de defesa

Muitas organizações têm promovido com sucesso a educação dos seus utilizadores relativamente ás formas de combater as ameaças associadas ao correio electrónico, e ao mesmo tempo que se combatem as ameaças baseadas na *Web* com a ajuda de tecnologias sofisticadas, é importante que se procure captar os utilizadores para a luta.

Muitas organizações dispõem de orientações e procedimentos que definem quais os sítios *web* que são considerados indesejáveis, mas poucas actualizam essa mesmas orientações. Uma boa política enfatizará que os empregados e colaboradores nunca deverão:

- Abrir mensagens de correio electrónico de *spam* recebidos de emissores desconhecidos;
- *Clicar* em *links* incluídos nas mensagens de correio electrónico recebidos de emissores desconhecidos.

A necessidade de protecção de todos os pontos das redes

Os cibercriminosos exploram qualquer vulnerabilidade que possam encontrar para infectar as redes das organizações.

Eles exploram falhas na segurança da *web* para fazer chegar *software* malicioso ao computador do utilizador em poucos segundos.

Os utilizadores são levados a visitar sítios *web* comprometidos em termos de segurança, tipicamente por via de *links* em mensagens de correio electrónico de *spam*.
Pode haver camadas de complexidade no sítio original, que leva até outro sítio, levando a um terceiro sítio e assim sucessivamente, terminando com um "troiano" descarregado no computador do utilizador – e tudo isso acontecendo numa questão de segundos.
As tarefas de segurança da rede contra isto – na *web*, no correio electrónico e no terminal – não deixa de ser um desafio assustador dos dias de hoje para os departamentos de TIC os quais estão a ser solicitados para fazer mais e mais com os seus orçamentos limitados.
Naturalmente que quem está "do outro lado" da *web* pode ser um terrorista… assim será conveniente, para apoiar a avaliação de riscos, "cristalizarmos" da seguinte forma a lógica do terrorismo:

1. A forma como vivemos hoje em dia, num mundo interligado, é muito mais vulnerável do que alguma vez o foi.

2. O terrorismo é uma actividade sofisticada e, como tal, tem que ser encarada estrategicamente.

3. A sociedade moderna "facilita" o terrorismo, como uma expressão crua de conflito e protesto.

4. Há contra-medidas, individuais e colectivas, que podem ser adoptadas no sentido de mitigar as ameaças ao nosso modo de viver.

Segurança dos utilizadores mais jovens

Os impactos e efeitos que as TIC produzem sobre os utilizadores mais jovens são potencialmente mais perigosos, não só porque as crianças e os adolescentes estão genericamente menos preparados para discernir as informações e actividades sérias em relação às que têm objectivos maléficos.

Este universo de utilizadores é particularmente fixado como alvo por parte de agentes criminosos que, através da Internet e dos serviços que sobre ela existem, desenvolvem acções destinadas a manipular e explorar os espíritos mais jovens.

Tanto a Internet como o telemóvel são excelentes ferramentas de integração social, educação e lazer.
Com elas podemos fazer coisas, em qualquer lugar, o que há alguns anos atrás seria impensável.
Comunicar através da voz ou de mensagens, ir buscar informações para os estudos e para o trabalho, fotografar, gravar pequenos vídeos, navegar na *WWW*, ouvir música, jogar, conversar em "chat", criar e consultar blogues, ser solidário, etc.

A quantidade de crianças e jovens que têm telemóvel é enorme.

As novas tecnologias fazem parte da vida dos jovens, os quais as conhecem melhor do que os seus pais e professores. Estes usam as tecnologias principalmente para se manterem em contacto uns com os outros e como fonte de diversão.

É crítico, neste universo de utilizadores, que se procure assegurar a promoção do uso responsável dos serviços que estão à sua disposição.

Nomeadamente e no que se refere aos serviços de telefonia móvel:

- Fomentar e divulgar o seu uso responsável através da colaboração entre pais e professores, promovendo-se acções de consciencialização e de aconselhamento para pais através de sítios *Web*.
- Ajudar as crianças a usarem conscientemente os acessos à WWW, aproveitando as possibilidades oferecidas pelas tecnologias, como por exemplo activando a filtragem de conteúdos indesejáveis.
- Desenvolver Políticas de protecção para grupos de utilizadores mais sensíveis.

Não podemos esquecer que um telemóvel é, de facto, um terminal de comunicações que integra TIC. Assim, algumas das preocupações que são evidentes quando nos referimos a um ambiente de TIC são aplicáveis neste domínio.

Não é fácil separarmos as preocupações relativas à protecção contra ameaças à segurança “imediata” de bens e serviços e contra ameaças à segurança “psicológica”.

Fomentar uma utilização responsável e uma responsabilidade partilhada

Para assegurar um uso responsável crescente do telemóvel, as operadoras devem ter um papel activo no processo, assim como outros actores, havendo que se procurar o envolvimento, num primeiro nível, dos pais e educadores, das instituições públicas a nível nacional e regional e dos próprios fornecedores de conteúdos.

Algumas acções possíveis nesse sentido são:

- Produção de normas que visem o aumento de medidas de protecção dos menores quando acederem a determinados conteúdos através do telemóvel.
- Acções afirmativas dos operadores de telefonia móvel de combate a conteúdos de pornografia infantil na Internet.

É muito importante que os pais e educadores estejam atentos ao uso que os menores que estão sob sua responsabilidade fazem das novas tecnologias.

É muito importante que consigamos, enquanto adultos e com responsabilidades para com a sociedade onde estamos inseridos, estabelecer um diálogo de confiança com as crianças. Os pais devem falar abertamente com os seus filhos, mas nunca de maneira alarmista. Principalmente, para manter essa base de confiança, não devem proibir o seu acesso à Internet ou ao uso do telemóvel como instrumento de ameaça ou castigo, ou porque pensam que podem sofrer algum tipo de desgraça enquanto navegam pela Internet. Isso impediria que as crianças falassem abertamente com seus pais caso encontrassem algum conteúdo impróprio ou sofressem algum tipo de assédio ou de contacto que os incomodasse.

É importante que, quando decidimos instalar um acesso à Internet a partir da nossa casa, levemos em consideração uma série de medidas que nos permitam aproveitar ao máximo esta tecnologia e, ao mesmo tempo, minimizar a possibilidade de a usar de forma inadequada.

São aconselháveis algumas medidas que ajudarão à segurança, pelo que salientamos algumas a título exemplificativo:

1. O computador deve estar sempre em um lugar da casa onde os pais possam ver o ecrã e controlar os conteúdos que são acedidos pelas crianças.

2. Ao contratar o serviço de acesso à Internet para uso pessoal e familiar, deve-se tomar conhecimento das opções de controlo de conteúdos e "controlos parentais" disponibilizados pelo prestador de serviços.

3. Devem instalar-se anteparas (*firewalls*) e antivírus para evitar que estranhos possam aceder ao computador para obter dados confidenciais e pessoais (*phishing*) e manipular o computador para utilizá-lo com fins ilegais (*spam*).

4. Não comunicar o número do telemóvel ou outros dados pessoais a pessoas que não conhecemos bem, pois eles podem vir a ser utilizados de forma inadequada.

5. Não responder a mensagens de *SPAM* (mensagens indesejadas) e nunca as reenviar.

Medidas de responsabilidade

1. Informar as crianças e os jovens de que na Internet nem tudo é o que parece ser.
   É preciso manter um diálogo aberto e explicar-lhes claramente que as pessoas podem mentir através da Internet com fins ilícitos.

2. Falar com os menores a nosso cargo, incentivando-os a contar-nos ou a algum adulto da sua confiança caso alguma coisa na Internet os incomode, ou se algum dos seus amigos da Internet lhe disser alguma coisa que não lhe pareça apropriada.

3. Explicar aos menores porque não se deve fornecer dados pessoais (nome completo, endereço, número de telefone fixo ou de telemóvel, nome do colégio, enviar fotos, etc.) nem seus nem de nenhum dos seus amigos, a nenhum amigo virtual e insistir em que esta norma seja sempre respeitada.
   Que comuniquem imediatamente a um adulto de sua confiança, caso através da Internet alguém tentar obter informações particulares sobre eles ou sobre alguma outra criança.

Não incomodar os outros

Quanto mais interagimos com outras pessoas, mais importante é procurarmos adoptar atitudes, através de educação e aculturação, que para além de permitirem criar e manter bons ambientes de inter-relacionamento ajudam a combater muitas das ameaças externas pois a actuação – individual e colectiva - é organizada e é consciente. Por exemplo:

(a) No colégio: aconselhar os filhos a respeitarem as normas internas referentes ao uso de telemóvel no sentido de uma melhor convivência entre todos.
(b) Nas actividades diárias: ajustar o som do telemóvel ao ambiente onde estiver (especialmente quando estiver em lugares públicos, na Igreja, no cinema ou em espectáculos...).
(c) Não fotografar nem filmar outras pessoas em situações anormais. Para além disso, é importante que se explique aos mais novos que é proibido distribuir esse tipo de imagens sem o consentimento dos visados.
(d) É proibido:
    1. Divulgar, através de um blogue ou de um sítio pessoal na *Web*, fotografias ou vídeos que atentem contra a imagem ou a vida privada de outras pessoas.
    2. Ameaçar, assediar, injuriar ou propagar calúnias por qualquer meio, incluindo o telemóvel.
(e) O telemóvel não deve ser utilizado para difundir rumores, nem expressar opiniões que difamem, insultem, ameacem ou intimem terceiros.
(f)

Reduzir a quantidade de mensagens *spam*

Na prática só o bom senso pode ajudar a reduzir o *spam*. Eis algumas atitudes básicas a adoptar:

1. Não comprar os produtos anunciados através de *spam*.
2. Usar filtros de *spam*.
3. Não abrir mensagens de destinatários suspeitos. Podem conter vírus que se activam quando abrimos a mensagem.

4. Nunca responder a uma mensagem de *spam*, não "clicar" nos links que aparecem na mensagem, nem ligar para os telefones que eles indicam. Se o utilizador fizer isso, poderá estar a confirmar que o seu endereço electrónico é válido e continuará receber mensagens de *spam*.
5. Desactivar a opção de "visualizar" das mensagens com formato HTML e desactivar a opção de "enviar sempre confirmação de leitura".
6. Não participar em "correntes" de correspondência enviada por correio electrónico.
7. Cuidar do endereço electrónico individual como se fosse um bem pessoal. Se possível, não o colocar em formulários suspeitos, sítios *Web* ou fóruns públicos.
8. Utilizar endereços de correio electrónico alternativos para se registar em sítios *Web* que não são de confiança.
9. Desactivar a opção "Para receber mais informações" que habitualmente aparece nessas mensagens.

EDUCAÇÃO	DOS UTILIZADORES COMO PRINCIPAL MEDIDA DE DEFESA
PROTECÇÃO	DE TODOS OS PONTOS DA REDE
SEGURANÇA	DOS UTILIZADORES MAIS JOVENS
FOMENTAR	UTILIZAÇÃO RESPONSÁVEL E RESPONSABILIDADE PARTILHADA
ADOPTAR	MEDIDAS DE RESPONSABILIDADE
NÃO	INCOMODAR OS OUTROS
REDUZIR	A QUANTIDADE DE MENSAGENS *SPAM*

Figura IV 17 - Segurança dos utilizadores

OS DIREITOS DIGITAIS

Sobre este tema considerámos adequado recorrer a partes do texto "Gestão de Direitos Digitais" - estudo elaborado pelo Grupo Ad-Hoc no âmbito da APDSI [APDSI200899].

Os Direitos Digitais (DD), no dizer do Glossário da Sociedade da Informação da APDSI [APDSI200799], são o "conjunto de tecnologias digitais que controlam o acesso à informação electrónica, para proteger os direitos de propriedade intelectual dos proprietários dos conteúdos". São, assim, dispositivos de tipos muito variados e têm funções instrumentais em relação à gestão, aos modelos de mercado e aos conceitos de propriedade e de uso de bens digitais…".

As principais questões "políticas" ou de interesse público que interessa (à APDSI) acompanhar são as questões do que deve ser em tese a liberdade de criar, de inovar, de funcionamento da inteligência colectiva, ou cooperativa, em que os criadores participam dialecticamente com os utilizadores na criação,

do antigo e neo-espírito académico, do espírito inicial da Internet "académica" baseado na ciência como informação do domínio público, da proliferação recente de modelos, aparentemente, de informação aberta ou livre na *Net*, como os blogues, Yahoo, Google, Wikipédia, Youtube, MySpace, Linux, Open Source, B-on, novos modelos de propriedade intelectual como os Creative Commons e outros.

A APDSI deverá preocupar-se mais com a importância da inovação ao serviço do desenvolvimento da sociedade da informação e do conhecimento, da economia social, da ciência enquanto bem público de acesso livre, contraposto à tecnologia em que a informação representa valor de mercado, e dos entraves dos actuais sistemas de protecção de patentes europeias e outros direitos de registo caro, que funcionam em benefício dos que têm muitos recursos tanto para registar, como para litigar, ou ameaçar litigar, e de direitos de autor cuja gestão mundial muito concentrada em multinacionais e sistemas por elas dominados, afectam a sobrevivência geral da informação de domínio público e a liberdade criativa mundial.

Embora pareçam mais flexíveis e "amigos" da liberdade de informação e de criação colectiva do que os modelos mais antigos de gestão de propriedade intelectual, que persistem na defesa de modelos jurídicos rígidos de manutenção do mercado, devem dar-se redobrada atenção aos mais recentes, mais flexíveis, menos conhecidos e muito mais ambiciosos modelos de negócio, aparentemente muito abertos e realmente poderosíssimos centralizadores de gestão da informação mundial. Sistemas que se atribuem como missão "organizar a informação universal tornando-a disponível e útil", tarefa que os deuses do Olimpo, e muitos outros deuses, eram obrigados a partilhar, deverão merecer atenção e serem a principal preocupação da APDSI.

GDD, ou seja, a exploração de direitos é apenas um aspecto instrumental da questão maior que é constituída pela definição do que pode ou deve ser protegido como propriedade intelectual, mais precisamente, como direitos de autor, ou outras formas mais flexíveis de propriedade intelectual. Não se trata de um problema que tenha especialidades nacionais e em que um Grupo de Trabalho nacional possa acrescentar mais-valias específicas sobre o mercado português.

No conjunto do problema dos Direitos Digitais, os dispositivos de GDD são meramente instrumentais, generalizadamente de uso comum em todas as formas de gestão, independentemente das tendências mundiais de aparente abertura e liberalização de acessos à informação e consequentes alterações de modelos de gestão de informação e de negócio.

Sobre os GDD, o BEUC[26] exige:

- O respeito do Direito de Cópia Privada

[26] Bureau Européen des Unions de Consommateurs

- Práticas Comerciais Leais
- Direito à Informação
- Direito de Devolução de Produtos Defeituosos
- Regime equilibrado e justo
- Direito ao respeito da Privacidade e da Protecção de Dados Pessoais
- Direito à Liberdade de Expressão
- A importância do princípio de que os GDD não podem contribuir para o fosso digital (Digital Divide)
- Direito à manutenção da Integridade da Propriedade Privada

E, ainda, o controlo internacional e, especialmente, da União Europeia, para que se impeçam, em casos concretos conhecidos, as alterações de modelos de negócio com vista a mudar as regras e defraudar os utilizadores.

…Os profissionais da informação podem contribuir com a disposição do Código de Ética da APDIS; BAD e INCITE que diz que "Os profissionais da informação em Portugal assumem como próprias as seguintes responsabilidades:

…

Opor-se à implementação de qualquer solução tecnológica que possa limitar ou manipular o acesso à informação"

A questão dos direitos de propriedade intelectual é uma questão muito importante também para uma análise das "TIC para um Mundo mais seguro".
As modernas tecnologias vieram criar novas oportunidades para os artistas serem criativos e distribuírem as suas obras, mas, também trouxeram acrescidas oportunidades aos infractores.

Assim, a complexidade inerente ao domínio das tecnologias aconselha a que, na prática, a gestão dos direitos patrimoniais envolvidos seja confiada a entidades de gestão colectiva.

As exigências do mundo do audiovisual e dos radiodifusores e, mais recentemente, dos prestadores de serviços nas redes digitais, implica a generalização da gestão colectiva.

Nalguns casos, a gestão colectiva é mesmo obrigatória, como resulta da Directiva Europeia n.º 93/83/CEE, de 27 de Setembro de 1993, relativa à coordenação de determinadas disposições em matéria de direito de autor e direitos conexos aplicáveis à radiodifusão por satélite e à retransmissão por cabo.

Cada vez mais, em todos os domínios, é previsível o aparecimento de entidades de gestão colectiva de direitos habilitadas e vocacionadas para a referida gestão.

No ambiente digital é muito possível que se vá assistir ao aparecimento de enérgicas entidades, capazes de gerirem uma grande variedade de direitos.

A questão dos direitos de autor passa também pelo melhoramento na sua cobrança e distribuição. Com as novas tecnologias, em particular a Internet, esses direitos estão fortemente ameaçados e, por essa razão, a gestão colectiva de direitos de autor torna-se imprescindível.

Deverá existir uma efectiva fiscalização da aplicação das regras de protecção dos direitos de autor e o sancionamento das respectivas infracções. Nesse sentido, o regime previsto no CDADC, com a aplicação de pena de prisão e multa, mostra-se eficaz no combate às práticas ilegais neste domínio, uma vez que a simples sanção contra-ordenacional consubstanciada na aplicação de uma coima não será, por si só, suficiente para o afastamento de práticas crescentemente generalizadas.

É, assim, indispensável adaptar a actual legislação às novas realidades do mercado.

Evidencia-se a urgência de criação de mecanismos que, não privando os titulares dos direitos da compensação equitativa pela sua obra, possam legitimar de forma ágil a utilização das obras protegidas em tempo útil, cenário que só será possível com a gestão colectiva uma vez que esta procede à fixação de uma remuneração equitativa destinada a compensar os titulares de direitos por todas as utilizações efectuadas.

Direito ao princípio de "neutralidade técnica"

Demorou muito tempo para que os consumidores conseguissem ter uma perspectiva clara dos seus direitos quando usam material audiovisual tradicional.

Algumas práticas existentes no ambiente digital ignoram os direitos do consumidor que estão estabelecidos. Actualmente, a indústria define quase por si só os termos, decide que informação é distribuída, o que é justo e o que é legal, como deve ser usado o material, etc.
Na prática isso corresponde a negar aos consumidores os benefícios das novas tecnologias: por exemplo, as pessoas com deficiências visuais precisam de converter os conteúdos para outros formatos que lhes permitam ler e interpretar (particularmente em Braille), acção que não é normalmente permitida pelos sistemas de GDD.

Relativamente a este e a outros exemplos, importa que se encontrem políticas que assegurem que consumidores e autores beneficiem do desenvolvimento tecnológico. A indústria não deve ter o poder de impor controlo excessivo sobre os conteúdos digitais.

Direito á protecção da privacidade

Se decidirmos descarregar um programa no nosso computador individual podemos estar a receber ao mesmo tempo um programa adicional, sem sabermos. Sem o nosso conhecimento e sem autorização, esse software adicional pode fazer duas coisas que não deve fazer: pode alterar a programação ou o sistema operativo do nosso computador – para limitar a forma como usamos o material que descarregámos e pode também enviar informação dos nossos hábitos e preferências de navegação.

Com o desenvolvimento de novos suportes digitais (incluindo a televisão digital), será possível em breve aos fornecedores de serviços de conteúdos conhecer as convicções políticas ou religiosas ou os centros de interesse de um utilizador, como uma função dos programas que ele está a ver.

Ao mesmo tempo que os sistemas de GDD se desenvolvem e se tornam mais sofisticados, será cada vez mais difícil permanecer anónimo e preservar a privacidade.

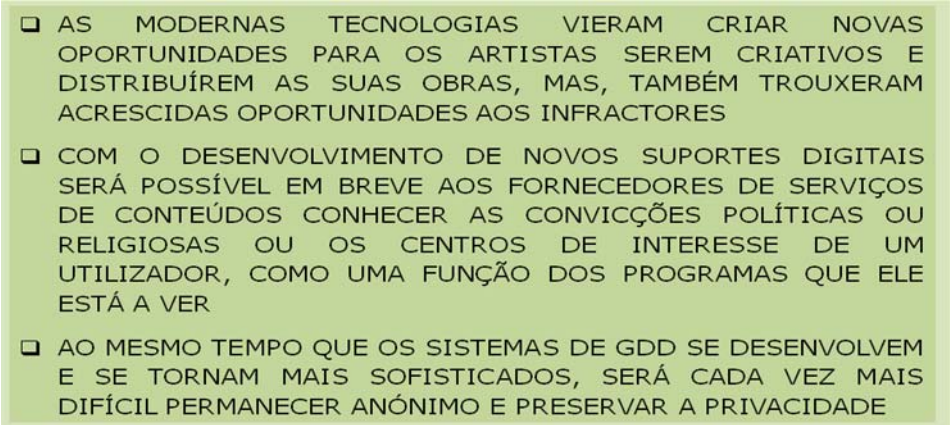

Figura IV 18 - Impacto da evolução dos Direitos Digitais na esfera da privacidade individual e colectiva

G. A PERSPECTIVA DAS ORGANIZAÇÕES

TRANSACÇÕES ELECTRÓNICAS

Baseamo-nos mais uma vez no texto "Sociedade da Informação, Sociedade (in)Segura?" [Veríssimo2007X].

O comércio electrónico tem vindo a desenvolver-se paulatinamente, mas a não ser que algo mude drasticamente, é a digitalização da banca, ou talvez mais propriamente do sector financeiro, que será o pivô de toda essa evolução. E se vimos há alguns anos atrás o pioneirismo da banca na introdução da informática na gestão da sua actividade, interna e interbancária, não observamos o mesmo sucesso na introdução da mesma informática para "vender", ou aquilo que se designa por B2C (do negócio para o consumidor), mormente no grande expoente deste negócio, a banca electrónica na Internet.

A resposta para esta questão apaixonante parece residir menos em factores tecnológicos sofisticados e mais, mas ironicamente, em alguns dos factores que fizeram o sucesso dos bancos de “pedra e cal”: intuição, conservadorismo, arrogância e complacência legal. Mas se foram factores de sucesso, porque ameaçam agora esse mesmo sucesso? Porque o mundo virtual é drasticamente diferente.

Durante muitos anos, a análise de risco foi eminentemente intuitiva e bem sucedida. Essa intuição ainda não se conseguiu transportar para os riscos do negócio virtual, levando à incapacidade de destrinçar situações extremamente arriscadas para o negócio, sejam elas a diferença entre falsificar uma assinatura num cheque ou falsificar um certificado digital, ou saber qual a efectiva autenticidade de uma palavra de passe, ou perceber que o PC de um cliente remoto não é «o próprio ao balcão», ou ainda qual é a diferença entre roubar PINs num ATM ou através da Internet.

Tendo sido dos primeiros a utilizar a informática, os bancos tratam-na essencialmente como um custo e assim têm feito ao longo dos anos. No entanto, hoje em dia ela é não só um factor produtivo, como se está a transformar *no* meio de negócio: as agências de pedra-e-cal passam a virtuais, os clientes tornam-se agentes de software na web, as notas de euros passam a posições de memória num *smart-card*, as cabalísticas assinaturas caligráficas são substituídas por funções criptográficas. Esta evolução requer investimento, em tecnologia e recursos humanos de alto nível que dominem o negócio virtual, a informática moderna, e tem sido muito difícil aos bancos compreendê-lo.

Pode parecer surpreendente como tem escapado à compreensão dos bancos que uma percentagem significativa dos problemas de segurança das operações remotas via Internet, tipo *phishing* por exemplo, se deve à falta de autenticação do lado do servidor, em adição à do lado do cliente, o que se chama autenticação mútua.

É essencial quantificar e fazer pagar os custos da falta de segurança informática e transferir para os operadores dos serviços *online* o ónus das falhas e fraudes, erradamente colocado do lado dos clientes, por vezes, de forma injustificada.

Mais do que para o consumidor, esta situação prejudica as próprias empresas porque as desmobiliza de desenvolverem processos tecnologicamente mais evoluídos e por isso mais competitivos. Esta questão abrange os legisladores e/ou regulamentadores, sem cuja acção moralizadora as empresas não evoluirão para melhores práticas.

A ESPIONAGEM

A espionagem é uma actividade que cria situações em que qualquer um de nós pode ver-se envolvido nalgum momento da vida sem que seja o seu autor ou executante consciente.

A sua concretização pode ter motivações associadas à economia, à política, ou a questões mais chãs como será o desejo de prejudicar uma pessoa simplesmente por inveja.

Ninguém tem dúvidas de que foram necessárias acções de espionagem por parte da Al-Qaeda para a preparação dos ataques terroristas de 9 de Setembro de 2001 e de 11 de Março de 2004 [27], tendo sido muito útil aos terroristas informação que estava disponível na Internet.

Segundo uma definição simples, existente na *Wikipedia*, **Espionagem** é a prática de se obter informações de carácter secreto ou confidencial dos rivais ou inimigos, sem autorização destes, para se alcançar certa vantagem militar, política ou económica.
Essa prática manifesta-se geralmente como parte de um esforço organizado (ou seja, como acção de um grupo governamental ou empresarial).

De um modo geral, a definição refere-se a um Estado que espia inimigos potenciais ou reais, principalmente para finalidades militares, mas ela abrange também a espionagem envolvendo empresas, conhecida como espionagem industrial, e de outros tipos

Nenhum serviço secreto de um Estado usa a palavra "espionagem" no seu nome ou para descrever as suas actividades de recolha de informações ou inteligência, embora todos declarem fazer “contra-espionagem”. Muitas nações espiam os seus inimigos de forma rotineira, mas também os seus aliados, embora geralmente o neguem.

A duplicidade que envolve a utilização do termo espionagem deve-se ao facto de essa actividade ser frequentemente ditada por objectivos secretos e por interesses publicamente inconfessáveis, enquanto os rivais ou inimigos procuram sempre denunciá-la e condená-la.
Um **Espião** é um agente utilizado para obter tais segredos.

Importa compreender que conforme os contextos - políticos. Legais, sociais, económicos e outros – em diferentes épocas e ambientes, a espionagem podem ser levada a efeitos usando métodos legais (embora sejam sempre ténues as linhas de fronteira entre o legal e o ilegal).

[27] Referidos habitualmente na Comunicação Social por 9-11 e 11-M.

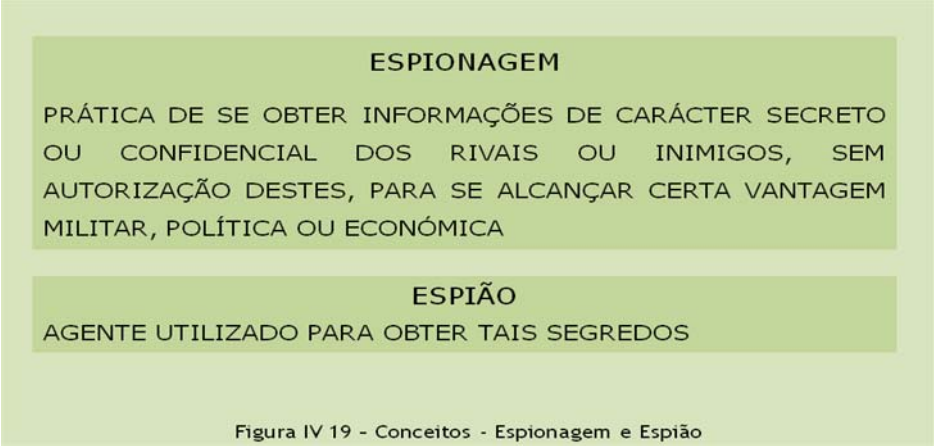

Figura IV 19 - Conceitos - Espionagem e Espião

De um modo geral, o presente texto procura abordar com maior ênfase as vertentes relacionadas com o que é criminoso.

As actividades criminosas tradicionais têm vindo (e continuarão) a ser transpostas para as redes electrónicas e para o ciberespaço, associadas à evolução da sua própria natureza.

Apresentamos a seguir um quadro resumido que procura ilustrar esta evolução:

Categoria de actividades	Acedem e utilizam sistemas de informação e a sistemas de	Através de acções de	Para fins de
Baixo nível	Comunicações	Entrada ilegal Furto de recursos	Vingança Vandalismo
Fraudulento	Comunicações Financeiros	Furto Observação de hábitos e da aplicação das regras legais	Extorsão
Crime organizado	Comunicações Financeiros	Furto Observação de hábitos e da aplicação das regras legais	Extorsão
Grupos marginais: Políticos; Religiosos e Outros	Órgãos de Comunicação Social Comunicações Publicidade	Furto	Sabotagem Disrupção Guerra de Informação
Espionagem Industrial	Negócio	Furto	Sabotagem
Espionagem Internacional	Recolha de dados e sua análise	Espionagem	Guerra de Informação
Terrorismo	Comunicações	Furto Procura de alvos "Inteligência"	Guerra de Informação Sabotagem

Figura IV 20 - Evolução das actividades criminosas

Não foi (nem é) raro que serviços de informações dessem cobertura a actividades paramilitares (incluindo assassinato, sequestro, sabotagem, guerra de guerrilha e golpes de estado). Desde o fim da Guerra Fria, que os serviços de informações e espionagem estão sobretudo preocupados com as actividades de organizações terroristas e com o tráfico de drogas.

Em muitos países, a espionagem é crime punível com prisão perpétua ou pena de morte. Nos EUA, por exemplo, a espionagem é ainda um crime capital, embora a pena de morte seja raramente aplicada nesses casos pois, em geral, o governo oferece ao acusado um abrandamento da pena em troca de informações.

A espionagem, quando praticada por um cidadão do próprio Estado alvo, é geralmente considerada como uma forma de traição.

No domínio económico, a Informação tem sido um factor essencial para o sucesso de qualquer negócio no mercado global, e a maior parte das organizações sabe que precisa de proteger os seus activos informacionais relativamente à deterioração da sua qualidade e à sua divulgação indevida, quer elas sejam acidentais ou maliciosas.

Contudo está a acontecer uma nova revolução no nível global: o Comércio Electrónico.

Esta nova forma de efectuar transacções comerciais vai para além do "simples" tratamento da informação, redefinindo a relação entre a empresa e os seus clientes, parceiros, fornecedores, vendedores e concorrentes. É claro que este novo ambiente só se tornou possível por via das tecnologias de Informação e da Comunicação.

Diversos atributos destas tecnologias têm impacto significativo sobre o comércio electrónico o que levou à redefinição do próprio negócio. Eles incluem: conexão e acesso global, rapidez de disponibilidade para o mercado[28] e requisitos legais e de regulação. Simultaneamente, esses mesmos atributos desempenham um papel importante potenciando ameaças orientadas para as infra-estruturas de informação do negócio.

Numa fase inicial da Informática, quando os negócios automatizaram as suas operações, a informação estava armazenada e era processada em grandes computadores[29], isolados e controlados fisicamente.

Hoje a informação pode residir em grandes equipamentos "servidores" conectados em rede e em muitos equipamentos "clientes" (habitualmente estações de trabalho mais pequenas[30]).

Essas redes – de âmbito local, metropolitano, ou nacional – estão cada vez mais ligadas a outras redes fora da organização individual ou regional, primariamente através da Internet.

[28] *Time to market.*

[29] *Mainframes*.

[30] *Desktops*.

Essas interligações atravessam fronteiras e interligam negócios, casas, escolas, serviços públicos, etc.

Toda esta evolução alargou e modificou o âmbito de acções de observação e tratamento da informação em formato digital, muitas vezes para fins diferentes para os quais todo o sistema foi criado.

ESPIONAGEM ELECTRÓNICA

Desde sempre que a História nos tem mostrado que muitos dos dispositivos e soluções tecnológicas que são em cada momento disponibilizados para uso civil (e que correspondem sempre a uma geração de dispositivos e sistemas que nunca é a mais recente) são sucedâneas das tecnologias desenvolvidas para fins militares.

O salto que a evolução electrónica (entre outras) deu a partir da II Guerra Mundial, e que permitiu por sua vez a evolução de tecnologias para tratamento automático da Informação (originalmente designada por Informática) e de Comunicações, tem vindo desde há muito a disponibilizar dispositivos e sistemas que possibilitam acções de espionagem mais eficientes e com maior alcance e abrangência de alvos, segundo formas que não podem deixar de assustar o cidadão preocupado com a facilidade com que se pode ter acesso a muito da sua vida quotidiana.

À espionagem electrónica é aquela que é realizada usando os modernos meios electrónicos. Muitos desse meios são digitais, e como tal, podem recolher, armazenar, modificar, apagar e transmitir informação.

São exemplos de espionagem electrónica actualmente levadas a efeito com o beneplácito de alguns Estados:

Escutas Na maior parte dos países este tipo de espionagem pode ser feito legalmente (segundo autorização judicial específica) para suporte a investigações de natureza policial e de natureza securitária.
Existe um sistema americano, que tem abrangência transnacional e que está disponível para os países anglo-saxónicos, sob direcção dos EUA, e que consiste num sistema que permite a gravação constante de todas as comunicações sem fios realizadas nos EUA e na Europa que utilizem satélites.
Este sistema é conhecido por *Echelon*, e suscitou há pouco tempo atrás acesa discussão por parte do Parlamento Europeu.
Após a gravação, poderá ser aplicado *software* especial (como por exemplo um designado por *Carnivore* utilizado pela CIA) que consegue filtrar transmissões com determinadas características e tratá-las autonomamente a seguir.
É claro que, utilizando dispositivos e sistemas que se encontram sem grande dificuldade no mercado, é possível escutarem-se conversas telefónicas (tanto de telefones móveis como de telefones fixos) de forma mais limitada… obviamente de modo ilegal.

Rastreio de circulação

È possível fazer-se algum rastreio electrónico de pessoas e bens (assim como de animais) caso tenham consigo dispositivos electrónicos que permitam sua localização permanente, nomeadamente: telemóveis, dispositivos de localização baseados em GPS, antenas de RFID.

Existem outros dispositivos, normalmente de uso autonomizado, que são baseados no som e na visão, os quais também podem apoiar um espião no rastreio de pessoas e bens.

Os exemplos mais comuns e que estão em expansão numérica por todo o mundo, são as câmaras de videovigilância que são instaladas em muitos sítios (normalmente públicos) e que permitem o registo e o arquivo de imagens sobre tudo o que acontece na respectiva área de cobertura.

Tal como acontece com todos os outros casos em que há registo e armazenamento de informação (sob qualquer forma), os aspectos mais sensíveis que se relacionam com estas acções de espionagem (habitualmente classificadas pelas entidades públicas como sendo de simples vigilância) residem na utilização que é feita posteriormente de todas essas informações.

Não é difícil de entender que o uso indevido dessas informações é relativamente fácil e facilita situações de intrusão de privacidade (individual e colectiva) e possibilita até situações extremas de manipulação do tipo *bigbrotheriano.*

Exploração do ciberespaço

A realização de acções no ciberespaço por parte de pessoas e organizações, com ênfase para o comércio electrónico, cria possibilidades muito apetecidas para actividades ilícitas de diversa natureza.

É frequente o "furto de identidade" [31] a utilizadores que realizam operações de natureza financeira – normalmente para compra e venda *on-line* de produtos – o que corresponde a acções concretas de espionagem electrónica, para que os piratas possam seguidamente realizar eles próprios acções diversas aquisições ou outras acções ilícitas no ciberespaço ou na vida real (que até pode estar associada com terrorismo) assumindo para o efeito a identificação do legítimo dono, a quem furtaram (ou copiaram) a respectiva identidade digital.

Estes aspectos constituem uma das preocupações que porventura mais preocupam hoje em dia os indivíduos mais atentos e as autoridades de todos os países.

Este tipo de furto sempre foi praticado no mundo, naturalmente que antes era concretizado fisicamente, e que tem assumido proporções e consequências que são cada vez mais importantes devido à sua crescente utilização por terroristas. O ciberespaço também não é imune a escutas de mensagens trocadas entre utilizadores – por correio electrónico, através de salas de conversação em linha, por conversas baseadas em comunicações do tipo "voz sobre IP", etc.

[31] Entende-se por FRAUDE todo o engano ou acção de má fé realizada com o fim de se procurar um benefício ilícito em prejuízo e a expensas de outro, ou, com outras palavras, todo o acto de lesão que se causa no património alheio de forma não violenta por meio de ardil ou engano e com intenção de lucro.

Figura IV 21 - Exemplos de Espionagem Electrónica

Em muitos casos dos que referimos atrás, a espionagem é potenciada – a montante e a jusante – pela utilização de potentes sistemas informáticos compostos por *hardware* e com *software* mais ou menos avançados e com bases de dados que permitem o a pesquisa e o cruzamento de informações mais ou menos sensíveis sobre pessoas, organizações, etc.

Como decorre do que dissemos antes, as tecnologias – electrónicas ou outras quaisquer – não asseguram por si só acções de espionagem "não oficiais".

No entanto, elas facilitam enormemente a realização dessas acções e a sua eficácia – tanto em rapidez, como em extensão, em abrangência e em focalização "cirúrgica".

Finalmente importa referir que os recentes atentados terroristas de 9-11 constituíram um marco indelével na história da segurança mundial moderna, não só pelo acto em si e pelas suas consequências directas, mas também por ter facilitado terreno para a implementação de fortes e alargadas medidas oficiais por parte de um Estado com objectivos securitários, mas com um âmbito tal que aumenta fortemente muitos outros riscos laterais relativamente à protecção dos direitos dos cidadãos, e particularmente os que se relacionam com a sua privacidade.

Na sequência do 9-11 o presidente dos EUA assinou uma lei, designada por *Patriot Act*, que expande a autoridade das agências americanas de *law enforcement* para o fim declarado de combate ao terrorismo nos EUA e no estrangeiro.

De entre as acções que são cobertas pela lei, está a autorização das agência de *law enforcement* para investigar comunicações (telefónicas e de correio electrónico) e registos – (médicos, financeiros e quaisquer outros).

ESPIONAGEM INDUSTRIAL

O acesso a informação empresarial sensível é o objectivo de muitas empresas e países estrangeiro.

Por vezes quem quer obter informação de outrem (organizações ou indivíduos) não se preocupam com a forma que a informação toma. Quer ela esteja em formato electrónico ou tenha sido deitada para o lixo, isso é irrelevante conquanto se consiga obter essa informação.

Na maior parte dos programas de segurança das organizações existem sobretudo preocupações com a segurança técnica, o que deixa obviamente a informação vulnerável a métodos básicos de espionagem.

Os profissionais de segurança da informação focam os seus esforços naquilo que melhor conhecem. Assim quando um orçamento é definido, ele vai reflectir as necessidades que foram percepcionadas, as quais correspondem basicamente a mecanismos de segurança técnica.

A informação existe e é transportada sob muitas formas, e em todas ela deve ser protegida.

A segurança da informação não é a segurança dos computadores, ela integra segurança física, pessoal, operacional e técnica.

Para atacar uma organização no seu ponto mais fraco, os espiões industriais sabem como contornar praticamente qualquer parte de um programa de segurança, mesmo as que são consideradas como "fortes".

Métodos de espionagem industrial

Actualmente é relativamente fácil a uma qualquer organização (que disponha de motivação e recurso financeiros suficientes) conseguir os serviços operacionais da *Inteligência* da antiga União Soviética, que actuam como *freelancers* para quem lhes pagar mais ou integrando empresas especializadas em *Inteligência*.

Essas empresas são detentoras de know-how muito bem testado em contextos reais.

Infelizmente a maior parte as empresas não estão precavidas quanto às ameaças que elas representam e aos métodos que empregam. Alguns deles podem ter natureza legal.

(a) Métodos legais

Esses métodos incluem principalmente a compra de empresas ou de produtos, havendo dessa forma uma transferência de tecnologia para quem era anteriormente um adversário ou concorrente.

Embora essas situações ameacem seriamente a competitividade de um país, há muito pouco que possa ser feito para as contrariar.

A prática de *joint ventures* com empresas concorrentes também possibilita boas oportunidades para uma empresa deixar passar para uma outra empresa informação sensível. Estas situações são algo complicadas pois por vezes a única forma de uma empresa conseguir expandir a sua actividade para outro país só é viável através da constituição de uma *joint venture* como empresas desse país.

Numa outra vertente, a informação de "fonte aberta" também fornece um conhecimento utilíssimo para as empresas. A informação aberta toma habitualmente várias formas, incluindo artigos em papel, relatórios anuais de contas, documentos sobre patentes pendentes, documentos legais, informação de *marketing*, etc. Revendo essa informação, uma empresa pode ficar a conhecer uma grande quantidade de informação acerca de um concorrente e dos seus produtos.

Se uma organização não consegue gerir de forma criteriosa a divulgação da sua informação, ela está sujeita a sofrer perdas enormes.

Por outro lado, o despedimento de empregados também pode resultar na transferência de conhecimento para uma organização concorrente. Embora muitos ex-empregados se mantenham íntegros e não divulguem informações sensíveis sobre o seu anterior empregador, é inevitável que haja transferência de conhecimento. É impossível que não seja tomado em conta o conhecimento que um novo empregado adquiriu e consolidou, naturalmente sobre o seu anterior emprego.

Muitas empresas frequentam feiras e conferências no sentido de obterem informações sobre os seus concorrentes. Tipicamente essas empresas enviam os seus empregados a esses eventos para ficarem a par das últimas pesquisas desenvolvidas pelos seus concorrentes.

(b) Métodos ilegais

Muitos dos métodos referidos anteriores são aplicados segundo uma fronteira com a ilegalidade que é difusa.

Muitos dos casos de espionagem industrial envolvem o uso de "gente da casa" [32] que são usados para furtar informação. A cooperação de *insiders* pode ocorrer de muitas maneiras, dependendo das circunstâncias.

Tal como acontece na espionagem tradicional, o recrutamento de "toupeiras"[33] é muito usado. Essas pessoas abusam dos acessos que têm normalmente, para furtar informação ou mesmo só

[32] *insiders*

para copiar informação a que já tem acesso. Elas estão bem estabelecidas dentro do alvo, e movimentam-se dentro da organização sem serem controlados.

Há métodos menos sofisticados mas ainda assim efectivos de desfrutar da informação de outrem.

A espionagem pode envolver a intrusão em edifícios e escritórios, para furtar a desejada informação. Os espiões industriais atravessam espaços dos escritórios (fechados e abertos), vasculham armários, examinam computadores que não estão protegidos, etc. Os espiões vão também atrás dos contentores e caixotes de lixo à procura da informação que pretendem.

Figura IV 22 - Métodos de Espionagem Industrial

Prevenção da espionagem industrial

Quando os métodos usados pelos espiões industriais são os mesmos dos usados pelos espiões tradicionais, pode-se prevenir a espionagem industrial com contramedidas usadas para prevenir a espionagem tradicional.

Podemos considerar que um programa compreensível de segurança integra:

Segurança técnica	São as contra medidas que se destinam a reduzir as vulnerabilidades de sistemas electrónicos. Elas procuram assegurar a confidencialidade, a integridade, e a disponibilidade de computadores e redes. Um bom sistema de segurança técnica também protege outros sistemas electrónicos, como por exemplo o correio de voz.
Segurança operacional	Orienta-se para os processos de negócio que são usados na empresa e em que a informação pode ser comprometida através de meios não técnicos. Algumas organizações – públicas e privadas – adoptaram explicitamente uma política que permite o acesso à informação somente numa base de "necessita de saber?"[34] a qual ajuda a prevenir a desnecessária divulgação de informação e assim reduzir os riscos. Com o mesmo fim, são aconselháveis políticas que restrinjam o uso de linhas de comunicação abertas (telefone, Internet) por parte dos empregados da organização.

[33] "Toupeiras" são empregados de uma empresa-alvo, ou alguém com acesso a essa empresa, que concorda em cooperar com os criminosos, habitualmente em troca de dinheiro.

[34] *Need to know*.

A segurança operacional é um tema complexo, e requer normalmente um estudo aprofundado do modo como uma organização (quer seja uma empresa ou de outro tipo) desenvolve a sua actividade.
As pessoas devem saber qual a informação que devem proteger, e especificamente como o fazer.

Segurança física

Muitas vezes a informação é comprometida devido a "simples" acções de penetração e furto.
Para dificultar isso, é importante que os acessos físicos às instalações sejam cuidadosamente regulados e controlados.
Essa regulação tanto inclui limitações para os visitantes (clientes, fornecedores, outros) como para os empregados.
Por norma, ninguém deverá vaguear facilmente por todas as instalações da empresa, e todos os empregados devem usar cartões de identificação com indicações que ajudem a uma fácil leitura visual de qual o nível de acesso correspondente.
Obviamente que é fundamental que haja uma prática de segurança que encoraje todos empregados a olharem para o cartão de identificação.
Deve também haver regras de segurança dirigidas para situações associadas ao dia-a-dia de cada empregado dentro da empresa.
Por exemplo, deve haver uma política de "secretária livre"[35], que requeira que a informação sensível (seja qual for o suporte em que se encontra) seja guardada e fechada.
Deve também ser norma bloquear o posto de trabalho pessoal sempre que empregado se afasta do mesmo, de modo prevenir-se contra o aceso por terceiros.

Segurança pessoal

A empresa deve prestar especial atenção aos empregados com acesso a informação sensível, assegurando uma adequada e não intrusiva observação dessas pessoas.
Algumas organizações não prestam a devida atenção aos acessos a que estão autorizados alguns tipos de empregados como: de limpeza; porteiros; guardas de segurança; contínuos.

Figura IV 23 - Prevenção de Espionagem Industrial

[35] *Clean desk*.

H. A PERSPECTIVA DOS ESTADOS

DEMOCRACIA ELECTRÓNICA

Segundo o estudo "Democracia Electrónica em Portugal" [APDSI200999]: A democracia electrónica vai muito para além da votação e disponibilização de informação sobre os candidatos através da Internet: trata-se de uma nova forma de fazer com que o cidadão comum participe em discussões e interacções com os poderes políticos, fazendo chegar a sua voz, não apenas durante as campanhas eleitorais, mas também nos períodos intercalares e a propósito dos problemas da sua vida quotidiana.

Muitos dos desafios que esta situação comporta serão culturais e estruturais da democracia moderna, não se encontrando necessariamente relacionados com as oportunidades e constrangimentos associados à utilização de TIC. Não deve ser afastada, contudo, a possibilidade de as TIC reunirem características que permitam a sua utilização no sistema político, criando oportunidades para o envolvimento dos cidadãos.

Uma primeira área de análise da utilização das TIC no sistema político corresponde ao acesso à tecnologia e a meios que possibilitem a expressão da vontade política, por parte dos cidadãos. Apesar de a Internet não ser a única tecnologia a poder desempenhar um papel relevante neste domínio, ela constitui-se como um recurso central e, em parte, também como um indicador para a caracterização indirecta do acesso a outras tecnologias.

Ao estender as fronteiras da Democracia electrónica estaremos naturalmente a intensificar a literacia do cidadão relativamente às TIC e a fomentar uma aculturação crescente e sustentada relativamente ao uso das TIC.

Como já referimos noutra ocasião, para nos protegermos – enquanto indivíduos e enquanto colectivo – é importante que estejamos "razoavelmente" aculturados relativamente às questões de segurança que mais podem afectar essa protecção, desempenhando aqui as TIC um papel de enorme importância… tanto como veículo facilitador de ameaças a essa segurança como também utensílio de apoio à nossa protecção.

A Democracia Electrónica envolve toda uma tradução e transferência dos processos tradicionais do funcionamento da sociedade democrática para a esfera digital, sobretudo o aspecto mais emblemático: a *votação electrónica* [Veríssimo, 2007].
Existem várias razões para uma sociedade enveredar pela votação electrónica, das quais as principais serão: (i) ajudar a assegurar as condições básicas para eleições livres e justas, em sociedades em que essas condições possam estar ameaçadas, por exemplo, por fraude ou pressão; (ii) melhorar as condições qualitativas das eleições num sistema já estável, por exemplo, a velocidade do escrutínio.

Existem bastos sistemas de voto electrónico que são mais do que insuficientes, mesmo que apresentados como «estando presentes em vários mercados», porque isso não é necessariamente prova de qualidade.
Como perceber, então, se um sistema de voto electrónico serve os objectivos de uma democracia estável e evoluída como a portuguesa? Parece-me que há dois factores que deviam ser dados como garantidos face a quaisquer escolhas tecnológicas que fossem feitas: (a) manutenção da confiança dos cidadãos no sistema de voto; (b) condições de confiabilidade e segurança no mínimo ao nível das dos sistemas tradicionais.
Significa isto que essas mesmas tecnologias devem justificadamente garantir que previnem: quebra do anonimato ou da privacidade; modificação ou eliminação dos votos individualmente expressos pelos eleitores; falhas de contagem ou de robustez do sistema; problemas de usabilidade.
É imperativo que um sistema de voto electrónico obedeça a especificações que possam ser verificadas e auditadas, face ao projecto, concretização e modo de operação do mesmo, no sentido de saber se cumprem, além dos objectivos de funcionalidade, os de confiabilidade e segurança. Para isso é necessário que toda a informação possa ser escrutinada com toda a transparência, por entidades independentes, com a competência adequada e representando a sociedade.
O voto é uma operação crítica para a sociedade. Todas as operações críticas de cariz tecnológico são certificadas e auditadas nos países desenvolvidos (aeronáutica, telecomunicações, energia, etc.), porque não o haveriam de ser os sistemas da democracia electrónica?

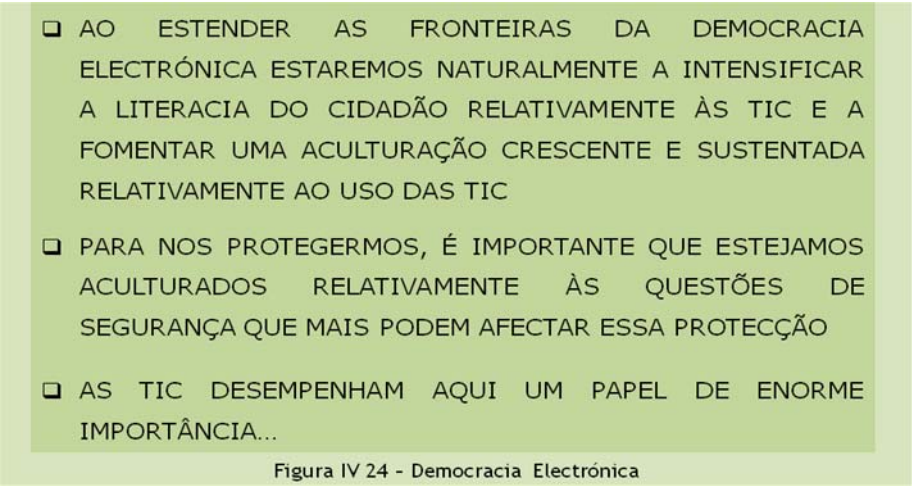

Figura IV 24 - Democracia Electrónica

A SEGURANÇA DAS INFRA-ESTRUTURAS CRÍTICAS

O termo genérico “Infra-estrutura” engloba as pessoas, organizações, processos, produtos, prestações, fluxos de informação dessas entidades, assim como as instalações e os equipamentos técnicos e físicos que, isoladamente ou em conjunto, permitem o funcionamento da sociedade, da economia e do estado.

Fala-se muito dos riscos que pendem sobre as redes de electricidade, de gás e de água, a rede Internet, as redes de telecomunicações, as redes de controlo de tráfego terrestre, aéreo, marítimo e de emergência [Veríssimo, 2007]).

Todas estas infra-estruturas pertencem àquilo que se designa por Infra-estruturas Críticas (IC): sistemas cujo eventual mau funcionamento tem um impacto negativo significativo para uma sociedade ou nação.

INFRA-ESTRUTURAS CRÍTICAS (IC)	INFRA-ESTRUTURAS DE INFORMAÇÃO CRÍTICAS (IIC)
SISTEMAS CUJA DISPONIBILIDADE OU DESTRUIÇÃO PODERÃO TER UM EFEITO DEBILITANTE SOBRE A SEGURANÇA NACIONAL E SOBRE O BEM-ESTAR ECONÓMICO E SOCIAL DE UMA NAÇÃO	COMPONENTE DA ESTRUTURA DE INFORMAÇÃO GLOBAL E NACIONAL QUE É ESSENCIAL PARA ASSEGURAR A CONTINUIDADE DOS SERVIÇOS PRESTADOS PELAS INFRA-ESTRUTURAS CRÍTICAS

Figura IV 25 - Infra-estruturas Críticas (IC) e Infra-estruturas de Informação críticas (IIC)

Durante muitos anos, funcionaram mais ou menos bem, e discretamente, como convinha. Hoje em dia, um conjunto de factores fez a situação mudar drasticamente: liberalização do mercado; abertura a múltiplos operadores; computorização e interligação em rede; espectro do terrorismo.

Por razões culturais, a análise de risco sobre as IC é frequentemente centrada numa de duas visões alternativas: considerar que as infra-estruturas virtuais só são atacáveis virtualmente; ou considerar que as infra-estruturas físicas só são atacáveis fisicamente. A verdade é que, tanto um serviço web pode perecer por um ataque à bomba ao centro de dados, como uma central eléctrica pode pegar fogo por um ataque vindo pela rede.

As IC tornaram-se progressivamente "redes de computadores" específicas, em que alguns desses computadores, em lugar de receberem correio electrónico ou navegarem na *World Wide Web*, são controladores de máquinas eléctricas, de bombas de água, de sinais de tráfego, de estações de telefone móvel ou de radar, de comutadores e encaminhadores Internet. A estrutura física das IC ficou assim exposta, quando antes só podia ser acedida local e internamente.

A liberalização do mercado e a abertura a múltiplos operadores, uma realidade incontornável, complicou o cenário do ponto de vista da divisão de responsabilidades e da introdução de tecnologias digitais comercialmente competitivas mas, por isso mesmo, com um grau de vulnerabilidades apreciável.

Convencionou-se denominar de infra-estruturas de Informação Crítica (IIC) as redes de computadores desempenhando funções críticas para a sociedade, incluindo não só a Internet e outras redes de

informação, mas também o suporte informático do controlo e comando das redes de telecomunicações, controlo de tráfego aéreo e terrestre, eléctricas, água, etc.

É hoje em dia assente por vários peritos que: as vulnerabilidades das infra-estruturas críticas são múltiplas; o nível e o tipo de ameaças a que estão sujeitas, varia com as condições políticas, geográficas e mesmo temporais. De tal modo, que os riscos em que essas infra-estruturas incorrem, tornaram-se muito mais difíceis de avaliar.

Mas sendo os riscos possíveis, serão prováveis? Dividamos os riscos em: riscos físicos acidentais, riscos físicos propositados, riscos informáticos acidentais, e riscos informáticos devidos a ciberataques. Ganha progressivamente corpo, em vários sectores, que os riscos mais elevados se centram hoje nas infra-estruturas de Informação Críticas (IIC), que pertencem à categoria dos ciberataques.

Os ciberriscos, isto é, os riscos para as IC veiculados pela sua infra-estrutura de informação e operação, tornaram-se mais importantes do que os riscos físicos. Existindo um conjunto de ciberataques com a potência e precisão adequadas, o risco de falha das infra-estruturas críticas é elevado.

A Internet e a interligação global são inegavelmente o veículo destes ataques. As vulnerabilidades dos sistemas são deficiências e insuficiências dos fabricantes, operadores, utilizadores e em última análise, legisladores e governantes.

O esforço que as sociedades dedicaram a tornar as suas ICs mais modernas, operacionalmente seguras e eficientes, tornando mais eficaz a gestão e supervisão dos riscos físicos das mesmas, revelou-se afinal uma faca de dois gumes.

A negação da realidade não vai ajudar a sociedade. É necessário pôr no terreno as medidas adequadas, numa área em que pode haver auto-suficiência nacional, começando pelos aspectos tecnológicos: suporte inequívoco à investigação e desenvolvimento de arquitecturas informáticas inovadoras para infra-estruturas de informação críticas e investimento na sua concretização, com partilha de esforços entre Estado e empresas. Este esforço deverá ser complementado com medidas societárias importantes: análises de risco que influenciem o planeamento e ordenamento territorial das IC e moderem as suas interdependências; regulamentação eficaz acerca de segurança e fiabilidade informática, que seja de facto responsabilizadora dos fornecedores de tecnologia e serviços nos sectores abrangidos e punidora dos transgressores.

De um modo geral, a protecção das IC tem por fim reduzir a probabilidade de ocorrência de danos e minimizar a amplitude das perturbações que estão associadas em resultado de falhas ou de destruição dessas IC assim como minimizar a duração da sua indisponibilidade.

A GUERRA DA INFORMAÇÃO

Mao Tse-Tung aconselhava: “para conseguirmos a vitória devemos, tanto quanto possível, tornar o inimigo cego e surdo, selando os seus olhos e os seus ouvidos, e conduzir os seus comandantes à distracção criando confusão nas suas mentes.”

O conceito de **Guerra da Informação**[36] surgiu em meados dos anos 90 como um tema quente de discussão. De acordo com um documento Americano, “Guerra de Informação” é o “conjunto de acções tomadas no sentido de afectar a informação e os sistemas de informação de um adversário enquanto se defende a sua própria informação e os seus sistemas de informação”. Para o efeito deste texto, tomemos como suficiente esta definição.

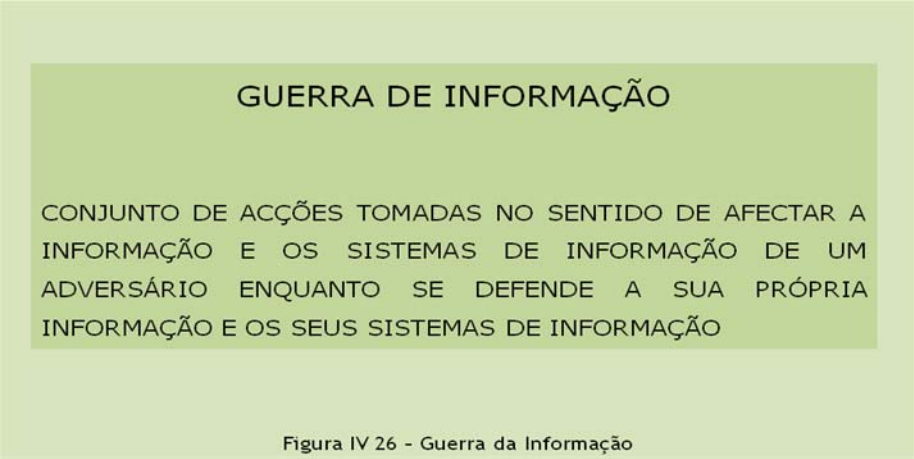

Figura IV 26 - Guerra da Informação

No centro da Guerra de Informação está obviamente a Informação. A informação guia a tomada de decisão em tempo de paz e de guerra, a um nível estratégico (por exemplo: decisão de declaração de guerra), operacional (por exemplo: decisão de deslocar uma divisão militar em direcção a um ataque), ou táctica (por exemplo: decisão para ordenar a um avião que se prepare para acção militar).

O objectivo de uma Guerra de Informação é de afectar o processo de tomada de decisão do adversário e implementar acções associadas para garantir a sua própria vantagem.

O resultado para o inimigo pode ser: decisões erradas, decisões atrasadas ou nenhuma decisão de todo. Isso possibilita ao atacante controlar o opositor ou, não sendo possível, evitar que ele tome uma decisão. A superioridade de informação requer ao mesmo tempo componentes ofensivas e defensivas,
A Guerra de Informação baseia-se em seis pilares:

Ataque físico/destruição O uso de força cinética (por exemplo com recurso a mísseis), para infligir danos nos sistemas inimigos ou no seu pessoal, de forma suficiente para os tornar inúteis.

[36] *Information Warfare*

Guerra Electrónica	Controlo do espectro electromagnético para minar as capacidades de guerra electrónica do inimigo através de energia electromagnética, energia dirigida e armas adequadas.
Ataque a rede de computadores	Uso de computadores e de equipamento de telecomunicações para provocar disrupção, negação, degradar e destruir computadores inimigos, redes de computadores e a informação que está a ser transmitida.
Criar engano militar	Manipulação, distorção e falsificação de informação para induzir em erro ou iludir o comando adversário, e assim forçar o inimigo a agir (ou a não agir) para sua própria desvantagem.
Operações psicológicas	Uso de comunicações (como é caso de propaganda) e acções destinadas a influenciar a percepção, motivos e emoções do inimigo.
Segurança das operações	Medidas de segurança que o inimigo recolha ou analise informação que possa ser-lhe útil.

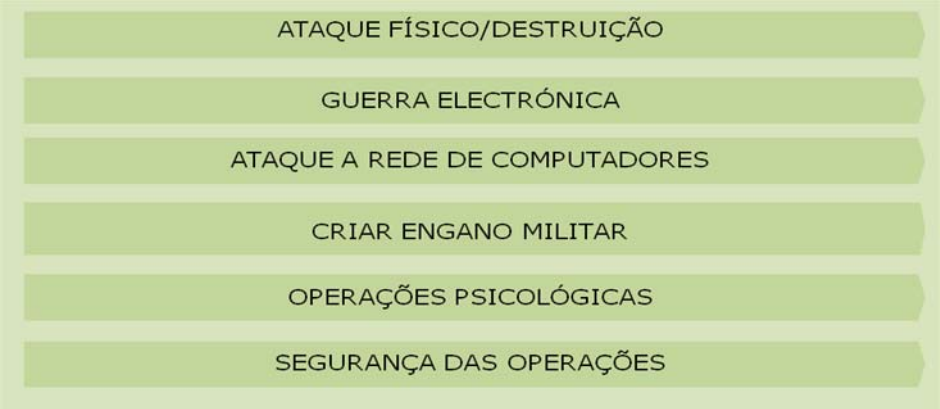

Figura IV 27 - Pilares da Guerra de Informação

I. ALGUNS ATAQUES RECENTES VIA CIBERESPAÇO

Numa notícia inserida na versão portuguesa da publicação Computerworld [COMPWORLD20091], um investigador americano afirmava que o crescente uso dos ataques de Negação de Serviço[37] para fins políticos está a militarizar a Internet.

Os governos estão especialmente interessados em usar ataques por DDOS uma vez que é muito difícil apanhar o rasto aos seus autores e financiadores.

Nos ataques de DDOS os *botnets*[38] tentam ligar-se em simultâneo ao sítio Web da vítima. O servidor que aloja o sítio não consegue responder à abundância de pedidos de comunicação e acaba por "ir abaixo" ou abrandar ao ponto de se tornar inacessível.

[37] Ou DDOS.

Já foram lançados ataques deste tipo, embora mal sucedidos, contra a rede do Pentágono na ocasião em que houve uma colisão entre um avião espião dos EUA e um caça chinês, a qual acabou por provocar a aterragem de emergência da segunda aeronave na China. Também o sítio Web da CNN sofreu ataques semelhantes depois de um dos seus repórteres ter feito comentários depreciativos sobre o facto de a China ser palco dos Jogos Olímpicos. Ambos os incidentes parecerem ter tido origem na China.

Os governos estão especialmente interessados em usar ataques por DDOS uma vez que é muito difícil apanhar o rasto aos seus autores e financiadores. Talvez por isso a Arbor Networks diz [CWORLD20091] não ser capaz de afirmar com 100% de certeza que os ataques perpetrados na Estónia foram ordenados pela Rússia.

O ritmo e complexidade dos ataques por DDOS, assim como por outras formas de acção, estão a aumentar. À medida que os grupos de oposição aos governos também recorrem cada vez mais à Internet, tornam-se alvos naturais.

O pior é que, como resultado deste ciberconflito, a Internet tornar-se-á potencialmente num campo de batalha.

Embora a generalidade dos governos se recuse a admitir que utiliza estes mecanismos, outros há que não têm tanto pudor. A China alegadamente divulgou a sua intenção de investir na ciberguerra e o governo russo terá admitido a utilização de campanhas de propaganda electrónica durante o seu conflito com a Geórgia.

No caso do conflito entre a Rússia e a Geórgia, estas campanhas basearam-se num sítio Web que apelava aos russos para utilizarem tácticas de ciberguerra contra outros sítios Web pró-Geórgia. Um desses sítios terá sido criado por apoiantes de Moscovo e assemelhava-se a um portal de notícias e foi para o ar imediatamente após os primeiros tiroteios entre as tropas georgianas e as russas.

Enquanto os governos desenvolvem estratégias de ciberguerra, tentam ao mesmo tempo criar defesas contra este tipo de ataque. A Estónia levou essa questão à NATO, mas o ritmo lento de adopção de regulamentos desta organização fez com que não se chegasse a qualquer acordo. Este tema também despoletou o interesse da União Europeia, que poderá vir a inseri-lo no âmbito da sua estratégia de segurança *on-line*.

Como "ilustração" de várias referências que fizemos neste texto, recordamos alguns casos de ataques recentes perpetrados através do ciberespaço:

a) Caso Tibetano (conhecido por ataque *Gohstnet*)
b) Caso Estónia
c) Caso Geórgia

[38] Grupo de computadores infectados e que são utilizados para fins malévolos.

CASO TIBETANO (CONHECIDO POR ATAQUE *GOHSTNET*) [GHOSTNET20091]

Consistiu em vigilância electrónica apoiada em *malware*[39], sobre uma organização política alegadamente por parte de agentes de uma Nação-Estado.

Ainda que os ataques de *malware* não sejam novidade, existem neste caso dois aspectos que o tornam importante objecto de estudo.

Em primeiro lugar, porque o ataque foi perpetrado para se conseguir a vigilância de um alvo específico, tendo sido concebido para recolher *inteligência* que pudesse ser utilizável pelos serviços de segurança de um Estado, com consequências potencialmente fatais para os expostos. Em segundo lugar, porque o modo de operação combinou *phishing* social com *malware* de grande sofisticação.

Esta combinação de *malware* bem desenhado com mensagens de correio electrónico apelativas[40] é muito efectiva.

Poucas organizações fora do sector da defesa e da *inteligência* podem fazer frente a estes tipos de ataques, e ainda que este caso particular envolva agentes de uma grande potência, o ataque poderia de facto ter sido montado por um indivíduo com motivação própria.

> A seguir à invasão chinesa do Tibete, o Dalai Lama exilou-se na Índia de onde passou a actuar como líder espiritual tibetano e feito campanha pela independência do Tibete.
>
> A sua campanha embaraçou frequentemente o governo chinês. Por exemplo, durante os Jogos Olímpicos de 2008 o tema Tibete tornou-se particularmente delicado: em Março de 2008 manifestações anti-chinesas em Lhasa e noutros sítios foram seguidas pela polícia chinesa, tendo havido prisões e mortes.
>
> As actividades do Dalai Lama e do governo tibetano no exílio são coordenadas pelo *Office of His Holiness the Dalai Lama*[41].
>
> A maior parte das suas actividades é aberta, tendo que ver com o trabalho diplomático e com a campanha permanente do Dalai Lama e a sua missão espiritual, incluindo festivais religiosos, cuidados pastorais para refugiados tibetanos, actividades escolares de rotina, etc.
>
> É natural que algum do seu trabalho necessite de ser protegido da divulgação intempestiva. Por exemplo, o OHHDL pode querer planear um golpe publicitário em segredo de modo a poder maximizar o seu efeito.
>
> Uma matéria táctica como esta pode requerer confidencialidade somente por algumas semanas ou meses e são moderadas as consequências de uma eventual fuga de informação (correspondendo tipicamente a alguma perda de efectividade operacional).
>
> Haverá contudo outras matérias em que a confidencialidade terá que ser mantida por muito mais tempo sendo as consequências de uma fuga severas.

[39] Termo anglo-saxónico que refere habitualmente software que foi concebido e desenvolvido para se infiltrar e/ou danificar e/ou provocar disrupção sobre um sistema informático. Inclui Vírus, Vermes (*Worms*), Cavalos de Tróia (*Trojans*), Espias (*Spyware*), etc.

[40] A que se chama *malware* social…

[41] OHHDL

> Desde que o OHHDL começou a usar a Internet para conversação e discursos públicos que o uso das TIC aumentou muito. O correio electrónico passou a ser o principal meio de comunicação dentro do OHHDL.
>
> Por outro lado, os tibetanos têm também gerado um grande número de documentos electrónicos nas suas actividades sendo a maior parte deles de natureza rotineira. Obviamente que existirão outros contendo matéria sensível, no sentido de que se esses documentos chegam ao conhecimento das autoridades chinesas o seu conteúdo pode ser usado para promover acções repressivas com consequências fatais para pessoas.

Em Março de 2009 a Universidade de Cambridge publicou um estudo [IWM20091] que teve por objectivo avaliar o alcance e a forma como foi perpetrado o ataque à rede de informações do OHHDL.

Ainda que o ataque estudado de caso tenha origem (segundo os seus autores) num grande governo, as técnicas que os seus agentes usaram estão disponíveis até para o indivíduo privado e são chocantemente efectivas.

Numa outra publicação, o segundo relatório da *Information Warfare Monitor* [IWM20091], é apresentada uma investigação de 10 meses sobre a alegada ciberespionagem chinesa contra instituições tibetanas.

Essa investigação descobriu uma rede de 1295 computadores infectados, em 103 países.

Cerca de 30% dos sistemas *host* infectados foi considerada como "alvo de elevado valor" e incluía computadores localizados em Ministérios dos Negócios Estrangeiros, Embaixadas, Organizações internacionais, Órgãos de Comunicação Social e Organizações Não Governamentais.

Os computadores "tibetanos" que foram investigados de forma não automática, no âmbito da investigação efectuada, foram consistentemente comprometidos por infecções múltiplas que deram aos atacantes acesso a informação potencialmente sensível.

Com a evidência que os investigadores tinham em seu poder, não era claro se os atacantes realmente sabiam o que tinham penetrado ou se a informação alguma vez foi explorada para obter valor comercial ou valor de *inteligência*.

> A rede *GhostNet* infectou directamente computadores através do download de um Cavalo de Tróia conhecido por *gh0st RAT* o qual permite aos atacantes conseguir o controlo completo e em tempo real. Essas instâncias do *gh0st RAT* eram controladas consistentemente a partir de um acesso comercial Internet localizado na ilha de Hainan, na República popular da China.
>
> A investigação revelou que GhostNet era capaz de assumir controlo total dos computadores infectados, incluindo pesquisar e fazer download de ficheiros específicos, e operar de forma sub-reptícia dispositivos ligados, incluindo microfones e câmaras de vídeo.
>
> O vector para espalhar a infecção *GhostNet* apoiava-se em meios sociais. Mensagens de correio electrónico contextualmente relevantes eram enviadas para alvos específicos acompanhados de documentos anexados, os quais tinham embebido código Troianos para exploração do computador. Uma vez comprometidos os ficheiros localizados em computadores infectados podem ser minados por informação de contacto, e usado para espalhar *malware* através de documentos de correio

electrónico e documentos com anexos que parecem vir de fontes legítimas, e conter documentos legítimos e mensagens.

Para além disso a existência da rede GohstNet é um facto significativo por si só.

No mínimo ele demonstra quão fácil é pelo *malware* instalado pode ser usado para construir uma capacidade robusta de inteligência de baixo custo e infectar uma rede de alvos potencialmente de alto valor.

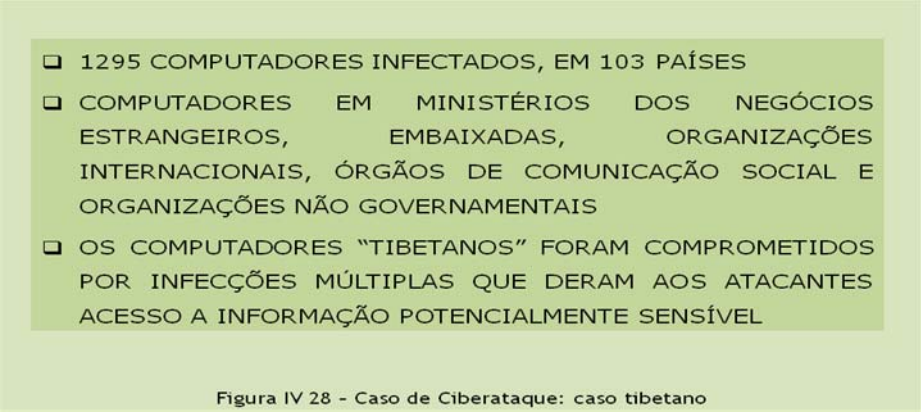

Figura IV 28 - Caso de Ciberataque: caso tibetano

CASO ESTÓNIA [COMPWORLD20091]

Em 2007 verificaram-se incidentes que provocaram a interrupção no funcionamento dos servidores do governo da Estónia.

As notícias veiculadas pela Comunicação Social da época indicaram que foi a Rússia quem, alegadamente, conduziu estes ataques, depois de o governo desta sua antiga república ter removido a estátua de um soldado russo.

Os autores dos ataques construíram ferramentas primitivas e lançaram uma campanha básica, mas no final conseguiram paralisar todo o governo do país.

> Segundo um texto inserido na Wikipedia, os ciberataques perpetrados sobre a Estónia (também conhecidos por "Ciberguerra Estoniana") referem-se a uma série de ataques que começaram em Abril de 2007 e tiveram como alvos os sítios Web de organizações estonianas, incluindo o Parlamento, bancos, ministérios e órgãos de comunicação social, num quadro de conflito com a Rússia acerca da relocalização de uma estátua de bronze do soldado de Tallin (um memorial soviético que recordava os soldados mortos em combate).
>
> A maior parte dos ataques teve impacto sobre o público em geral, perturbando a vida de indivíduos e de organizações, através do uso de variados métodos de baixa tecnologia como inundação de *pings* e até pelo aluguer de *botnets*, usados para distribuição de *spam*.
>
> Foram enviadas inúmeras mensagens de *spam* para portais importantes e foram alterados as páginas principais (*defacement*) de importantes sítios Web.
>
> Alguns observadores referiram que os ataques atingiram um grau de sofisticação pouco comum.

O caso passou a ser extensivamente objecto de estudo em âmbitos militares e foi considerado um acto significativo de ciberguerra.

O Ministério dos Negócios Estrangeiros estoniano acusou imediatamente o Kremlin de envolvimento directo nos ciberataques. Em Setembro de 2007 o Ministro da Defesa da Estónia admitiu que não tinha nenhuma evidência que ligasse as autoridades russas aos ciberataques. Em Janeiro de 2008 um cidadão da Estónia, de etnia russa, foi então acusado e condenado como responsável pelos ciberataques.

O ciberataque paralisou toda a infra-estrutura de Internet do País durante um período de tempo relativamente longo e só após muitos esforços e com uma forte intervenção coordenada dos CERTs/CSIRTs de várias partes do mundo é que foi possível restabelecer a normalidade.

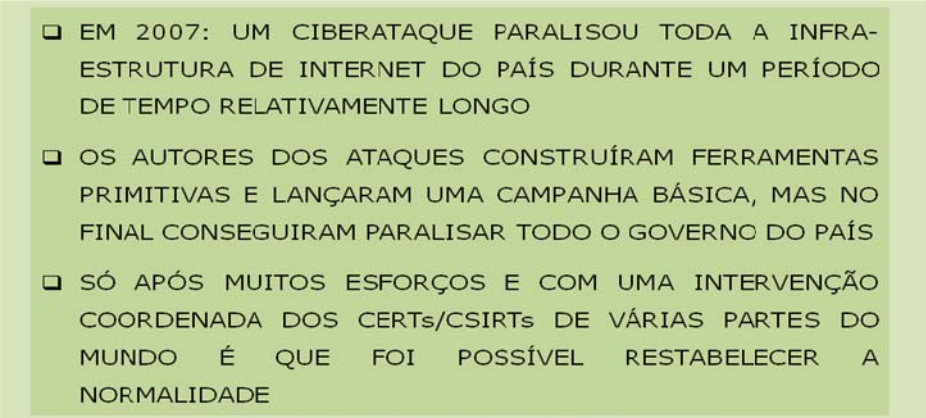

Figura IV 29 - Caso de Ciberataque: caso estoniano

CASO GEÓRGIA [COMPWORLD20091]

A Rússia foi também alegadamente responsável pelo ataque por Negação de Serviço dirigido em Agosto de 2008 contra a Geórgia, outra antiga república da ex-União Soviética.

Entretanto, a Rússia lançou um ataque militar contra a Geórgia como forma de suporte a uma facção separatista.

Os ciberataques contra os sítios *Web* do governo do país invadido coincidiram assim com a campanha militar.

Recorrendo mais uma vez a textos inseridos na WWW (neste caso na Wikipedia): Durante a guerra da Ossétia do Sul verificaram-se diversos ciberataques perpetrados sobre numerosos sítios Web de organizações da Geórgia, da Rússia, da Ossétia do Sul e do Azerbeijão.

Um desses ataques incidiu sobre os sítios *Web* do Parlamento e sobre o Ministério dos Estrangeiros da Geórgia com alterações das imagens e das mensagens das páginas principais (comparando o Presidente da Geórgia com Adolfo Hitler…).

Outros ataques envolveram situações de negação de serviço e de desactivação de numerosos sítios Web georgianos e do Azerbeijão.

É interessante referir que outros governos, nomeadamente o estoniano, o polaco e o ucraniano ofereceram assistência técnica e activaram sítios Web "espelho" de sítios Web georgianos durante os ataques.

Como resposta a acusações das entidades georgianas de que teriam sido os serviços da inteligência russa a conduzir os ataques, as autoridades russas negaram essa responsabilidade.

Segundo um antigo responsável do CERT israelita, em 2008, os ataques às infra--estruturas da Internet georgiana resultaram mais de uma "ciber--manifestação" do que de uma ciberguerra.

Recentemente, investigadores de segurança da empresa americana Greylogic concluíram que as organizações russas GRU (Inteligência Militar) e FSB (Serviço de Segurança Federal) terão muito provavelmente desempenhado um papel chave na coordenação e organização desses ataques.

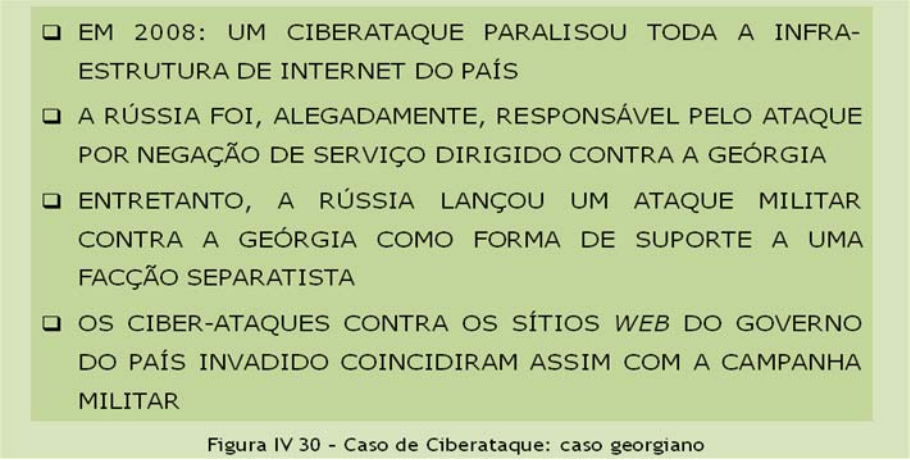

Figura IV 30 - Caso de Ciberataque: caso georgiano


apdsi
associação para a
promoção e desenvolvimento
da sociedade da informação

V.CONCLUSÕES

O estudo elaborado ao longo dos capítulos anteriores permite as seguintes conclusões:

- Existe um sentimento generalizado de insegurança à escala mundial, motivado pela incerteza, imprevisibilidade, complexidade e volatilidade do ambiente estratégico internacional, o que implica um conceito de segurança adaptado a novas fronteiras (económica, cultural, interesses) para além das tradicionais fronteiras política e geográfica e alargado a domínios como a política, a economia, o ambiente, a educação, a cultura, a ciência e a saúde.

  Neste contexto, a segurança passou da previsibilidade para uma segurança orientada para riscos diversos, mais difusos na forma, na origem, no espaço e nos actores, fazendo aumentar desta forma as condições para a eclosão de conflitos.

- Para sermos rigorosos, quando a nossa principal preocupação é a segurança da informação, temos de optar por uma de duas atitudes – estar desligado ou estar ligado.

  A primeira corresponde a uma situação de isolamento com um nível de segurança muito grande, e a segunda corresponde a uma situação sujeita a riscos que temos de saber gerir, construindo e implementando esquemas e medidas que garantam a confidencialidade, autenticidade, integridade e disponibilidade dessa informação, e que protejam quer os equipamentos quer os meios de comunicação.

- As novas ameaças que afectam a segurança, distinguem-se das tradicionais, pelo seu carácter transnacional, desterritorializado, disseminado e individualizado.

  O seu paradigma é genericamente não governamental, não convencional, dinâmico, não linear, com regras de empenhamento desconhecidas, com um modo de actuação e uma doutrina assimétrico e imprevisível

- A informação é vital para a vida dos Estados, das Organizações e dos Indivíduos desempenhando um papel crucial em todas as actividades humanas.

- As TIC providenciam o suporte para o processamento, armazenamento e transporte dessa informação, estando presentes em praticamente todas as áreas da actividade humana, com aplicações intensivas em todos os tipos de empresas, nas Administrações Públicas e na generalidade das famílias.

  Existe uma influência mútua entre as TIC e a sociedade: por um lado, as TIC e as áreas do conhecimento que as suportam, constituem-se como motores de desenvolvimento das sociedades, influenciando e alterando a forma de pensar, de produzir riqueza, de nos relacionarmos, ou de nos entretermos e, por outro, a própria sociedade produz sinais relativamente aos caminhos apontados e percorridos pelas TIC, incorporando ou rejeitando as novas propostas, encorajando ou contrariando o ritmo das alterações tecnológicas.

  No âmbito das TIC, a Internet, utilizada por cerca de 20% da população mundial**,** sendo um gigantesco conglomerado de redes de computadores, interligadas à escala mundial, permite a transferência de dados e o acesso a todo tipo de informações.

  As TIC, como tecnologias emergentes, têm um papel crucial no contexto da globalização, sendo cada vez mais evidente que têm um impacto profundo e extenso na estrutura e no desenvolvimento das sociedades.

  O facto de dependemos cada vez mais de dispositivos tecnológicos corresponde a uma vulnerabilidade da sociedade que estamos a construir, para a qual muito contribui a vulnerabilidade dos dispositivos de TIC em causa.

- Todos precisamos de ter consciência de que o “individual pode pôr em risco o colectivo”.

  Como parte da sua própria protecção – individual e colectiva – é importante que o cidadão entenda que a “criação de um mundo seguro” significa que todos devemos ser capazes de salvaguardar vidas, de proteger estruturas e indústrias críticas e de providenciar um ambiente seguro para a actividade diária normal. Temos também que reconhecer que a nossa insegurança contribui para a insegurança dos outros.

- Ninguém pode ignorar o risco de que grupos terroristas e grupos de crime organizado venham a usar as TIC nas suas actividades, pelo que os Governos precisam de rever e incrementar os obstáculos legais e técnicos colocados a essas actividades, tornando o quadro legal mais efectivo.

- No que se refere a segurança, temos que reconhecer que não existe “segurança absoluta” e que mais vale investir do que despender.

As acções de segurança passam pelo tripé Tecnologia, Processos e Pessoas. Destes três pilares, o mais fraco é o que se refere às Pessoas.

- Os pais e educadores devem estar permanentemente atentos ao uso que os menores fazem das novas tecnologias.

  Os impactos e os efeitos que as TIC produzem sobre os utilizadores mais jovens são potencialmente perigosos, podendo influenciar indelevelmente e de forma inadequada muitos deles.

- Com as TIC, e em particular com a Internet, o tema "direitos de autor" assume novas formas e é acompanhado de novas preocupações.

  A gestão colectiva de direitos de autor no ciberespaço revela-se também como parte a ter em conta na organização de sistemas de protecção dos indivíduos e da sociedade, principalmente porque os modelos que forem adoptados irão facilitar ou dificultar o acesso a informações a terceiros indesejáveis, conforme os níveis de restrições ou de liberdades desses mesmos modelos.

- O comércio electrónico, como nova forma de efectuar transacções comerciais, vai para além do "simples" tratamento da informação, redefinindo a relação entre a empresa e os seus clientes, parceiros, fornecedores, vendedores e concorrentes.

  Os novos cenários para "fazer negócio" trazem novos desafios à sociedade quanto às protecções a considerar e às acções a tomar em caso de ameaças e ataques ao seu normal funcionamento.

  Com o alargamento do uso do comércio electrónico, mais crítico ele se tornará para o Sociedade actual constituindo assim uma infra-estrutura crítica.

- Na maior parte das organizações, os programas de segurança preocupam-se sobretudo com a segurança técnica, o que deixa a informação vulnerável a métodos básicos de espionagem – os quais facilmente explorados por espiões.

- A Democracia Electrónica é uma nova forma de fazer com que o cidadão comum participe em discussões e interacções com os poderes políticos, fazendo chegar a sua voz, não apenas durante as campanhas eleitorais, mas também nos períodos intercalares e a propósito dos problemas da sua vida quotidiana.

  A Democracia Electrónica, ao mesmo tempo que contribui para intensificar a literacia do cidadão relativamente às TIC, envolve toda uma tradução e transferência dos processos tradicionais do funcionamento da sociedade democrática para a esfera digital.

Essa literacia constituirá uma mais-valia importantíssima para que os cidadãos absorvam uma cultura de segurança que integre na sua acção quotidiana hábitos de prevenção e de protecção mais ou menos básicos, tanto ao nível individual como da sociedade em que se inserem.

- Os ciberriscos tornaram-se praticamente mais importantes do que os riscos físicos, para as Infra-estruturas de Informação Críticas, cujo eventual mau funcionamento terá um impacto muito negativo para uma sociedade ou nação.

  Os esforços que as sociedades têm dedicado a tornar as suas Infra-estruturas de Informação Críticas mais modernas, seguras e eficientes, tornando a sua gestão mais eficaz e supervisionando os riscos físicos das mesmas, através da utilização das TIC, revelam-se ao mesmo tempo uma faca de dois gumes.

- Em cenários de conflito entre partes rivais, normalmente entre Estados, a informação constitui o centro da chamada Guerra de Informação, a qual tem por principal objectivo afectar o processo de tomada de decisão do adversário e implementar acções associadas a essa influência informacional, naturalmente no sentido de garantir vantagens sobre ele.

VI. RECOMENDAÇÕES

O presente estudo pretendeu trazer a lume um conjunto reflexões sobre a segurança do mundo actual na sua interdependência com as cada vez mais presentes tecnologias de informação e comunicação.

Estas reflexões pretenderam ser suficientemente abrangentes, desenvolvendo-se sob a perspectiva da interdependência dos indivíduos, das organizações, e do Estado, com as TIC, e de que forma estes mesmos actores são simultaneamente agentes activos na construção e implementação de medidas de segurança relacionados com as TIC, e também 'vítimas' de utilização inadequada.

O estudo não ficaria completo se, do conjunto de reflexões expostas, não saísse um conjunto de recomendações que tentem, de algum modo, apresentar orientações para podermos viver na Era da Informação num Mundo mas seguro.

Seguramente estas recomendações, de uma forma isolada ou em conjunto, já foram apresentadas, dissecadas, desenvolvidas e, em muitos casos até implementadas. Mas o que consideramos importante neste caso, mais do que procurar recomendações inovadoras é a preocupação de que as recomendações sejam efectivamente seguidas, implementadas, e monitorizadas de uma forma contínua.

A segurança, no seu todo e nas TIC em particular, deve corresponder a um processo contínuo de implementação, análise e reajuste às situações sempre renovadas que a era da informação nos apresenta. Só assim poderemos minimizar os riscos numa era de constantes mutações.

Esse processo deve obviamente ter em atenção que há que se proteger a Informação e os sistemas que a tratam, que a armazenam e que a transportam pois só assim estaremos a ajudar a proteger os Indivíduos, as Entidades Públicas, as Entidades Privadas, os Estados, o Mundo…

Sem pretendermos ser redutores nas recomendações, pois elas poder-se-ão alargar noutras vertentes, consideramos que é importante definirem-se quatro eixos de actuação na utilização das TIC para um Mundo mais seguro.

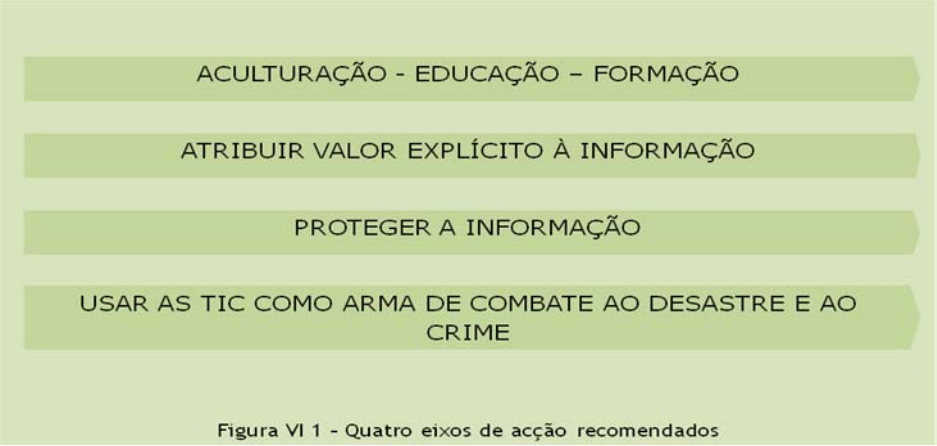

Figura VI 1 - Quatro eixos de acção recomendados

EIXO 1: ACULTURAÇÃO - EDUCAÇÃO - FORMAÇÃO

A educação e a formação, como em qualquer área do conhecimento, devem ser uma das preocupações básicas na utilização da tecnologia. As TIC não fogem a este princípio básico. No entanto, é importante que esteja associada à educação sobre as TIC, desde o início, a formação sobre os perigos que estas podem representar a diversos níveis.

> Servindo um pouco como analogia, quando uma pessoa começa a ter aulas de condução, desde o início, é lhe imposto formação nas regras do código da estrada, e porquê? Fundamentalmente para salvaguardar a sua segurança, e a de terceiros, quando circula na rede rodoviária.
>
> O mesmo se deve aplicar na formação das TIC para os utilizadores. Ao circular nas redes cibernéticas (sejam externas, leia-se web, ou internas leia-se nas organizações públicas ou privadas) os conceitos da segurança da informação devem estar sempre presente, de forma a garantir a segurança da sua informação, mas também da informação que pode ser crítica para terceiros.

Os perigos inerentes à utilização da informação e das tecnologias que a controlam, assim como os mecanismos de defesa (tecnológicos, comportamentais e culturais) devem fazer parte, desde o início, dos currículos de formação dos utilizadores / administradores das TIC que, no fundo, somos todos nós.

Deverão ser incentivadas iniciativas que promovam uma cultura de segurança, isto é, aumentem a literacia dos utilizadores em geral sobre os perigos e cuidados recomendáveis no ciberespaço. Estas iniciativas serão muito relevantes quando estiverem em causa públicos mais jovens, uma vez que a facilidade de penetração destas tecnologias nestas camadas etárias é muito grande e corresponde, infelizmente, a uma postura inconsciente e muitas vezes irresponsável quando em interacção no ciberespaço. Decididamente, qualquer tipo de iniciativa na área das TIC (como serem facultados computadores), deverá ser acompanhada de um programa robusto e apelativo, dirigido ao público-alvo

em causa, que promova os comportamentos adequados à protecção dos próprios utilizadores, contribuindo para um ciberespaço mais seguro.

A formação em TIC, incluindo a componente de segurança, deve ser o mais abrangente possível, desde os bancos da escola, com a existência das salas TIC, passando pela educação dos próprios pais no simples acto da oferta de um computador pessoal ao filho, até à formação a nível empresarial na sensibilização dos colaboradores para um dos bens mais valiosos das empresas que são as suas bases informacionais.

Um outro aspecto em que a formação é importante, passa pela formação cívica dos cidadãos e os seus direitos de privacidade, competência essa que passa em primeira instância pelo Estado, mas não só.

> Numa altura em que os ataques terroristas são imprevisíveis e podem acontecer em qualquer parte do mundo, é importante consciencializar os cidadãos de que é necessário reflectirem sobre a necessidade de terem que abdicar de alguns direitos de privacidade (e reforçamos: **apenas alguns**) a bem da implementação de sistemas de controlo e vigilância que podem reforçar a segurança colectiva. Referimo-nos a sistemas de videovigilância, gravação de comunicações de voz, rastreio de mensagens electrónicas, etc.
>
> O dilema entre o direito à privacidade *versus* o dever da preservação da segurança colectiva é uma discussão que terá de fazer-se de uma forma contínua pois as tecnologias evoluem constantemente e o que é válido hoje sobre o equilíbrio entre a privacidade individual e a segurança colectiva deixa de ser válido num futuro próximo.

Assim, cremos que há uma recomendação particularmente adequada e básica: o Estado deverá equacionar a elaboração de um "Plano Nacional para uma Cultura de Segurança Informática"[42] [43].

Esse Plano deverá abordar, entre outros:

- Aspectos relacionados com a sensibilização cívica dos cidadãos, incluindo não só acções de informação geral, mas também a eventual incorporação deste tema nos programas de ensino e formação.
- Para além dos efeitos directos destas acções no domínio da segurança individual e das famílias, elas constituiriam o indispensável alicerce para o sucesso das medidas adoptadas pelas organizações, públicas e privadas, já que esse sucesso está largamente dependente do empenhamento individual dos indivíduos que fazem parte dessas organizações.
- Aspectos relacionados com a sensibilização das organizações, públicas e privadas, que incluam acções de informação sobre os diferentes riscos e sobre boas práticas para os atenuar.

[42] Naturalmente que o nome pode ser outro…

[43] À semelhança de outros planos de natureza estratégica como, por exemplo, o "Plano Nacional Para o Uso Eficiente da Água" e o "Plano Nacional Para a Eficiência Energética".

- Aspectos relacionados com o enquadramento legal deste tema, incluindo acções de divulgação do normativo já existente e a identificação de áreas que carecem de iniciativas legislativas.

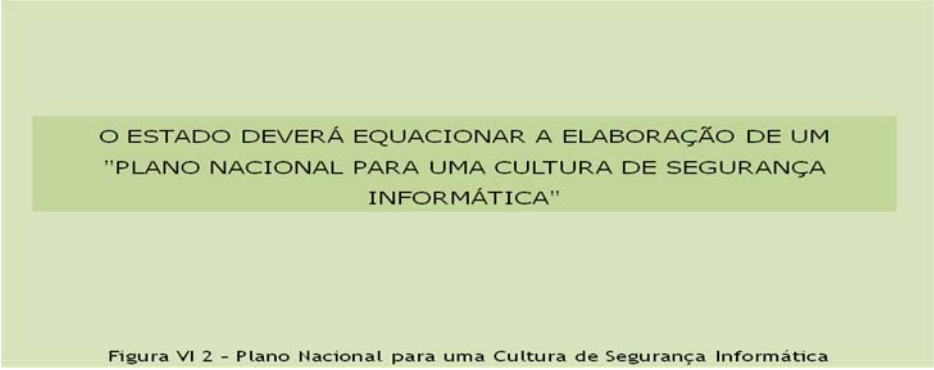

Figura VI 2 - Plano Nacional para uma Cultura de Segurança Informática

Sendo uma questão de interesse nacional este tema deverá ter o envolvimento do Governo, nomeadamente:

- ❖ Liderando o desenvolvimento de uma Cultura de Segurança de Informação.
- ❖ Desenvolvendo uma política nacional de segurança da informação, assegurando cooperação internacional[44] para a promoção de uma Cultura Global de Segurança.
- ❖ Servindo de exemplo na utilização e divulgação da Cultura de Segurança, garantindo que (pelo menos) todos os utilizadores da Administração Pública têm consciência do seu papel e da sua importância, que conhecem as suas responsabilidades e que ajustam as suas formas de actuar.
- ❖ Desenvolvendo um programa de âmbito escolar alargado, dirigido para a sensibilização para o uso correcto das TIC e que inclua, nomeadamente:

a) Difusão de atitudes básicas, individuais e colectivas, designadamente as que são destinadas a compreender e a evitar os perigos do *spam*.
b) Fomentar a educação dos utilizadores, na sua generalidade, quanto à forma de combater as ameaças associadas ao correio electrónico (via Web, telemóvel ou outros meios).
c) Educar os mais jovens, reconhecendo-se que a educação recomendada em a) é particularmente necessária entre os mais jovens, uma vez que são eles os maiores utilizadores quer da Internet quer do telemóvel.
d) Educar os pais e educadores, proporcionando-lhes os conhecimentos necessários para que, por meio de acções activas e passivas, possam colaborar nas medidas de segurança adequadas.

[44] Particularmente no quadro da União Europeia.

- Desenvolver iniciativas junto das PME para a sua promoção.

- Envolver as entidades privadas na disseminação da cultura de segurança em particular as que pelo seu papel na sociedade tem um maior envolvimento nestas questões: ex. Operadores de Telecomunicações, Banca, entidades directamente envolvidas com Comércio Electrónico, fabricantes de TIC, etc.

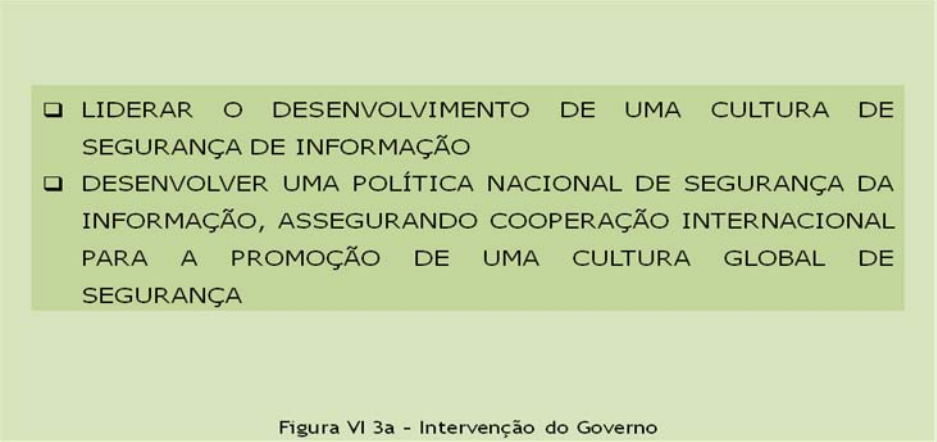

Figura VI 3a - Intervenção do Governo

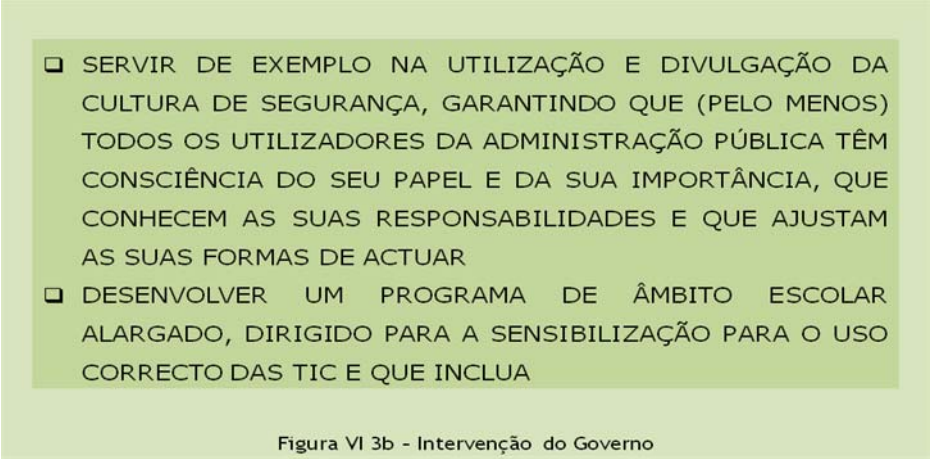

Figura VI 3b - Intervenção do Governo

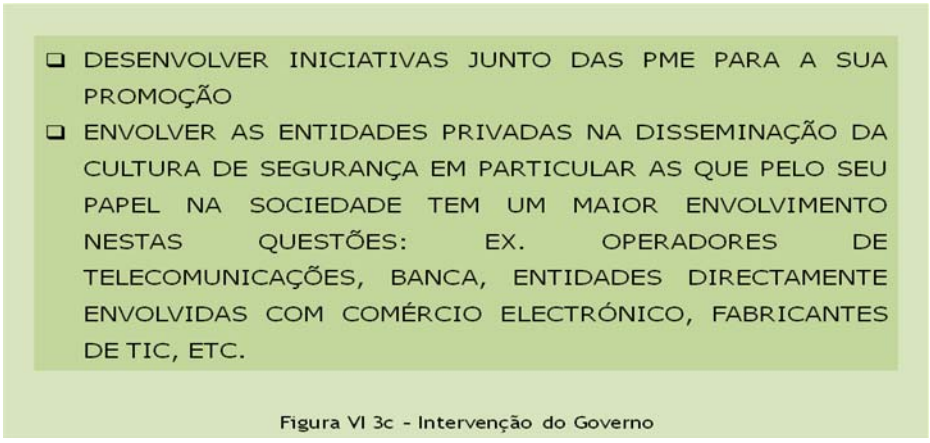

Figura VI 3c - Intervenção do Governo

As iniciativas a desenvolver poderão tomar os seguintes formatos:

- Elaboração de Políticas e de Guias de Boas Práticas de Segurança de Informação orientadas para todos os níveis de agentes: Organização, Gestor, Colaborador, Cidadão, Aluno.
- Recomendações de boas práticas em zonas de acesso frequente dos utilizadores (portais Web, Correio electrónico, etc.).
- Realização de Eventos.
- Promoção do "Dia Nacional da Segurança da Informação".

EIXO 2: ATRIBUIR VALOR EXPLÍCITO À INFORMAÇÃO

Vivemos na Era da Informação e, como tal, informação é poder. Um bem tão valioso como a informação tem de ser tratada com igual cuidado como os bens dos indivíduos, das organizações, do domínio público. E a primeira acção que devemos ter em mente, ao lidar com a informação, é saber classificá-la.

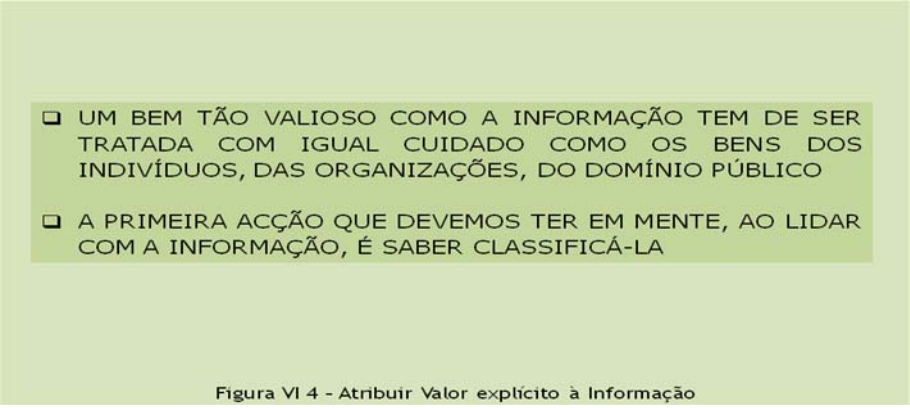

Figura VI 4 - Atribuir Valor explícito à Informação

Desde o indivíduo que escreve num pedaço de papel uma informação que, no entanto, lhe pode ser essencial, como por exemplo, o contacto de um médico numa situação de desespero por um problema de saúde, até uma organização que baseia o seu negócio na informação que recolhe e trata, é fundamental que essa informação seja classificada e tratada tendo em conta a importância relativa que ela representa para quem detém responsabilidade sobre ela.

Nem toda a informação tem o mesmo valor e/ou criticidade, e a mesma informação poderá ter graus de importância diferentes para indivíduos e/ou organizações diferentes. Saber classificar a informação, tendo em conta a criticidade, confidencialidade, disponibilidade, valor histórico, etc., é um aspecto fundamental

para a segurança da informação. Se não soubermos classificar a nossa informação não poderemos, de uma forma efectiva, protegê-la dos múltiplos perigos que pode correr. Desde a simples perda até ao roubo da mesma.

> Todos nós, de uma forma mais ou menos intuitiva, conseguimos classificar a importância que têm os diversos bens que possuímos. Por exemplo, é natural colocarmos num cofre um conjunto de jóias de elevado valor monetário e/ou afectivo. Este mesmo procedimento de classificação de valor (que diríamos quase intuitivo), deve ser realizado com a informação com que lidamos diariamente, a bem da sua segurança e, consequentemente, da segurança do que ela representa.

Só classificando bem a informação é que se pode, posteriormente implementar medidas de gestão e de protecção dessa informação.

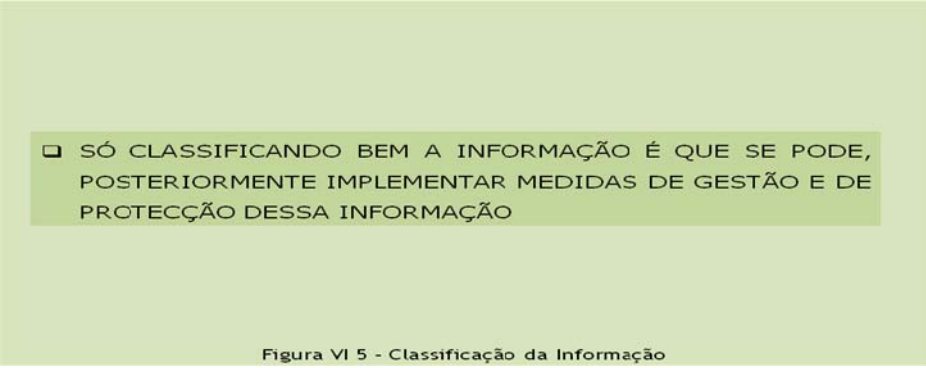

Figura VI 5 - Classificação da Informação

EIXO 3: PROTEGER A INFORMAÇÃO

Como referimos atrás, a classificação da informação (ou seja, a atribuição de um determinado nível importância) é fundamental para se determinar quais as medidas de segurança que devem ser aplicadas na sua gestão.

Da mesma forma que a informação não tem toda a mesma importância, também as medidas as adoptar para a sua segurança devem estar de acordo com a classificação atribuída à mesma.

> Como sabemos, nos tempos de crise (económica, financeira, de confiança, social) que atravessamos, é cada vez mais difícil implementar sistemas de segurança da informação pelos custos associados a essa mesma implementação, sobretudo porque é um custo que não se conseguirá associar de forma visível a resultados imediatos (o que só acontecerá em caso de desastre ou ataque). Se não soubermos muito bem quais são os diferentes graus de importância que a informação tem, possivelmente os níveis de protecção dessa mesma informação serão nivelados por baixo (exactamente pelos motivos apontados acima).

A classificação da informação irá permitir estabelecer um conjunto de regras, procedimentos, métodos e ferramentas de segurança diferenciadas mediante o grau de importância da informação, o que permitirá não só aumentar a segurança no seu todo, como também optimizar os investimentos associados.

É claro que é fundamental que se tenha consciência de que a aplicação de metodologias e ferramentas eficazes de protecção da informação não implica a garantia automática de ausência de riscos, apenas permite minorá-los e, eventualmente, controlar melhor os danos dos potenciais riscos.

Por tudo isto é fundamental a existência de Planos de Contingência, a todos os níveis e em praticamente todos os universos – Indivíduo, Sector Público, Sector Privado, Sector Social, etc. - Empresa, Organismo público, Administração Pública, no sentido de se poder dar resposta aos perigos de perda informação ou de ataque à informação ou aos sistemas que a suportam.

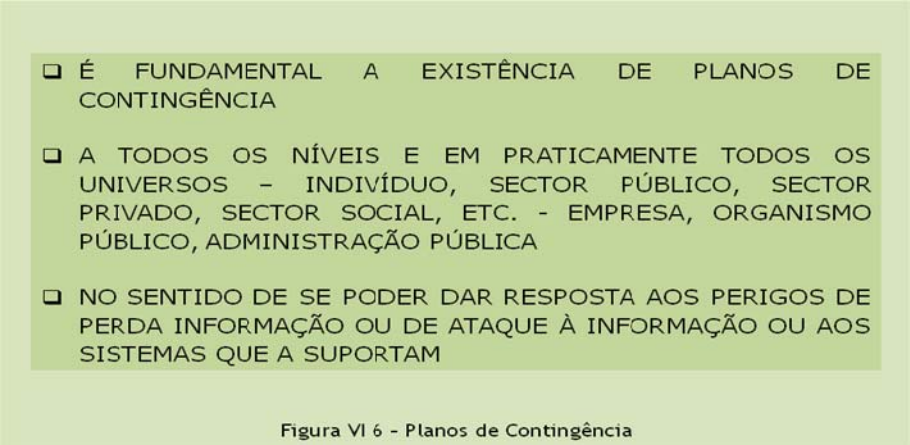

Figura VI 6 - Planos de Contingência

É importante que asseguremos a protecção dos nossos próprios dados pessoais que se encontram em dispositivos variados[45] (computadores pessoais, telemóveis, agendas, etc.) pois neles pode residir informação que, mesmo sendo pessoal, pode influenciar dramaticamente a nossa interacção com o mundo que nos rodeia, até aos complexos planos de continência orientados para mitigar eventuais disrupções de serviços críticos à sociedade, tais como as redes de energia, de telecomunicações, de transportes, etc.

Os planos de contingência não se devem restringir às componentes tecnológicas, é necessário igualmente contemplar a componente dos processos e das pessoas. De que serviria existir uma infra-estrutura tecnológica alternativa a uma organização que sofresse um desastre, se não tivesse contemplado igualmente um espaço de trabalho alternativo para os seus colaboradores, no caso do seu local de trabalho habitual tivesse ficado afectado? Ou não estivesse definido os procedimentos de actuação em caso de desastre? …Possivelmente a organização ficaria inactiva e morreria.

[45] …que até podem não ser electrónicos

Assim, cremos que uma outra medida a adoptar consistirá na criação de um Observatório de Segurança de Informação que deverá envolver entidades com um papel relevante na segurança da informação nacional:

1. CSIRT Nacional.
2. Entidades com responsabilidades concentradas sobre Infra-estruturas Criticas (CII).
3. Entidade Reguladora para as Telecomunicações (ANACOM).
4. Entidade Reguladora para a Banca (Banco de Portugal).
5. Entidade Reguladora para os Seguros (Instituto de Seguros de Portugal)
6. Comissão Nacional de Protecção de Dados (CNPD).
7. Gabinete Nacional de Segurança (GNS).
8. Outros (a definir).

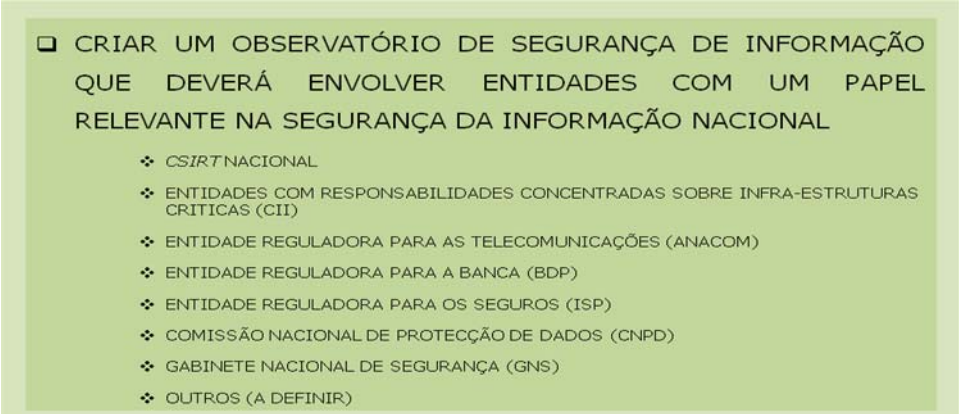

Figura VI 7 - Observatório de Segurança de Informação

Naturalmente que é fundamental promover-se a colaboração interna e externa.

Este Observatório terá que se relacionar, segundo processo a definir, com entidades de iniciativa privada e pública, nacionais[46] e internacionais, que possam constituir uma mais-valia para os objectivos em causa.

[46] Como por exemplo: Observatório de Segurança.

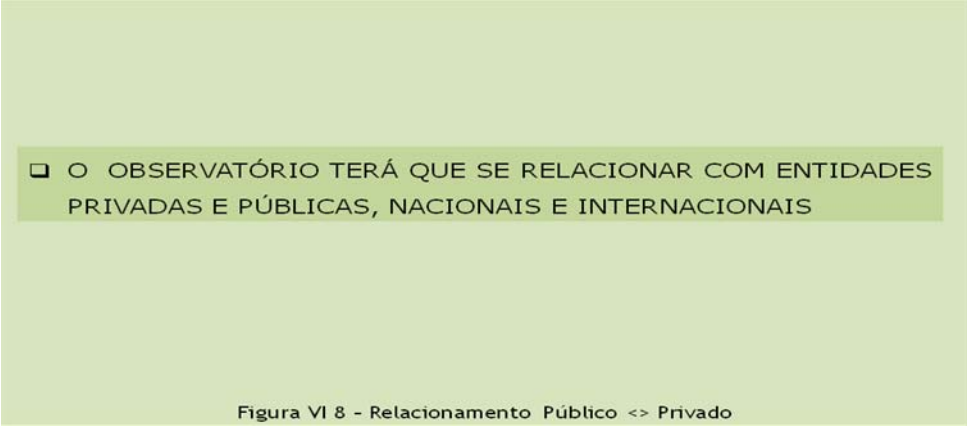

Figura VI 8 - Relacionamento Público <> Privado

Neste quadro haverá que se analisar a possibilidade de se potenciar o papel das operadoras no processo geral de segurança, em especial no que respeita a conteúdos, quer na Internet quer através de telemóveis.

Por outro lado, existem aspectos relacionados com ameaças transnacionais que ultrapassam as capacidades dos indivíduos e das organizações nacionais, pelo que a sua identificação e processo de mitigação deverá ser uma preocupação institucional do Estado, devendo ser criadas as condições institucionais internas e externas, que promovam essa colaboração.

EIXO 4: USAR AS TIC COMO ARMA DE COMBATE AO DESASTRE E AO CRIME

Concluímos das reflexões efectuadas ao longo do trabalho, que as TIC são uma arma extremamente importante para a realização de crimes dos mais variados tipos, abrangendo áreas de actuação tão variadas que podem ir dos nossos computadores de utilização pessoal, até aos sistemas ultra sofisticados de grandes organizações públicas e privadas. Verificamos igualmente que as transformações que a nossa sociedade tem sofrido ao nível ambiental, industrial, climatérico, etc., têm provocado a eclosão de desastres, sejam eles de origem natural ou provocados pela intervenção humana.

Neste quadro, as tecnologias de informação e comunicação terão de ser o motor para o combate e sobretudo para a prevenção de desastres e do crime, seja eles do tipo cibernético ou simples crime comum.

> Hoje em dia existem tecnologias que permitem, ao nível do combate aos desastres dos mais variados tipos, uma actuação rápida que permite minorar os efeitos nefastos dos mesmos. O mesmo se passa ao nível do crime. Sabemos hoje que as guerras serviram sempre como motor de desenvolvimento de tecnologias para a sua aplicabilidade em teatro de guerra. Muita dessa

tecnologia pode e dever ser aplicada no combate aos desastres, mas também ao crime seja ele de que tipo for. No fundo, o combate ao crime não é mais do que uma guerra de guerrilha entre as forças policiais e o crime, seja ele organizado, ou não.

Uma das áreas onde as TIC poderão e deverão ser exploradas até à exaustão é na prevenção. As sofisticadas tecnologias que hoje existem para analisar a informação que está espalhada por múltiplas fontes, a capacidade de análise e estudo de comportamentos, de padrões e de tendências facilita a antecipação e previsão de ocorrências de desastres, ou a descoberta de padrões de comportamento e de actuação que auxiliará a descobrir actividades criminosas (possivelmente mesmo antes de elas ocorrerem).

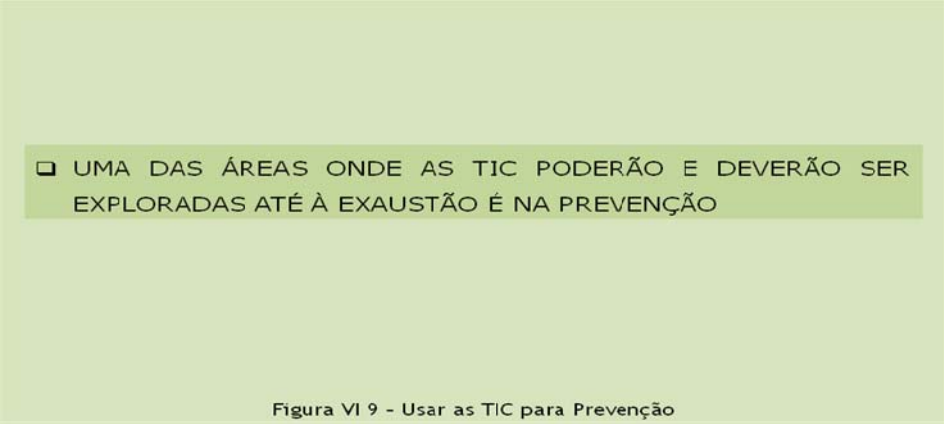

Figura VI 9 - Usar as TIC para Prevenção

Importa reafirmar que a eficiência da utilização das TIC nas acções preventivas tem como pré-requisito algumas das recomendações prévias, ou seja, elevados níveis de educação e formação na utilização das tecnologias e uma correcta classificação da informação para que possa haver uma eficaz exploração da mesma.

A existência de um CSIRT nacional, com missão que não se limite a um determinado sector de actividade constitui uma necessidade.

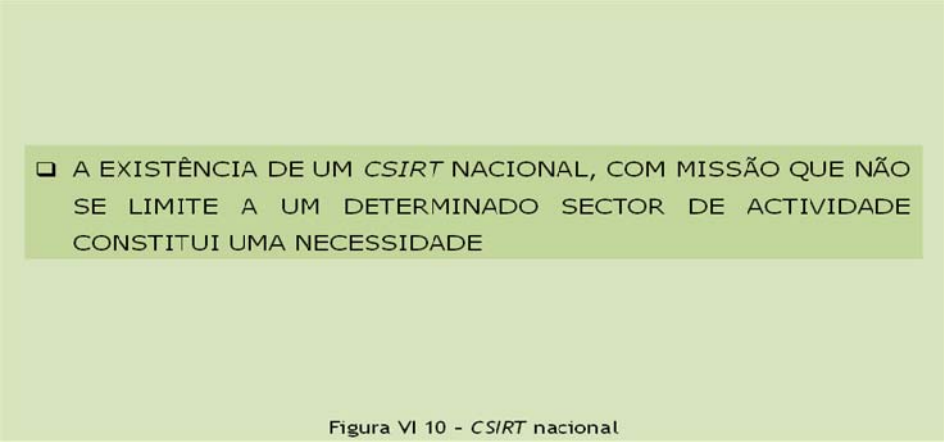

Figura VI 10 - *CSIRT* nacional

Para que seja possível encontrar, de forma mais precisa, as medidas que acrescentem efectivo mais valor à segurança do ciberespaço, deverão ser criadas condições para que seja possível melhorar o mais possível o ciberespaço português, no que diz respeito à sua anatomia aplicacional, comportamento, vulnerabilidades e exposição.

O estabelecimento dessas condições pressupõe que haja articulação público-privada, desejavelmente com o envolvimento de I&D, uma vez que estes domínios contêm actores fundamentais para que seja possível alcançar este propósito.

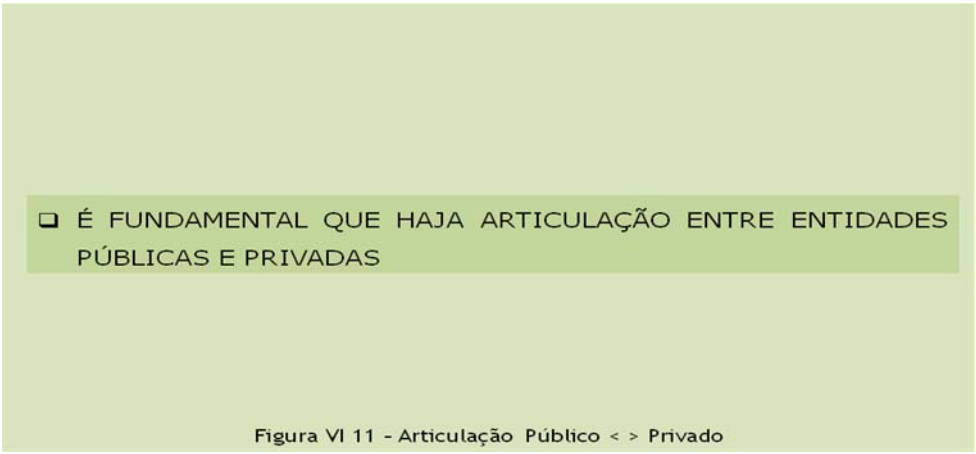

Figura VI 11 - Articulação Público < > Privado

Já o que se refere à protecção de infra-estruturas críticas, é preciso que haja uma forte componente de I&D que promova uma abordagem aos diferentes vectores, tendo em vista o estudo de arquitecturas de informação e tecnológicas inovadoras, com a integração de diferentes dimensões da segurança, consolidada numa Arquitectura de Segurança da Informação que deverá ter a participação de diferentes actores públicos e privados.

VII. BIBLIOGRAFIA USADA

De entre muitas fontes bibliográficas consultadas, apresentamos a seguir as referências que foram mais directamente utilizadas na elaboração do presente Estudo:

[GRAY20081]	**21st Century Security Environment and the Future of War (The)** Colin S. Gray 2008
[Garcia 20072]	**As Ameaças Transnacionais e a Segurança dos Estados**
[Costa20051]	**As Novas Ameaças à Segurança** Francisco Seixas da Costa 2005
[Garcia 20071]	**As Novas Ameaças Transnacionais e o Espaço do Mediterrâneo** Francisco Proença Garcia 2007
[Matai20041]]	**Asymmetric Threats Contingency Alliance** DK Matai February 2004
[Matai20011]	**Asymmetric Warfare - Business Continuity in the Face of Terrorism** DK Matai mi2g November 2001
[CHATAM20081]	**British Agenda for Europe (A) - Designing our own future** A Chatham House Commission Report; www.chathamhouse.org.uk 2008
[APDSI20073]	**Carta dos Direitos do Cidadão na Sociedade da Informação** Tomada de posição do Grupo de Alto Nível APDSI; http://www.apdsi.pt 2007
[APDSI20061]	**Cartão do Cidadão** Tomada de posição do Grupo de Alto Nível APDSI; http://www.apdsi.pt 2006
[COMPWORLD20091]	**Ciber-ataques políticos militarizam a Web** Notícia Computerworld Portugal; http://www.computerworld.com.pt/site Março 2009

[LONG20021] **Computers – Information Technology in Perspective**

Larry Long and Nancy Long
2002, 10th Edition

[KING20081] **Culture of Security (A): Making It Automatic**

Steve King
Report to the Subcommittee on Emerging Threats, Cyber security, and Science and Technology
Committee on Homeland Security, House of Representatives
United States Government Accountability Office
September 2008

[DHS2008071] **Cyber Analysis and Warning**

DHS Faces Challenges in Establishing a Comprehensive National Capability
United States Government Accountability Office
July 2008

[LEWIS20061] **Cyber security and Critical Infrastructure Protection**

James A. Lewis
Center for Strategic and International Studies
January 2006

[NAYEF20061] **Definitions of Globalization: A Comprehensive Overview and A Proposed Definition**

Nayef R.F. Al-Rodhan and Gérard Stoudmann
Geneva Centre for Security Policy;
http://www.gcsp.ch/e/publications/Globalisation/index.htm.
2006

[SSD20041] **Delivering Security in a Changing World - Future Capabilities**

Presented to Parliament by The Secretary of State for Defence
July 2004

[APDSI20081] **Desenvolvimento da Democracia Electrónica em Portugal (O)**

Estudo coordenado por Filipe Montargil
APDSI; http://www.apdsi.pt
Dezembro de 2008

[ALEXANDRE20061] **Engenharia Social: A Construção da Firewall Humana**

Carlos Alexandre
Simpósio Internacional sobre Competitividade e Segurança na Era da Informação
Academia Militar
Maio 2006

[UE20031] **Estratégia Europeia em Matéria de Segurança**

Conselho da União Europeia

2003

[ENISA20091] **European Network and Information Security Agency**

http://www.enisa.europa.eu
2009

[UN20041]	**Follow-up to the outcome of the Millennium Summit** Note by the Secretary-General United Nations General Assembly - Fifty-ninth session December 2004
[LEWIS20071]	**Foreign Influence on Software Risks and Recourse** James A. Lewis A Report of the Technology and Public Policy Program Center for Strategic and International Studies; www.csis.org/ March 2007
[GCSP20031]	**Forum Report On Critical Infrastructure and Continuity Of Services In A Increasingly Interdependent World** Conference Report Geneva Centre for Security Policy; www.gcsp.ch October 2003
[WEBSTER20071]	**Future of Information Security (The)** http://www.webster.com 2007
[SHONIREGUN20061]	**Future of Internet Security (The)** Charles Adetokunbo Shoniregun http://www.acm.org/ubiquity/views/c_shoniregun_1.html Mars 2006
[APDSI20072]	**Gestão de Direitos Digitais** Estudo coordenado por José Matos Pereira APDSI; http://www.apdsi.pt Junho 2007
[NIC20051]	**Globalization and Future Architectures*: Mapping the Global Future* 2020 Project** Conference organized by Chatham House and The National Intelligence Council June 2005
[APDSI20074]	**Glossário da Sociedade Informação** APDSI; http://www.apdsi.pt Fevereiro 2007
[UMIC20071]	**Guia para a Segurança Internet** UMIC – Agência para a Sociedade do Conhecimento; Direcção Geral de Inovação e Desenvolvimento Curricular/CRIE, do Ministério da Educação; Fundação para a Computação Científica Nacional – FCCN; Microsoft Portugal www.internetsegura.pt Julho 2007
[BCS20051]	**Human Factor in Information Security (The)** British Computer Society (This article first appeared in July 2005 *ITNOW*extra) http://www.bcs.org/server.php?show=conWebDoc.2790
[APDSI20071]	**Identidade Digital**

Estudo coordenado por Paulo Esteves Veríssimo
APDSI; http://www.apdsi.pt
Abril 2007

[OCDE20081] **Information Security and Privacy**

http://www.oecd.org/sti/security-privacy
OCDE
2009

[FINAUD20061] **Information Technology, Terrorism and Global Security - GCSP Policy Brief No. 1**

Marc Finaud
Program on the Geopolitical Implications of Globalization and Transnational Security
Geneva Centre for Security Policy
June 2006

[CCE20051] **Livre Vert sur un Programme Européen de Protection des Infrastructures Critiques**

COMMISSION DES COMMUNAUTÉS EUROPÉENNES
Novembre 2005

[NIC20041] **Mapping the global future**

Report of the National Intelligence Council's 2020 Project
USA Government Printing Office (GPO)
December 2004

[ORWELL] **Mil Novecentos e Oitenta e Quatro**

George Orwell

[GIDDENS19991] **Mundo na Era da Globalização (O)**

Anthony Giddens
1999

[MATAI20081] **Opportunities and Challenges of 21st Century - Emerging Technologies**

DK Matai
Center for Policy on Emerging Technologies (C-PET)
January 2008

[VERISSIMO20031] **Protecção da Informação em Sistemas Críticos (A)**

Paulo Esteves Veríssimo
2003

[OTAN20071] **Protection des Infrastructures Critiques Européennes (La)**

Séminaire conjoint Parlement Européen - l'Assemblée parlementaire de l'OTAN
Janvier 2007

[APDSI20062] **Repensar o Futuro da Sociedade da Informação - *Segurança, Privacidade e Identidade Digital***

5º Fórum da Arrábida
APDSI; http://www.apdsi.pt
Outubro de 2006

[SOPHOS20082] **Safe and productive browsing in a dangerous web world: The challenge for business**

Sophos white paper
February 2008

[ESS20031] **Secure Europe In A Better World (A)**

European Security Strategy
December 2003

[LEWIS20081] **Securing Cyberspace for the 44th Presidency**

A Report of the CSIS Commission on Cyber security for the 44th Presidency
Project Director: James A. Lewis
Center for Strategic and International Studies; www.csis.org/
December 2008

[SOPHOS20081] **Security threat report: 2009**

Sophos Plc
2008

[VERISSIMO20061] **Seis princípios para uma maior segurança dos Sistemas Informáticos**

Paulo Esteves Veríssimo
2006

[CERT20091] **Serviço de Resposta a Incidentes de Segurança Informática**

www.cert.pt
2009

[CERT20092] **CERT© Coordination Center**

www.cert.org
2009

[VERISSIMO20071] **Sociedade da Informação, Sociedade (in)Segura?**

Paulo Esteves Veríssimo
Texto incluído no livro Sociedade da Informação – O Percurso Português
APDSI
2007

[Steele20021] **The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats.**

Robert Steele
2002

[NAG& AND20091] **The Snooping Dragon: Social malware surveillance of the Tibetan Movement**

Shishir Nagaraja, Ross Anderson
Technical Report VCAM-CL-TR-746 Nbr 746
University of Cambridge, Computer Laboratory
www.cl.cam.ac.uk
2009

[SOPHOS20083] **Top five strategies for combating modern threats - Is anti-virus dead?**

Sophos white paper
October 2008

[INFOWAR20091] **Tracking GhostNet: Investigating a Cyber Espionage Network**

http://www.infowar-monitor.net/ghostnet
http://www.tracking-ghost.nett
March 2009

[IWM20091]	**Tracking GhostNet: Investigating a Cyber Espionage Network Information** Information Warfare Monitor The SecDev Group, Canada www.infoware-monitor.net/ghostnet/ 2009
[CAMERON20061]	**Transcultural Issues, Globalization and Global Security - GCSP Policy Brief No. 2** Fraser Cameron Program on the Geopolitical Implications of Globalization and Transnational Security The European Policy Centre, Brussels June 2006
[NOIE20021]	**Trusting the internet – small business guide to e–security** NOIE National Office for the Information Economy- Australia; www.noie.gov.au/trustingtheinternet July 2002
[HPGD20041]	**Working Priorities Of The Track On Human Security** Helsinki Process on Globalization and Democracy February 2004

VIII. LEGISLAÇÃO PORTUGUESA RELACIONADA COM TIC

Incluímos nesta secção uma selecção da legislação portuguesa relacionada com as TIC e que julgamos ser a mais significativa no quadro do presente relatório.

Fontes: www.datajuris.pt, www.incm.pt, www.pj.pt

[DL882009]	**Decreto-Lei nº 88/2009, de 2009-04-09** Procede à quarta alteração ao Decreto-Lei n.º 290-D/99, de 2 de Agosto, que estabelece o regime jurídico dos documentos electrónicos e da assinatura digital, e à primeira alteração ao Decreto-Lei n.º 116-A/2006, de 16 de Junho, que cria o Sistema de Certificação Electrónica do Estado
[PORT3072009]	**Portaria nº 307/2009, de 2009-03-25** Sede e a área geográfica de intervenção das unidades da Polícia Judiciária
[DL182008]	**Decreto-Lei nº 18/2008, de 2008-01-29** Código dos Contratos Públicos (2008)
[PORT220A2008[	**Portaria nº 220-A/2008, de 2008-03-04** Cria uma secretaria-geral designada por Balcão Nacional de Injunções (BNI)
LEI322008]	**Lei nº 32/2008, de 2008-07-17** Transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas ou de redes públicas de comunicações
[PORT1142008]	**Portaria nº 114/2008, de 2008-02-06** Regula vários aspectos da tramitação electrónica dos processos judiciais (alterada pelas Portarias nºs 1538/2008, de 2008-12-30 e 457/2008, de 2008-06-20)
[PORT15932007]	**Portaria nº 1593/2007, de 2007-12-17** Cria um balcão único virtual para apresentação de denúncias de natureza criminal e estabelece os procedimentos a adoptar pela GNR, PSP e SEF com vista à prestação do novo serviço
[PORT5932007]	**Portaria nº 593/2007, de 2007-05-14** Define os meios de assinatura electrónica e os sistemas informáticos a utilizar na prática de actos processuais em suporte informático pelos magistrados e pelas secretarias judiciais (alterada pela Portaria nº 114/2008, de 2008-02-06)
[DL1762007]	**Decreto-Lei nº 176/2007, de 2007-05-08** Procede à primeira alteração à Lei n.º 5/2004, de 10 de Fevereiro (Lei das Comunicações Electrónicas), estabelecendo o regime sancionatório da aquisição, propriedade e utilização de dispositivos ilícitos para fins privados no domínio de comunicações electrónicas
[RCM462007]	**Resolução do Conselho de Ministros nº 46/2007, de 2007-03-21** Autoriza a realização da despesa com a concepção, produção, personalização e emissão do cartão de cidadão

[PORT1702007]	**Portaria nº 170/2007, de 2007-02-06** Estabelece os requisitos da apresentação de requerimentos de certificados do registo criminal e da respectiva transmissão, por via electrónica, aos serviços de identificação criminal da Direcção-Geral da Administração da Justiça (alterada pela Portaria nº 286/2009, de 2009-03-20)
[LEI72007]	**Lei nº 7/2007, de 2007-02-05** Cria o cartão de cidadão e rege a sua emissão e utilização
[DL1532007]	**Decreto-Lei nº 153/2007 , de 2007-04-27** Orgânica da UMIC - Agência para a Sociedade do Conhecimento (2007)
[RCM632006]	**Resolução do Conselho de Ministros nº 63/2006, de 2006-05-18** Aprova o Programa Legislar Melhor
[RCM1132006]	**Resolução do Conselho de Ministros nº 113/2006, de 2006-09-14** Autoriza a abertura de concurso público para a contratação de serviços de transmissão de dados e acesso à Internet, pelo período de três anos, para os organismos que integram a Rede de Comunicações da Justiça (RCJ)
[DL116B2006]	**Decreto-Lei nº 116-B/2006, de 2006-06-16** Primeira alteração à Lei Orgânica do Centro de Gestão da Rede Informática do Governo, aprovada pelo Decreto-Lei n.º 184/98, de 6 de Julho, adaptando-a ao Sistema de Certificação Electrónica do Estado - Infra-Estrutura de Chaves Públicas
[DL116A2006]	**Decreto-Lei nº 116-A/2006, de 2006-06-16** Procede à criação do Sistema de Certificação Electrónica do Estado - Infra-Estrutura de Chaves Públicas e designa a Autoridade Nacional de Segurança como autoridade credenciadora nacional (alterado pelo DL nº 88/2009, de 2009-04-09)
[RCM1712005]	**Resolução do Conselho de Ministros n.º 171/2005, de 2005-11-03** Aprova a criação da Entidade de Certificação Electrónica do Estado (ECEE)
[DESPMJ213222005]	**Despacho n.º 21322/2005 (II série), de 2005-10-11** Gabinete do Ministro da Justiça: Generalização e operacionalização das compras electrónicas; representante de cada organismo no projecto piloto das compras electrónicas.
[RCM1372005]	**Resolução do Conselho de Ministros n.º 137/2005, de 2005-08-17** Determina a adopção do sistema de facturação electrónica pelos serviços e organismos da Administração Pública
[RCM902005]	**Resolução do Conselho de Ministros n.º 90/2005, de 2005-05-13** Estabelece o regime da Unidade de Coordenação da Modernização Administrativa (UCMA) e nomeia o seu coordenador (revogada pelo DL nº 240/2007, de 2007-06-21)
[DL662005]	**Decreto-Lei n.º 66/2005, de 2005-03-15** Regula a transmissão e recepção por telecópia e por via electrónica de documentos com valor de certidão respeitantes aos arquivos dos serviços dos registos e do notariado
[DL682005]	**Decreto-Lei n.º 68/2005, de 2005-03-15** Altera o regime de construção, gestão e acesso a infra-estruturas instaladas no domínio público do Estado para alojamento de redes de comunicações electrónicas
[DESPCONJ892005]	**Despacho conjunto n.º 89/2005, de 2005-01-28** Valor probatório dos documentos electrónicos, a assinatura electrónica e a actividade de certificação de entidades certificadoras - pagamento de taxas por parte das entidades

	certificadoras.
[RCM1812004]	**Resolução do Conselho de Ministros nº 181/2004, de 2004-12-22** Aprova o Guia para as Comunicações na Administração Pública, que fixa os princípios por que se devem reger as comunicações na Administração Pública
[DESPCONJ6512004]	**Despacho conjunto n.º 651/2004, de 2004-11-09** Plano de Acção para a Justiça na Sociedade da Informação
[RAR6620049	**Resolução da Assembleia da República n.º 66/2004, de 2004-10-15** Recomenda ao Governo a tomada de medidas com vista ao desenvolvimento do software livre em Portugal
[LEI412004]	**Lei nº 41/2004, de 2004-08-18** Transpõe para a ordem jurídica nacional a Directiva nº 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas
[DR2520049	**Decreto Regulamentar nº 25/2004, de 2004-07-15** Regulamenta o Decreto-Lei nº 290-D/99, de 2 de Agosto, que aprova o regime jurídico dos documentos electrónicos e da assinatura digital
[LEI52004]	**Lei nº 5/2004, de 2004-02-10** Lei das Comunicações Electrónicas (alterada pelos DL´s nº 35/2008, de 2008-07-18, e 176/2007, de 2007-05-08)
[LEI72003]	**Lei nº 7/2003, de 2003-05-09** Autoriza o Governo a legislar sobre certos aspectos legais dos serviços da sociedade da informação, em especial do comércio electrónico, no mercado interno, transpondo para a ordem jurídica nacional a Directiva nº 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho
[DL622003]	**Decreto-Lei nº 62/2003, de 2003-04-03** Altera o Decreto-Lei nº 290-D/99, de 2 de Agosto, que aprova o regime jurídico dos documentos electrónicos e da assinatura digital
[RCM1072003]	**Resolução do Conselho de Ministros nº 107/2003, de 2003-08-12** Aprova o Plano de Acção para a Sociedade de Informação, principal instrumento de coordenação estratégia e operacional das políticas do XV Governo Constitucional para o desenvolvimento da sociedade da informação em Portugal.
[LEICONST12001]	**Lei Constitucional n.º 1/2001, de 2001-12-12** (5ª Revisão da Constituição da República Portuguesa) Artº 35º - Utilização da Informática
[PORT1178E2000]	**Portaria n.º 1178-E/2000, de 2001-12-15** Determina que as peças processuais a apresentar em suporte digital devam sê-lo em disquete de 3,5" ou em CD-ROM (alterada pelas Portarias nºs 8-A/2001, de 2001-01-03 e 337-A/2004, de 2004-03-31)
[DL1222000]	**Decreto-Lei n.º 122/2000, de 2000-07-04** Transpõe para a ordem jurídica interna a Directiva nº 96/9/CE, do Parlamento Europeu e do Conselho, de 11 de Março, relativa à protecção jurídica das bases de dados
[RECT6C2000]	**Declaração de rectificação nº 6-C/2000, de 2000-05-31** De ter sido rectificado o Decreto-Lei nº 58/2000, do Ministério da Economia, que transpõe para o direito interno a Directiva nº 98/48/CE, do Parlamento Europeu e do Conselho, de 20 de Julho, relativa aos procedimentos de informação no domínio das normas e regulamentações técnicas

[DL582000]	**Decreto-Lei nº 58/2000, de 2000-04-18** Transpõe para o direito interno a Directiva nº 98/48/CE, do Parlamento Europeu e do Conselho, de 20 de Julho, relativa aos procedimentos de informação no domínio das normas e regulamentações técnicas e às regras relativas aos serviços da sociedade da informação
[DL3521999]	**Decreto-Lei n.º 352/99, de 1999-09-03** Estabelece o regime jurídico dos ficheiros informáticos da Polícia Judiciária
[DL290D1999]	**Decreto-Lei n.º 290-D/99, de 1999-09-02** Aprova o regime jurídico dos documentos electrónicos e da assinatura digital (alterado pelos DL´s nºs 88/2009, de 2009-04-09, 116-A/2006, de 2006-06-16, 165/2004, de 2004-07-06, 62/2003, de 2003-04-03)
[RCM941999]	**Resolução do Conselho de Ministros nº 94/99, de 1999-08-25** Aprova o Documento Orientador da Iniciativa Nacional para o Comércio Electrónico
[RECT221998]	**Declaração rectificação n.º 22/98, de 1998-11-28** De ter sido rectificada a Lei nº 67/98 [Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva nº 95/46/CE, do Parlamento Europeu e do Conselho]
[LEI671998]	**Lei n.º 67/98, de 1998-10-26** Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva nº 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995
[LEI651998]	**Lei n.º 65/98, de 1998-09-02** Altera o Código Penal (Artº nº 221º - Burla informática e nas comunicações)
[DL1841998]	**Decreto-Lei nº 184/98, de 1998-07-06** Aprova a nova Lei Orgânica do Centro de Gestão da Rede de Informática do Governo (CEGER)
[RCM1151998]	**Resolução do Conselho de Ministros n.º 115/98, de 1998-09-01** Cria a Iniciativa Nacional para o Comércio Electrónico
[DL481995]	**Decreto-Lei n.º 48/95, de 1995-03-15** Aprova o Código Penal (Artº 193º - Devassa por meio de informática)
[LEI1091991]	**Lei n.º 109/91, de 1991-08-17** Lei da criminalidade informática (alterada pelo DL nº 323/2001, de 2001-12-17)
[RCM51990]	**Resolução do Conselho de Ministros nº 5/90, de 1990-02-28** Aprova as instruções sobre a segurança informática (SEGNAC 4)
[CONST1976]	**Constituição da República Portuguesa de 1976** (com as respectivas alterações legislativas)

www.apdsi.pt

Lisboa, 24 de Junho de 2009

OS OBJECTIVOS DA APDSI

A APDSI tem por objecto a promoção e o desenvolvimento da Sociedade da Informação e do Conhecimento em Portugal.

Para a prossecução do seu objecto, a Associação poderá desenvolver todas as actividades que julgue necessárias ou convenientes, nomeadamente:

• Informar, aconselhar e apelar para o Estado em questões políticas e legais relativas à Sociedade da Informação e do Conhecimento;

• Informar os cidadãos, empresas e outras entidades em questões relativas à Sociedade da Informação e do Conhecimento;

• Contribuir para o combate à info-exclusão;

• Apoiar e desenvolver actividades que façam chegar os benefícios da Sociedade da Informação ao maior número possível de cidadãos;

• Promover e dinamizar projectos de utilidade pública no âmbito da Sociedade da Informação e do Conhecimento.

Em harmonia com estes objectivos, a Visão da APDSI é a de Portugal ser um país na frente do desenvolvimento mundial da Sociedade da Informação e do Conhecimento e em que todos, sem distinção de classe social, de nível educacional, de deficiências físicas ou mentais, de idade ou de outros factores, possam ter acesso aos benefícios da Sociedade da Informação.

CONTACTOS DA APDSI

APDSI - ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO

Rua Alexandre Cabral, 2C - Loja A

1600-803 Lisboa, Portugal

Tel.: +351 217 510 762

Fax: +351 217 570 516

E-mail: secretariado@apdsi.pt

URL: www.apdsi.pt

PATROCINADORES GLOBAIS

accenture
High performance. Delivered.

hp invent

Microsoft

Millennium bcp
A vida inspira-nos

noLimits CONSULTING

UNISYS

ERICSSON

Jun.09_1077