Academia Militar

Direcção de Ensino

Curso de Infantaria

Trabalho de Investigação Aplicada

Ciber-Guerra: Ciber-Ameaças

Autor – Aspirante Aluno Infantaria André Bento

Orientador – Tenente-Coronel Transmissões João Rocha

Lisboa, Maio de 2008

Academia Militar

Direcção de Ensino

Curso de Infantaria

Trabalho de Investigação Aplicada

Ciber-Guerra: Ciber-Ameaças

Autor – Aspirante Aluno Infantaria André Bento

Orientador – Tenente-Coronel Transmissões João Rocha

Lisboa, Maio de 2008

Aproveito esta oportunidade para dedicar o presente trabalho aos meus pais, à minha irmã e aos meus amigos que ao longo destes anos de curso me apoiaram e ajudaram em tudo o que podiam.

Agradecimentos

Foram muitas as pessoas que me ajudaram na elaboração deste trabalho, contudo, quero agradecer àqueles que mais contribuíram para a sua realização.

Inicialmente quero agradecer ao Tenente-Coronel de Transmissões Rocha que, como orientador do trabalho, demonstrou sempre uma grande disponibilidade e onde as suas contribuições me permitiram atingir os objectivos a que me propus.

Agradeço ao engenheiro Luís Sousa Cardoso, co-orientador, que sempre que possível me auxiliou na procura de respostas para solucionar o problema científico proposto.

Agradeço ao Tenente-Coronel Infantaria Comando Emanuel Almeida Luís por ao longo deste difícil ano, ter estado sempre disponível a ajudar e durante três anos ter sido um exemplo na forma de estar, pensar e agir.

Ao meu curso de Infantaria um muito obrigado por todo o apoio que me deram, não só na elaboração do trabalho, mas também durante a nossa estada em Mafra.

A Todos o meu muito obrigado.

Índice

Índice de Quadros:

Índice de Figuras:

Resumo

A nível estratégico a guerra da informação implica um domínio do ciberespaço, pois os "ciber-ataques", vírus e cavalos de Tróia não podem ser descurados. Esta forma diferente de guerra implica a adopção de uma política de segurança e defesa para o ciberespaço, pois este impôs uma nova dimensão geopolítica.

A definição de uma política de segurança nacional para a área das infra-estruturas de telecomunicações é fundamental. A sua implementação que visa a redução do risco, inclui iniciativas de prevenção/protecção e a atenuação dos efeitos de incidentes. A redução do risco também exige sistemas de alerta antecipado e previsão de ameaças iminentes, para cuja realização é imprescindível a cooperação internacional. No mínimo a dissuasão colabora para a redução do risco.

A segurança das redes é, pois, um tema que precisa urgentemente de ser tratado de uma forma racional e usando uma linguagem simples. Dever-se-á ter em conta que tratar riscos de segurança das redes de informações apenas com soluções tecnológicas é adiar um problema.

Com este trabalho pretendemos elucidar e realçar quão importante é este problema ao nível do Exército Português. Para isto foram definidos dois tipos de objectivos: Um objectivo geral e alguns objectivos específicos.

Como objectivo geral, para este problema, salientamos a importância de saber se o Exército Português, está de facto, preparado para fazer face a este tipo de ameaças. Como objectivos específicos, pretendemos alertar para a importância destas ameaças na sociedade civil e no meio militar, classificar estas ameaças quanto à sua capacidade letal, listar as várias "ciber-ameaças" menos divulgadas e saber se existe alguma unidade vocacionada para defesa destas ameaças no Exército Português.

Este novo tipo de guerra está ao nível de quem possui capacidades tecnológicas sofisticadas, bem como de dinheiro para implementar novas tecnologias, como iremos ter oportunidade de referir durante o trabalho.

Portugal e as forças militares estão a passar por um processo de transformação tendo vindo a aperfeiçoar-se para fazer face às ameaças que a era da informação gera, tentando precaver-se da melhor forma possível para fazer face às ciber-ameaças.

PALAVRAS-CHAVE: Ciber-Guerra; Ciber-Ameaças; Infra Estrutura de Informação Nacional; Ciberespaço; Internet; Capacidade Militar Centrada em Rede;

Abstract

Strategically speaking, it is necessary to know cyberspace for information war, because we can't forget cyber attacks, viruses and Trojan horses.

This kind of war implies new security policies and defenses for cyberspace, due to the new geopolitical dimension created by it.

Defining national security policies for network area is essential. Its implementation, aiming risk, has protection/prevention initiative and helps to reduce nasty effects.

Reducing risk also demands pre-alert systems and prediction of eminent threats, for which is essential international cooperation.

Network safety is a theme that is necessary to be taken care of racionally. Taking care of network security using only technological means is to delay a problem. So, this dissertation intend to show how important is this problem in the Portuguese Army.

As general purpose, we point out knowing if the Portuguese Army is prepared to face out this kind of threats. As specific purpose, we intend to enhance threats' value in civil society and military sphere, to classify menaces about its lethal capacities, point out various "cyber threats" that are less known and find out if it exist units to face these threats in Portuguese Army.

This new kind of war is only possible for those who have technological resources, as well as financial means to purchase them.

Portugal and armed forces are in a transforming process, trying to evolve to face threats that the information age is creating, protecting its systems to face a new reality in war – the cyber-threats.

Introdução

Quando nos foi dada a oportunidade de escolher um tema a desenvolver no trabalho de investigação aplicada e após ter assistido a um simpósio na Academia Militar, ocorreu-nos que o tema da Ciber-Guerra poderia ser um bom tema, já que é bastante actual.

Assim, o tema que propomos abordar na elaboração do trabalho de investigação aplicada, consiste na "Ciber-Guerra" e o impacto que este novo tipo de "guerra" terá no Exército.

Tendo em conta a tipologia e metodologia de trabalhos de investigação formulamos uma questão central, ou problema, de forma a limitar o tema. O problema formulado consiste em abordar que novas formas de prevenção existem ou terão de ser implementadas para prevenir as "ciber-ameaças" presentes neste novo tipo de guerra, ou seja, se estará o Exército Português preparado para fazer face a este tipo de ameaças?

A escolha do tema e da sua questão central é pertinente quer a nível científico, quer a nível social. Do ponto de vista científico trata-se de uma nova forma de abordar a guerra e dos novos meios que são utilizados para prevenir as ameaças provenientes da "ciber-guerra", bem como utilizar este tipo de ameaças para fazer face ao adversário, para que este não obtenha vantagem sobre nós. É então necessário ter em conta novos conceitos e novos métodos para abordar este problema.

Do ponto de vista social este problema é bastante relevante. Basta ter em atenção que os ataques terroristas, utilizando as ciber-ameaças não atingem apenas alvos militares, estando todo o tipo de componentes electrónicos à sua mercê, quer numa empresa ou numa casa particular, sendo por isto, mesmo, um problema transversal a toda a sociedade não confinado apenas aos "experts[1].

A finalidade da resolução deste problema tem em vista conhecer pormenorizadamente se estas "ciber-ameaças" são de facto uma utopia ou não e em que medida o Exército Português está preparado, como organização, para fazer face a este novo tipo de ameaças, devendo colocar-se a questão se podem os terroristas, sem recorrerem ao uso de bombas ou explosivos, afectarem um sector e criar a desordem em qualquer canto do mundo. Pretendemos também no final da elaboração do trabalho, caso seja possível, propor a concepção de um sistema de *awarness*[2] para fazer face a estas ameaças, visto, como já foi referido não existir no seio da organização.

[1] Um bom exemplo disto pode verificar-se actualmente quando todos se preocupam em possuir um anti-vírus para proteger os seus documentos pessoais ou informação que consideram importante.

[2] Durante o presente trabalho não iremos traduzir este termo pelo que este provem do Inglês *"aware"* que significa percepção/consciência de…; *Awarness* consiste na percepção ou na capacidade de tomar consciência dos problemas.

André Bento
Aspirante-Aluno Infantaria

No que diz respeito às perguntas de investigação ou questões derivadas compete-nos referir que ao abordar estas questões e ao responde-las, pretendemos apontar uma solução viável para as novas fontes de ameaças baseadas nas novas tecnologias.

Assim, como a primeira e a mais importante pergunta de investigação consideramos o problema a abordar:

1- Estará o Exército Português preparado para fazer face a este novo tipo de ameaças?
2- Existe no Exército Português alguma unidade para ataque e defesa do "ciber-espaço"?
3- Existe no Exército Português alguma unidade dedicada ao *awarness* nesta área?
4- Existe no Exército Português alguma participação na definição e protecção das infra-estruturas críticas das tecnologias de informação?
5- Como defende o Exército Português estas infra-estruturas dos diferentes tipos de ataques?
6- Quais as acções de defesa nesta área que cabem ao Exército Português?

Tendo em conta o problema proposto, formulam-se várias hipóteses para a sua resolução.

1- O Exército Português não possui um sistema de *awarness*, não estando protegido deste tipo de ameaças, sendo portanto, actualmente um alvo fácil para o "ciber-terrorismo";
2- O Exército Português possui actualmente, nos Serviços de Informações Militares, sistemas monitorizados capazes de realizar este sistema de awarness, sendo por isto capaz de prevenir as "ciber-ameaças".
3- O Exército Português está preparado para estas "ciber-ameaças" possuindo um avançado sistema de *awarness*, capaz de as prevenir, bem como de lançar ataques a outros Estados, estando preparado para uma "ciber-guerra".
4- Com um sistema de monitorização avançado, cabe ao Exército não só defender a sua Organização, mas também toda a nação, utilizando os seus sistemas para proteger outras infra-estruturas críticas de tecnologias de informação.
5- Apesar de não possuir um capaz e eficiente sistema de defesa contra as "ciber-ameaças", não cabe ao Exército a protecção da nação neste tipo de guerra, cabendo-lhe apenas a sua própria protecção nesta área.

Começaremos com um enquadramento geral do que é a guerra da informação, onde se insere a ciber-guerra, quais as teorias subjacentes e os meios que existem para se lidar com uma ciber-guerra, bem como o novo espaço de batalha e quais as infra-estruturas a serem atacadas neste tipo de guerra. Após uma análise global da ciber-guerra e das estruturas, iniciaremos a procura de resposta à questão central, investigando o que são as ciber-ameaças, classificando-as, quais os principais actores e quais as maiores

vulnerabilidades exploradas pelas ciber-ameaças. Nesse capítulo analisaremos a que resposta o Exército poderá ou não dar a este tipo de guerra.

Na última parte abordaremos a capacidade militar centrada em rede já desenvolvida por alguns especialistas existentes em Portugal. Esta capacidade encontra-se directamente relacionada com a ciber-guerra, assim como uma melhoria de poder de combate no novo campo de batalha, onde se sente cada vez mais, a evolução tecnológica.

CAPÍTULO 1- NOVAS TECNOLOGIAS

Actualmente as novas tecnologias vêm rentabilizar os modos de funcionamento de qualquer tipo de Organização[3], daí que o sistema aberto[4] se adeque à sociedade competitiva em que nos inserimos e às necessidades da maior parte das Organizações, tal como o Exército, que pretende acompanhar a evolução da tecnologia para ser, cada vez mais, capaz no moderno campo de batalha.

Os *inputs* podem provocar mudanças directamente no interior da Organização, que têm como consequência a produção de efeitos externos, ou seja, podem remodelar ou transformar completa ou parcialmente uma Organização, com vista às necessidades da mesma. Segundo o General Espírito Santo, a revolução dos assuntos militares passa essencialmente pela inovação das novas tecnologias[5] (*inputs*). (2007) De que servirá um Exército que não acompanha a evolução das tecnologias? Ou melhor, que faria um Exército de Napoleão, nos dias de hoje, contra uma unidade tecnologicamente desenvolvida? A resposta é certamente nada, pois não haveria evolução, que lhe permita actuar no moderno campo de batalha.

1.1 - A Mudança das Organizações face às novas Tecnologias

Com o impacto das novas tecnologias ocorrem mudanças organizacionais que influenciam o aparecimento de novos comportamentos: na aquisição de novas competências, na reorganização de processos de trabalho, mudança de valores e princípios, assim como na autonomização de subunidades. A mudança organizacional afecta os indivíduos, os grupos e a organização, conduzindo a uma maior produtividade que contribuí para o sucesso da mesma. As novas tecnologias impõem mudanças nas organizações que lhes vão permitir sobreviver, tornarem-se competitivas e evoluir.

[3] As Organizações, no seu meio e método de funcionamento podem ser vistas como um sistema aberto (se actuarem como um sistema que recebe informações externas), um sistema fechado (se actuarem de forma fechada, não mantendo comunicação com o exterior), ou um misto dos dois (se interagirem com o exterior mas não de uma forma efectiva e total).

[4] O sistema aberto consiste em receber *inputs*, possuir um processo de transformação e obter resultados, que se denominam *outputs*.

[5] "A literatura especializada sobre este assunto proliferou e alguns começaram a falar numa *Revolução nos Assuntos Militares*, tentando comparar as transformações em curso devidas essencialmente a inovações tecnológicas, com outros períodos da História quando outras inovações tecnológicas fizeram o seu aparecimento (arma de fogo, mobilidade, comunicação à distância, armas nucleares e outras) ". (Espírito Santo, 2007)

1.2 - Impacto das Novas Tecnologias no Meio Militar

As tecnologias que constituem o sistema bélico são definidas como *inputs* no meio militar. Os vários sistemas de apoio à decisão sempre foram e continuam a ser marcados pelas múltiplas formas como a informação se desenvolve e como chega ao decisor, pelo que o universo de aplicação das informações continua a ser decisivo no moderno campo de batalha, que se caracteriza pelo extensivo emprego de equipamentos tecnologicamente avançados, em que para estes funcionarem correctamente é necessário um cuidadoso controlo da informação. (Viegas Nunes, 1999)

1.2.1 - Guerra da Informação

A acção das Forças Armadas é caracterizada pela informação, bem como a sua gestão, devido ao seu carácter crítico que circula nos sistemas de comando e controlo.

A tecnologia desempenha um papel fundamental na guerra da informação, pois para além de garantir a eficácia dos sistemas de informação existentes, também pode torná-los inoperacionais, se necessário. Isto é chamado *Guerra da Informação*, onde queremos obter toda a informação possível acerca do nosso adversário sem darmos a conhecer a nossa. (Viegas Nunes, 1999)

O conceito de guerra de informação segundo o manual militar, o *Field Manual 100-6, Information Operations* consiste num "conjunto de acções desenvolvidas para obter a superioridade de informação, processos baseados em informação, sistemas de informação e redes baseadas em computadores, enquanto se defende a nossa informação, sistemas de informação e redes baseadas em computadores."[6] Ser mais rápido que o inimigo/adversário a obter e examinar a informação de uma forma cuidada e eficiente é já a chamada Guerra da Informação. A tecnologia garante a eficácia dos sistemas de informação existentes que suportam da Guerra da Informação.

A evolução tecnológica na área das telecomunicações e da informática trouxe novas formas de reestruturação, novos conceitos e novos termos como a digitalização do campo de batalha, integração, globalização, jogos de guerra, sistema de comando e controlo, computadores, comunicações e informações (C4I), Internet militar e "piratas informáticos". Devido a estes factores, temos de utilizar medidas activas, Guerra de Informação ofensiva e medidas passivas, Guerra de Informação defensiva.

A Guerra da Informação tem duas vertentes – a vertente militar e a vertente não militar. A guerra de informação não militar pode ser, por exemplo, a espionagem industrial

[6] Segundo a tradução do autor.

ou económica, através de agentes governamentais ou privados, procurando obter vantagem competitiva sobre um adversário.

Será considerado guerra de informação militar se os *"infoespiões"* actuarem ao nível da tecnologia militar. A guerra de informação é importante para recolher informação acerca da posição do adversário, da sua organização, da sua táctica de combate e informação e ainda, sobre o campo de batalha em geral. A guerra de informação materializa-se através do combate aos *sistemas de comando e controlo (C2), segurança operacional, Ciber-Guerra, guerra electrónica, pirataria electrónica, bloqueio de informação, guerra baseada na informação ou mesmo guerra psicológica.*

O combate aos sistemas de C2 é efectuado por acções que tentam impedir o adversário de controlar e comunicar com as suas forças. A segurança operacional visa impedir que o adversário se apodere de informação confidencial, assim como descodificar as nossas mensagens electrónicas. A guerra electrónica[7] começou a ser utilizada na 2ª Guerra Mundial, e hoje constitui-se como uma arma poderosa de qualquer Exército. (Viegas Nunes, 1999)

A Ciber-Guerra envolve a utilização da informática para conseguir derrubar os sistemas electrónicos e de comunicações do Inimigo, mantendo os nossos sistemas operacionais. Foram os militares a encarar e a utilizar a área tecnológica[8], onde os "cibersoldados" se encontram em Centros de Informação de Combate (CIC), equipados com monitores, computadores e outros equipamentos de alta tecnologia. A sua missão consiste na actualização de dados conforme as situações verificadas no campo de batalha, permitindo assim aos Comandantes verificarem a eficácia do equipamento, bem como conseguir ter a informação necessária e precisa do Inimigo em tempo real, sem que a nossa informação seja obtida pelo adversário. (Arquilla e Ronfeldt, 1993)

Com a introdução de redes de computadores globais, onde a Internet é o melhor exemplo[9], surgiu o fenómeno da pirataria electrónica que tem sido utilizada como uma arma militar[10], pois é vital aceder ao sistema de informações do inimigo em tempo de guerra.

O bloqueio de informação é muito importante, mas para ser conseguido é preciso que se destruam equipamentos que canalizam a informação para o interior do território inimigo.

A guerra psicológica continua a ser muito utilizada. Consiste em utilizar a informação como uma arma contra o adversário, difundindo, por vezes, informação enganosa destinada

[7] Surgiu para neutralizar os sistemas de comando e controlo inimigos, actuando para tal nas suas comunicações e no seu sistema electrónico.
[8] O serviço Mecanográfico do Exército foi o primeiro centro de dados de Portugal.
[9] Uma grande quantidade de programadores, técnicos e curiosos da informática com tempo disponível e intenções maliciosas cruzam as redes de computadores à procura de falhas ou quebras de segurança dos sistemas de informação quer das Forças Armadas quer das grandes Empresas.
[10] Um pirata informático do Exército Chinês de Libertação Popular (ELP) conseguiu entrar no sistema electrónico não confidencial do Pentágono, segundo denúncias de funcionários de Washington.

a desmoralizar o inimigo. Na guerra psicológica, podemos actuar sobre a informação que circula nos sistemas inimigos, vedando-lhes a sua utilização, ou podemos defender-nos contra este tipo de acções, tentando eliminar a informação manipulada pelo Inimigo. (Viegas Nunes, 1999)

Operações de informação são conduzidas permanentemente em tempo de paz e em tempo guerra. Os ataques de guerra da informação fazem sentir-se em Infra-estruturas de Informação Nacional e de Defesa, procurando intimidar o possível adversário através das acções referidas. A partir do momento em que se entra em guerra convencional, a guerra de informação privilegia os ataques ao C2.

Em guerra baseada na informação, os Governos sentem a necessidade de controlar os meios de comunicação social, para filtrar a informação que lhes é mais conveniente, moldando assim a opinião pública[11]. (Viegas Nunes, 1995)

1.3 - Evolução da Internet e a Guerra da Informação

A origem da Internet, como a conhecemos hoje, remonta aos anos 60. Era a época da Guerra Fria entre as duas potências mundiais, os Estados Unidos da América e a União Soviética. As inovações na manipulação de dados electrónicos provinham principalmente de iniciativas militares.

Em 1961 a Universidade da Califórnia (UCLA) em Santa Bárbara, herdou da Força Aérea um computador IBM, o Q-32. A primeira rede de computadores foi construída entre a Universidade da Califórnia em Los Angeles, o Stanford Research Institute (SRI), a Universidade de Utah e a Universidade da Califórnia em Santa Bárbara em Dezembro de 1969 e assim "nascia" a ARPANET (Advanced Research Project Agency Network)[12], em que computadores militares e pertencentes ao meio Universitário foram ligados através de uma rede telefónica, a fim de se criarem projectos técnicos, onde era mais rápido a informação ser processada e chegar ao decisor o mais rapidamente possível. Os quatro nós iniciais da rede foram ampliados para trinta em Agosto de 1972.

A importância da ARPANET era tal que, em 1972, foi rebaptizada DARPANET em que o D significava Defense e lembrava que a rede dependia do Pentágono, o qual financiava os

[11] Um bom exemplo é a Guerra do Golfo, em que apenas um jornalista mostrou para todo o mundo a guerra em directo. Esta foi uma forma dos Estados Unidos da América pressionarem a Comunidade Internacional, controlando a comunicação social que é um dos maiores meios de divulgação da informação.

[12] No início, a actividade principal que se desenvolvia na comunidade virtual da ARPANET era o actualmente banal correio electrónico (e-mail). As discussões "on-line" (actualmente denominadas "fóruns") e milhares de mensagens pessoais circulavam entre os membros da comunidade acelerando o desenvolvimento de programas utilitários que simplificavam a utilização deste instrumento nunca antes utilizado.

investimentos para a ligação entre computadores geograficamente afastados de modo a ser permitido o seu acesso remoto e a partilha de fontes de dados.
Surge então a ideia da criação de uma "International Network" (rede internacional) e de uma "Interconnected Networks" (conexão de redes regionais e nacionais que ainda não comunicavam entre si). Estas expressões apadrinharam a futura denominação "Internet".

Em 1990, o Departamento de Defesa dos Estados Unidos da América desmantelou a ARPANET que foi substituída por uma rede com a denominação Internet. Para expansão da utilização da Internet foi decisiva a criação da World Wide Web[13]. O que se entende por Internet nos dias de hoje não é uma rede única e homogénea, mas sim, uma interligação de muitas redes territoriais ou organizacionais menores. A Internet transforma-se num sistema mundial público de redes de computadores, numa rede de redes, ao qual qualquer pessoa ou computador, previamente autorizado, pode conectar-se. Obtida a conexão o sistema permite a transferência de informação entre computadores. A infra-estrutura utilizada pela Internet é a rede mundial de telecomunicações. (Basílio Susana, 2006)

Com a crescente adesão de membros, em 1990 a Internet registava já mais de dez milhões de utilizadores, o que fez com que aumentasse o número de riscos associados a quebras de segurança. Independentemente de todos os riscos associados à internet, esta tornou-se demasiado valiosa para deixar de ser utilizada, mas também apresenta um nível de risco elevado: existe sempre o perigo de um qualquer utilizador entrar no nosso computador ou na nossa rede e poder usufruir da informação que nós possamos ter armazenada. "Esta situação é muito mais perigosa do que era há meio século atrás, quando as únicas redes existentes eram as redes telefónicas". (Viegas Nunes, 1999)

1.3.1 - Internet como elemento activo da Guerra da Informação

Actualmente os sistemas automatizados são muito utilizados, onde máquinas "comunicam" com máquinas e onde a intervenção humana é mínima.

"Embora executem tarefas simples e repetitivas, as máquinas são muitas vezes vitais, pois se uma delas cometer um erro, uma cidade pode, por exemplo, ficar sem energia eléctrica, ou um banco pode ser roubado". (Viegas Nunes, 1999)

Tais situações contribuíram para a evolução da Guerra da Informação, pois se um indivíduo tiver a oportunidade de aceder a umas destas máquinas pode anular um processo

[13] Vulgo *www que* significa "rede de alcance mundial". Nessa nova cara da Internet, as páginas passam a ser escritas em hipertextos. São textos comuns que podem ser interligados a outros. Quem faz a ponte são os links, as palavras-chave em que clicamos. Elas levam-nos de uma página para a outra.

e aceder a toda a informação vital, usando-a para sabotar um conjunto de sistemas[14], contudo não é fácil conseguir aceder a estas máquinas e utilizar a sua informação. A informação que transita em rede pode ser sempre codificada, apesar de esta situação não garantir total segurança, pois existem equipamentos que podem "ler" a informação nos cabos de rede a distâncias consideráveis, não necessitando de aceder directamente às máquinas. (Viegas Nunes, 1999)

1.4 - Ciberespaço

O nosso mundo é marcado pelo crescente fluxo de informação, bens e capitais que se realiza à escala mundial a que se dá o nome de globalização. Os grandes progressos que se fizeram sentir na área da informática e das telecomunicações obrigam-nos a redefinir conceitos ligados ao transporte e utilização da informação. Com o aparecimento da internet, esta interacção existente no tempo real, conduziram à construção de um espaço de comunicação virtual, centrado em torno da rede de cobertura mundial, que é a internet. A este "novo" espaço virtual, que não é físico ou territorial, chama-se *ciberespaço.*

Para existir o ciberespaço apesar de este não ser "algo" físico, é necessário possuir infra-estruturas que armazenem e façam circular a informação, infra-estruturas de informação e comunicação:

- Os computadores, que asseguram o acesso à rede global;
- A internet;
- Os fornecedores do serviço de acesso;
- As linhas de comunicação, que asseguram a livre circulação dos fluxos de informação, as chamadas "auto-estradas de informação". (Viegas Nunes, 2003)

Assim o ciberespaço pode ser hoje entendido segundo duas perspectivas:

- Como uma infra-estrutura tecnológica de informação (composta pela interligação física de redes de computadores que constitui a *World Wide Web*) (Castells, 1999)
- Como um espaço virtual, que se constitui como o palco de interacções sociais, económicas, políticas e culturais.

Considerando estes conceitos, torna-se assim importante que os Estados desenvolvidos procurem, cada vez mais, criar condições para se ligarem ao ciberespaço, de modo a usufruírem das suas vantagens, mas também precaverem-se para as ameaças que dele advêm.

[14] Estima-se que mais de 90% das comunicações militares utiliza ligações de dados comerciais. O utilizador individual, o sistema bancário e o Ministério da Defesa utilizam as mesmas linhas telefónicas. Embora muitos destes dados sejam enviados de uma máquina para outra sem intervenção humana, é possível intervir sobre eles se tivermos acesso ao sistema.

Podemos constatar que a evolução da tecnologia influencia as teorias geopolíticas[15], definindo o espaço onde se desenvolvem as projecções de poder. Assim, o ciberespaço é um dos espaços da afirmação dos Estados no plano Internacional, pois existe uma grande preocupação dos responsáveis políticos na percepção das interdependências que existem neste espaço virtual como base para a tomada de decisões estratégicas mais informadas. (Viegas Nunes, 2003)

1.4.1 - Infra-Estrutura de Informação Nacional (IIN)

A territorialidade do ciberespaço não só é caracterizado pela Internet, mas também por todo o conjunto de infra-estruturas e de recursos de comunicações, ou seja, aquilo que nos permite construir um mundo virtual, sem fronteiras físicas.

A Infra-Estrutura de Informação Nacional representa grande parte das estruturas de suporte à vivência diária nos dias de hoje. Se se considerar o funcionamento da rede de transportes, o sistema de distribuição de águas ou de energia eléctrica, chega-se à conclusão que existe aqui uma interdependência, em que a quebra dos fluxos de informação, necessária ao funcionamento destes sistemas poderá ter consequências graves. Para um Estado ter acesso seguro à Internet quer na utilização quer na transferência de informação, é necessário haver um cuidadoso planeamento do desenvolvimento estrutural da Infra-Estrutura Nacional de Informação.

O ciberespaço enquanto espaço sem fronteiras físicas, e enquanto espaço de defesa dos interesses nacionais, assume uma importância crescente para a segurança Nacional, obrigando os estados à defesa da sua Infra-Estrutura Nacional de Informação. A sua segurança e defesa terá que passar por uma análise das possíveis ameaças e vulnerabilidades existentes, tendo por base a identificação dos recursos chave que se pretendem defender ou preservar. (Viegas Nunes, 2003)

1.5 - Ciberterrorismo

O terrorismo é entendido pela sociedade como um fenómeno aleatório, onde existe, na maioria dos casos, a perda de vidas inocentes. Estes ataques pretendem sempre provocar o pânico, o terror e o medo, residindo aí o seu impacto e poder[16].

Englobando o terrorismo no âmbito deste trabalho, pode verificar-se que, se o ciberespaço é hoje um espaço onde se desenvolvem as projecções de poder, a sua utilização para actos de terrorismo não pode ser ignorada.

[15] Confira em "O Novo Ambiente Estratégico" 1995, IAEM, NC 71-00-15, Lisboa

[16] A dimensão pública do terrorismo aumentou bastante graças aos meios de comunicação. As tecnologias de informação e comunicação vieram ampliar o fenómeno da expressão das actividades terroristas.

1.5.1 - Definição de ciberterrorismo

Sendo os Estados Unidos da América o mais avançado Estado no que diz respeito à evolução tecnológica, utilizando cada vez mais as redes de computadores ligados à Internet, definiram o ciberterrorismo como " um acto criminoso perpetrado através de computadores que resulta em violência, morte ou destruição e que gera o terror com o objectivo de coagir um governo a alterar as suas políticas". (NSSC, 2003).

1.5.2 - Enquadramento do Ciberterrorismo

Embora o ciberterrorismo não seja a única fonte de perigo de computadores, infra-estruturas, etc – a Internet é também uma grande fonte de perigo, pois é constituída por milhares de computadores que ao transferirem informação, utilizam software e ficheiros compatíveis possíveis de serem acedidos de forma ilícita.

A internet tem vindo a tornar-se num autêntico campo de batalha digital, sendo, muitas vezes, o palco de retaliações entre hackers[17] associados, bem como, por ser um meio aberto de interacção digital, tem também vindo a ser utilizada extensivamente por grupos terroristas, para difusão de mensagens, como para coordenação das suas acções, tendo em vista actividades ligadas ao terrorismo.

O ciberterrorismo pode assim, também ser encarado, como um suporte para o terrorismo tradicional. (Viegas Nunes, 2004)

Actualmente todo o tecido social, político, empresarial, financeiro e militar, está cada vez mais dependente das novas tecnologias de informação. Ora com toda esta evolução, também o terrorismo se está a modernizar, despertando também para estas novas tecnologias, utilizando-as não só para troca de informações, mas também como instrumentos efectivos na prossecução do crime organizado[18].

Num futuro próximo é bem provável que através do ciberterrorismo se possam corromper sistemas bancários, incapacitar transacções financeiras e operações da bolsa, fazendo com que os países afectados possam perder a confiança nos sistemas económicos. Este tipo de medidas é um dos principais objectivos do terrorismo, que consiste em levar um país à anarquia, ao medo e à destabilização, através das novas tecnologias.

[17] Hackers, também designados por "piratas informáticos", são pessoas que, normalmente, possuem maior conhecimento técnico que os amadores. Estes indivíduos apresentam também um conhecimento mais ou menos profundo dos processos utilizados e reflectem a intenção de violar a segurança ou as defesas do sistema alvo dos seus ataques. (Nunes, 2004)

[18] Podemos notar que terrorismo não é sinónimo de crime organizado. Muitas vezes este é usado para financiar actividades terroristas.

1.5.3 - Diferença entre ciberterrorismo e ciber-guerra

Falando de ciberterrorismo, não devemos misturar tal termo com ciber-guerra. Enquanto o *ciberterrorismo* se constitui como um ataque político premeditado levado a cabo por terroristas que utilizam as novas tecnologias para efectuar ataques que possam provocar o caos, normalmente contra alvos não combatentes, a *ciber-guerra*, materializa acções de defesa e de ataque contra todo o género de estruturas de informação e redes de computadores, em que o campo de batalha é conduzido numa dimensão digital.

Note-se que não se podem confundir estes dois termos, devido à sua legitimidade, ou seja, em guerra, em ciber-guerra existe a legitimidade de um Estado se proteger, ou porventura atacar outro, pelo que no terrorismo isso não acontece.

Este novo tipo de guerra pode processar-se de forma assimétrica, como o terrorismo, pois é um facto de que nem todos os Estados podem acompanhar financeiramente a evolução tecnológica que se tem vindo a fazer notar, sendo que uns Estados são e estão melhores preparados do que outros para desenvolver o seu aparelho militar com estas novas tecnologias de informação.

É um facto que quanto mais hábil for um Exército na aquisição e gestão da informação de determinado contexto táctico-estratégico de um conflito em que esteja empenhado, maior será a sua capacidade de minimizar as suas fraquezas. Por outro lado, terá maior capacidade de identificar as vulnerabilidades do adversário e potenciar a sua força militar contra ele – *ciber-guerra*. Em termos mais específicos, derivam várias acções, das quais se destacam o acesso ilegítimo a redes de computadores, e ataques de navegação a serviços, sabotagem a equipamento através do ciberespaço e manipulação de fontes de informação com o objectivo de influenciar os processos de gestão de informação e de decisão do adversário[19]. (Santos *et al* 2008)

[19] Um exemplo de ciber-guerra a grande escala, foi um episódio que ocorreu na guerra do Golfo, em que houve um acesso ilegítimo por meios informáticos ao sistema de controlo de comunicações aéreo militar do Iraque e o tornou inoperacional, de forma a "cegar" a sua Força Aérea.

CAPÍTULO 2 - CIBER-AMEAÇAS

2.1 - Ameaças a que um Estado pode estar sujeito

Hoje em dia, apesar das inúmeras transformações que têm vindo a ocorrer, o Estado continua a ser o principal interveniente da cena internacional. Contudo, alguns grupos terroristas, tal como a Al-qaeda, emergiram e possuem alguma capacidade de influência no sistema internacional, levando a cabo acções terroristas que provocam o medo e o caos.

O mundo contemporâneo é caracterizado pela mudança contínua, o que gera incertezas e riscos, que podem evoluir para crises profundas. Os problemas de natureza económica, social e política, as diferenças religiosas e étnicas, os extremismos e fundamentalismos, as reformas inadequadas, a violação dos direitos humanos, a dissolução de Estados e os actos de terrorismo, sabotagem e crime organizado têm provocado a instabilidade de territórios e regiões sendo alguns dos geradores dos problemas dos nossos tempos. Também a proliferação de armas nucleares, químicas e biológicas e dos vectores capazes de as lançar, consequência da evolução tecnológica e do mais fácil acesso às matérias-primas necessárias, possibilitam a sua disseminação. Isto leva a que os Estados e os grupos terroristas organizados mostrem cada vez mais interesse para a procura deste tipo de armas. Como consequência, "potenciais adversários" – incluindo actores menores da cena internacional – podem deter sistemas de armas sofisticados aumentando a sua capacidade de provocar danos.

"As ameaças e riscos para a segurança nacional e internacional assumem um carácter de imprevisibilidade, que se pode dever ao facto do sistema internacional ser marcado pela globalização e heterogeneidade de modelos políticos e civilizacionais". (Prata Gil, 2007) Como surgiram novas fontes de instabilidade para a segurança e paz mundial, tem vindo a desenvolver-se um novo conceito de segurança – um conceito alargado, com um papel crescente das organizações internacionais, para tentar prevenir eventuais focos de crise ou tentar que estes focos sejam apaziguados ou não se agravem.

A Segurança é um dos Objectivos Permanentes dos Estados[20]. As acções que visem contrariar a prossecução dos Objectivos constituem Ameaças ao Estado Português. Estas ameaças, segundo o texto constitucional e em diplomas legais, dividem-se em ameaças externas, quando têm origem no exterior ou são protagonizadas por agentes externos e ameaças internas, quando se exercem no interior do território, nomeadamente através da criminalidade violenta e organizada, da sabotagem, da espionagem e do terrorismo.

[20] Segundo a Constituição da República Portuguesa, os Objectivos Permanentes do Estado são a Segurança, a Justiça e o Bem-Estar.(CRP Cap I, Artº 9, Artº 23, Cap.II Artº 27)

2.1.1 - Definição de Ameaça e Risco

O termo ameaça[21] é frequentemente usado como sinónimo de agressão ou de risco. No entanto devemos entender ameaça como a possibilidade de uma acção praticada por um interveniente, seja um Estado, um grupo político ou um grupo criminoso, e que envolva o emprego da coacção. Os agentes[22] das ameaças tanto podem ser Estados como outros actores menores da cena internacional[23].

O Risco é a consciência do grau de perigo influenciado pela probabilidade de ocorrência da ameaça. Dependendo do perigo da sua concretização, no respeitante a interesses e danos provocados face aos custos, podemos falar em Riscos aceitáveis e Riscos não aceitáveis. Este grau de probabilidade assim como o grau de perigo resultante da ameaça, é maior ou menor em função das vulnerabilidades que o alvo apresentar. Um Estado deixou de considerar como ameaça apenas outro Estado ou coligação de Estados para passar também a preocupar-se com outros grupos sociais, um grupo terrorista por exemplo. Um grupo terrorista não dispõe da capacidade militar de um Estado, mas consegue influenciar a sua vontade política[24]. São as chamadas ameaças assimétricas, em que os actores que se confrontam têm uma capacidade militar muito desigual e o Estado está impedido, pela própria natureza do actor menor, de utilizar o seu poder. (Gil Prata, 2007)

Como elemento da definição de ameaça, a coacção tem a ver com o uso, ou a possibilidade de uso, da força. Assim, a coacção pode ser exercida através de formas não violentas de pressão (diplomática, económica, política, psicológica) em que está sempre presente a ameaça de uso da força.

"Para salvaguardar a Segurança, tem de existir uma avaliação permanente dos diferentes tipos de ameaças que o Estado está sujeito ou poderá vir a estar sujeito, para se poder diminuir cada vez mais o Risco"[25]. (Prata Gil, 2007)

[21] Genericamente, uma ameaça é qualquer acontecimento ou acção (em curso em previsível) que contraria a consecução de um objectivo e que, normalmente, é causadora de danos morais ou materiais. (Couto,1988)
[22] Considera-se Agente, aquele que poderá ameaçar ou causar dano; o sujeito da ameaça: grupos ou instituições ou indivíduos que possam constituir acções que provocam danos morais ou materiais.
[23] Exemplo de Grupos organizados de terroristas, Grupos Ideológicos apartidários, Grupos religiosos.
[24] A este propósito pode referir-se o ataque a 11 de Março em Espanha, que foi perpetrado com a finalidade de influenciar os resultados das eleições legislativas.
[25] Um Estado não é capaz de conseguir fazer face a todas as ameaças a que está sujeito, sendo por isso que se precavê para as mais prováveis de se realizarem. Desta forma e deixando as outras ameaças para segundo plano nasce a consciência do Risco.

2.1.2 - Possibilidade de um Estado estar sujeito a uma Ameaça

Determinada situação é geradora de uma ameaça se o seu agente tiver possibilidades ou capacidades para a sua concretização e se também tiver intenções de a provocar. Só existe ameaça se estes dois factores estiverem reunidos no agente: se dispuser de capacidade militar e económica para desenvolver uma actividade contra nós e se tiver intenção para tal. (Cabral Couto,1988)

No entanto existe outro factor relevante para a configuração de uma ameaça, o seu alvo. A existência de vulnerabilidades ou limitações estruturais, como cisões internas, elevada dependência energética, recursos financeiros escassos e Forças Armadas inadequadas, potencia as ameaças a que um Estado pode estar sujeito, constituindo factores de risco para a sua segurança. Quanto mais vulnerável for um Estado, maior será a probabilidade de ser ameaçado. (Prata Gil, 2007)

2.2 - Espectro de Novas Ameaças

As tecnologias de informação e a crescente necessidade de aumentar a eficiência das infra-estruturas fizeram com que estas coexistissem num processo cada vez mais automatizado e interligado.

Estas infra-estruturas são hoje o suporte de estruturas de comunicação, alargando assim o espectro das ameaças existentes, onde a Internet é a face mais visível. As novas tecnologias de informação, suportadas em estruturas de comunicação integradoras, provocaram uma revolução civilizacional e do espectro das ameaças. À escala planetária, infra-estruturas nevrálgicas, como as governamentais, financeiras, militares, de telecomunicações, de energia, de transporte, de saúde, sistemas de rede de água e de serviços de emergência, são em parte controladas através da Internet, estando sujeitas às ameaças que dela advêm.

Os elementos de redes e software associados à Internet estão sujeitos a um conjunto de ameaças que exploram as suas vulnerabilidades. Com a grande acessibilidade a potenciais alvos, a facilidade de aprendizagem das técnicas de *hacking*[26] e o difícil controlo do ciberespaço contribuíram para que estes tipos de ameaças se tornem credíveis. (Bessa *et al*, 2008)

[26] *Hacking* constitui-se pelas técnicas que os *hackers* usam para violar a segurança das redes de computadores.

2.2.1 - Motivações dos Agentes das Ameaças das Tecnologias de Informação e Comunicação (TIC)

As principais causas ou motivações que materializam as ameaças aos sistemas tecnológicos, que suportam actividades críticas de uma organização, ou dos serviços de um país, podem ser vários:

1. Ganhos Pessoais - Vantagem competitiva, progressão na carreira, ganhos financeiros, reconhecimento.
2. Vingança – Expectativas profissionais defraudadas, incompatibilidade com a hierarquia, diferenças ideológicas e políticas.
3. Curiosidade e procura de desafios – Desejo em ser *hacker*, procura de aventura, razões de "saber como funciona", perspectiva de poder, afirmação pessoal.
4. Repto Intelectual – Paixão em aprender, necessidade de ser aceite pela comunidade de *Hackers*, sentimento de controlo, ultrapassar os limites.
5. Propósitos Morais ou Ideologias – Convicções Religiosas, radicalismos filosóficos ou culturais, agitação regional e internacional, heroísmos.
6. Informações Militares – Informação em tempo real sobre o adversário, Acções de sabotagem e controlo; Acesso a informação estratégica; Potenciar acções de destruição
7. Informações Políticas e Económicas – Obter informação empresarial e partidária[27], ganhar vantagens na condução de negociações; Obter informações tecnológicas valiosas que seriam muito onerosas, ou impossíveis de obter se fossem alcançadas por conta própria.
8. Informações Negociais – Atingir vantagem competitiva, obter segredos de mercado, obter especificações de produtos de mercado, obter informações valiosas resultantes de investigação.
9. Terror – Criar situações que atentem à vida, destabilizar o equilíbrio de forças, fomentar sentimento de insegurança, criar medo, fragilizar a cultura e valores.
10. Ignorância – Segurança deficiente dos Sistemas de Informação que permite que, por desconhecimento e curiosidade se saber mais, sejam provocadas danos profundos com grande impacto nos sistemas e no funcionamento das organizações. (Bessa *et al, 2008)*

[27] Caso Watergate, onde o presidente dos Estados Unidos Nixon, para obter vantagem nas eleições de 1972, autorizou que se usassem escutas na sede do partido da oposição, usando as informações para obter uma esmagadora vitória nas eleições.

2.2.2 - Limitações e restrições aos Agentes das ameaças

Para que um Agente de ameaça possa ser efectivo deve ter motivações, intenções associadas, assim como oportunidades, recursos e capacidades, que são os chamados Factores Genéricos. Qualquer factor, ou incidente, que possa limitar ou eliminar um dos Factores Genéricos – os Factores Limitativos – poderá restringir ou anular ameaças.

No quadro seguinte, pretendemos demonstrar quais são os factores que consideramos essenciais para que uma ameaça seja considerada, que se encontram na coluna da esquerda, bem como as restrições para cada um desses factores essenciais, presentes na coluna da direita.

Factores Genéricos	**Factores limitativos**
Motivação	Interesse; Percepção da probabilidade de sucesso; Probabilidade de ser detectado;
Intenções/Compromissos	Valores morais e culturais; Imagem; Percepção da probabilidade de punição Percepção de Insucesso.
Oportunidade	Awarness; Acessibilidade aos Alvos;
Recursos	Financeiros; Disponibilidade Tecnológica; Tempo; Informação;
Capacidades	Perícia; Conhecimento; Experiência; Treino e Formação

Quadro 1 – Factores Influenciadores das ameaças

(Santos *et al,* 2008)

2.2.3 - Potenciais Agentes das Ameaças

Existem vários agentes que podem constituir ameaças e estão directamente ligados aos factores influenciadores anteriormente referidos. Com o quadro seguinte pretende-se demonstrar o número de potenciais agentes ameaçadores que podem intervir nos sistemas de tecnologias de informação, bem como o factor de risco associado a cada um deles, ou seja, onde é que eles podem surgir como ameaça. Na coluna da esquerda encontram-se os agentes, ou seja, os Estados, as organizações, ou grupos que podem constituir ameaças. Na coluna da direita estão presentes os factores de cada um dos possíveis Agentes, bem como o seu grau de Risco, de onde se poderá intuir se uma ameaça será credível ou não.

Potencias agentes	**Definição de factores de risco**
Informações dos países estrangeiros (Intelligence Estrangeira)	Provenientes dos aliados, países neutrais e países inimigos; Ameaças constantes e, por vezes, imprevisíveis.
Forças Militares Estrangeiras (Estados Rivais, ou Inimigos)	Provenientes de aliados, países neutrais e países inimigos; Acções Militares directas e indirectas; Posse de Informações (Intelligence); Hostilidades previsíveis ou imprevisíveis.
Políticas e Ideológicos (grupos partidários, Grupos religiosos)	Impacto dos temas políticos; Impacto de possíveis eleições; Impacto de notícias provenientes dos meios de comunicação social; Permanente ambiente de mudança que se opera a nível nacional e internacional. Relacionados e confinados a princípios
Económicos	Novas dinâmicas e exigências de competitividade económica; Mundialização da economia; Inexistência de estratégias.
Educacionais	Existência de informações críticas de projectos científicos

André Bento
Aspirante-Aluno Infantaria

Terroristas (*Hackers,* Grupos terroristas, Criminosos)	Motivações imprevisíveis; Grande domínio das tecnologias de informação; Grande probabilidade de serem recrutados por forças subversivas e militares Capacidade de intervenção em qualquer lugar, e em qualquer altura; Grande posse e capacidade de operacionalização de Informações Acções imprevisíveis Exploração de factor "oportunidade"; Possibilidade de obter valores derivados que são advenientes de outros crimes de suporte; Acessibilidade dos alvos; Aprendizagem criminal; Facilidade de acesso à informação

Quadro II – Potenciais agentes e factores de risco de uma ameaça

(Santos *et al,* 2008)

2.2.4 - Recursos e Vulnerabilidades do Sistema de Informação

Os agentes atrás descritos, procuram sempre explorar as vulnerabilidades. É certo que uma ameaça só será assim considerada se possuir os factores genéricos associados, bem como se um sistema ou recurso se encontrar vulnerável e se essa vulnerabilidade for explorada. Tendo em conta o conjunto de recursos dos sistemas de informação, existem inúmeras vulnerabilidades. Um sistema de informações é constituído por diversos equipamentos que são responsáveis pelo seu funcionamento, onde para cada um desses equipamentos existem possíveis vulnerabilidades em que a sua exploração deve ser acautelada. No quadro seguinte, apresentamos na coluna da esquerda quais os recursos do sistema que podem ser atingidos por uma ameaça e na coluna da direita algumas das vulnerabilidades que podem ser exploradas em cada um dos vários recursos apresentados.

Recursos do Sistema	Vulnerabilidades
PESSOAL	. Acesso a informação, equipamentos críticos; . Nível de formação e conhecimento; . Probabilidade do erro humano; . Falta de ética; . Frustrações no trabalho;
INSTALAÇÕES	. Quebra de segurança física; . Segurança não implementada de raiz; . Localização inapropriada das instalações;
HARDWARE DE REDE	. Configurações físicas mal efectuadas; . Acessos inseguros; . Ferramentas de administração deficientes; . Más políticas de segurança; . Falta de planos de contingência; . Falta de renovação de equipamentos; . Hardware não testado; . Políticas de integração deficientes; . Danos físicos;
SOFTWARE DE REDE	. Não alteração da configuração base; . Passwords de origem não alteradas; . Protocolos inseguros; . “Bugs”; . Má administração e exploração do software; . Heterogeneidade do software; . Software não testado;
DISPOSITIVOS PERIFÉRICOS	. Localização;

André Bento
Aspirante-Aluno Infantaria

	. Segurança física deficiente; . Políticas de segurança e de pessoal deficientes; . Conexões fantasma; . Dispositivos não testados;
DISPOSITIVOS DE ARMAZENAMENTO	. Gestão ineficiente; . Más políticas de segurança; . Falha de equipamento; . Dispositivos em ambiente não controlado;
SISTEMAS OPERATIVOS	. *Passwords* de origem não alteradas; . Características de Segurança fora de uso; . Má gestão das configurações de segurança; . Deficiente aplicação das políticas de segurança;
APLICAÇÕES DE NÍVEL DE SISTEMA	. Políticas de Acesso; . Más configurações de segurança;
DADOS DE ACESSO	. Deficientes políticas de *backup* e de *recovery;* . Falta de planos de contingência; . Corrupção de dados;

Quadro III – Recursos e Vulnerabilidades dos Sistemas de Informação
(Santos *et al,* 2008)

2.2.5 - Ameaças nos Sistemas de Informação de uma Organização

Depois da análise do quadro III, podemos constatar que é essencial supervisionar programadores e gestores de sistema que trabalham com as tecnologias de informação de uma organização. Estes devem ser alertados para as necessidades de segurança dos diversos sistemas que gerem. A segurança informática em redes de computadores deve socorrer-se de meios adequados para impedir, prevenir, detectar e corrigir violações de

segurança no domínio das informações, devendo os indivíduos, que o gerem, serem sensibilizados para tal, criando-se um esquema de segurança e de auditoria.

Devem ser projectadas políticas continuadas e planos de segurança, que considerem a integridade dos dados, o seu carácter confidencial e as áreas de informação de uso exclusivo. "A segurança não é um fim, mas sim um percurso permanente. O objectivo da organização será estar sempre um passo à frente dos diversos agentes de ameaças de modo a não estar sujeita a nenhuns ou significativos Riscos". (Bessa *et al*, 2008)

2.3 - Infra-estrutura de Informação Nacional (IIN)

O ciberespaço pode ser materializado pelas infra-estruturas que fazem com que ele funcione, permitindo as interacções electrónicas e os fluxos de informação que nos permitem construir um mundo virtual.

Assim, a infra-estrutura de informação nacional *"é um simples conjunto de sistemas independentes, ligados e interoperáveis",* (Herzfeld, 1999) mas que são essenciais à vivência diária.

2.3.1 - Necessidade da Infra-estrutura de Informação Nacional para um Estado

No contexto de uma economia globalizada, a competitividade de um país, relativamente aos seus principais parceiros comerciais traduz-se por gerar riqueza e também pela estrutura e enquadramento das infra-estruturas de informação de que dispõe. (Herzfeld, 1999)

"Partindo do facto que a Internet é uma "rede de redes", podemos dizer que a Infra-estrutura Global de Informação é constituída com base nas interligações das Infra-estruturas de Informação Nacionais dos vários Estados". (Nunes, 2003) Para tal, se um Estado quer prosperar e evoluir, ligando-se ao ciberespaço terá que efectuar um cuidadoso planeamento e desenvolvimento da sua Infra-estrutura de Informação Nacional.

"Caracterizando a Infra-estrutura de Informação Nacional, podemos constatar que se constitui por rede telefónica, através da qual se processa normalmente o acesso à internet, os Fornecedores de Serviço de Acesso à Internet, os cabos de redes de telecomunicações e de TV por cabo e até a porção da própria Internet que permite garantir um acesso global aos recursos de informações residentes no exterior do País". (Nunes, 2003)

Após esta caracterização não nos podemos esquecer que a Internet é muito mais que uma simples rede global. Esta definição não engloba as empresas privadas, que também se

podem ligar à Internetde variadas formas, que o Estado não controla, tenta antes regulá-la. É também importante referir que existem outros tipos de ligações que não utilizam somente os serviços referidos anteriormente, como por exemplo os satélites, a rede GSM, etc.

2.3.2 - Vulnerabilidades da IIN

Conhecendo a IIN e o conjunto de infra-estruturas que dela dependem, infra-estruturas críticas[28], percebe-se que existe uma grande inter-dependência entre as infra-estruturas críticas e a infra-estrutura de informação nacional. Esta interdepêndencia começou a assumir especial importância na passagem do milénio, com a ameaça de ocorrência de um problema informático,[29] que obrigou à realização de testes exaustivos a todas as infra-estruturas que utilizassem processadores. Também os cortes de energia que se fizeram sentir no Reino Unido[30], devido à acção de um vírus informático chamado *Blaster*[31], constituem motivo de reflexão.

Esta infra-estrutura constituída por sistemas tecnológicos agregados, difíceis de testar até ao limite pela sua natureza complexa, revela pontos fracos que podem ser explorados por actores hostis.

De seguida apresenta-se um quadro onde se pode ver a interdependência das infra-estruturas críticas nacionais à rede eléctrica nacional.

[28] Definição apresentada na Directiva Ministerial de Defesa Militar de 2002
[29] Bug do ano 2000
[30] A Zona Sul e Sudeste de Londres, no dia 28 de Agosto de 2003, ficou cerca de 6 horas privada de energia devido a uma falha registada no seu sistema de abastecimento eléctrico, tornando inoperacional 60% da rede de metro de Londres, provocou engarrafamentos caóticos, devido ao não funcionamento dos semáforos e afectou a rede ferroviária uma vez que não foi possível recorrer a geradores porque a falha era de grande dimensão. (Público, 2003)
[31] Segundo o Eng. Sousa Cardoso em entrevista (na sua qualidade de Especialista na área de Segurança da Informação).

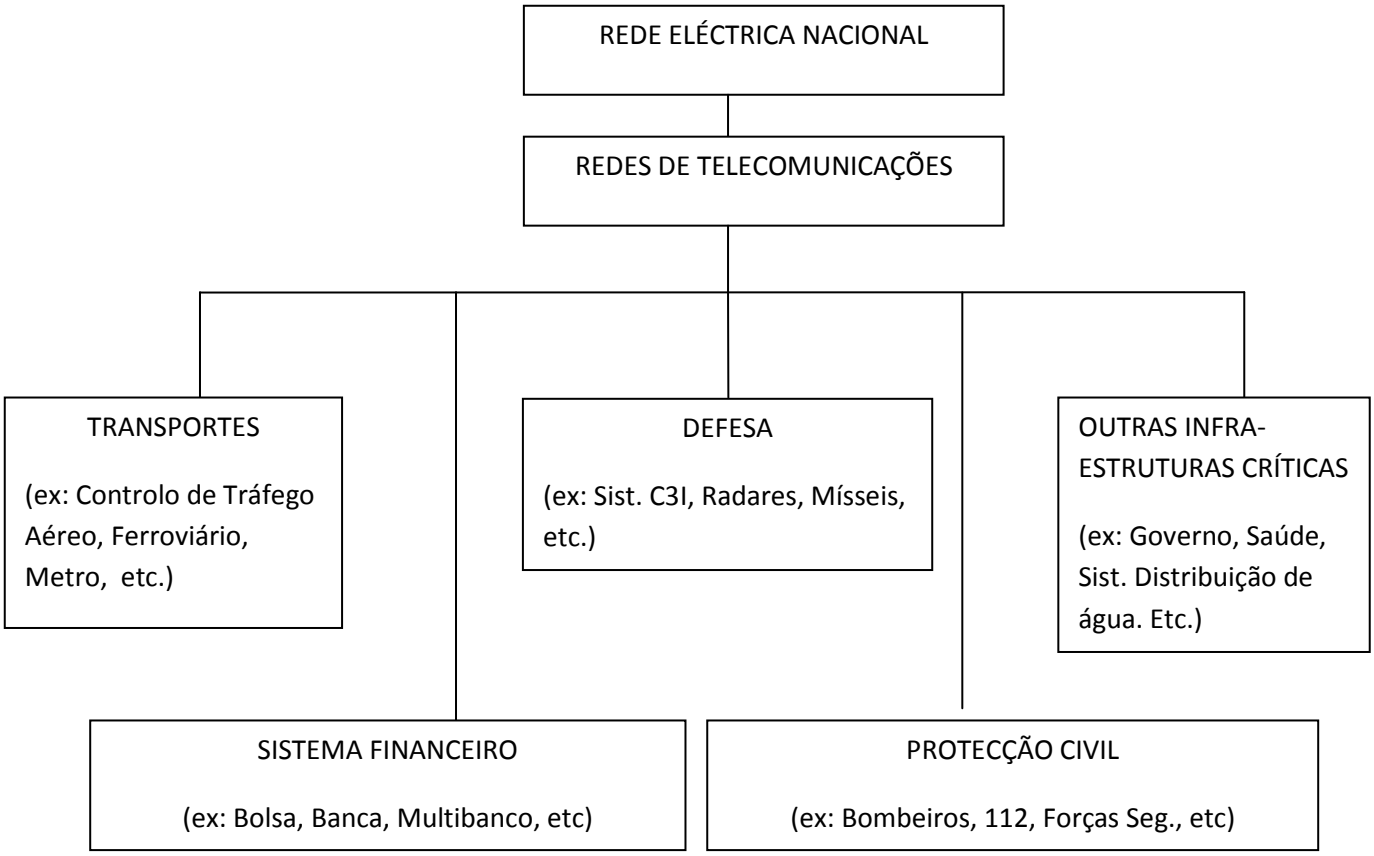

FIG.1 - Modelo de Interdependência das Infra-estruturas Críticas Nacionais[32]

Todas as infra-estruturas críticas nacionais apresentam uma dependência estrutural relativamente à Rede Eléctrica Nacional e uma dependência funcional relativamente à IIN, pelo que importa analisar o risco associado a estas duas infra-estruturas para tentar determinar qual o potencial impacto de um ataque ciberterrorista à IIN, com o objectivo de adoptar as medidas e contra-medidas necessárias.

Um ataque à IIN pode ter o resultado de um decréscimo de produtividade, gerando prejuízos financeiros, entre outros, criar a instabilidade, o caos social e eventualmente a perda de vidas humanas.

2.3.3 - Ciberdefesa da IIN

Tendo por base a prossecução do objectivo nacional de garantir a protecção da IIN, torna-se necessário criar uma organização que proteja essa infra-estrutura permitindo a sua ciberdefesa. É imprescindível estabelecer normas de segurança para infra-estruturas de

[32] Adaptado de General Pinto Ramalho (2003) e Sousa Cardoso (2003).

informação governamentais devendo-se recomendar também que as infra-estruturas críticas privadas adoptem normas de segurança.

Para tal é importante a criação de um *Computer Emergence Response Team* (CERT)[33] Nacional, a implementação de programas de treinos e de educação, financiamento e desenvolvimento de mecanismos de segurança. A par destas medidas é fundamental a redundância das infra-estruturas de informação, o desenvolvimento de regimes de cooperação e actuação internacional na área da protecção da IIN. (Cardoso, 2003)

Segundo Viegas Nunes, na implementação do conceito de protecção de infra-estruturas crítica de informação devem-se articular em três pontos: Protecção, Detecção e Reacção; para tal assumem particular importância medidas de ciberdefesa. (Nunes, 2004)

2.3.4 - Papel das Forças Armadas/Exército na Defesa da IIN

A implementação de um sistema de ciberdefesa deverá passar pela criação de um CERT nacional tutelado pelas Forças Armadas[34], a que responderiam os CERTs sectoriais de cada ministério, o que permitiria uma permanente avaliação de ameaça, relatando incidentes ocorridos nas Infra-estruturas de Informação Nacionais.

Este sistema poderia ser estruturado com base num *Network Operation Center* (NOC) e numa rede de CERTs que constituiriam uma *Rede de Alerta de Relato Nacional* (RARN), de acidentes ocorridos nas redes e sistemas de informação dos diversos sectores ou áreas críticas[35]. A existência de uma RARN obrigaria as diversas entidades da rede a relatar os incidentes, permitindo implementar um plano de recuperação da IIN. Dentro deste contexto deverá ser levantada uma Infra-estrutura de Informação Crítica Mínima Nacional.[36] (Nunes,2004)

---

[33] O CERT é já utilizado em diversos países, e pressupõe o estudo das vulnerabilidades da segurança da Internet, em sistemas ligados à Internet e desenvolve o treino para a adopção de medidas e contra-medidas de segurança.

[34] A função de um CERT é variada, mas fundamentalmente é proteger a infra-estrutura de telecomunicações de eventuais ciber-ataques. Ora, esta é uma função de protecção das infra-estruturas críticas e consequentemente podem afectar a segurança nacional, principalmente quando se tratam de ameaças externas. Então será função das Forças Armadas. É evidente que os dados colhidos pelo CERT podem então ser passados para a forças policiais quando solicitados, existe a lei de protecção dos dados (em Anexo A) que clarifica a situação, para posterior uso em matéria de investigação criminal.

[35] As áreas funcionais críticas a envolver neste sistema poderiam ser as seguintes: Intranet do Governo, Sector das telecomunicações, área da Defesa e das Forças de Segurança, Rede Eléctrica nacional, Transportes, Serviço Nacional de Bombeiros e Protecção Civil, Sistema Interbancário de Serviços, PETROGAL.

[36] No caso português o Sistema Integrado das Redes de Emergência e Segurança de Portugal (SIRESP) constitui a primeira aproximação a uma Infra-estrutura de informação crítica mínima nacional, assegurando as comunicações das Forças Armadas e de Segurança e dos serviços de emergência nacionais. Esta rede, em caso de emergência, poderá garantir a centralização do comando e da coordenação nacional.

Estas áreas deveriam ser criadas, desenvolvidas e supervisionadas por militares e civis (Forças Policiais) especialmente vocacionados para tal, para se poder efectuar uma política de segurança de informação contra ciberataques. Com a criação destes sistemas é necessário, também, existirem alterações ao nível estrutural, de doutrina e de orientações da política do Estado.

2.4 - Sistema de Informações e Comunicações ao Nível do Exército

Em Portugal a ciberdefesa da IIN está ainda a desenvolver-se pelo que se apontam algumas teorias para a sua implementação. Esta defesa deve ser tutelada pelas forças armadas, como vimos no ponto anterior. Embora ainda não haja uma participação significativa das Forças Armadas, nomeadamente do Exército, na defesa das ameaças ao sistema de informações nacional, o Exército tem vindo a desenvolver um projecto que se traduz como um Sistema de Informações e Comunicações Táctico (SIC-T), para a actuação no campo de batalha, onde assenta o Sistema de Comando e Controlo do Exército (SICCE).

2.4.1 - Sistema de Informações e Comunicações Táctico (SIC-T)

As modernas tecnologias podem afectar o comando e o controlo (C2) se forem integradas nas estruturas de comando, acelerando os procedimentos de recepção de notícias, apoiando o Comandante a aumentar a eficácia da sua decisão. Neste contexto os comandantes têm de definir quais as informações que precisam para um C2 efectivo, e ao mesmo tempo reconhecer as vulnerabilidades que as novas tecnologias acarretam, já que transformam a informação num elemento preponderante e de valor significativo.

Assim a eficácia da capacidade de C2, com a garantia de interoperabilidade entre as informações, realizada através da troca de informação pertinente, relevante e oportuna, é vital para o eficaz desempenho do processo de decisão táctico.

Para o nosso Exército elegeu-se como prioritário o âmbito táctico e, nesse sentido, a capacidade de C2 insere-se dentro deste projecto. O SIC-T deverá contemplar aplicações operacionais, um sistema de C2 (SICCE), um serviço de mensagens ou correio electrónico militar e uma infra-estrutura de transporte da informação. O SIC-T tem como objectivo “definir, desenvolver e implementar, de forma faseada e modular, a estrutura, a organização, a tecnologia, as funcionalidades, os serviços e as interoperabilidades de um SIC-T para o Exército Português, constituindo unidades/órgãos ou módulos SIC destacáveis, típicos do

escalão Brigada/Batalhão, com especial ênfase para a sua aplicação em ambientes de actuação das FNDs.[37]" (DST, 2003)

O SIC-T apresenta uma capacidade real de integração operacional, para um melhor e mais eficaz desempenho nas operações militares terrestres, explorando o estado da arte das comunicações, dos computadores, dos sensores e sistemas de armas, sendo assim o primeiro passo para a digitalização do sistema de forças nacional (SFN), de modo a proporcionar vantagens técnicas que permitam alcançar, ao nível táctico e nas capacidades de C2, os desafios do novo milénio:

. Fácil adaptação e integração com o conceito de Operações Centradas em Rede;

. Apoio eficaz às principais funções de planeamento e Estado Maior, reduzindo ao mínimo o tempo utilizado;

. A situação operacional encontra-se permanentemente actualizada;

. Transmissões mais rápidas e eficientes dos planos o que torna as ordens mais eficazes;

O SIC-T deverá fornecer aos utilizadores diferentes serviços totalmente integrados, voz, mensagem, dados e imagem. Um projecto desta envergadura tem custos elevados, pelo que não basta montar o sistema e fazê-lo funcionar, pois embora traga vantagens como a velocidade de recepção de notícias, devemos ter em conta as possíveis vulnerabilidades inerentes ao sistema, pois para além da segurança física do sistema, ao ser ligado em rede fica sujeito a outro tipo de ameaças - as ciber-ameaças

O estudo das necessidades de um sistema SIC-T para o SFN deve centrar-se no apoio a um determinado escalão de Comando que possibilite uma projecção rápida, para garantir a actuação em ambiente operacional, instrução e treino moderno e eficaz dos quadros e tropas.

Ao nível nacional, o possível emprego do sistema SIC-T, não deve ultrapassar em cada momento o escalão brigada ou batalhão, embora deva ter uma zona de acção de dimensões superiores às de uma brigada ou batalhão convencional. (DST, 2003)

2.4.2 - Sistema de Informações de comando e controlo do Exército (SICCE)

"O SICCE pretende afirmar-se como um "Sistema dos Sistemas de Informação", pelo que terá de dispor de um moderno sistema de comunicações, dotado de arquitectura fiável e flexível que garanta a interoperabilidade e a integração funcional das redes de comunicações de escalão Brigada/Batalhão, com especial ênfase para a sua utilização em ambientes de actuação das FNDs". (Viegas Nunes, 2005)

[37] FND- Forças Nacional Destacada

O SICCE, foi assim desenvolvido devido à necessidade de informatizar o TO a todos os níveis, de forma a que todos conheçam as alterações do campo de batalha em tempo real, de forma a melhorar o comando e controlo das operações. (DST, 2003)

O SICCE tem como principais características:

- Capacidade real de integração do sistema com as forças operacionais e entre as forças operacionais;

- Como o sistema de tratamento de imagem é realizado, através de vectores, a imagem nunca perde nitidez;

- Permite uma visualização a 3D;

- Possui *firewall*[38] e sistemas de defesa para impedir possíveis ciber-ataques;

- Capacidade para difundir ordens directamente dos Postos de Comando para o terreno em tempo real;

- Capacidade de introduzir nos planos de operações as condições meteorológicas previstas;

O SICCE possui também um sistema de gestão de rede com uma arquitectura modular. Este sistema de gestão de rede é o cérebro do sistema de comunicações, o que permite o controlo e supervisão de todo o equipamento operacional de cada um dos módulos.

Caso a ligação onde se encontra o sistema de gestão de rede seja destruído, o sistema não perde nem fica diminuído em nenhuma das suas potencialidades, pois o sistema de gestão de rede auxiliar fica imediatamente activo.

Este sistema tem algumas capacidades, entre as quais, pode reconfigurar a rede sempre que necessário, pode transmitir mensagens encriptadas, gere as chaves criptas, gere a frequência de rede, dependendo dos equipamentos, tem a capacidade de monitorização dos equipamentos da rede que se encontram activos e cada utilizador tem a sua chave de acesso à rede. (DST, 2003)

No nosso Exército este sistema não funciona na sua plenitude, apesar de existir uma equipa de gestão deste sistema na Escola Prática de Transmissões, onde caso seja necessário se introduzam novas informações. O sistema ainda não possui a informação necessária para o planeamento das operações pois a actualização da informação não é feita por parte dos utilizadores de forma regular.

[38] *Firewall* consiste num dispositivo de uma rede de computadores que tem como objectivo aplicar uma política de segurança a um determinado ponto de controlo da rede. A sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão ou recepção de acessos nocivos não autorizados de uma rede para outra.

2.4.3 - Capacidade de fazer face às ameaças ao Sistema de Informações e de Comunicações ao nível do Exército

Face ao exposto anteriormente, este tipo de sistemas que o Exército está a desenvolver é conseguido através de redes e de computadores. Uma falha do sistema, em tempo de guerra, por exemplo, pode fazer com que os dados contidos na rede, ou seja a informação nela contida, possa ser "desviada" para onde não deve ir, pondo em perigo a sobrevivência de uma operação.

Neste tipo de sistema tem de se ter em conta o ciclo da segurança que consiste: na prevenção, detecção e na resposta. Estando um sistema como o SIC-T, ou o SICCE ligado à Internet ou a uma rede local, pode ser atacado. Nesse caso podem ter-se em conta dois tipos de ataque:

- Levado a cabo por um atacante casual de forma indiscriminada, um vírus por exemplo;
- Levado a cabo por ataques de indivíduos determinados a obter a nossa informação;

Em relação aos vírus, os Sistemas de Comunicações e de Informações do Exército terão de adquirir *Firewalls*[39], ou equipamentos tipo, mas sempre actualizados, fazer a manutenção de ferramentas de *Malware*[40] e aplicar *Patches*[41], que consiste em anular o erro ou a vulnerabilidade que foi atingida pelo vírus, sendo que este tipo de problema o sistema consegue resolver.

No caso de ataques de indivíduos determinados a obter a nossa informação o problema torna-se mais grave, pois é necessário conter a progressão do ataque e ser apoiado por uma equipa especializada para travar as acções *hacking*, devendo para isso estes tipos de sistemas, possuírem essas equipas especializadas. (Bessa *et al*, 2008)

[39] Equipamento físico, que constitui uma barreira de protecção entre duas redes, neste caso, Internet e rede local, negando o acesso de utilizadores não autorizados a um determinado computador ou ficheiro.

[40] O termo malware provém do termo inglês *malicious software*, que consiste num software destinado a infiltrar-se num sistema de um computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informação. (cavalos de Tróia, spyware, são considerados malware)

[41] *Patch,* do inglês significa penso, ou remendo e é utilizado em Sistemas de Informação para designar uma correcção que deve ser implementada num determinado programa, de modo a anular uma vulnerabilidade ou erro.

CAPÍTULO 3 - CAPACIDADE MILITAR CENTRADA EM REDE

As Forças Armadas actuam num ambiente em que a necessidade de informação é permanente e indispensável para a sua actividade e têm vindo a passar por importantes transformações. As transformações afectam as Forças Armadas ao nível político, com o fim do serviço militar obrigatório, a nível tecnológico com a aquisição de novos meios, bem como o modo de obtenção de informação credível e ao nível social com as FNDs.

Neste âmbito as estruturas militares devem dar lugar as estruturas mais descentralizadas e "horizontalizadas" da Era da Informação, como tem vindo a ocorrer nas organizações civis.

A capacidade militar centrada em rede não deve ser vista como uma forma de organização militar do futuro, mas sim como o que caracteriza a sociedade em que vivemos, que traduz a estrutura social da "Era da Informação" pois, à semelhança das restantes actividades do homem, também a condução da guerra depende da troca de informação em rede. (Nunes, 2005)

"O espaço onde a informação circula é o fundamento daquilo que podemos considerar a lógica inerente às novas formas de decisão, a rede." (Nunes, 2005)

3.1 - Implicações para o C2

A dinâmica do campo de batalha sempre colocou aos chefes militares duas formas de reduzir, ou lidar com a incerteza: centralização das acções de comando e a descentralização.

No que respeita à centralização um único homem comandava um Exército, onde cada um dos seus subordinados estava apenas autorizado a efectuar aquilo que o comandante pudesse controlar. A descentralização que é hoje suportada por redes de comunicações fiáveis e flexíveis, permitiu estruturar organizações e conceber operações sem a necessidade de um controlo contínuo, o que originou que o comandante pudesse alterar as suas intenções a cada momento, caso assim o entendesse.

Assim sendo e pretendendo a instituição militar tipificar a tomada de decisão através do processo de C2, é necessário que exista uma rede que viabilize os fluxos de informação, para que o processo funcione.

Sem esta rede é impossível que um comandante controle e comande a sua força, pois para o fazer necessita de informação actual, fiável e oportuna, já que qualquer decisor necessita de dados que lhe permitam resolver um determinado problema no menor tempo possível. Assim, utilizando esta rede de informação um comandante tem uma melhor percepção e um melhor conhecimento operacional, o que permite compreender as

dinâmicas envolventes externas (pontos fracos, pontos fortes do oponente) e internas (as suas próprias fraquezas e potencialidades). Utilizando esta rede o comandante não toma desde o início uma solução efectiva, podendo alterá-la conforme se vão desenrolando os acontecimentos, mantendo o inimigo na incerteza sobre o seu próximo passo.

Os comandantes devem então ser capazes de visualizar as suas opções e se necessário mudar rapidamente com o desenrolar da situação, ou seja, devem demonstrar uma elevada flexibilidade e agilidade no exercício de C2 das suas forças. Para esta situação ser possível e eficaz a rede de informações tem de ser tecnologicamente evoluída. (Alberts, 1999)

3.2 - Conceito de Capacidade Militar Centrada em Rede

Segundo alguns cientistas norte americanos a Capacidade Militar Centrada em Rede consiste "num conceito de operações, resultante da obtenção da superioridade de informação, que gera um maior poder de combate a partir da integração em rede de sensores, decisores e atiradores para obter uma percepção partilhada, uma maior rapidez da acção de comando, um melhor tempo das operações, maior letalidade, melhor capacidade de sobrevivência, e um determinado grau de auto-sincronização." (Perry *et al,* 2002)

O conceito acima referido baseia-se na ideia de que é possível obter superioridade no domínio da informação e utilizar esta superioridade para obter uma percepção melhorada da situação, reduzir a duração do processo de decisão, ajustar o "tempo" das operações, melhorar tanto a protecção como a sustentação da força e a própria sincronização das actividades militares. O objectivo desta abordagem é o aumento da capacidade para recolher, processar e gerir a informação. A Capacidade Militar Centrada em Rede focaliza-se na interacção gerada entre processos, tecnologia e competências das organizações, permitindo obter uma superioridade qualitativa e quantitativa na condução das operações militares. (Nunes, 2005)

3.2.1 - Dimensões da Guerra Centrada em Rede

Tentando traduzir uma visão estrutural, funcional e organizacional, podemos dizer que uma força que procure explorar a capacidade militar centrada em rede, depende da existência de uma infra-estrutura de rede, porta de entrada, dos fluxos de informação que permitem a decisão e das pessoas que tomam as decisões.

A Guerra Centrada em Rede possui assim três dimensões: redes, informações e pessoas.

Todos os princípios associados à guerra centrada em rede partilham o conceito de rede de redes, defendendo que um ambiente de informação em rede fornecerá uma capacidade de aquisição, produção, distribuição, manipulação e utilização da informação.

Desta forma os sistemas de informações devem evoluir para sistemas integrados, para se atingir uma interoperabilidade global dos sistemas, pois, seja qual for o estado final pretendido[42], o importante é a informação necessária estar disponível para os decisores e para os responsáveis das actividades militares. O acesso e a utilização de informação sempre foi importante, mas nem sempre existiu a capacidade para disponibilizar a informação de forma eficaz. Qualquer decisor ou comandante tem de saber identificar a informação necessária, obtê-la e processá-la, dentro do intervalo de tempo de que dispõe para decidir.

O funcionamento em rede vem acelerar este processo, encurtando o ciclo o ciclo da informação e aumentando a informação disponível. A recolha e gestão da informação em rede pode ser a chave para a obtenção da superioridade de informação sobre um adversário. À medida que são introduzidos novos sistemas de informação, a gestão da informação crescerá em importância e as ferramentas que permitem explorar o seu valor assumirão um papel central na condução de praticamente todas as actividades militares.

A dimensão humana do processo de uma capacidade militar centrada em rede baseia-se na necessidade de formar e treinar todo o pessoal militar e não militar das Forças Armadas para que estes possam utilizar os seus conhecimentos e experiência em prol do futuro desenvolvimento desta capacidade. As pessoas terão de desenvolver processos de colaboração e aprender como partilhar e encontrar a informação necessária e depois utilizá-la para planear e apoiar o comandante na tomada de decisões.

Apesar de uma rede permitir transferir a informação entre diversos locais, cada vez com volume maior e em tempo real, o ser humano revela-se determinante para a sua utilização e para a exploração do poder contido na informação, pois os sistemas de apoio à decisão vão ajudar a reduzir o esforço cognitivo dos decisores, na maior parte das situações, mas será sempre um ser humano a tomar a decisão final. (Nunes, 2005)

[42] Este estado final, tanto pode ser aplicado ao ambiente operacional como ao ambiente não operacional. Se o estado final for a obtenção de um determinado efeito no espaço operacional, ou se o objectivo for assegurar a continuidade das operações e o fornecimento em tempo útil do apoio logístico necessário.

3.3 - Desenvolvimento de uma Capacidade Militar Centrada em Rede e sua protecção

Antes de se começar a falar na aplicação de uma capacidade militar centrada em rede é necessário conhecer a missão, a combinação mais adequada de um conceito de operação, uma abordagem de C2, uma estrutura organizacional e o conjunto de fluxos de informação. Estes dados devem ser complementados com uma centricidade em rede adequada. A capacidade militar centrada em rede não se limita apenas à guerra em si, foi também concebida para apoiar outros tipos de conceitos, como o terrorismo. Não é suficiente saber que a missão foi bem sucedida, ou apenas conhecer o seu estado final, mas antes controlar e conhecer todas as fases que se ultrapassam para se atingir a finalidade da missão. O C2 torna-se assim muito mais importante dentro deste novo tipo de guerra.

Para se pensar e desenvolver uma capacidade militar centrada em rede é necessário criarem-se algumas medidas, pelo que para se desenvolver uma capacidade militar centrada em rede necessitamos de colocar as seguintes questões:

1) Quem é o elemento, no campo de batalha, a tomar a decisão o mais rapidamente possível?
2) O conceito de operação, doutrina, organização e treino suporta esta capacidade que se pretende implementar?
3) Em que medida esta capacidade é viável, quando as decisões são esperadas o mais rapidamente possível?
4) Quais as decisões que poderiam ser automatizadas e qual é a melhor maneira de distribuir as restantes decisões?
5) Qual é a informação mais importante, quais os tempos críticos de apoio à tomada de decisão e quando pode ser colocada à disposição do decisor?
6) Qual é o impacto das equipas distribuídas que partilham o acesso à informação e que actuam sem prévia sincronização? (Alberts, 1999)

As perguntas acima ilustram a natureza das incógnitas que têm de ser exploradas, se se quer obter o máximo partido das oportunidades oferecidas por uma Capacidade Militar centrada em Rede.

Actualmente, para implementar um sistema desta envergadura consideram-se cinco níveis básicos de medidas:

- Medidas de desempenho das infra-estruturas;
- Medidas de *Awarness* do espaço de batalha (neste caso a rede);
- Medidas de Conhecimento do funcionamento do espaço de batalha;
- Medidas de Utilização do espaço de batalha (utilização da rede);

- Medidas da utilidade Militar no espaço de batalha;

Estas medidas se seguidas e exploradas são a base para a implementação de um sistema fiável de uma Capacidade Militar Centrada em Rede, onde o primeiro nível envolve medir o desempenho do C4ISR[43] que se pode traduzir pela capacidade de transmitir ou distribuir informação, da conectividade entre as partes e pela largura de banda. Na outra ponta das medidas a adoptar, encontram-se medidas relacionadas directamente com a missão.

Para além destas medidas é necessário sermos capazes de identificar e medir características-chave de uma Capacidade Militar Centrada em Rede. (Alberts *et al*, 1999)

Para desenvolver uma capacidade militar centrada em rede é necessário possuir uma boa protecção, para que a informação que circule na rede não seja conhecida pelo inimigo.

Um programa de segurança bem desenvolvido e apoiado em tecnologias de informação, deve ser constituído para em primeiro se lugar desenvolver uma política de segurança informática, informar os utilizadores das suas responsabilidades de segurança em tecnologias de informação, bem como os processos de acompanhamento e de revisão do programa de segurança.

Um programa de segurança desta envergadura deve ser implementado a todos os níveis da organização, incluindo as altas patentes e o restante pessoal, no caso de uma organização como o Exército, para que a segurança esteja presente em todos os níveis da estrutura hierárquica. A eficácia deste esforço vai determinar e eficácia do próprio programa de segurança em tecnologias de informação. Medidas de sensibilização e de formação poderão ser o veículo a ser utilizado para comunicar os requisitos de segurança por toda a organização. Com esta formação todos os utilizadores saberiam os comportamentos a tomar e as regras a seguir para a utilização dos sistemas de informação, conhecendo desde o inicio as expectativas, adquirindo a responsabilidade depois de informados, treinados e conscientes da informação a ser tratada. Desenvolver esta estratégia de sensibilização e formação, permite à organização uma avaliação das necessidades para o desenvolvimento, implementação e manutenção do programa de segurança.

Existem algumas medidas[44] que devem ser referidos e discutidos na implementação de de segurança, para além de *software* que protejam a rede e o seu acesso a estranhos, pois o principal vector da ameaça, apesar de tudo, continua a ser o ser humano. Para tal a organização, nomeadamente esta rede, deve estar protegida e implementar tais regras de segurança para que rapidamente se resolvam os problemas que dela advêm. (NIST, 2003)

[43] Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance, traduzido seria Comando, controlo, comunicações, informações, vigilância e reconhecimento.
[44] Em Anexo B encontram-se os tópicos/medidas para se desenvolver um programa de segurança, interna e externa, num sistema de informações ligados a uma rede global ou interna.

Capítulo 4 - Conclusões

O Ciberespaço define-se como um local onde os interesses nacionais devem também ser defendidos, onde se impõem novas interacções e novas relações entre actores políticos. Neste domínio as estratégias usadas são baseadas no valor que a informação possui, bem como as suas fontes, onde o seu valor é utilizado para efectuar operações de protecção do ciberespaço.

Apesar de a sua implementação ser bastante complexa, não podemos ignorar a necessidade de uma Estratégia de Informação Nacional. Se tal Estratégia não existir, num contexto internacional, qualquer país poderá ocorrer num risco de ser simplesmente empurrado para onde as super-potências queiram, ou por organizações que conduzam actividades de Guerra de Informação.

Podemos concluir que existe uma extrema necessidade de acção para lidar com o presente e com os desafios que existem actualmente, dos quais a defesa contra possíveis ataques às infra-estruturas críticas de informação nacional, podem afectar a capacidade das autoridades responsáveis a conseguir levar a cabo o quotidiano normal, fazendo com que todo um país possa parar. De acordo com isto é recomendado uma série de acções para melhorar e preparar um Estado para este tipo de guerra – Guerra da Informação.

Ao longo de todo o trabalho pudemos ver que as novas tecnologias de informação têm sido profundamente difundidas no Exército. Mostrámos também que a guerra centrada em rede trouxe um valor acrescentado à capacidade de C2, concluindo que uma nova forma de guerra é possível. A percepção existente de que os mecanismos existentes, bem como os processos de segurança têm dificuldade em acompanhar a tecnologia e a dinâmica das vulnerabilidades, faz com que seja urgente uma forte campanha nacional para chamar a atenção de que é importante defender e preservar as infra-estruturas nacionais de informação e os seus recursos. Isto obrigará os Estados a rever o seu conceito de defesa nacional.

As ameaças existentes são inúmeras, pelo que as que foram abordadas no corrente trabalho foram as ciber-ameaças, que envolvem essencialmente computadores ligados em rede e Internet. Tais ameaças têm hoje em dia um peso notável, pois a maior parte dos Estados têm vindo a evoluir tecnologicamente. Os Estados mais evoluídos tecnologicamente transferem e tratam a maior parte das suas informações em rede. Muitas vezes essa rede pode ser a base de informação essencial e, caso seja atacada, pode vir a perder a informação, que num caso extremo possa contrariar a continuidade do bem-estar e da segurança nacional, pelo que se têm de tomar cada vez mais medidas para preservar a segurança de informação. Depois de um estudo acerca das eventuais ameaças que podem

afectar um sistema de informações em rede propomos a criação de um CERT nacional tutelado pelas Forças Armadas. Com a criação de um CERT seria possível alertar em tempo oportuno a ocorrência de possíveis falhas. Para que este sistema funcionasse criar-se-iam CERTs sectoriais, onde por exemplo o Exército seria um dos CERTs sectoriais, que responderiam ao CERT nacional.

Para já o Exército tem vindo a acompanhar esta fabulosa evolução e estamos cientes que o SIC-T e o SICCE são passos bastante seguros na prossecução de um futuro CERT, pelo que ainda têm de se centralizar numa só unidade, ou subunidade, para que os sistemas de informações possam funcionar correctamente, não estando divididos pelo país, tal como acontece actualmente.

Um computador só é realmente importante quando pode interagir com outros dispositivos e criar valor para quem o utiliza. As redes de interligação dos diferentes computadores apresentam-se como as estruturas mais críticas de todo o ciberespaço. Em termos de falhas não é apenas a rede a causadora das mesmas, o homem, como utilizador, em conjunto com as infra-estruturas são as principais Agentes de falhas. A razão da criação de um sistema de informações prende-se com a existência de dados e a necessidade de os manipular, distribuir e interpretar, retirando o máximo proveito destes.

As acções militares só por si, no moderno campo de batalha já não conseguem resolver todos os problemas de segurança. Pelo contrário, as acções militares necessitarão, cada vez mais, de integração de todos os instrumentos do poder disponíveis para a obtenção do sucesso operacional. É portanto necessário o levantamento de uma capacidade militar centrada em rede, sem a qual o sucesso operacional poderá ser condicionado ou mesmo limitado. A capacidade para responder de forma mais rápida e precisa, utilizando um menor número de recursos, de maior qualidade e interligados, funcionará como um multiplicador de forças, permitindo ao Exército e às Forças Armadas obter facilmente o sucesso na missão.

Reconhecida a importância da utilização dos princípios de uma Capacidade Militar Centrada em Rede, torna-se portanto necessário prosseguir as acções de formação e de informação nesta área, favorecendo a implementação e o desenvolvimento de uma capacidade militar centrada em rede.

Importa que as Forças Armadas e o Exército continuem a implementar um processo de modernização tecnológica e o desenvolvimento de novas capacidades, explorando para esse efeito a iniciativa que sempre as caracterizou e adaptando-se à sociedade da informação e à dinâmica social da sua envolvente.

Bibliografia

LIVROS:

ALBERTS, GARSTKA e STEIN (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority,* CCRP Publication Series

ARQUILLA, John e RONFELDT David (1993). "Cyberwar is Comming." In *In Atheana's Camp Preparing for Conflict in the Information Age*, Rand.

ARQUILLA, John e RONFELDT, David (2001). *Network and Netwars: the Future of Terror, Crime and Military*; National Defense research Institute- RAND

CASTELLS, Manuel (1999). *A Sociedade em Rede.* São Paulo, Paz e Terra

COUTO, Cor Art Abel Cabral, (1988). Elementos de Estratégia, Apontamentos coligidos pelo Instituto de Altos Estudos Militares.

PERRY, *et al*. (2002). *Measures of effectiveness for the Information-Age Navy: The Effects of Network-Centric Operations on Combat Outcomes.* Santa Monica, Rand.

TOFFLER, Alvin (1991). *The Third Wave,* New Work Bantam Books, New York

SANTOS, Paulo BESSA, Ricardo, PIMENTEL, Carlos e (2008) *Ciberwar: O Fenómeno, as Tecnologias e os Autores*; Lidel FCA;

Artigos de Revistas e Trabalhos:

BASÍLIO, Susana (2006). *A evolução dos Computadores e da Internet.* Disponível em: http://www1.ci.uc.pt/diglit/DigLit%20Ensaios/Ensaios%202005-2006/Ensaio29.htm

CARDOSO, Sousa (2003). *Guerra no Ciberespaço: Um Novo Método de Conflito,* Conferência proferida na Academia Militar em Guerra de Informação/Competetive Intelligence, Julho

DST, (2003) Projecto SIC Táctico: SITACO, SICCE; Grupo de Projecto, Maio 2003; Direcção do Serviço de Transmissões.

HERZFELD, Charles (1999). *The Defense of Infrastructure*, em Information Impacts Magazine, Setembro.

NEC_MOB (2004). *NetWork Enable Capability: An Introduction*, Pamphlet of Minstry of Defense, April

NUNES, Paulo, (1999). *Impacto das Novas Tecnologias no Meio Militar: A Guerra de Informação*, Revista Militar, Novembro Pp 1721-1745

NUNES, Paulo, (2003). "*A Geopolítica do Ciberespaço* ", Revista Militar, Outubro. Pp 1007-1029

NUNES, Paulo, (2004). *Ciberterrorismo: Aspectos de Segurança*, Revista Militar, Novembro Pp 937-957

NUNES, Paulo (2006). *Operações de Informação: Enquadramento e Impacto Nacional*, Revista Militar, Outubro. Pp 1037-1057

NUNES, Paulo, (2005*) O Impacto da Aplicação do Conceito de Network Centric Warfare nas Forças Armadas Portuguesas: Subsídios para o Levantamento de uma Capacidade Militar Centrada em Rede,* Lição Inaugural, Abertura Solene do Ano Lectivo de 2005/06, Academia Militar, Novembro.

SANTO, Espírito (2007). *Revolução dos Assuntos Militares e Revolução Militar,* Revista Militar, Fevereiro

Artigos em PDF retirados da internet:

Cohen, Fred (1999). *Strategic Security Intelligence: Information Warfare*, Fred Cohen & Associates. Disponível em: http://www.dodccrp.org/events/11th_ICCRTS/html/papers/064.pdf

FM 100-6, (1996). *Information Operations*, Documento doutrinário dos EUA, 27 de Agosto

Emerging CyberThreats: Report for 2008

Gu, Chen, Porras *et al* (2007). *Misleading and Defeating Importance-Scanning Malware Propagation*, Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm 2007), Mice, France, Setembro. Disponível em http://www.cyber-ta.org/

Mahimkar A, Dange J. *et al.* (2007). *dFence: Transparent network-based denial of service mitigation,* Proceedings of 4th USENIX Symposium on Networked Systems Design and Implementation (NSDI 2007), Cambridge, MA, Abril. Disponível em http://www.cyber-ta.org/

MOFFAT, James. Complexity Theory and network Centric Warfare

Porras, Shmatikov *et al.* (2006). *Large-scale collection and sanitization of network security data: risks and challenges,* Proceedings of the New Security Paradigms Workshop, Dugstuhl, Germany, Setembro. Disponível em http://www.cyber-ta.org/

Shmatikov V, Wang (2007). *Security Against Probe-Response Attacks in Collaborative Intrusion Detection*, Workshop on Large-Scale Attack Defense (LSAD), Agosto. Disponível em http://www.cyber-ta.org/

Shmatikov M.H. Wang, (2006). *Timing analysis in low-latency mix networks: attacks and defenses,* Proceedings of the 11th European Symposium on Research in Computer Security (ESORICS), Hamburg, Germany, Setembro. Disponível em http://www.cyber-ta.org/

The Implemention of Network Centric Warfare disponivel em http://www.oft.osd.mil/library/library_files/document_387_NCW_Book_LowRes.pdf

UKMD (2004). *Network Enable Capability: An introduction*, UK Minitry of Defense. Disponível em: http://www.cyber-ta.org/

WELCH, Thomas (2004), *Revolution in military affairs: one perspesctive*, National Defense University Disponível em http://www.cyber-ta.org/

WILSON Mark e HASH Joan NIST (2003) Building an Information tecnlogy security awarnes and training program: computer security , Outubro

Sites e Páginas da Internet:

GIL, Prata (2007). *As Ameaças à Segurança Nacional e a Guerra* Preventiva. Alameda Digital Nº5.v Disponível em: http://www.alamedadigital.com.pt/n5/guerra_preventiva.php

SCHWARTZ, John (2004). *When Computers Attack,*BitWars, Junho. Disponivel em: http://www.nytimes.com/2007/06/24/weekinreview/24schwartz.html

http://www.military.com/forums/0,15240,138895,00.html

http://www.gtisc.gatech.edu/pdf/GTISC%20Cyber%20Threats%20Report.pdf

Anexos

Índice de Anexos:

André Bento
Aspirante-Aluno Infantaria

Anexo A

Lei de Protecção de Dados

Lei n.º 67/98

de 26 de Outubro

LEI DA PROTECÇÃO DE DADOS PESSOAIS
(TRANSPÕE PARA A ORDEM JURÍDICA PORTUGUESA A DIRECTIVA 95/46/CE, DO PARLAMENTO EUROPEU E DO CONSELHO, DE 24 DE OUTUBRO DE 1995, RELATIVA À PROTECÇÃO DAS PESSOAS SINGULARES NO QUE DIZ RESPEITO AO TRATAMENTO DOS DADOS PESSOAIS E À LIVRE CIRCULAÇÃO DESSES DADOS).

A Assembleia da República decreta, nos termos da alínea c) do artigo 161.º, das alíneas b) e c) do n.º 1 do artigo 165.º e do n.º 3 do artigo 166.º da Constituição, para valer como lei geral da República, o seguinte:

Capítulo I
Disposições gerais
Artigo 1.º
Objecto

A presente lei transpõe para a ordem jurídica interna a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Artigo 2.º
Princípio geral

O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais.

Artigo 3.º
Definições

Para efeitos da presente lei, entende-se por:

a) «Dados pessoais»: qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;
b) «Tratamento de dados pessoais» («tratamento»): qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou

por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;
c) «Ficheiro de dados pessoais» («ficheiro»): qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;
d) «Responsável pelo tratamento»: a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinados por disposições legislativas ou regulamentares, o responsável pelo tratamento deve ser indicado na lei de organização e funcionamento ou no estatuto da entidade legal ou estatutariamente competente para tratar os dados pessoais em causa;
e) «Subcontratante»: a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento;
f) «Terceiro»: a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular dos dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade directa do responsável pelo tratamento ou do subcontratante, esteja habilitado a tratar os dados;
g) «Destinatário»: a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo a quem sejam comunicados dados pessoais, independentemente de se tratar ou não de um terceiro, sem prejuízo de não serem consideradas destinatários as autoridades a quem sejam comunicados dados no âmbito de uma disposição legal;
h) «Consentimento do titular dos dados»: qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objecto de tratamento;
i) «Interconexão de dados»: forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade.

Artigo 4.º
Âmbito de aplicação

1 - A presente lei aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados.
2 - A presente lei não se aplica ao tratamento de dados pessoais efectuado por pessoa singular no exercício de actividades exclusivamente pessoais ou domésticas.
3 A presente lei aplica-se ao tratamento de dados pessoais efectuado:
a) No âmbito das actividades de estabelecimento do responsável do tratamento situado em território português;
b) Fora do território nacional, em local onde a legislação portuguesa seja aplicável por força do direito internacional;
c) Por responsável que, não estando estabelecido no território da União Europeia, recorra, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território português, salvo se esses meios só forem utilizados para trânsito através do território da União Europeia.
4 - A presente lei aplica-se à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas sempre que o responsável pelo tratamento esteja domiciliado ou sediado em Portugal ou utilize um fornecedor de acesso a redes informáticas e telemáticas estabelecido em território português.

5 - No caso referido na alínea c) do n.º 3, o responsável pelo tratamento deve designar, mediante comunicação a Comissão Nacional de Protecção de Dados (CNPD), um representante estabelecido em Portugal, que se lhe substitua em todos os seus direitos e obrigações, sem prejuízo da sua própria responsabilidade.
6 - O disposto no número anterior aplica-se no caso de o responsável pelo tratamento estar abrangido por estatuto de extraterritorialidade, de imunidade ou por qualquer outro que impeça o procedimento criminal.
7 - A presente lei aplica-se ao tratamento e dados pessoais que tenham por objectivo a segurança pública, a defesa nacional e a segurança do Estado, sem prejuízo do disposto em normas especiais constantes de instrumentos de direito internacional a que Portugal se vincule e de legislação específica atinente aos respectivos sectores.

Capítulo II
Tratamento de dados pessoais

Secção I
Qualidade dos dados e legitimidade do seu tratamento

Artigo 5.º
Qualidade dos dados

1 - Os dados pessoais devem ser:

a) Tratados de forma lícita e com respeito pelo princípio da boa fé;
b) Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades;
c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados;
d) Exactos e, se necessário, actualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou rectificados os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente;
e) Conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.
2 - Mediante requerimento do responsável pelo tratamento, e caso haja interesse legítimo, a CNPD pode autorizar a conservação de dados para fins históricos, estatísticos ou científicos por período superior ao referido na alínea e) do número anterior.
3 - Cabe ao responsável pelo tratamento assegurar a observância do disposto nos números anteriores.

Artigo 6.º
Condições de legitimidade do tratamento de dados

O tratamento de dados pessoais só pode ser efectuado se o seu titular tiver dado de forma inequívoca o seu consentimento ou se o tratamento for necessário para:

a) Execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efectuadas a seu pedido;
b) Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito;

c) Protecção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento;
d) Execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;
e) Prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados.

Artigo 7.º
Tratamento de dados sensíveis

1 - É proibido o tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos.
2 - Mediante disposição legal ou autorização da CNPD, pode ser permitido o tratamento dos dados referidos no número anterior quando por motivos de interesse público importante esse tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, ou quando o titular dos dados tiver dado o seu consentimento expresso para esse tratamento, em ambos os casos com garantias de não discriminação e com as medidas de segurança previstas no artigo 15.º.
3 - O tratamento dos dados referidos no n.º 1 é ainda permitido quando se verificar uma das seguintes condições:

a) Ser necessário para proteger interesses vitais do titular dos dados ou de uma outra pessoa e o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento;
b) Ser efectuado, com o consentimento do titular, por fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas actividades legítimas, sob condição de o tratamento respeitar apenas aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem consentimento dos seus titulares;
c) Dizer respeito a dados manifestamente tornados públicos pelo seu titular, desde que se possa legitimamente deduzir das suas declarações o consentimento para o tratamento dos mesmos;
d) Ser necessário à declaração, exercício ou defesa de um direito em processo judicial e for efectuado exclusivamente com essa finalidade.
4 - O tratamento dos dados referentes à saúde e à vida sexual, incluindo os dados genéticos, é permitido quando for necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde, desde que o tratamento desses dados seja efectuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional, seja notificado à CNPD, nos termos do artigo 27.º, e sejam garantidas medidas adequadas de segurança da informação.

Artigo 8.º
Suspeitas de actividades ilícitas, infracções penais e contra-ordenações

1 - A criação e manutenção de registos centrais relativos a pessoas suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias só pode ser mantida por serviços públicos com competência específica prevista na respectiva lei de organização

e funcionamento, observando normas procedimentais e de protecção de dados previstas em diploma legal, com prévio parecer da CNPD.
2 - O tratamento de dados pessoais relativos a suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias pode ser autorizado pela CNPD, observadas as normas de protecção de dados e de segurança da informação, quando tal tratamento for necessário à execução de finalidades legítimas do seu responsável, desde que não prevaleçam os direitos, liberdades e garantias do titular dos dados.
3 - O tratamento de dados pessoais para fins de investigação policial deve limitar-se ao necessário para a prevenção de um perigo concreto ou repressão de uma infracção determinada, para o exercício de competências previstas no respectivo estatuto orgânico ou noutra disposição legal e ainda nos termos de acordo ou convenção internacional de que Portugal seja parte.

Artigo 9.º
Interconexão de dados pessoais

1 - A interconexão de dados pessoais que não esteja prevista em disposição legal está sujeita a autorização da CNPD solicitada pelo responsável ou em conjunto pelos correspondentes responsáveis dos tratamentos, nos termos previstos no artigo 27.º.
2 - A interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis dos tratamentos, não implicar discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados, ser rodeada de adequadas medidas de segurança e ter em conta o tipo de dados objecto de interconexão.

Secção II
Direitos do titular dos dados

Artigo 10.º
Direito de informação

1 - Quando recolher dados pessoais directamente do seu titular, o responsável pelo tratamento ou o seu representante deve prestar-lhe, salvo se já dele forem conhecidas, as seguintes informações:
a) Identidade do responsável pelo tratamento e, se for caso disso, do seu representante;
b) Finalidades do tratamento;
c) Outras informações, tais como:
Os destinatários ou categorias de destinatários dos dados;
O carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder;
A existência e as condições do direito de acesso e de rectificação, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir ao seu titular um tratamento leal dos mesmos.
2 - Os documentos que sirvam de base à recolha de dados pessoais devem conter as informações constantes do número anterior.
3 - Se os dados não forem recolhidos junto do seu titular, e salvo se dele já forem conhecidas, o responsável pelo tratamento, ou o seu representante, deve prestar-lhe as informações previstas no n.º 1 no momento do registo dos dados ou, se estiver prevista a comunicação a terceiros, o mais tardar aquando da primeira comunicação desses dados.
4 - No caso de recolha de dados em redes abertas, o titular dos dados deve ser informado, salvo se disso já tiver conhecimento, de que os seus dados pessoais podem circular na rede sem condições de segurança, correndo o risco de serem vistos e utilizados por terceiros não autorizados.

5 - A obrigação de informação pode ser dispensada, mediante disposição legal ou deliberação da CNPD, por motivos de segurança do Estado e prevenção ou investigação criminal, e, bem assim, quando, nomeadamente no caso do tratamento de dados com finalidades estatísticas, históricas ou de investigação científica, a informação do titular dos dados se revelar impossível ou implicar esforços desproporcionados ou ainda quando a lei determinar expressamente o registo dos dados ou a sua divulgação.
6 - A obrigação de informação, nos termos previstos no presente artigo, não se aplica ao tratamento de dados efectuado para fins exclusivamente jornalísticos ou de expressão artística ou literária.

Artigo 11.º
Direito de acesso

1 - O titular dos dados tem o direito de obter do responsável pelo tratamento, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos:
a) A confirmação de serem ou não tratados dados que lhe digam respeito, bem como informação sobre as finalidades desse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados;
b) A comunicação, sob forma inteligível, dos seus dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem desses dados;
c) O conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito;
d) A rectificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente lei, nomeadamente devido ao carácter incompleto ou inexacto desses dados;
e) A notificação aos terceiros a quem os dados tenham sido comunicados de qualquer rectificação, apagamento ou bloqueio efectuado nos termos da alínea d), salvo se isso for comprovadamente impossível.
2 - No caso de tratamento de dados pessoais relativos à segurança do Estado e à prevenção ou investigação criminal, o direito de acesso é exercido através da CNPD ou de outra autoridade independente a quem a lei atribua a verificação do cumprimento da legislação de protecção de dados pessoais.

3 - No caso previsto no n.º 6 do artigo anterior, o direito de acesso é exercido através da CNPD com salvaguarda das normas constitucionais aplicáveis, designadamente as que garantem a liberdade de expressão e informação, a liberdade de imprensa e a independência e sigilo profissionais dos jornalistas.
4 - Nos casos previstos nos n.^{os} 2 e 3, se a comunicação dos dados ao seu titular puder prejudicar a segurança do Estado, a prevenção ou a investigação criminal ou ainda a liberdade de expressão e informação ou a liberdade de imprensa, a CNPD limita-se a informar o titular dos dados das diligências efectuadas.
5 - O direito de acesso à informação relativa a dados da saúde, incluindo os dados genéticos, é exercido por intermédio de médico escolhido pelo titular dos dados.
6 - No caso de os dados não serem utilizados para tomar medidas ou decisões em relação a pessoas determinadas, a lei pode restringir o direito de acesso nos casos em que manifestamente não exista qualquer perigo de violação dos direitos, liberdades e garantias do titular dos dados, designadamente do direito à vida privada, e os referidos dados forem exclusivamente utilizados para fins de investigação científica ou conservados sob forma de dados pessoais durante um período que não exceda o necessário à finalidade exclusiva de elaborar estatísticas.

Artigo 12.º
Direito de oposição do titular dos dados

O titular dos dados tem o direito de:
a) Salvo disposição legal em contrário, e pelo menos nos casos referidos nas alíneas d) e e) do artigo 6.º, se opor em qualquer altura, por razões ponderosas e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, devendo, em caso de oposição justificada, o tratamento efectuado pelo responsável deixar de poder incidir sobre esses dados;
b) Se opor, a seu pedido e gratuitamente, ao tratamento dos dados pessoais que lhe digam respeito previsto pelo responsável pelo tratamento para efeitos de *marketing* directo ou qualquer outra forma de prospecção, ou de ser informado, antes de os dados pessoais serem comunicados pela primeira vez a terceiros para fins de *marketing* directo ou utilizados por conta de terceiros, e de lhe ser expressamente facultado o direito de se opor, sem despesas, a tais comunicações ou utilizações.

Artigo 13.º
Decisões individuais automatizadas

1 - Qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento.
2 - Sem prejuízo do cumprimento das restantes disposições da presente lei, uma pessoa pode ficar sujeita a uma decisão tomada nos termos do n.º 1, desde que tal ocorra no âmbito da celebração ou da execução de um contrato, e sob condição de o seu pedido de celebração ou execução do contrato ter sido satisfeito, ou de existirem medidas adequadas que garantam a defesa dos seus interesses legítimos, designadamente o seu direito de representação e expressão.
3 - Pode ainda ser permitida a tomada de uma decisão nos termos do n.º 1 quando a CNPD o autorize, definindo medidas de garantia da defesa dos interesses legítimos do titular dos dados.

Secção III
Segurança e confidencialidade do tratamento

Artigo 14.º
Segurança do tratamento

1 - O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito; estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.
2 - O responsável pelo tratamento, em caso de tratamento por sua conta, deverá escolher um subcontratante que ofereça garantias suficientes em relação às medidas de segurança técnica e de organização do tratamento a efectuar, e deverá zelar pelo cumprimento dessas medidas.
3 - A realização de operações de tratamento em subcontratação deve ser regida por um contrato ou acto jurídico que vincule o subcontratante ao responsável pelo tratamento e que estipule, designadamente, que o subcontratante apenas actua mediante instruções do responsável pelo tratamento e que lhe incumbe igualmente o cumprimento das obrigações referidas no n.º 1.

4 - Os elementos de prova da declaração negocial, do contrato ou do acto jurídico relativos à protecção dos dados, bem como as exigências relativas às medidas referidas no n.º 1, são consignados por escrito em documento em suporte com valor probatório legalmente reconhecido.

Artigo 15.º
Medidas especiais de segurança

1 - Os responsáveis pelo tratamento dos dados referidos no n.º 2 do artigo 7.º e no n.º 1 do artigo 8.º devem tomar as medidas adequadas para:
a) Impedir o acesso de pessoa não autorizada às instalações utilizadas para o tratamento desses dados (controlo da entrada nas instalações);
b) Impedir que suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada (controlo dos suportes de dados);
c) Impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados pessoais inseridos (controlo da inserção);
d) Impedir que sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalações de transmissão de dados (controlo da utilização);
e) Garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização (controlo de acesso);
f) Garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das instalações de transmissão de dados (controlo da transmissão);
g) Garantir que possa verificar-se *a posteriori*, em prazo adequado à natureza do tratamento, a fixar na regulamentação aplicável a cada sector, quais os dados pessoais introduzidos quando e por quem (controlo da introdução);
h) Impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada (controlo do transporte).
2 - Tendo em conta a natureza das entidades responsáveis pelo tratamento e o tipo das instalações em que é efectuado, a CNPD pode dispensar a existência de certas medidas de segurança, garantido que se mostre o respeito pelos direitos, liberdades e garantias dos titulares dos dados.
3 - Os sistemas devem garantir a separação lógica entre os dados referentes à saúde e à vida sexual, incluindo os genéticos, dos restantes dados pessoais.
4 - A CNPD pode determinar que, nos casos em que a circulação em rede de dados pessoais referidos nos artigos 7.º e 8.º possa pôr em risco direitos, liberdades e garantias dos respectivos titulares, a transmissão seja cifrada.

Artigo 16.º
Tratamento por subcontratante

Qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, bem como o próprio subcontratante, tenha acesso a dados pessoais não pode proceder ao seu tratamento sem instruções do responsável pelo tratamento, salvo por força de obrigações legais.

Artigo 17.º
Sigilo profissional

1 - Os responsáveis do tratamento de dados pessoais, bem como as pessoas que, no exercício das suas funções, tenham conhecimento dos dados pessoais tratados, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções.
2 - Igual obrigação recai sobre os membros da CNPD, mesmo após o termo do mandato.
3 - O disposto nos números anteriores não exclui o dever do fornecimento das informações obrigatórias, nos termos legais, excepto quando constem de ficheiros organizados para fins estatísticos.
4 - Os funcionários, agentes ou técnicos que exerçam funções de assessoria à CNPD ou aos seus vogais estão sujeitos à mesma obrigação de sigilo profissional.

Capítulo III
Transferência de dados pessoais

Secção I
Transferência de dados pessoais na União Europeia

Artigo 18.º
Princípio

É livre a circulação de dados pessoais entre Estados membros da União Europeia, sem prejuízo do disposto nos actos comunitários de natureza fiscal e aduaneira.

Secção II
Transferência de dados pessoais para fora da União Europeia

Artigo 19.º
Princípios

1 - Sem prejuízo do disposto no artigo seguinte, a transferência, para um Estado que não pertença à União Europeia, de dados pessoais que sejam objecto de tratamento ou que se destinem a sê-lo só pode realizar-se com o respeito das disposições da presente lei e se o Estado para onde são transferidos assegurar um nível de protecção adequado.
2 - A adequação do nível de protecção num Estado que não pertença à União Europeia é apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, devem ser tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no Estado em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse Estado.
3 - Cabe à CNPD decidir se um Estado que não pertença à União Europeia assegura um nível de protecção adequado.
4 - A CNPD comunica, através do Ministério dos Negócios Estrangeiros, à Comissão Europeia os casos em que tenha considerado que um Estado não assegura um nível de protecção adequado.
5 - Não é permitida a transferência de dados pessoais de natureza idêntica aos que a Comissão Europeia tiver considerado que não gozam de protecção adequada no Estado a que se destinam.

Artigo 20.º
Derrogações

1 - A transferência de dados pessoais para um Estado que não assegure um nível de protecção adequado na acepção do n.º 2 do artigo 19.º pode ser permitida pela CNPD se o titular dos dados tiver dado de forma inequívoca o seu consentimento à transferência ou se essa transferência:
a) For necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;
b) For necessária para a execução ou celebração de um contrato celebrado ou a celebrar, no interesse do titular dos dados, entre o responsável pelo tratamento e um terceiro; ou
c) For necessária ou legalmente exigida para a protecção de um interesse público importante, ou para a declaração, o exercício ou a defesa de um direito num processo judicial; ou
d) For necessária para proteger os interesses vitais do titular dos dados; ou
e) For realizada a partir de um registo público que, nos termos de disposições legislativas ou regulamentares, se destine à informação do público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar um interesse legítimo, desde que as condições estabelecidas na lei para a consulta sejam cumpridas no caso concreto.

2 - Sem prejuízo do disposto no n.º 1, a CNPD pode autorizar uma transferência ou um conjunto de transferências de dados pessoais para um Estado que não assegure um nível de protecção adequado na acepção do n.º 2 do artigo 19.º, desde que o responsável pelo tratamento assegure mecanismos suficientes de garantia de protecção da vida privada e dos direitos e liberdades fundamentais das pessoas, bem como do seu exercício, designadamente, mediante cláusulas contratuais adequadas.
3 - A CNPD informa a Comissão Europeia, através do Ministério dos Negócios Estrangeiros, bem como as autoridades competentes dos restantes Estados da União Europeia, das autorizações que conceder nos termos do n.º 2.
4 - A concessão ou derrogação das autorizações previstas no n.º 2 efectua-se pela CNPD nos termos de processo próprio e de acordo com as decisões da Comissão Europeia.
5 - Sempre que existam cláusulas contratuais-tipo aprovadas pela Comissão Europeia, segundo procedimento próprio, por oferecerem as garantias suficientes referidas no n.º 2, a CNPD autoriza a transferência de dados pessoais que se efectue ao abrigo de tais cláusulas.
6 - A transferência de dados pessoais que constitua medida necessária à protecção da segurança do Estado, da defesa, da segurança pública e da prevenção, investigação e repressão das infracções penais é regida por disposições legais específicas ou pelas convenções e acordos internacionais em que Portugal é parte.

Capítulo IV
Comissão Nacional de Protecção de Dados

Secção I
Natureza, atribuições e competências

Artigo 21.º
Natureza

1 - A CNPD é uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República.
2 - A CNPD, independentemente do direito nacional aplicável a cada tratamento de dados em concreto, exerce as suas competências em todo o território nacional.
3 - A CNPD pode ser solicitada a exercer os seus poderes por uma autoridade de controlo de protecção de dados de outro Estado membro da União Europeia ou do Conselho da Europa.
4 - A CNPD coopera com as autoridades de controlo de protecção de dados de outros Estados na difusão do direito e das regulamentações nacionais em matéria de protecção de dados pessoais, bem como na defesa e no exercício dos direitos de pessoas residentes no estrangeiro.

Artigo 22.º
Atribuições

1 - A CNPD é a autoridade nacional que tem como atribuição controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei.
2 - A CNPD deve ser consultada sobre quaisquer disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições comunitárias ou internacionais, relativos ao tratamento de dados pessoais.
3 - A CNPD dispõe:
a) De poderes de investigação e de inquérito, podendo aceder aos dados objecto de tratamento e recolher todas as informações necessárias ao desempenho das suas funções de controlo;
b) De poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, bem como o de proibir, temporária ou definitivamente, o tratamento de dados pessoais, ainda que incluídos em redes abertas de transmissão de dados a partir de servidores situados em território português;
c) Do poder de emitir pareceres prévios ao tratamentos de dados pessoais, assegurando a sua publicitação.
4 - Em caso de reiterado não cumprimento das disposições legais em matéria de dados pessoais, a CNPD pode advertir ou censurar publicamente o responsável pelo tratamento, bem como suscitar a questão, de acordo com as respectivas competências, à Assembleia da República, ao Governo ou a outros órgãos ou autoridades.
5 - A CNPD tem legitimidade para intervir em processos judiciais no caso de violação das disposições da presente lei e deve denunciar ao Ministério Público as infracções penais de que tiver conhecimento, no exercício das suas funções e por causa delas, bem como praticar os actos cautelares necessários e urgentes para assegurar os meios de prova.
6 - A CNPD é representada em juízo pelo Ministério Público e está isenta de custas nos processos em que intervenha.

Artigo 23.º
Competências

1 - Compete em especial à CNPD:
a) Emitir parecer sobre disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições comunitárias e internacionais, relativos ao tratamento de dados pessoais;
b) Autorizar ou registar, consoante os casos, os tratamentos de dados pessoais;
c) Autorizar excepcionalmente a utilização de dados pessoais para finalidades não determinantes da recolha, com respeito pelos princípios definidos no artigo 5.º;
d) Autorizar, nos casos previstos no artigo 9.º, a interconexão de tratamentos automatizados de dados pessoais;
e) Autorizar a transferência de dados pessoais nos casos previstos no artigo 20.º;
f) Fixar o tempo da conservação dos dados pessoais em função da finalidade, podendo emitir directivas para determinados sectores de actividade;
g) Fazer assegurar o direito de acesso à informação, bem como do exercício do direito de rectificação e actualização;
h) Autorizar a fixação de custos ou de periodicidade para o exercício do direito de acesso, bem como fixar os prazos máximos de cumprimento, em cada sector de actividade, das obrigações que, por força dos artigos 11.º a 13.º, incumbem aos responsáveis pelo tratamento de dados pessoais;
i) Dar seguimento ao pedido efectuado por qualquer pessoa, ou por associação que a represente, para protecção dos seus direitos e liberdades no que diz respeito ao tratamento de dados pessoais e informá-la do resultado;
j) Efectuar, a pedido de qualquer pessoa, a verificação da licitude de um tratamento de dados, sempre que esse tratamento esteja sujeito a restrições de acesso ou de informação, e informá-la da realização da verificação;
k) Apreciar as reclamações, queixas ou petições dos particulares;
l) Dispensar a execução de medidas de segurança, nos termos previstos no n.º 2 do artigo 15.º, podendo emitir directivas para determinados sectores de actividade;
m) Assegurar a representação junto de instâncias comuns de controlo e em reuniões comunitárias e internacionais de entidades independentes de controlo da protecção de dados pessoais, bem como participar em reuniões internacionais no âmbito das suas competências, designadamente exercer funções de representação e fiscalização no âmbito dos sistemas Schengen e Europol, nos termos das disposições aplicáveis;
n) Deliberar sobre a aplicação de coimas;
o) Promover e apreciar códigos de conduta;
p) Promover a divulgação e esclarecimento dos direitos relativos à protecção de dados e dar publicidade periódica à sua actividade, nomeadamente através da publicação de um relatório anual;
q) Exercer outras competências legalmente previstas.

2 - No exercício das suas competências de emissão de directivas ou de apreciação de códigos de conduta, a CNPD deve promover a audição das associações de defesa dos interesses em causa.
3 - No exercício das suas funções, a CNPD profere decisões com força obrigatória, passíveis de reclamação e de recurso para o Tribunal Central Administrativo.
4 - A CNPD pode sugerir à Assembleia da República as providências que entender úteis à prossecução das suas atribuições e ao exercício das suas competências.

Artigo 24.º
Dever de colaboração

1 - As entidades públicas e privadas devem prestar a sua colaboração à CNPD, facultando-lhe todas as informações que por esta, no exercício das suas competências, lhe forem solicitadas.
2 - O dever de colaboração é assegurado, designadamente, quando a CNPD tiver necessidade, para o cabal exercício das suas funções, de examinar o sistema informático e os ficheiros de dados pessoais, bem como toda a documentação relativa ao tratamento e transmissão de dados pessoais.
3 - A CNPD ou os seus vogais, bem como os técnicos por ela mandatados, têm direito de acesso aos sistemas informáticos que sirvam de suporte ao tratamento dos dados, bem como à documentação referida no número anterior, no âmbito das suas atribuições e competências.

Secção II
Composição e funcionamento
Artigo 25.º
Composição e mandato

1 - A CNPD é composta por sete membros de integridade e mérito reconhecidos, dos quais o presidente e dois dos vogais são eleitos pela Assembleia da República segundo o método da média mais alta de Hondt.
2 - Os restantes vogais são:
a) Dois magistrados com mais de 10 anos de carreira, sendo um magistrado judicial, designado pelo Conselho Superior da Magistratura, e um magistrado do Ministério Público, designado pelo Conselho Superior do Ministério Público;
b) Duas personalidades de reconhecida competência designadas pelo Governo.
3 - O mandato dos membros da CNPD é de cinco anos e cessa com a posse dos novos membros.
4 - Os membros da CNPD constam de lista publicada na 1.ª série do *Diário da República.*
5 - Os membros da CNPD tomam posse perante o Presidente da Assembleia da República nos 10 dias seguintes à publicação da lista referida no número anterior.

Artigo 26.º
Funcionamento

1 - São aprovados por lei da Assembleia da República:
a) A lei orgânica e o quadro de pessoal da CNPD;
b) O regime de incompatibilidades, de impedimentos, de suspeições e de perda de mandato, bem como o estatuto remuneratório dos membros da CNPD.
2 - O estatuto dos membros da CNPD garante a independência do exercício das suas funções.
3 - A Comissão dispõe de quadro próprio para apoio técnico e administrativo, beneficiando os seus funcionários e agentes do estatuto e regalias do pessoal da Assembleia da República.

Secção III
Notificação

Artigo 27.º
Obrigação de notificação à CNPD

1 - O responsável pelo tratamento ou, se for caso disso, o seu representante deve notificar a CNPD antes da realização de um tratamento ou conjunto de tratamentos, total ou parcialmente automatizados, destinados à prossecução de uma ou mais finalidades interligadas.
2 - A CNPD pode autorizar a simplificação ou a isenção da notificação para determinadas categorias de tratamentos que, atendendo aos dados a tratar, não sejam susceptíveis de pôr em causa os direitos e liberdades dos titulares dos dados e tenham em conta critérios de celeridade, economia e eficiência.
3 - A autorização, que está sujeita a publicação no *Diário da República*, deve especificar as finalidades do tratamento, os dados ou categorias de dados a tratar, a categoria ou categorias de titulares dos dados, os destinatários ou categorias de destinatários a quem podem ser comunicados os dados e o período de conservação dos dados.
4 - Estão isentos de notificação os tratamentos cuja única finalidade seja a manutenção de registos que, nos termos de disposições legislativas ou regulamentares, se destinem a informação do público e possam ser consultados pelo público em geral ou por qualquer pessoa que provar um interesse legítimo.
5 - Os tratamentos não automatizados dos dados pessoais previstos no n.º 1 do artigo 7.º estão sujeitos a notificação quando tratados ao abrigo da alínea a) do n.º 3 do mesmo artigo.

Artigo 28.º
Controlo prévio

1 - Carecem de autorização da CNPD:
a)O tratamento dos dados pessoais a que se referem o n.º 2 do artigo 7.º e o n.º 2 do artigo 8.º;
b) O tratamento dos dados pessoais relativos ao crédito e à solvabilidade dos seus titulares;
c) A interconexão de dados pessoais prevista no artigo 9.º;
d) A utilização de dados pessoais para fins não determinantes da recolha.
2 - Os tratamentos a que se refere o número anterior podem ser autorizados por diploma legal, não carecendo neste caso de autorização da CNPD.

Artigo 29.º
Conteúdo dos pedidos de parecer ou de autorização e da notificação

Os pedidos de parecer ou de autorização, bem como as notificações, remetidos à CNPD devem conter as seguintes informações:
a) Nome e endereço do responsável pelo tratamento e, se for o caso, do seu representante;
b) As finalidades do tratamento;
c) Descrição da ou das categorias de titulares dos dados e dos dados ou categorias de dados pessoais que lhes respeitem;
d) Destinatários ou categorias de destinatários a quem os dados podem ser comunicados e em que condições;
e) Entidade encarregada do processamento da informação, se não for o próprio responsável do tratamento;
f) Eventuais interconexões de tratamentos de dados pessoais;

g) Tempo de conservação dos dados pessoais;
h) Forma e condições como os titulares dos dados podem ter conhecimento ou fazer corrigir os dados pessoais que lhes respeitem;
i) Transferências de dados previstas para países terceiros;
j) Descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para garantir a segurança do tratamento em aplicação dos artigos 14.º e 15.º.

Artigo 30.º
Indicações obrigatórias

1 - Os diplomas legais referidos no n.º 2 do artigo 7.º e no n.º 1 do artigo 8.º, bem como as autorizações da CNPD e os registos de tratamentos de dados pessoais devem, pelo menos, indicar:
a) O responsável do ficheiro e, se for caso disso, o seu representante;
b) As categorias de dados pessoais tratados;
c) As finalidades a que se destinam os dados e as categorias de entidades a quem podem ser transmitidos;
d) A forma de exercício do direito de acesso e de rectificação;
e) Eventuais interconexões de tratamentos de dados pessoais;
f) Transferências de dados previstas para países terceiros.
2 - Qualquer alteração das indicações constantes do n.º 1 está sujeita aos procedimentos previstos nos artigos 27.º e 28.º.

Artigo 31.º
Publicidade dos tratamentos

1 - O tratamento dos dados pessoais, quando não for objecto de diploma legal e dever ser autorizado ou notificado, consta de registo na CNPD, aberto à consulta por qualquer pessoa.
2 - O registo contém as informações enumeradas nas alíneas a) a d) e i) do artigo 29.º.
3 - O responsável por tratamento de dados não sujeito a notificação está obrigado a prestar, de forma adequada, a qualquer pessoa que lho solicite, pelo menos as informações referidas no n.º 1 do artigo 30.º.
4 - O disposto no presente artigo não se aplica a tratamentos cuja única finalidade seja a manutenção de registos que, nos termos de disposições legislativas ou regulamentares, se destinem à informação do público e se encontrem abertos à consulta do público em geral ou de qualquer pessoa que possa provar um interesse legítimo.
5 - A CNPD deve publicar no seu relatório anual todos os pareceres e autorizações elaborados ou concedidas ao abrigo da presente lei, designadamente as autorizações previstas no n.º 2 do artigo 7.º e no n.º 2 do artigo 9.º.

Capítulo V
Códigos de conduta

Artigo 32.º
Códigos de conduta

1 - A CNPD apoia a elaboração de códigos de conduta destinados a contribuir, em função das características dos diferentes sectores, para a boa execução das disposições da presente lei.
2 - As associações profissionais e outras organizações representativas de categorias de responsáveis pelo tratamento de dados que tenham elaborado projectos de códigos de conduta podem submetê-los à apreciação da CNPD.
3 - A CNPD pode declarar a conformidade dos projectos com as disposições legais e regulamentares vigentes em matéria de protecção de dados pessoais.

Capítulo VI
Tutela administrativa e jurisdicional

Secção I
Tutela administrativa e jurisdicional

Artigo 33.º
Tutela administrativa e jurisdicional
Sem prejuízo do direito de apresentação de queixa à CNPD, qualquer pessoa pode, nos termos da lei, recorrer a meios administrativos ou jurisdicionais para garantir o cumprimento das disposições legais em matéria de protecção de dados pessoais.

Artigo 34.º
Responsabilidade civil
1 - Qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto que viole disposições legais em matéria de protecção de dados pessoais tem o direito de obter do responsável a reparação pelo prejuízo sofrido.
2 - O responsável pelo tratamento pode ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável.

Secção II
Contra-ordenações

Artigo 35.º
Legislação subsidiária
Às infracções previstas na presente secção é subsidiariamente aplicável o regime geral das contra-ordenações, com as adaptações constantes dos artigos seguintes.

Artigo 36.º
Cumprimento do dever omitido

Sempre que a contra-ordenação resulte de omissão de um dever, a aplicação da sanção e o pagamento da coima não dispensam o infractor do seu cumprimento, se este ainda for possível.

Artigo 37.º
Omissão ou defeituoso cumprimento de obrigações
1 - As entidades que, por negligência, não cumpram a obrigação de notificação à CNPD do tratamento de dados pessoais a que se referem os n.^{os} 1 e 5 do artigo 27.º, prestem falsas informações ou cumpram a obrigação de notificação com inobservância dos termos previstos no artigo 29.º, ou ainda quando, depois de notificadas pela CNPD, mantiverem o acesso às redes abertas de transmissão de dados a responsáveis por tratamento de dados pessoais que não cumpram as disposições da presente lei, praticam contra-ordenação punível com as seguintes coimas:
a) Tratando-se de pessoa singular, no mínimo de 50 000$ e no máximo de 500 000$;
b) Tratando-se de pessoa colectiva ou de entidade sem personalidade jurídica, no mínimo de 300 000$ e no máximo de 3 000 000$.
2 - A coima é agravada para o dobro dos seus limites quando se trate de dados sujeitos a controlo prévio, nos termos do artigo 28.º.

Artigo 38.º
Contra-ordenações

1 - Praticam contra-ordenação punível com a coima mínima de 100 000$ e máxima de 1 000 000$, as entidades que não cumprirem alguma das seguintes disposições da presente lei:
a) Designar representante nos termos previstos no n.º 5 do artigo 4.º;
b) Observar as obrigações estabelecidas nos artigos 5.º, 10.º, 11.º, 12.º, 13.º, 15.º, 16.º e 31.º, n.º 3.
2 - A pena é agravada para o dobro dos seus limites quando não forem cumpridas as obrigações constantes dos artigos 6.º, 7.º, 8.º, 9.º, 19.º e 20.º.

Artigo 39.º
Concurso de infracções

1 - Se o mesmo facto constituir, simultaneamente, crime e contra-ordenação, o agente é punido sempre a título de crime.
2 - As sanções aplicadas às contra-ordenações em concurso são sempre cumuladas materialmente.

Artigo 40.º
Punição da negligência e da tentativa

1 - A negligência é sempre punida nas contra-ordenações previstas no artigo 38.º.
2 - A tentativa é sempre punível nas contra-ordenações previstas nos artigos 37.º e 38.º.

Artigo 41.º
Aplicação das coimas

1 - A aplicação das coimas previstas na presente lei compete ao Presidente da CNPD, sob prévia deliberação da Comissão.
2 - A deliberação da CNPD, depois de homologada pelo Presidente, constitui título executivo, no caso de não ser impugnada no prazo legal.

Artigo 42.º
Destino das receitas cobradas

O montante das importâncias cobradas, em resultado da aplicação das coimas, reverte, em partes iguais, para o Estado e para a CNPD.

Secção III
Crimes

Artigo 43.º
Não cumprimento de obrigações relativas a protecção de dados

1 - É punido com prisão até um ano ou multa até 120 dias quem intencionalmente:
a) Omitir a notificação ou o pedido de autorização a que se referem os artigos 27.º e 28.º;
b) Fornecer falsas informações na notificação ou nos pedidos de autorização para o tratamento de dados pessoais ou neste proceder a modificações não consentidas pelo instrumento de legalização;
c) Desviar ou utilizar dados pessoais, de forma incompatível com a finalidade determinante da recolha ou com o instrumento de legalização;

d) Promover ou efectuar uma interconexão ilegal de dados pessoais;
e) Depois de ultrapassado o prazo que lhes tiver sido fixado pela CNPD para cumprimento das obrigações previstas na presente lei ou em outra legislação de protecção de dados, as não cumprir;
f) Depois de notificado pela CNPD para o não fazer, mantiver o acesso a redes abertas de transmissão de dados a responsáveis pelo tratamento de dados pessoais que não cumpram as disposições da presente lei.
2 - A pena é agravada para o dobro dos seus limites quando se tratar de dados pessoais a que se referem os artigos 7.º e 8.º.

Artigo 44.º
Acesso indevido

1 - Quem, sem a devida autorização, por qualquer modo, aceder a dados pessoais cujo acesso lhe está vedado, é punido com prisão até um ano ou multa até 120 dias.
2 - A pena é agravada para o dobro dos seus limites quando o acesso:
a) For conseguido através de violação de regras técnicas de segurança;
b) Tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais;
c) Tiver proporcionado ao agente ou a terceiros, benefício ou vantagem patrimonial.
3 - No caso do n.º 1 o procedimento criminal depende de queixa.

Artigo 45.º
Viciação ou destruição de dados pessoais

1 - Quem, sem a devida autorização, apagar, destruir, danificar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis ou afectando a sua capacidade de uso, é punido com prisão até dois anos ou multa até 240 dias.
2 - A pena é agravada para o dobro nos seus limites se o dano produzido for particularmente grave.
3 - Se o agente actuar com negligência, a pena é, em ambos os casos, de prisão até um ano ou multa até 120 dias.

Artigo 46.º
Desobediência qualificada

1 - Quem, depois de notificado para o efeito, não interromper, cessar ou bloquear o tratamento de dados pessoais é punido com a pena correspondente ao crime de desobediência qualificada.
2 - Na mesma pena incorre quem, depois de notificado:
a) Recusar, sem justa causa, a colaboração que concretamente lhe for exigida nos termos do artigo 24.º;
b) Não proceder ao apagamento, destruição total ou parcial de dados pessoais;
c) Não proceder à destruição de dados pessoais, findo o prazo de conservação previsto no artigo 5.º.

Artigo 47.º
Violação do dever de sigilo

1 - Quem, obrigado a sigilo profissional, nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais é punido com prisão até dois anos ou multa até 240 dias.
2 - A pena é agravada de metade dos seus limites se o agente:

a) For funcionário público ou equiparado, nos termos da lei penal;
b) For determinado pela intenção de obter qualquer vantagem patrimonial ou outro benefício ilegítimo;

c) Puser em perigo a reputação, a honra e consideração ou a intimidade da vida privada de outrem.
3 - A negligência é punível com prisão até seis meses ou multa até 120 dias.
4 - Fora dos casos previstos no n.º 2, o procedimento criminal depende de queixa.

Artigo 48.º
Punição da tentativa

Nos crimes previstos nas disposições anteriores, a tentativa é sempre punível.

Artigo 49.º
Pena acessória

1 - Conjuntamente com as coimas e penas aplicadas pode, acessoriamente, ser ordenada:
a) A proibição temporária ou definitiva do tratamento, o bloqueio, o apagamento ou a destruição total ou parcial dos dados;
b) A publicidade da sentença condenatória;
c) A advertência ou censura públicas do responsável pelo tratamento, nos termos do n.º 4 do artigo 22.º.

2 - A publicidade da decisão condenatória faz-se a expensas do condenado, na publicação periódica de maior expansão editada na área da comarca da prática da infracção ou, na sua falta, em publicação periódica da comarca mais próxima, bem como através da afixação de edital em suporte adequado, por período não inferior a 30 dias.
3 - A publicação é feita por extracto de que constem os elementos da infracção e as sanções aplicadas, bem como a identificação do agente.

Capítulo VII
Disposições finais

Artigo 50.º
Disposição transitória

1 - Os tratamentos de dados existentes em ficheiros manuais à data da entrada em vigor da presente lei devem cumprir o disposto nos artigos 7.º, 8.º, 10.º e 11.º no prazo de cinco anos.
2 - Em qualquer caso, o titular dos dados pode obter, a seu pedido e, nomeadamente, aquando do exercício do direito de acesso, a rectificação, o apagamento ou o bloqueio dos dados incompletos, inexactos ou conservados de modo incompatível com os fins legítimos prosseguidos pelo responsável pelo tratamento.
3 - A CNPD pode autorizar que os dados existentes em ficheiros manuais e conservados unicamente com finalidades de investigação histórica não tenham que cumprir os artigos 7.º, 8.º e 9.º, desde que não sejam em nenhum caso reutilizados para finalidade diferente.

Artigo 51.º
Disposição revogatória

São revogadas as Leis n.^{os} 10/91, de 29 de Abril, e 28/94, de 29 de Agosto.

Artigo 52.º
Entrada em vigor

A presente lei entra em vigor no dia seguinte ao da sua publicação.

Aprovado em 24 de Setembro de 1998.

O Presidente da Assembleia da República, *António de Almeida Santos*
Publique-se.
O Presidente da República, Jorge Sampaio.
Referendada em 14 de Outubro de 1998.
O Primeiro-Ministro, *António Manuel de Oliveira Guterres*

Anexo B: Tópicos para a Construção de um Programa de Protecção

NIST Special Publication 800-50

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Building an Information Technology Security Awareness and Training Program

Mark Wilson and Joan Hash

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8933

October 2003

U.S. Department of Commerce

Donald L. Evans, Secretary

Technology Administration

Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology

Arden L. Bement, Jr., Director

4. Developing Awareness and Training Material

Once the awareness and training program has been designed, supporting material can be developed. Material should be developed[15] with the following in mind:

- **"What behavior do we want to reinforce?" (awareness); and**
- **"What skill or skills do we want the audience to learn and apply?" (training).**

In both cases, the focus should be on specific material that the participants should integrate into their jobs. Attendees will pay attention and incorporate what they see or hear in a session if they feel that the material was developed specifically for them. Any presentation that "feels" canned – impersonal and so general as to apply to any audience – will be filed away as just another of the annual "we're here because we have to be here" sessions. An awareness and training program can be effective, however, if the material is interesting and current.[16]

At some point the question will be asked, "Am I developing awareness *or* training material?" Generally, since the goal of awareness material is simply to focus attention on good security practices, the message that the awareness effort sends should be short and simple. The message can address one topic, or it can address a number of topics about which the audience should be aware.

The awareness audience must include all users in an organization. The message to be spread through an awareness program, or campaign,[17] should make all individuals aware of their commonly shared IT security responsibilities. On the other hand, the message in a training class is directed at a specific audience. The message in training material should include everything related to security that attendees need to know in order to do their jobs. Training material is usually far more in-depth than material used in an awareness session or campaign.

4.1 Developing Awareness Material

The question to be answered when beginning to develop material for an organization wide awareness program or campaign is, "What do we want all agency personnel to be aware of regarding IT security?" The awareness and training plan should contain a list of topics. E-mail advisories, online IT security daily news websites, and periodicals are good sources of ideas and material. Agency policy, program reviews, internal audits, internal controls program reviews, self-assessments, and spot-checks can also identify additional topics to address.

---

15 Awareness and training material can be developed in-house, adapted from other agencies' or professional organizations' work, or purchased from a contractor/vendor. For information about contracting for services and products, see draft NIST Special Publication 800-35, *Guide to Information Technology Security Services*, and draft NIST Special Publication 800-36, *Guide to Selecting Information Technology Security Products*. For more extensive guidelines on contracting issues see draft NIST Special Publication 800-4A, *Security Considerations in Federal Information Technology Procurements – A Guide for Procurement Initiators, Contracting Officers, and IT Security Officials*.

16 Changing peoples' attitudes and behavior in terms of IT security can be a challenging task. New security policies are often seen as conflicting with the way users have done their job for years. For example, departments and agencies that once operated with the full and open sharing of information are now being required to control access to, and dissemination of, that information. A technique that has been successfully used to acclimate users to these necessary changes is to begin an awareness module or session by discussing IT security issues in the context of personal life experiences (e.g., identify theft, inappropriate access to personal health or financial data, hacking incidents).

17 An organization may decide to mount a security awareness campaign to focus on a particular issue. For example, if users are becoming targets of social engineering attacks or a particular virus, an awareness campaign can be quickly implemented that uses various awareness techniques to "get the word out." Such a campaign differs from the normal implementation of an awareness program by the need for a timely dissemination of information on a particular topic or group of topics.

4.1.1 Selecting Awareness Topics

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign.[18] Topics may include:

- Password usage and management – including creation, frequency of changes, and protection
- Protection from viruses, worms, Trojan horses, and other malicious code – scanning, updating definitions
- Policy – implications of noncompliance
- Unknown e-mail/attachments
- Web usage – allowed versus prohibited; monitoring of user activity
- Spam
- Data backup and storage – centralized or decentralized approach
- Social engineering
- Incident response – contact whom? "What do I do?"
- Shoulder surfing
- Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)
- Inventory and property transfer – identify responsible organization and user responsibilities (e.g., media sanitization)
- Personal use and gain issues – systems at work and home
- Handheld device security issues – address both physical and wireless security issues
- Use of encryption and the transmission of sensitive/confidential information over the Internet – address agency policy, procedures, and technical contact for assistance
- Laptop security while on travel – address both physical and information security issues
- Personally owned systems and software at work – state whether allowed or not (e.g., copyrights)
- Timely application of system patches – part of configuration management
- Software license restriction issues – address when copies are allowed and not allowed
- Supported/allowed software on organization systems – part of configuration management
- Access control issues – address least privilege and separation of duties
- Individual accountability – explain what this means in the organization
- Use of acknowledgement statements – passwords, access to systems and data, personal use and gain

[18] A thorough discussion of topics, organized as management, operational, and technical controls, can be found in NIST Special Publications 800-12, 800-18, and 800-26.

- Visitor control and physical access to spaces – discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity
- Desktop security – discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems
- Protect information subject to confidentiality concerns – in systems, archived, on backup media, in hardcopy form, and until destroyed
- E-mail list etiquette – attached files and other rules.

4.1.2 Sources of Awareness Material

There are a variety of sources of material on security awareness that can be incorporated into an awareness program. The material can address a specific issue, or in some cases, can describe how to begin to develop an entire awareness program, session, or campaign. Sources of timely material may include:

- E-mail advisories issued by industry-hosted news groups, academic institutions, or the organization's IT security office;
- Professional organizations and vendors;
- Online IT security daily news websites;
- Periodicals; and
- Conferences, seminars, and courses.

Awareness material can be developed using one theme at a time or created by combining a number of themes or messages into a presentation. For example, a poster or a slogan on an awareness tool should contain one theme, while an instructor-led session or web-based presentation can contain numerous themes. (Dissemination techniques are covered in greater depth in Section 5.) Regardless of the approach taken, the amount of information should not overwhelm the audience. Brief mention of requirements (policies), the problems that the requirements were designed to remedy, and actions to take are the major topics to be covered in a typical awareness presentation.[19]

A more complex awareness presentation that incorporates basics and literacy material (see Chapter 3 of NIST Special Publication 800-16) should go into more depth on a particular subject. Because basics and literacy is the bridge between awareness and training, this additional level of detail and complexity is appropriate.

4.2 Developing Training Material

The question to be answered when beginning to develop material for a specific training course is, "What skill or skills do we want the audience to learn?" The awareness and training plan should identify an audience, or several audiences, that should receive training tailored to address their IT security responsibilities. NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (http://csrc.nist.gov/publications/nistpubs/index.html), contains a methodology for building training

[19] The NIST Computer Security Division website's awareness, training, education, and professional development pages http://csrc.nist.gov/ATE contain a number of links to government, industry, and academic sites that offer or sell both awareness and training material.

courses for a number of different audiences. The methodology in the NIST publication will be discussed in this section. Other sources of training courses and material will also be identified and discussed.

4.2.1 A Model for Building Training Courses: NIST Special Pub. 800-16

The methodology in NIST Special Publication 800-16 provides a useful tool with which to develop IT security training courses. This section provides background information on the purpose of the publication and describes how to use the methodology to develop training courses.

Purpose and Methodology: Special Publication 800-16 represents the IT security training needs in the current distributed computing environment, as opposed to the mainframe-oriented environment of the mid- to late-1980s. The document identifies 26 roles that have some degree of responsibility for IT security. Special Publication 800-16 provides flexibility in its methodology for extension of roles and other parameters to accommodate future technologies and organizational roles. The methodology also allows for training courses to be developed at the beginning, intermediate, and advanced levels of training. Sample learning objectives are provided for each level to guide the course developer. Agencies should consider using the publication to map needed training to new and existing roles that have significant IT security responsibilities.

Using the Special Publication to Develop a Training Course: NIST Special Publication 800-16 includes a number of resources that a course developer can use to build a training course. The resources are: the IT security learning continuum model, 26 roles and role-based matrices, 46 training matrix cells, 12 body of knowledge topics and concepts, 3 fundamental training content categories, and 6 functional specialties.

Once an audience has been identified as needing IT security training, Appendix E of the NIST Special Publication can be used to assist in course selection.[20] Agencies can tailor this approach based on specific positions used in their organizations. Appendix E contains 26 matrices, one for each of the 26 roles identified in the publication. Figure 4-1 provides a sample matrix for a course for system administrators.

[20] Once training needs are identified, some agencies rely on curriculum builders – professional training development specialists – to develop the training material. Since training development specialists are usually not IT security professionals, the specialist will work closely with the IT security staff to ensure accuracy of the material as well as the proper level of complexity.

IT Security Training Matrix - *System Administrator*

Training Areas	Functional Specialities						
	A Manage	B Acquire	C Design and Develop	D Implement and Operate	E Review and Evaluate	F Use	G Other
1. Laws and Regulations				1D ✓			
2. Security Program							
2.1. Planning							
2.2. Management				2.2D ✓			
3. System Life Cycle Security							
3.1 Initiation				3.2D ✓			
3.2. Development				3.3D ✓			
3.3. Test and Evaluation				3.4D ✓			
3.4. Implementation			3.4C ✓	3.4D ✓			
3.5. Operations	3.5A ✓		3.5C ✓	3.5D ✓			
3.6. Termination				3.6D ✓			
4. Other							

Figure 4-1: Sample IT Security Training Matrix

Within each matrix, there are a number of cells that are used to build the course material. There are a total of 46 cells, but only specific cells are used for each course. Some course matrices have as few as 2 cells, and the course matrix for an IT security officer/manager uses all 46 cells. Most matrices use 7 to 10 cells.

The matrix is organized by six role categories – or functional specialties – relative to three fundamental training content categories – or training areas (i.e., laws and regulations, security program, and system life cycle security). The six role categories or functional specialties are:

- **Manage** – This category is for individuals who manage IT-based functions in an organization.
- **Acquire** – This category is for those individuals who are involved in the acquisition of IT products and/or services (e.g., serve on a source selection board to evaluate vendor proposals for IT systems). This is especially important for those who serve as a contracting officer's technical representative (COTR).
- **Design and Develop** – This category is for those individuals who design and develop systems and applications.
- **Operate** – This category is for those individuals who operate (administer) IT systems (e.g., web servers, e-mail servers, file servers, LANs, WANs, mainframes).
- **Review and Evaluate** – This category is for individuals who review and evaluate (audit) IT functions as part of an organization's internal controls program, internal review, or an external audit program (e.g., inspector general).

- **Use** – This category is for individuals who access IT resources and/or use IT to do their jobs.

Categories (or functional specialties) are arranged in each matrix along the top, from left to right. A placeholder exists in the seventh column, called "Other," designed to be used if an additional role category or functional specialty is developed. These six categories allow a training course to be tailor-fit to an audience and allow the course to address specific functions within a role. For example, a system administrator may manage the function or may administer (operate) a system or systems. Training course material should be organized by role – by an individual's job function – within the organization.

In Figure 4-1, the sample matrix for a system administrator course, ten cells will be developed into the course material. Each cell can be seen as a building block for the course material. In this example, most of the cells fall in the "Implement and Operate" specialty or column, because it is assumed that the system administrator will be running (operating) a system or systems. Because this course will address system management, design, and development, several of the ten cells are shown in those specialties or columns.

4.2.2 Sources of Training Courses and Material

The first step in determining sources of training material to build a course(s) is to decide if the material will be developed in-house or contracted out. If the agency has in-house expertise and can afford to allocate the necessary resources to develop training material and courses, NIST Special Publication 800-16 can be used.

Figure 4-2 contains some key issues to consider in making the decision to develop a course in-house or to outsource.

- Do we have the in-house resources to do the job? This includes people with the right skills and enough people to do the work.
- Is it more cost-effective to develop the material in-house versus outsourcing?
- Is there a funding mechanism in place (budget)?
- Do we have a person on staff that can serve as the contracting officer's technical representative (COTR) and effectively monitor contractor activity?
- Does the agency have the necessary resources (e.g., funding and staff with necessary expertise) to maintain the material, if it is developed by a contractor?
- Does the course content sensitivity preclude use of a contractor?
- Does outsourcing allow for critical training delivery schedules to be met?

Figure 4-2: Key Questions – Develop Training Material In-house or Outsource?

If the agency decides to outsource its training course development, there are a number of vendors that offer "off-the-shelf" courses that are suitable for particular audiences or that can be developed for specific audiences. Prior to selecting a particular vendor, agencies should have a thorough understanding of their training needs and be able to determine if a prospective vendor's material meets their needs.

Maximizing Partnerships: Agencies have more options from which to choose than to simply decide if they will develop training course material with existing resources or outsource. Agencies can establish (or maximize existing) partnerships with other agencies to develop material or coordinate training events that meet their IT security training needs. For example, several agencies may combine resources and expertise and develop a training course for a particular audience. If agency-specific material is contained in, and limited to, a single module in the course, all involved agencies can use the majority of the material developed. Agencies would then have to modify or tailor-fit only the module that contains the agency-specific material.

Similarly, an agency might organize an IT security day or an annual or regional conference and announce that the events are open to other agencies' personnel. While the material presented might not match exactly what is needed by both agencies, it can be a fairly inexpensive way to meet some of a particular audience's training needs. If such an arrangement is made, a process must be established to allow each participating agency to track attendance, ensure applicability of the training material, determine accountability, and address other administrative and management issues.

Agencies can explore the use of training material that has been developed by other agencies and that can be edited inexpensively rather than developing a completely new course. Care should be taken that the available material is applicable to the intended audience, and that the material addresses what prospective attendees need to know to satisfy their IT security responsibilities.

Within an agency, IT security program managers can build new partnerships, or reinforce existing ones, with the organization's training function or with functional managers who coordinate or conduct their own training. Functional training developed in-house (e.g., financial applications, personnel management) often lacks adequate discussion of related IT security issues. Through a partnership, the IT security program manager can offer to review existing references to security in the training material, checking for completeness and accuracy. The IT security program manager can also assist the training or functional manager by developing a security module for that functional material that has no security component. The IT security program manager can also review contract specifications for functional training development to be outsourced, ensuring that the appropriate security issues are addressed in sufficient detail and complexity for the intended audience.

5. Implementing the Awareness and Training Program

An IT security awareness and training program should be implemented only after:

- A needs assessment has been conducted;
- A strategy has been developed;
- An awareness and training program plan for implementing that strategy has been completed; and
- Awareness and training material has been developed.

Figure 5-1 shows these key steps leading to the implementation of the awareness and training program.

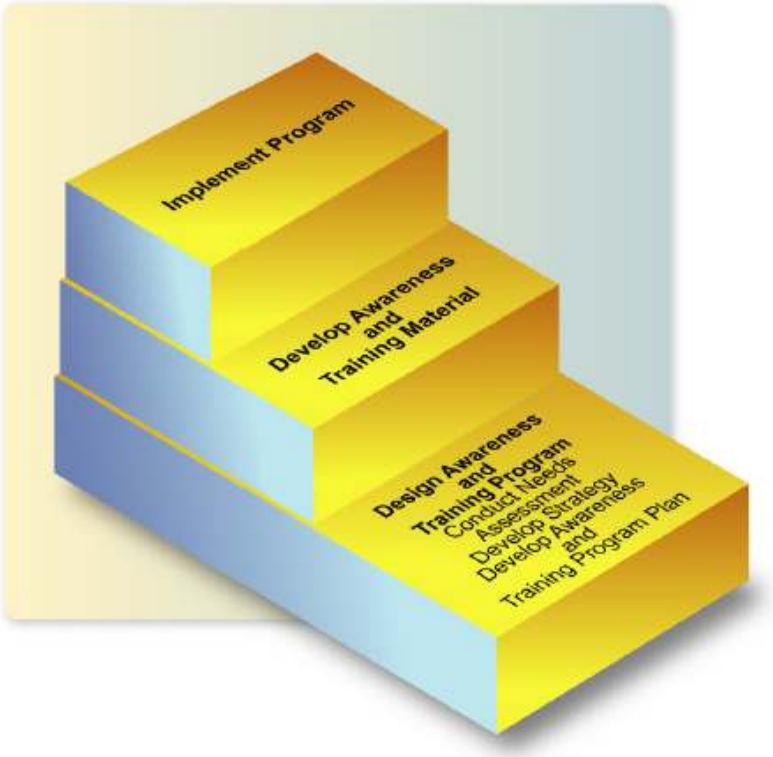

Figure 5-1: Key Steps Leading to Program Implementation

5.1 Communicating the Plan

The program's implementation must be fully explained to the organization to achieve support for its implementation and commitment of necessary resources. This explanation includes expectations of agency management and staff support, as well as expected results of the program and benefits to the organization. Funding issues must also be addressed. For example, agency managers must know if the cost to implement the awareness and training program will be totally funded by the CIO or IT security

program budget, or if their budgets will be impacted to cover their share of the expense of implementing the program. It is essential that everyone involved in the implementation of the program understand their roles and responsibilities. In addition, schedules and completion requirements must be communicated.

Communication of the plan can be mapped to the three implementation models discussed in Section 3. Typical scenarios follow.

- **Centralized Program Model Communication Scenario**: In this model, the CIO and/or IT security program manager develop all agency IT security awareness and training policy, develop the strategy and program plan, and implement the program. Therefore, all necessary funding for material development and implementation is controlled and provided by the CIO and IT security program manager. By the time the program is to be implemented, they have conducted the needs assessment, developed the training plan, and developed the awareness and training material. The CIO and/or IT security program manager should brief the agency head and senior management on the implementation plan and get approval to communicate it throughout the agency. Once the implementation plan is approved, the CIO and/or IT security program manager should communicate the plan to organizational unit management, providing the schedule for awareness and training offerings, and allocating slots in each session, where applicable, for each unit. The organizational unit managers should then communicate the plan to their staff, identify the awareness and training required, schedule attendees, and submit their nominations for each offering to the CIO or IT security program manager as required.
- **Partially Decentralized Program Model Communication Scenario**: In this model, the CIO and/or the IT security program manager develop all agency IT security awareness and training policy and develop the strategy. They also conduct the needs assessment, from which the strategy is derived. Organizational unit managers are then given an awareness and training budget, develop training plans for their own unit, and implement the program. They should provide status reports to the CIO and/or IT security program manager as required.
- **Decentralized Program Model Communication Scenario**: In this model, the CIO and/or IT security program manager disseminate broad policy and expectations regarding the IT security awareness and training program. Execution of the remainder of the program is the responsibility of the organizational units. The organizational unit managers are expected to conduct a needs assessment, formulate a strategy, develop a training plan, develop awareness and training material, and implement the awareness and training program. They should provide status reports to the CIO and/or IT security program manager as required.

Once the plan for implementing the awareness and training program has been explained to (and accepted by) agency management, the implementation can begin. There are a number of ways that awareness material and messages can be presented and disseminated throughout an organization.

5.2 Techniques for Delivering Awareness Material

Many techniques exist to get an IT security awareness message, or a series of messages, disseminated throughout an agency. The technique(s) chosen depend upon resources and the complexity of the message(s).

Techniques an agency may consider include, but are not limited to:

- Messages on awareness tools (e.g., pens, key fobs, post-it notes, notepads, first aid kits, clean-up kits, diskettes with a message, bookmarks, Frisbees, clocks, "gotcha" cards)

- Posters, "do and don't lists," or checklists
- Screensavers and warning banners/messages
- Newsletters
- Desk-to-desk alerts (e.g., a hardcopy, bright-colored, one-page bulletin – either one per desk or routed through an office – that is distributed through the organization's mail system)
- Agency wide e-mail messages
- Videotapes
- Web-based sessions
- Computer-based sessions
- Teleconferencing sessions
- In-person, instructor-led sessions
- IT security days or similar events
- "Brown bag" seminars
- Pop-up calendar with security contact information, monthly security tips, etc.
- Mascots
- Crossword puzzles
- Awards program (e.g., plaques, mugs, letters of appreciation)

Some techniques that lend themselves to dissemination of a single message are the use of awareness tools, posters, access lists, screensavers and warning banners, desk-to-desk alerts, agency wide e-mail messages, brown bag seminars, and awards programs.

Techniques that can more easily include a number of messages include "do and don't lists," newsletters, videotapes, web-based sessions, computer-based sessions, teleconferencing sessions, in-person instructor-led sessions, and brown bag seminars.

Techniques that can be fairly inexpensive to implement include messages on awareness tools, posters, access lists, "do and don't lists," checklists, screensavers and warning banners, desk-to-desk alerts, agency wide e-mail messages, in-person instructor-led sessions, brown bag seminars, and rewards programs. Appendix D contains sample awareness posters.

Techniques that can require more resources include newsletters, videotapes, web-based sessions, computer-based sessions, and teleconferencing sessions.

In addition to making awareness material interesting and current, repeating an awareness message and using a variety of ways of presenting that message can greatly increase users' retention of awareness lessons or issues. For example, discussion in an instructor-led session about avoiding being a victim of a social engineering attack can be reinforced with posters, periodic agency wide e-mail messages, and messages on awareness tools that are distributed to users.

5.3 Techniques for Delivering Training Material

Techniques for effectively delivering training material should take advantage of technology that supports the following features:

- **Ease of use** (e.g., easy to access and easy to update/maintain);
- **Scalability** (e.g., can be used for various audience sizes and in various locations);
- **Accountability** (e.g., capture and use statistics on degree of completion); and
- **Broad base of industry support** (e.g., adequate number of potential vendors, better chance of finding follow-on support).

Some of the more common techniques that agencies can employ include:

- **Interactive video training (IVT)** – IVT is one of several distance-learning techniques available for delivering training material. This technology supports two-way interactive audio and video instruction. The interactive feature makes the technique more effective than non-interactive techniques, but it is more expensive.
- **Web-based training** – This technique is currently the most popular for distributed environments. "Attendees" of a web-based session can study independently and learn at their own pace. Testing and accountability features can be built in to gauge performance. Training models incorporating this technique are beginning to provide the additional benefit of interaction between instructor and student or among students.
- **Non-web, computer-based training** – This technique continues to be popular even with web availability. It can still be an effective method for distribution of training material, especially if access to web-based material is not feasible. Like web-based training, this technique does not allow for interaction between the instructor and students or among students.
- **Onsite, instructor-led training (including peer presentations and mentoring)** – This is one of the oldest, but one of the most popular techniques for delivering training material to an audience. The biggest advantage of the technique is the interactive nature of the instruction. This technique, however, has several potential disadvantages. In a large organization, there may be difficulty in scheduling sufficient classes so that all of the target audience can attend. In an organization that has a widely distributed workforce, there may be significant travel costs for instructors and students. Although there are challenges for distributed environments, some learners prefer this traditional method over other methods.

Blending various training delivery techniques in one session can be an effective way to present material and hold an audience's attention. For example, showing videos during an instructor-led session allows the audience to focus on a different source of information. The video can also reinforce what the instructor has been presenting. IVT, web-based training, and non-web, computer-based training can also be used as part of an instructor-led training session.

André Bento
Aspirante-Aluno Infantaria