



Rafael Aranha ^(*)(1)
Tenente Transmissões

1. INTRODUÇÃO

A proliferação actual de tecnologia e a acentuada dependência das organizações em sistemas informáticos e nas redes de computadores revela um conjunto de novas ameaças e novos desafios. Esta dependência, quando utilizada em sistemas críticos, como hospitais, é transferida também para o cidadão individual. Muitos dos possíveis cenários de ataque a infra-estruturas físicas podem e devem ser transpostos para o campo digital, nomeadamente a Internet.

Pretende-se neste artigo apresentar alguns cenários e situações reais que demonstrem as vulnerabilidades e consequentes preocupações e atenções que devem ser dadas aos sistemas informáticos. A interdependência e a interligação entre as diversas redes existentes leva a que haja a necessidade de um acompanhamento e actualização tecnológica permanente, que possibilite o aconselhamento e a supervisão das infra-estruturas críticas.

São também analisados diversos tipos de ameaças que se poderão encontrar no ciberespaço e o modo como poderão afectar os indivíduos, as organizações ou mesmo um país.

(*) A desempenhar funções na Companhia de Transmissões da Brigada Mecanizada Independente.

(1) Trabalho realizado em Dezembro de 2000. Actualizado em Fevereiro de 2005 e gentilmente revisto pelo Sr. Major TM (Eng) Paulo Fernandes Viegas Nunes.

2. CENÁRIO

São oito horas da manhã, Inverno, hora de ponta. Pessoas e carros movem-se lentamente pela cidade em direcção ao local de trabalho. De repente, em Lisboa, a energia falha e os semáforos deixam de funcionar. Entretanto, em Madrid, os sistemas de abastecimento de água e gás paralisam. Em Paris, o tráfego aéreo fica caótico quando se verificam interferências nos radares de controlo. Em Londres, o metro pára devido a um problema nos computadores de gestão de tráfego. Aparentemente os acontecimentos parecem não estar relacionados. Mas algumas pessoas mais atentas rapidamente os atribuiriam a um possível ataque terrorista, muito bem coordenado, extremamente eficiente, e por isso anónimo, deixando os seus alvos sem saberem o que realmente aconteceu. Um grupo terrorista que, não violentando directamente a população, queria marcar uma posição. Ataques a sistemas de produção, distribuição e comunicação, incluindo os militares, sistemas de controlo de tráfego aéreo, redes financeiras, software de controlo de sistemas de bombagem de poços de petróleo ou de gás, a relógios de sistemas regidos temporalmente, a bases de dados governamentais, a registos de bancos e de empresas, a sistemas de emergência médica, são exemplos de alvos propensos a sabotagens cuja destruição teria consequências mais elevadas do que à primeira vista poderia parecer. Há uns anos atrás nenhum grupo poderia obter tal protagonismo, mas hoje existe a possibilidade de que tais actividades se materializem.

3. ACERVO CONCEPTUAL

Ao tipo de acções referidas no parágrafo anterior, podem muitas vezes ser atribuídos significados que não correspondem à realidade. Para melhor distinguir as actividades e os que as praticam são aqui apresentadas as seguintes definições ²: *Activismo* (*activim*) refere-se ao normal uso da Internet em apoio a um grupo, causa ou ideal. As acções nesta área restringem-se à procura de informação, construção de *sites* para divulgação, transmissão electrónica de publicações, memorandos por e-mail, uso dos *grupos de discussão* (Usenet - *newsgroups*), formação de grupos de interesse, planeamento e coordenação de actividades. *Hactivismo* (*hactivim*) refere-se à junção dos interesses dos activistas e das acções dos hackers. Aqui é preciso realçar que existe uma grande diferença

² As definições apresentadas, apesar de baseadas na literatura, expressam o ponto de vista do autor. As definições dos termos em itálico encontram-se no glossário.

entre hackers e crackers. O primeiro termo deverá ser aplicado a alguém que resolve problemas (“a problem solver”), no entanto a noção comum que se tem do termo é outra. Embora juridicamente não o haja, os primeiros são muitas vezes motivados por causas ideológicas e têm objectivos não destrutivos. Praticam normalmente essas actividades pelo simples prazer de ultrapassar barreiras. Tradicionalmente, um hacker quando consegue entrar num sistema não retira qualquer tipo de informação. Deixa sim uma nota para o administrador do sistema em que refere como conseguiu entrar, de modo a que este possa corrigir a falha. Pelo contrário, um cracker tem geralmente motivos financeiros. Este, embora utilizando métodos idênticos (o que leva muitas vezes à confusão entre os dois grupos), extrai informação e potencialmente danifica o sistema em que penetrou. Assim, o hacktivismismo utiliza técnicas contra um alvo (normalmente um *site*) na Internet, com o intuito de prejudicar o seu normal funcionamento mas sem causar destruição. Exemplos disto são a substituição de páginas oficiais por outras com o objectivo de criticar os seus proprietários, *e-mail bombs*, *vírus* e *worms*.

O ciber-terrorismo é a convergência de actividades terroristas com o espaço virtual. A sua motivação é normalmente política e recorre a acções destrutivas e espectaculares, como por exemplo a paragem de sistemas que originam elevados estragos financeiros ou perdas humanas. Um exemplo seria a penetração num sistema de tráfego aéreo com o intuito de provocar a colisão de dois aviões. A ciber-guerra (*cyberwarfare*) refere-se a operações e actividades militares tendo por base o espaço virtual (ciberespaço³) onde se encontram duas forças distintas em conflito, normalmente países. Poderá também consistir em ataques não militares perpetrados por indivíduos ou grupos paramilitares.

A ciber-espionagem tem um propósito idêntico à espionagem tradicional, que poderá integrar a análise da informação obtida de sistemas informáticos de pessoas, organizações ou países. Poderá também ter o propósito de alcançar segredos ou tecnologias no âmbito empresarial e obter assim vantagens comerciais. A Netwar tem a ver com os ideais das forças em oposição e a tentativa de os difundir, estando mais ligada a conflitos sociais ou ao crime. O conflito Israelo-Árabe ou alguns episódios políticos entre os Estados Unidos e a China têm desencadeado alguma actividade nesta área.

³ O ciberespaço é constituído pelos diversos componentes que formam uma rede. Desde os computadores terminais, passando pelos elementos activos da rede (e.g. routers, servidores) até à própria informação digital. A Internet é o exemplo mais comum de ciberespaço.

As várias definições foram apresentadas aqui em separado, mas as fronteiras que as limitam são, como se irá constatar, um pouco difusas.

3.1 *Ciber-guerra*

O conceito de ciber-guerra prende-se com a condução de operações militares no domínio da informação. Tem como finalidades a inutilização ou a destruição dos sistemas de comunicação e a consequente perda de informação por parte do inimigo, a tentativa de saber tudo sobre o adversário enquanto se procura que este nada saiba sobre as nossas forças. Significa adquirir e manter em nosso poder a informação e o conhecimento que daí resulta, principalmente no caso em que o equilíbrio de forças é desfavorável, usando-os para que menos recursos sejam despendidos, rentabilizando assim os meios de emprego.

Apesar de questionável, um exemplo recente é a suposta capacidade instalada no novo submarino USS Jimmy Carter de executar escutas em cabos submarinos de fibra-óptica⁴. É de notar que a maior parte das comunicações actuais são transmitidas por fibra-óptica.

A ciber-guerra poderá também envolver o conceito de Guerra Electrónica no que concerne ao empastelamento, decepção, sobrecarga e intrusão nos circuitos de informações e comunicações do adversário.

3.2 *Guerra da Informação*

A Guerra da Informação (GI) não deverá ser confundida com a ciber-guerra (que envolve um controlo efectivo das redes). A GI inclui diversos tipos de tratamento de informação, sendo a mente humana o seu alvo primordial e consequentemente aqueles que tomam as decisões sobre a guerra ou a paz e sobre o emprego dos meios ao seu dispor. Embora exista efectivamente uma diferença, com o tempo, ela tornar-se-á mais difícil de detectar, à medida que os computadores são, cada vez mais, parte integrante das actividades diárias. Velocidade, coordenação e precisão são factores decisivos nos campos económicos, militares e políticos. A utilização da tecnologia como um factor multiplicador do potencial de uma força, pode descrever a razão que leva à implementação de um sistema digital de comunicações numa organização.

⁴ *New submarine can tap fiber-optic cables* - <http://www.cnn.com/2005/US/02/18/submarine.secrets.ap/>
Todos os sites referidos neste artigo foram confirmados em Fevereiro de 2005.

Uma organização deste tipo, pode produzir resultados desproporcionados à sua dimensão, comparativamente com o que se verificava na era industrial. A posse de uma estrutura digital constitui, desta forma, um elemento-chave tanto para o emprego do poder militar, como para o universo das empresas que desenvolvem uma actividade comercial. Isto verifica-se no campo financeiro, no mercado bolsista, na investigação, no desenvolvimento e na produção de bens e serviços. Desta forma, aqueles que dominarem a tecnologia digital poderão alcançar vantagens competitivas sobre aqueles que não o fizerem. Um esquema de classificação possível das actividades associadas ao emprego da GI será o seguinte:

- Negação de informação – o esconder, camuflar ou proteger a informação. O uso de técnicas de *criptação* e *autenticação* ou mesmo a separação física dos sistemas para impedir que alguém tenha acesso ou descubra o que não deveria.
- Decepção – a inserção propositada num sistema, de informação enganosa. Por exemplo, o uso de várias técnicas para esconder a identidade do atacante de uma rede ou de um sistema ou a alteração de bases de dados.
- Incapacitar e destruir – a inserção de informação que produzirá um mau funcionamento do sistema do adversário e que poderá levar à sua destruição. Neste domínio poderemos assistir desde um ataque de *negação de serviço (DoS)* até à utilização de bombas de impulsos electromagnéticos que destruirão fisicamente os sistemas.
- Subversão – a inserção de informação que despoleta um processo auto-destrutivo do sistema alvo. Exemplo disto são os *vírus*, *worms* e outros programas destrutivos que utilizam os recursos do próprio sistema para executar a sua destruição.

No âmbito da gestão do risco e nomeadamente no grau e probabilidade de ocorrência de ameaças, as actividades de guerra da informação poderão ser ainda classificadas em ofensivas, defensivas, terroristas e criminosas⁵.

3.3 *Ciber-terrorismo*

O ciber-terrorismo confere aos terroristas, tanto nacionais como estrangeiros, a capacidade de infligir danos sem consequências para eles próprios e uma diminuta probabilidade de serem detectados. É uma maneira dos mais fracos

⁵ Classificação efectuada por Michael Erbschloe (2001).

atacarem os mais fortes, particularmente para provocarem danos numa força superior num momento chave de uma operação.

Por norma, os grupos terroristas não são apoiados por Estados, mas diluem-se na população civil. Blindados, aviões de combate e mísseis guiados são ineficazes contra um inimigo que se mistura com a população. Operando “via modem”, estes grupos passam a trabalhar numa estrutura que usa mensagens de e-mail cifradas como meio de comunicação com a rede da organização a que pertencem e, conseqüentemente, reduzem assim a probabilidade de serem localizados.

“No que diz respeito aos alvos via ciberespaço, os terroristas certamente só empregarão ataques electrónicos se aqueles forem remuneradores. À medida que as infra-estruturas industriais se vão modernizando, procurando tirar partido das tecnologias da informação, este tipo de ataques tornar-se-á cada vez mais provável.

O terrorismo certamente já existia antes da Internet, mas para o pôr em prática, o seu agente tinha que estar fisicamente no local”(Regan, 1999, p.17)⁶.

Será o ciber-terrorismo, o futuro? Para estes grupos a sua prática terá certamente muitas vantagens. Se comparados com os tradicionais métodos, estes ataques oferecem a possibilidade de serem perpetrados à distância e no anonimato, são mais baratos, não envolvem o manuseamento de explosivos ou o recurso a missões suicidas e apresentam certamente uma grande cobertura dos media. *“O terrorismo do futuro poderá fazer mais com um teclado do que com uma bomba”*⁷. Face a esta observação, coloca-se a inevitável questão de saber porque é que quem pode tornar inoperacional uma rede eléctrica se poderá contentar em danificar apenas um poste de electricidade.

No entanto, o elevado nível de conhecimento e formação que esta área implica, leva à necessidade de recrutar pessoas ou grupos com um elevado grau de especialização. Grosseiramente, a situação poderá ser comparada à proliferação de cientistas e peritos em armas NBQ por todo o mundo após o fim da guerra-fria. A diferença poderá estar em que as acções no ciberespaço apenas necessitam de “matéria-prima e propulsores” que facilmente se encontram no mercado⁸.

⁶ Ed Roche do grupo Concours - firma internacional que estuda assuntos sobre a segurança na Internet.

⁷ National Research Council, “Computers at Risk”, National Academy Press, 1991.

⁸ Apesar dos Estados Unidos ou o Reino Unido terem um elevado número de denominados hackers, países como o Brasil, Rússia, Índia, China ou mesmo o Paquistão possuem grandes comunidades.

4. EXEMPLO DE ACÇÕES PERPETRADAS NO CIBERESPAÇO

A aparente ausência⁹ de tais incidentes poderia levar a concluir que tais acções não foram ainda efectuadas, o que não corresponde à verdade. Actualmente muitos ataques já foram postos em prática. O que se verifica é que muitas vezes os alvos ou aceitam a chantagem imposta ou tentam esconder o sucedido para manterem a credibilidade da sua rede, não revelando desta forma as suas vulnerabilidades. Exemplo disto são os bancos e as lojas on-line.

Enquanto, durante a guerra da ex-Jugoslávia, a NATO bombardeou todos os canais informativos de saída contendo propaganda política de Milosevic, não bombardeou intencionalmente os *servidores de acesso à Internet (ISP-Internet service providers)* ou desligou as ligações por satélite que forneciam o acesso à Internet a partir da Jugoslávia. O objectivo era, pelo contrário, manter a Internet activa. Indirectamente, a Internet pode ter condicionado a opinião pública sobre a guerra, facto que por sua vez poderá ter influenciado o processo de tomada de decisão durante o conflito. Ironicamente, o próprio governo sérvio tinha em seu poder os quatro servidores de acesso pertencentes à Jugoslávia mas também não os desligou, para com eles poder efectuar desinformação e propaganda.

Outro tipo de ataques são aqueles similares ao executado por um pirata sueco que colocou inoperacional o sistema de emergência (911) na Florida, embora não haja provas que tenha tido motivações hostis¹⁰.

Outro destes ciber-ataques¹¹ ocorreu em Março de 1994 quando os administradores dos sistemas informáticos dum centro de desenvolvimento espacial descobriram um *sniffer*¹² escondido num dos seus sistemas. Esse centro era um dos quatro maiores laboratórios da força aérea americana que desenvolvia sistemas tecnológicos para comando, controlo, comunicações, computadores e informações (C4I). As áreas de pesquisa incluíam sensores de vigilância, engenharia de software e computadores entre os quais um sistema de gestão militar. Investigações mais aprofundadas revelaram que todos os trinta sistemas do laboratório tinham sido infiltrados e usados como pontos de acesso para obter informações de outros sistemas (militares, governamentais, académicos, comerciais e até estrangeiros).

⁹ Não noticiada pelos media.

¹⁰ O atacante entrou no sistema informático da Southern Bell e gerou simultaneamente centenas de chamadas provocando o congestionamento das linhas troncas do serviço 911 na Florida (equivalente ao 112 em Portugal). Ver em http://www.911dispatch.com/911_file/history/hacking911.html.

¹¹ Ver em <http://staff.washington.edu/dittrich/cyberwarfare.html>.

¹² Programa que “fareja” um sistema e recolhe informação.

A investigação levou a concluir que o ataque tinha sido perpetrado por um jovem inglês de 16 anos que gostava de atacar *sites* militares (.mil) devido à sua falta de segurança. Depois de um interrogatório, ele admitiu que tinha tido ajuda de um tal Kuji. Constatou-se que o rapaz apenas conhecia Kuji “electronicamente”. Aparentemente este tinha treinado e conferido ao rapaz os conhecimentos necessários. A identidade, a residência, a aparência ou mesmo qualquer tipo de informação sobre Kuji nunca foram descobertas, assim como os seus motivos e o que foi feito com a informação roubada. O que se ficou a saber é que Kuji conseguiu entrar nos computadores do Departamento de Defesa americano (DoD), roubar informação e evadir-se sem ninguém dar por isso.

Outro aspecto a ter em conta é que, se necessário, alguns Estados não terão problemas em incentivar este tipo de actividades. O ataque electrónico chinês a alvos americanos depois do bombardeamento da embaixada chinesa em Belgrado é um bom exemplo. Não tem custos para o Estado e este pode alegar que nada teve a ver com o ataque, se é que realmente teve.

O seguinte cenário¹³ demonstra os possíveis efeitos dum ataque ciber-terrorista. Durante os sucessivos fracassos dos acordos de paz e em resposta às agressões dos croatas e muçulmanos aos sérvios, um grupo auto denominado Serbian Council for The Liberation of Bosnia (SCLiB) é formado, integrando elementos paramilitares no país e estrangeiro, pessoas influentes no meio político e estudantes simpatizantes na Eslovénia, Hungria e Jugoslávia. O grupo é constituído, assim que os membros se começam a encontrar virtualmente e a comunicarem pela Internet utilizando a tecnologia de *criptação PGP*. O seu objectivo é a vingança.

Tendo conseguido suficiente apoio financeiro e económico, o grupo formula um ataque. Utilizando o boletim meteorológico da CNN, o golpe é marcado para uma noite com mau tempo. Membros paramilitares introduzem-se na frequência das torres de controlo do aeroporto de Brcko. Voando para a pista com as luzes apagadas devido a informações que relatam trocas de fogo no solo, um C-130 é autorizado a aterrar pelos intrusos, que tinham conhecimento dos protocolos utilizados nas comunicações rádio. Outro C-130, cheio de combustível, é autorizado a levantar voo. O resultado foi o choque dos aviões numa mesma pista e a morte de todos os que iam a bordo. Os intrusos enviam

¹³ Devost, Matthew G. e outros, *Information Terrorism: Can you trust your Toaster?*, The Terrorism Research Center.

um sinal celular para a Eslovénia onde os membros nesse país enviam um comunicado electrónico para cerca de 30000 endereços de e-mail direccionando aqueles que o recebem para um *site*, em Amesterdão, gerido por estudantes eslovenos através de um *servidor* de Internet na Finlândia. Vinte e quatro horas depois o *site* já tinha tido cerca de 1 milhão de visitas. Os primeiros a visitar o *site* já tinham sido afectados por um programa – *trojan (cavalo de Tróia)* – concebido em *Java* que exploraria uma vulnerabilidade que apagaria irremediavelmente os ficheiros dos computadores que acessem ao *site* utilizando um browser específico. Devido à falta de um tratado internacional, a NATO nada pôde fazer para investigar os *servidores*.

Na Internet existem servidores cuja função é traduzir os endereços dos sites (e.g. www.cnn.com) em números (endereço IP), para que os diversos componentes que constituem uma rede possam entender os pedidos. Estes serviços, denominados de DNS, estão escalados hierarquicamente¹⁴. No topo da hierarquia existem treze destes servidores. Em 2002 foi-lhes realizado um ataque¹⁵. O objectivo seria paralisar os servidores efectuando-lhes uma enorme quantidade de pedidos – *distributed-denial-of-service*. Apesar de se ter notado alguns problemas na Internet, a rede manteve-se intacta. No entanto, alguns especialistas comentaram que o ataque utilizou técnicas simples e foi pouco elaborado. Se este tivesse resultado, haveria uma elevada probabilidade de a Internet passar a ser formada por pequenas redes separadas entre si.

Actualmente a Comissão Europeia tem tentado chegar a acordo com os Estados Unidos para que possa ter em território Europeu alguns destes servidores e assim participar na sua administração. Presentemente dez dos treze servidores de DNS de topo encontram-se nos Estados Unidos e são geridos pelo *Internet Corporation for Assigned Names and Numbers (ICANN)*, que se encontra na Califórnia.

De 16 a 18 de Novembro de 2005, em Tunes, irá realizar-se uma cimeira mundial, patrocinada pelas Nações Unidas, em que um dos objectivos é chegar a acordo sobre a administração dos servidores de topo da Internet¹⁶.

¹⁴ A hierarquização tem como objectivo, não só delegar competências de resolução de nomes a outros servidores, como de redistribuir a carga entre eles. Na prática, cada rede pode ter o seu próprio servidor de DNS. No entanto, as tabelas destes são sempre temporárias e necessitam de actualizações periódicas efectuadas pelos servidores de topo.

¹⁵ Ver em http://www.csoonline.com/read/120902/briefing_dns.html.

¹⁶ Richard Wray, *EU says internet could fall apart*, em <http://tecnology.guardian.co.uk/news/story/0,16559,1589967,00.html>.

5. A TÊNUE FRONTEIRA ENTRE O CIVIL E O MILITAR

Em que medida é que o terrorismo informático é uma preocupação das forças de segurança ou das forças armadas? Onde se encontra a linha que separa a ameaça interna da ameaça externa e dos correspondentes meios a utilizar?

Uma possível definição seria a atribuição de áreas de intervenção tendo como base as distinções entre a guerra e o crime, entre o que vem de fora e o doméstico, entre o que é governamental e o privado.

Consideremos um cenário em que as redes de electricidade e de comunicações são interrompidas. Ambos são alvos que colocariam questões de jurisdição, na medida em que pode ser discutível se tais acontecimentos provocam ou não baixas civis e um mal generalizado na população.

Outra questão seria a da resposta a dar a tais ataques, isto é, a posição a tomar perante uma situação deste tipo. Certamente, um ataque desta envergadura seria efectuado do estrangeiro devido à maior dificuldade de detecção. Iria apenas restabelecer-se o normal funcionamento, tentar descobrir os culpados ou responder de uma forma apropriada e proporcional. Mas quem teria competência para tal? A dificuldade está em que, na maioria dos países, as estruturas de informação são partilhadas entre o governo, os militares e organizações comerciais. Se no caso de um ataque a um sistema de defesa aérea também se danificar a rede que apoia os hospitais, qual será a reacção a tomar e como se poderá detectar o seu responsável? Sem um sistema integrado com as responsabilidades e áreas de acção bem definidas, um ataque dos tipos apresentados anteriormente poderia provocar danos elevados, enquanto se discute quem tem a competência para lhe responder. Mais importante do que responder será prevenir e antecipar. Como tal, torna-se imperativo que existam organismos que não só estudem e estejam constantemente actualizados quanto a novas vulnerabilidades, como tenham competências para implementar normas de conduta, de aconselhamento e se necessário efectuar testes de segurança a redes informáticas. Este tipo de equipas são usualmente denominadas de *Computer Emergence Response Team (CERT)*. O objectivo deste tipo de equipas não é o controlo da informação ou a sua recolha mas sim prevenir que, por exemplo, redes mal configuradas possam pôr em causa outras redes e infra-estruturas adjacentes.

Apesar do que foi referido no parágrafo anterior, a área da recolha de informações é crucial para a defesa dos interesses nacionais, e a Internet é actualmente um dos principais meios de proliferação de informação. A vulgarização de redes sem fios e correspondentes HotSpots, o incremento exponencial da utilização

de voz na Internet (e.g. VoIP) e de vídeo-conferência, a utilização de sistemas de cifra, entre outras tecnologias, torna necessário que os meios tradicionais ao dispor dos serviços de informação sejam complementados na área das redes de computadores. Como exemplo e a nível Europeu, o Sistema de Informação Schengen II pretende, entre outras, obter novas funcionalidades na área das novas tecnologias comparativamente ao sistema original¹⁷.

6. O PERIGO DA HEGEMONIA TECNOLÓGICA

Os Estados Unidos têm um sistema chamado “Carnívoro”¹⁸ que executa escutas a toda a informação digital que passa por servidores de Internet controlados ou com acordos com o Estado. O FBI, após ordem expressa do tribunal, pode filtrar informação vinda de uma determinada fonte. Mas essa fonte não precisa de ser nacional, apenas necessita de passar pelos seus servidores, o que não é difícil, visto estes serem numerosos.

Todos os pacotes enviados pela Internet têm um endereço de destino e um de remetente o que torna relativamente fácil essa acção. Existem métodos para contornar esta situação nomeadamente alterando continuamente o endereço do remetente ou utilizando software de *criptografia* (e.g. *PGP*). Outro método mais elaborado é obrigar os pacotes de dados a seguirem um determinado caminho (*routers* específicos). Em causa não está o sistema em si, mas sim a informação filtrada que não só pode ser aleatória como ultrapassar as fronteiras físicas do país.

Um exemplo simples é o serviço de mensagens, sendo o Messenger da Microsoft o mais conhecido. Uma mensagem enviada de Lisboa para Oeiras passa por um servidor da hotmail, que se encontra, com grande probabilidade, nos Estados Unidos. A questão não se coloca pela empresa em causa, pois poderia ter acontecido a outra grande empresa. Pretende-se sim sublinhar que a segurança de uma rede poderá ser comprometida por um computador vulnerável e/ou um utilizador incauto. No entanto, é também importante referir que a utilização em massa da mesma tecnologia, como é o caso dos sistemas operativos da Microsoft ou dos routers da Cisco, leva a que o surgimento de uma vulnerabilidade afecte um elevado número de redes. Em 2001, o *worm* denominado Code Red¹⁹ afectou

¹⁷ Ver em http://www.carloscoelho.org/apresentacao/relatorios.asp?id_menu=1&sub_menu=18.

¹⁸ Independent review of the Carnivore system – draft report, ITT Research Institute, 17 de Novembro de 2000.

¹⁹ Ver em <http://www.cert.org/advisories/CA-2001-19.html>

muitos dos servidores de web da Microsoft e alguns serviços da Cisco²⁰, paralisando muitas empresas e originando elevados prejuízos.

Como foi visto, os Estados Unidos estão longe de serem apenas vítimas, pois eles próprios exploram as vulnerabilidades de redes em todo o mundo. A Europa acusou os Estados Unidos de alegadamente efectuarem escutas permanentes aos sistemas de telecomunicações em todo o mundo e de utilizarem alguma dessa informação para privilegiar empresas americanas. O sistema, denominado de Echelon, foi alvo de uma investigação por parte de uma comissão de inquérito do Parlamento Europeu e que originou um polémico relatório²¹.

A probabilidade deste tipo de acções acontecer aumenta à medida que existe uma maior uniformização no tipo de hardware e software utilizado. Sistemas com níveis de segurança elevados não podem ser constituídos por “componentes” cuja utilização está generalizada e normalizada.

“Neste momento, outros sistemas operativos estão a ser adquiridos por países e por organizações privadas de forma a suprimir as necessidades de informatização que se lhes deparam. Os custos destas aquisições, que totalizam milhões de euros, podem ser reduzidos – ou mesmo anulados – pela opção, por exemplo, de software disponível gratuitamente, em alternativa ao software proprietário.

A França, Brasil e China já legislaram no sentido de todo o sector público do estado dar prioridade à instalação de software “open source” em detrimento de soluções proprietárias. Esta medida deve-se ao facto de a curto prazo os custos serem drasticamente reduzidos e a médio prazo se diminuir a dependência face a software cujo controlo e política de evolução estejam nas mãos de uma única empresa”²².

Um outro assunto que tem tido pouca atenção por parte dos media mas que pode influenciar muito o futuro do desenvolvimento de *software*, é o acordo a ser realizado pelo Conselho de Ministros da União Europeia no que diz respeito às patentes de software.

²⁰ É de referir no entanto que, segundo a Security Space, cerca de 70% dos servidores de web são Apache e não IIS (Microsoft), apesar dos primeiros tanto correrem em sistemas operativos da Microsoft como em Linux. Ver em http://www.securityspace.com/s_survey/data/200501/index.html.

²¹ Ver em http://www.carloscoelho.org/apresentacao/relatorios/echelon.asp?id_menu=1&sub_menu=18.

²² Manifesto em <http://p3m.gul.pt/>.

Daqui resulta a necessidade da criação de uma área tecnológica que na impossibilidade de ser própria de um só Estado, esteja confinada a uma zona de interesse comum restrita²³. Núcleos de investigação e desenvolvimento estão a ser criados em toda a Europa, inclusive em Portugal, para criar alternativas fiáveis e seguras. As redes tornar-se-ão assim, um meio de comunicação universal caracterizado pela “globalização contra-hegemónica”.

7. TECNOLOGIA AO ALCANCE DE TODOS

Até há pouco tempo o acesso às tecnologias de comunicação implicava elevados custos em redes telefónicas, torres com antenas de microondas, estações repetidoras, tubagens, mão de obra qualificada, etc. A era da informação veio provocar o declínio radical das despesas de hardware neste tipo de tecnologias. Novos aparelhos como emissores/receptores portáteis de satélite, eliminam a exclusividade do acesso aos meios de informação e a necessidade de meios filares e sistemas de distribuição baseados em fibra óptica. Ao mesmo tempo, conferem ao utilizador a capacidade de alcançar audiências na ordem dos milhares.

Uma das consequências deste tipo de liberalização tecnológica é a de qualquer grupo com escassos recursos humanos e financeiros²⁴ poder criar um sistema de comunicações, mobilizando e influenciando um elevado número de pessoas. Com este tipo de tecnologias é possível exercer um comando e controlo efectivo em grupos que podem estar geograficamente separados, mas em que a reunião das suas capacidades pode originar sérias ameaças.

O director do CERT²⁵ refere dois aspectos fundamentais dos muitos relacionados com a segurança informática. O maior é do uso exponencial da Internet e das tecnologias, estar a ultrapassar em muito o número de especialistas que sabem realmente configurar e gerir um sistema seguro.

Outro problema é o relativo à complexidade exigida na configuração de um sistema. Enquanto que há dez anos atrás, só os especialistas configuravam um sistema, hoje em dia existe muita gente a fazê-lo mas deficientemente, o que origina graves falhas na segurança. Operar correctamente um sistema exige um

²³ Ex. União Europeia.

²⁴ Comparativamente ao das grandes potências.

²⁵ Computer Emergency Response Team. Organismo criado em 1988 pela DARPA, visando tratar questões de segurança em redes, em particular na Internet - www.cert.org. A título complementar, esclarece-se que CERT é um tipo de equipas; no entanto a primeira equipa auto-denominou-se CERT.

elevado grau de conhecimento e conseguir que todos os sistemas obtenham um nível de segurança aceitável levará no mínimo cinco anos.

Um exemplo actual é a proliferação da venda de pontos de acesso sem fios à Internet. Por um lado é espantoso e por outro preocupante o número de redes sem fios e sem qualquer tipo de protecção que se conseguem apanhar na zona de Lisboa, permitindo a um qualquer transeunte com um portátil ou PDA ligar-se à Internet ou, eventualmente, à rede interna de uma empresa²⁶. Apesar de poderem ser facilmente configurados de forma a permitir uma maior segurança, o desconhecimento leva a que estes pontos, a maior parte em zonas residenciais, se encontrem desprotegidos.

“Alguém com poucos conhecimentos de computadores pode causar vários estragos”, afirmou Steven Aftergood, analista da área de defesa da Federation of American Scientists²⁷.

8. DE ONDE PODERÃO VIR AS AMEAÇAS

Neste teatro existe o mais variado leque possível de actores. Desde os tradicionais governos e exércitos, passando pela área dos negócios (e.g. espionagem industrial), de agentes políticos não pertencentes ao governo, por ONGs, por grupos de rebeldes, por grupos de cariz ideológico ou religioso que utilizam a Internet e as redes internacionais de comunicação para influenciar, trocar informação ou coordenarem acções políticas nacionais ou internacionais. Outro bloco serão os terroristas internacionais, grupos de guerrilhas, cartéis do tráfico de droga, facções étnicas, grupos tribais ou raciais, crime organizado (e.g. Máfia Russa) ou grupos extremistas. Como exemplo, um relatório da RAND²⁸ diz que a Al Queda aparenta ter implementado um sistema tecnológico de informações. Membros egípcios dessa organização são acusados de ajudarem a implementar uma rede de comunicações que se baseia na Internet, e-mail, em listas de notícias (*newsgroups*) e que possuem equipamento de comunicações e um largo número de discos para

²⁶ Este tipo de acção é denominada de War Driving, e consiste em uma pessoa se deslocar pelas ruas, com um portátil ou PDA, à procura de acesso à internet gratuitamente. Por vezes estes locais encontram-se marcados ou referidos em sites. Tal acção pode não só implicar um elevado tráfego na rede encontrada e consequente facturação, como pode permitir o total anonimato a possíveis atacantes.

²⁷ Expresso on-line, 15 de Dezembro de 2000, www.expresso.pt.

²⁸ Uma instituição sem fins lucrativos que tem como objectivo auxiliar as tomadas de decisões a partir da investigação e desenvolvimento – www.rand.org

armazenamento, de modo a permitir que os membros troquem informação sem correrem o risco de serem detectados pelas organizações anti-terroristas.

O Hamas também é suspeito de estar a tirar partido da Internet para a troca de informações e planos, comunicando os operacionais entre si por e-mail e salas de conversa (chat rooms).

A Internet como janela para o mundo tornou-se uma das mais importantes armas no arsenal deste tipo de grupos, não só lhes permitindo a angariação de membros e o aperfeiçoamento da sua organização, mas também o estabelecimento de alianças com outros grupos que, há uns tempos atrás, eram desconhecidos mutuamente. Desta forma, será possível prever que um ataque a um determinado alvo seja obra não de um mas de vários grupos com fins diferentes mas meios idênticos.

A imagem tradicional de um jovem de 18 anos, com o cabelo comprido, agarrado a um computador 24 horas por dia com o intuito de conseguir entrar num sistema só pelo prazer de o fazer terá que ser abandonada. Assim como o estereótipo do oponente com forças convencionais e equivalentes ao mundo ocidental. A assunção de que um oponente sem as capacidades da Europa ou dos Estados Unidos não cometerá um ataque é errada. Mas esse assunto será tratado com mais detalhe posteriormente.

“Por volta de 2002, cerca de 19 milhões de pessoas em todo o mundo terão a habilidade para montar um *cyber attack*” disse ²⁹ Frank G. Cilluffo, Director dum grupo ³⁰ especializado em sistemas de segurança e guerra da informação.

9. TIPOS DE ATAQUE UTILIZADOS

Apesar de existirem diversos tipos de ataques referem-se de seguida, de uma forma simplista, três destes tipos de acções.

O primeiro pode ser comparado à utilização de grafites nas paredes de uma rua. Os estragos são tão evidentes que rapidamente se podem reparar. O atacante consegue entrar no *site* da Internet do seu alvo e alterar o que lá aparece. Exemplo disto foi o que um grupo de Hackers portugueses fez ao *site* do governo indonésio, colocando neste mensagens a favor da causa timorense;

O outro tipo de ataque é conhecido por *negação de serviço* (*DoS - denial of service*) e tem como objectivo sobrecarregar e consequentemente tornar

²⁹ Warfare & Information Assurance, Abril 2001.

³⁰ Task Force on Information.

inoperacional um servidor “bombardeando-o” com e-mails ou *pings*. Para realizar tal acção é conveniente ter vários pontos de partida e conseguir um esforço concertado que pode ser difícil de organizar. Convém também que as várias acções partam de servidores diferentes pois estes ataques são de fácil detecção e podem ser anulados. Na Internet pode-se encontrar software para este efeito com nomes como EvilPing, WinSmurf ou Putdown. Exemplos deste tipo de ataques foram os realizados em Fevereiro de 2000 contra *sites* americanos e que os inoperacionalizaram durante algumas horas (Yahoo, Buy.com, eBay, Amazon e CNN, a ZDnet e a Etrade).

Acções similares podem muitas vezes originar elevados prejuízos. Um auto-intitulado Doctor Nuker, fundador dum grupo chamado “Pakistan Hackerz Club” não só alterou o conteúdo de diversos *sites* como retirou os dados dos cartões de crédito de 700 pessoas. Este grupo tinha já anteriormente alterado o *site* oficial da Índia em apoio aos separatistas de Caxemira.

Em Maio de 1999³¹, Nicodemo S. Scarfo, acusado de estar ligado à máfia, utilizava no seu computador o software de *criptação PGP* para proteger o seu PC dos olhares mais curiosos. Apesar disso, o FBI encontrou uma forma de ultrapassar esse software, instalando um dispositivo no teclado que gravou a sua palavra-chave quando ele a escreveu.

O terceiro tipo refere-se a ameaças vindas de *vírus*³² *informáticos*, de *worms*, de *cavalos de Tróia*, de *back doors*, em que estes programas ou aproveitam falhas de concepção do sistema, ou inserem nele fragmentos de código ou mesmo programas para destruir ou dar acesso a uma rede³³.

Um tipo de ataque muito mais elaborado foi o realizado contra a Microsoft, no ano 2000. O FBI sugere que ele tenha sido posto em prática da seguinte maneira³⁴: Um funcionário desconhecido recebeu uma mensagem de correio electrónico que trazia anexada um ficheiro tipo *cavalo de Tróia* chamado QAZ³⁵ que, uma vez activado, se escondeu no disco do seu computador “disfarçado” do editor de texto Notepad o qual era executado cada vez que o computador era ligado.

³¹ Ver em <http://www.epic.org/crypto/scarfo.html>.

³² Devido ao aumento das capacidades dos telemóveis têm surgido recentemente vírus para estes dispositivos. Um dos primeiros é o denominado Cabir, que poderá “infectar” telefones com o sistema operativo Symbian e com interface Bluetooth. Ver em <http://www.f-secure.com/v-descs/cabir.shtml>.

³³ Revista BIT, nº9, Junho de 1999.

³⁴ Artigo de 27 de Outubro de 2000 em: <http://tek.sapo.pt/470/225457.html>.

³⁵ <http://www.cert.org/summaries/CS-2000-04.html>.

O QAZ enviou então dados para um computador na Ásia com a informação exacta do computador infectado e a sua localização (o *endereço IP*) na Internet; o FBI considera provável que, nesta altura, o QAZ tenha obtido e instalado automaticamente, a partir de um *servidor* algures no Pacífico Sul, ferramentas adicionais para facilitar o acesso;

Os hackers usaram um outro programa que recolheu palavras-chave de vários utilizadores e as enviou para um endereço de correio electrónico na Rússia; para o sistema, estes hackers eram interpretados como funcionários da Microsoft que estavam a trabalhar fora das instalações da empresa e a usar acesso remoto.

Embora muitos dos programas utilizados e falhas exploradas estejam largamente documentadas na Internet, é de salientar que a origem deste tipo de ataques é muitas vezes de fácil detecção, pois como foi referido atrás, qualquer bloco de dados enviado contem o *endereço IP* do remetente e os *servidores* normalmente guardam informações sobre o que entrou e saiu. Só com acções cuidadosamente planeadas e com conhecimentos elevados, é possível realizá-las sem se ser localizado. Este tipo de acções pode demorar dias até se conseguir descobrir uma falha num sistema e meses até se conseguir explorá-la sem se ser detectado.

10. EFEITOS COLATERAIS

Poderíamos ser tentados a dizer que Portugal se encontra afastado desta realidade mas assim não é. Não só pode servir como ponte ou ponto de passagem para ataques a alvos não nacionais como também, sendo um país a iniciar a sua actividade neste âmbito, transformar-se num campo de testes.

Desta forma, cada país tem que desenvolver a sua própria estrutura de segurança e garantir uma capacidade de resposta credível. Se tal não acontecer, sujeita-se a ser apenas um pião no meio dum conflito e um alvo apenas pela razão de ser mais vulnerável. Se vitimando pequenos e indefesos países ajudar a exercer pressão sobre grandes potências, alianças ou coligações, o atacante não hesitará em fazê-lo. Assim, tais países são atacados simplesmente porque se encontram vulneráveis. A participação de um país em organizações como a União Europeia ou a NATO leva a que haja uma acrescida credibilidade a manter no que concerne à segurança das informações. A troca de informações e a inerente confiança entre diferentes países só poderá acontecer quando todos tiverem sistemas que garantam essa mesma segurança.

O ambiente geoestratégico de um mundo globalizante favorece a chamada abordagem indirecta³⁶. Constatando-se que hoje em dia muitos dos satélites de comunicações pertencem a consórcios, será possível a um potencial agressor tentar intervir num determinado país para chantagear outros países membros do consórcio, incluindo os alegadamente neutros.

11. DEFENSIVA, OFENSIVA E RETALIAÇÃO

Nas sociedades altamente dependentes dos sistemas de informação, a interferência nesses pode causar inconveniência a curto prazo, mas mais importante, pode também ter como consequência a falta de confiança no seu funcionamento no longo prazo. Retomando o exemplo da Microsoft, se nem a sua própria rede é segura como poderá ela garantir a segurança da rede de terceiros³⁷?

Imagine-se mais uma vez que de tempos a tempos um sistema bancário de um país é atacado e sofre assim cortes de longos períodos. Até que ponto é que as pessoas continuariam a confiar nesse sistema?

Enquanto é aceitável que um segurança de um banco abra fogo sobre um assaltante armado que entra pela porta da frente, a perspectiva de ter um administrador de um sistema informático bancário a lançar um ataque em resposta a uma tentativa criminosa de entrar na rede interna do banco é no mínimo legalmente problemática. O que provavelmente aconteceria era o servidor a partir do qual foi iniciado o ataque processar o banco em causa.

Os Estados Unidos consideram estes tipos de ataques ou qualquer acção contra organizações militares ou sistemas de segurança tão graves como ameaças directas à vida, logo seguida de ataques a infra-estruturas da Internet que provoquem a interrupção ou perda de serviços.

12. PRIVACIDADE

No quotidiano andamos onde queremos sem ninguém saber e falamos com quem queremos. Quem pode, compra o que quiser; na televisão vemos ou não os anúncios, numa livraria compramos aquilo que escolhemos livremente. Quando

³⁶ Termo utilizado por Liddell Hart (1968).

³⁷ Apesar de ser uma questão pertinente, qualquer rede é potencialmente insegura, seja qual for a tecnologia utilizada, se for mal configurada, não efectuar actualizações regulares ou não tiver uma eficaz política de acessos e permissões.

vamos ao médico esperamos que só ele saiba dos nossos problemas e do banco que só este conheça o nosso saldo. Transponhamos agora tudo isto para a Internet mas tirando-lhe uma coisa: é que há mais gente a saber tudo aquilo que fazemos. Nos *sites* a que temos acesso existe, cada vez mais, um *cookie* à espreita. As lojas on-line já conhecem as nossas preferências, apresentando-nos, mal entramos, os livros, as roupas, ou outros artigos do tipo que comprámos da última vez. Agora imagine-se que toda esta informação é cruzada numa só base de dados³⁸. Se lhe juntarmos mais alguns dados quase que se pode traçar um perfil psicológico. Quem estaria interessado em tais dados? Como exemplo, as empresas de marketing e as seguradoras.

Juntando ao puzzle anterior as bases de dados dos registos civis, dos números de contribuinte, dos registos médicos e bancários³⁹ e as recentes tecnologias de localização por telemóvel obtém-se tudo menos privacidade. Este enredo é parecido com a narrativa do filme “The Net” e que aparentemente pouco pode ter de real. Mas o que é certo é que nem toda a gente anda apenas a vender produtos de consumo ou apólices de seguro...

O surgimento, em Dezembro de 2000, de um pacote de programas designado por DSniff⁴⁰ veio originar uma quebra de segurança em *protocolos* antes considerados seguros (*SSL*, *SSH*). Estes protocolos são usados para a transmissão segura de dados⁴¹ que passaram a estar ameaçados por programas “prontos a usar” disponíveis gratuitamente na Internet.

³⁸ SQL é a linguagem de programação mais utilizada para criar, consultar e modificar bases de dados. Como tal, muitas das vulnerabilidades exploradas em lojas on-line recorrem a erros de programação destas mesmas bases de dados.

³⁹ é possível consultar, efectuar pagamentos e transferências através da Internet.

⁴⁰ Este pacote foi desenvolvido por Dug Song, investigador na área da segurança informática da Universidade de Michigan. É de salientar que muitos dos pacotes e programas desenvolvidos com características idênticas são-o por especialistas na área da segurança e têm como objectivo efectuar análises de tráfego, testar a segurança em redes ou efectuar o *proofs of concept* de falhas em protocolos. No entanto estes programas são utilizados, por vezes, com objectivos menos nobres e muito diferentes do que para aqueles que foram criados.

É também importante referir que este tipo de acções implicam que o atacante tenha acesso a um segmento da rede onde o tráfego está a passar e o consiga redireccionar e alterar – denominado “man in the middle attack”, o que nem sempre é possível. De uma forma muito simplista, o problema fundamental nos protocolos seguros através da Internet é que para o serem existe a necessidade de haver uma autenticação inicial e o estabelecimento de uma ligação segura entre dois pontos. Se estes não se “conhecerem” (e.g. certificados de **ambos** os lados) terão que trocar informação entre eles e será nesta fase que um dos tipos de ataque referidos anteriormente poderá ter sucesso.

⁴¹ Ex. comércio electrónico.

Segundo o analista de segurança Kirt Seifield, do *site* SecurityPortal.com, «sem uma reestruturação geral dos *protocolos* de segurança *SSH* e *SSL*, há muito pouco que possa ser feito para resolver o problema»⁴². Actualmente estes protocolos sofreram algumas alterações e são considerados seguros tendo o *SSL* evoluído para o *TLS*.

Também em Dezembro de 2000 a loja on-line Egghead.com⁴³ sofreu um ataque que poderá ter posto a descoberto informações financeiras de cerca de 3,5 milhões de clientes. Em Setembro, já o *site* Western Union tinha sido atacado. Para além de cinco dias off-line, a Western Union⁴⁴ viu ainda roubar-lhe cerca de 15 mil números de cartões de crédito e débito. Este tipo de acções tem ocorrido frequentemente e muitas vezes não vem a público devido ao receio de má publicidade por parte das empresas que sofreram os ataques. As vulnerabilidades nestes casos são normalmente encontradas nas bases de dados, apesar de muitas das vezes ser necessário explorar um conjunto delas para alcançar o objectivo pretendido.

13. O FUTURO...

Actualmente, um dos índices mais importantes da bolsa de Nova Iorque é o Nasdaq. É um índice onde as maiores empresas na área tecnológica estão cotadas. Se essas empresas fossem alvo de um ataque às suas redes e fossem roubadas informações cruciais na área da I&D, isto é, de futuros produtos, certamente todas as bolsas do mundo sentiriam o impacto. Ficção?

Em Agosto de 2000 um estudante californiano⁴⁵, fazendo-se passar por um trabalhador da Emulex, enviou um e-mail para os meios de comunicação social que dizia que a empresa estava sob investigação das autoridades bolsistas norte-americanas e que teria que apresentar de novo os seus resultados. Acrescentava ainda que o director-geral da empresa tinha apresentado a sua demissão. Tendo sido a informação considerada verdadeira, a sua divulgação provocou assim uma queda acentuada no preço das acções da empresa. A capitalização bolsista da empresa caiu 2.5 mil milhões de dólares em poucos minutos. De seguida, o estudante comprou um elevado número de acções a baixo preço, na esperança de as vender assim que a verdade fosse reposta e as acções voltassem a subir.

⁴² Expresso on-line, 23 de Dezembro de 2000.

⁴³ Ver em <http://news.com.com/2100-1017-250308.html?legacy=cnet>.

⁴⁴ Ver em <http://www.computerworld.com/securitytopics/security/story/0,10801,49970,00.html>.

⁴⁵ Ver em <http://money.cnn.com/2000/08/31/companies/emulex/>.

Será preciso ter em atenção que a mentalidade e as reacções da sociedade ocidental perante as novas tecnologias, poderá não coincidir com as de outras sociedades ética, cultural e psicologicamente distintas, em que as regras para a utilização do poder concedido pelo novo domínio, poderão ser muito diferentes e consequentemente originar novos impasses.

Embora se pudesse levar a crer que este tipo de guerra levaria a conflitos sem sangue, tal assunção é utópica. Embora se pudesse acreditar que os países ocidentais, perante um ataque a centrais eléctricas ou redes de telecomunicações, não reagiriam violentamente, o mesmo não se pode supor de outras partes, lideradas por um líder carismático ou cegas pelo extremismo de uma religião. A manipulação violenta certamente que continuará e a era da informação ajudará ainda mais na sua proliferação. Não será difícil de imaginar uma transmissão em directo da tortura de um prisioneiro de guerra ou de um rapto. Situações como aquelas encontradas na Somália, na ex-Jugoslávia, na Argélia, na Chechénia, no Sri Lanka e muito recentemente no Iraque não pertencem infelizmente ao passado, mas continuarão certamente a anteverem-se no futuro. A infra-estrutura digital será um alvo lucrativo em todos os sentidos, na medida em que se torna um dos poucos pontos fracos nas sociedades economicamente e militarmente avançadas. Mas embora sendo um alvo transforma-se simultaneamente numa arma.

Diariamente cerca de 5000 “piratas” vagueiam na Internet, alguns a trabalhar para empresas privadas ou para serviços governamentais ou mesmo por iniciativa própria. O que se espera é que este tipo de pessoas venha a ser guardião e não atacante. No futuro, eles podem não ser apenas amadores mas sim pessoas muito bem pagas para inserirem um vírus ou realizarem um ataque virtual em qualquer parte do mundo onde exista um computador ligado a uma rede.

Richard Clarke⁴⁶, antigo coordenador de segurança e protecção das infra-estruturas no Conselho Nacional de Segurança da Casa Branca disse: *“Os EUA estão vulneráveis a um ataque surpresa por via electrónica, uma espécie de Pearl Harbour digital com um potencial igualmente devastador, como quando os japoneses bombardearam Pearl Harbour há 59 anos. Várias nações criaram esquadrões de guerrilha informática; estas organizações estão a desenvolver técnicas para tornarem as redes de computadores inoperacionais”*⁴⁷;

⁴⁶ Autor do livro “Against All Enemies: Inside America’s War on Terror”.

⁴⁷ Ver em <http://archives.cnn.com/2000/TECH/computing/12/08/security.summit.ap/>.

Clarke foi um dos especialistas convidados para a conferência SafeNet2000 e as suas declarações foram proferidas um dia após o 59º aniversário do bombardeamento japonês de Pearl Harbour.

Apesar do tom alarmista do discurso proferido, não existe uma ameaça concreta ou iminente ao tipo de infra-estruturas aqui apresentadas, mas apenas uma possibilidade.

Uma possível previsão será a divisão do mundo em dois. Não em dois blocos como no tempo da guerra-fria mas entre aqueles que possuem infra-estruturas digitais e os que mantêm uma economia principalmente industrial ou mesmo agrária. No primeiro bloco, a riqueza irá concentrar-se nas mãos daqueles que possuem as tecnologias, e os que não as têm, irão tornar-se dependentes ou mesmo mais pobres.

A Internet poderá contribuir para aproximar os países, desde que se afirme como uma tecnologia barata e de fácil acesso, concluíram os participantes num debate do Conselho Económico e Social das Nações Unidas (ECOSOC) em Julho de 2000. Num recente relatório elaborado pelo Banco Mundial⁴⁸ é referido que *“a divisão digital está rapidamente a desaparecer [...] O acesso [às telecomunicações] nos países subdesenvolvidos é cada vez maior e tem crescido a um ritmo incrível – muito mais acelerado do que o verificado no passado”*.

Existe contudo outros aspectos a ter em conta, nomeadamente o impacto efectivo do desenvolvimento tecnológico no desenvolvimento social e económico em países subdesenvolvidos.

Conclusões

Foi assim apresentada uma abordagem que demonstra que na actualidade a gestão, o controlo e a supremacia nas redes de informação podem ser decisivas e influenciar directamente o combate ao nível virtual e físico.

O desenrolar de uma guerra num terreno fundamentalmente económico e comercial, compatível com a ausência de um inimigo declarado, leva a uma outra dimensão do conflito em que existe a necessidade de adaptação e mudança em relação aos conceitos tradicionais da guerra.

Resumindo, as instituições podem ser derrotadas pelas redes, e serão necessárias outras redes para contra-atacar. O futuro poderá pertencer a quem controlar estas redes. Este facto sugere que as instituições militares ou governamentais não serão

⁴⁸ Ver em <http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=7731166>.

os únicos alvos num futuro conflito, mas também o serão as grandes organizações comerciais com implicações muito elevadas. Pierre Lacoste, Almirante francês, disse: “*a informação apresenta como principal característica ser indissociável de toda a iniciativa estratégica; por natureza, está ligada a todas as formas de acção política, diplomática, militar, económica e social*”.

É uma corrida em que todos têm possibilidade de entrar e onde “os mais pequenos” podem, por vezes, estar em vantagem. Por um lado, os mais pobres poderão utilizar este tipo de ameaças mas estarão muitas vezes imunes a elas pois não têm as infra-estruturas tão desenvolvidas como os seus alvos. Por outro lado, o impacto que as novas tecnologias terão nas sociedades menos desenvolvidas e mais influenciáveis, à medida que os custos de as adquirir vão diminuindo, poderá ser imprevisível, na medida em que elas terão acesso a meios que se consideravam à partida só acessíveis às grandes potências e que por isso não constituíam uma séria ameaça – na Internet não é preciso ser rico para ser poderoso, basta ser inteligente”.

Este tipo de análise, muitas vezes, peca por deixar de lado as consequências sociais, ou seja, as pessoas. Enquanto que numa perspectiva europeia ou americana pode ser relativamente fácil de fazer uma previsão, já tal não acontece com todas as outras partes do mundo. Existem muitas culturas diferentes, religiões variadas e padrões comportamentais distintos. O que pode ser racional e lógico num país pode ser inconcebível noutra. A velocidade que a revolução digital está a adquirir nos países desenvolvidos, como por exemplo no Japão, poderá não ser benéfica para o resto do mundo. Esse crescimento não só pode provocar o aumento do fosso como provocar consequências imprevistas⁴⁹.

Imagine-se um país a tentar entrar directamente na era digital vindo ainda da fase agrária – Uma criança na Universidade. As novas tecnologias podem, por seu lado, ser uma ferramenta para obter um melhor bem-estar mundial (ex. medicina à distância) e proporcionar meios que pelos tramites tradicionais levariam anos a alcançar. No entanto, a disponibilização destas tecnologias trás custos que actualmente os países menos desenvolvidos não podem suportar. Como tal, os mais desenvolvidos terão certamente que financiar esses investimentos, se necessário sem qualquer margem de lucro⁵⁰.

⁴⁹ Exclusivamente sobre este assunto foi realizada uma reunião do G8.

⁵⁰ O Massachusetts Institute of Technology tem em desenvolvimento um computador portátil que custará menos de 100 dólares e que tem como alvo, estudantes de países sub-desenvolvidos. Ver em <http://news.bbc.co.uk/1/hi/tecnology/4292854.stm>.

Qualquer mudança, alteração de situação ou resolução de um problema passa, doravante, por uma solução tecnológica, nomeadamente em termos de informação e comunicação. O recurso à análise histórica e às consequências sociais não devem ser ignoradas, podendo cair-se no risco de se vir a ter o olhar unicamente voltado para o presente, encandeado por uma solução técnica que não pode deixar de ser um meio para alcançar um fim.

A capacidade de acompanhar a revolução digital não será muito diferente daquela que se alcançou com a invenção de Gutenberg. O analfabeto não será mais aquele que não souber escrever ou ler, mas sim aquele que não souber usar as novas tecnologias. O maior número de benefícios surgirão pois para aqueles que as conseguirem melhor explorar.

GLOSSÁRIO

Back doors – ou trap doors - acesso directo a um programa ou sistema sem passar pelos sistemas de segurança. Criados usualmente pelos programadores para efectuarem testes. O perigo está quando outros tomam conhecimento desses acessos.

Cavalo de Tróia – programa colocado num sistema (ex. recebido por e-mail e executado inadvertidamente) que pode recolher informação (ex. passwords) e enviá-la para o exterior.

Código-fonte – um sistema, programa ou aplicação na sua linguagem original.

Cookie – um tipo de informação enviada por um servidor para o browser do cliente. Estes dados permitem que sempre que um cliente consulte uma página nesse servidor, este possa identificá-lo e, e.g., apresentar-lhe uma página personalizada.

Criptografia – método matemático utilizado para tornar os dados secretos. Para o fazer (encriptação) é necessária uma “chave”, assim como para desencriptar (as chaves podem ser diferentes).

Darpa - Defense Advanced Research Projects Agency – organização de investigação e desenvolvimento para o departamento de defesa americano.

Denial of service (DoS) – um tipo de ataque a uma rede com o objectivo de a tornar inoperacional, inundando-a com tráfego supérfluo (ex. ping). Existe software para limitar ou mesmo anular o ataque, mas como os vírus, novos tipos de ataques DoS podem ser inventados.

Flood – traduzido à letra seria inundação. Refere-se a um fluxo constante de dados inúteis de forma a congestionar uma rede ou mesmo bloqueá-la.

E-mail bombs - envio de quantidades elevadas de e-mails de forma a prejudicar o normal funcionamento de um servidor de correio.

Encrytação – ver criptografia.

Endereço IP - endereço atribuído (pode ser fixo ou não) a uma máquina quando se liga à Internet.

Grupos de discussão – ver newsgroups.

HTML - Hypertext Markup Language. É uma linguagem de descrição de páginas de informação, standard no WWW. Com essa linguagem (que, para além do texto, tem comandos para introdução de imagens, formulários, alteração de fontes, etc.) podem-se definir páginas que contenham informação nos mais variados formatos: texto, som, imagens e animações.

Internet service providers (ISP) – empresas que dão acesso à Internet ao utilizador final. O utilizador liga-se ao *servidor* do ISP.

IP - Internet Protocol. Um dos protocolos mais importantes do conjunto de protocolos da Internet. Responsável pela identificação das máquinas e redes e encaminhamento correcto das mensagens entre elas. Corresponde ao protocolo de nível 3 do modelo OSI.

Java – é uma linguagem de programação com características adequadas para uso na Internet. Pequenas aplicações em Java são chamadas de “applets”.

Negação de serviço – ver *denial of service*.

Newsgroups – abreviatura de Usenet News, as news são grupos de discussão, organizados por temas (mais de 10.000!), a maior parte deles com distribuição internacional, podendo haver alguns distribuídos num só país ou numa instituição apenas. Nesses grupos, públicos, qualquer pessoa pode ler artigos e escrever os seus próprios, assim como perguntas e mesmo compra e venda. Alguns grupos são moderados, significando isso que uma pessoa designado para o efeito lê os artigos antes de serem publicados, para constatar da sua conformidade para com o tema do grupo. No entanto, a grande maioria dos grupos não são moderados.

Open source – programa em que o *código-fonte* é cedido ao utilizador e que assim pode saber como o programa funciona, quais as suas falhas e fazer as alterações que deseje.

PGP – Pretty Good Privacy – técnica de *criptografia*. Imagine-se um envelope que só o destinatário pode abrir e em que este tem a certeza de quem é o remetente. O PGP ficou conhecido pelo seu elevado grau de segurança virtualmente inquebrável.

Ping - Pequeno utilitário utilizado para ver se uma determinada ligação se encontra activa e qual o tempo que uma mensagem leva para ir de um ponto ao outro da ligação. O ping envia pacotes (geralmente 64 bytes) para um ponto, que responde enviando um outro pacote equivalente.

Protocolo - Um protocolo é para os computadores o que uma linguagem (língua) é para as pessoas. Dois computadores para poderem transferir informações entre si devem utilizar o mesmo protocolo (ou ter um terceiro que perceba os dois protocolos e faça a tradução).

Rede – vários computadores ligados uns aos outros para troca de informação. Ver *Protocolo*.

Routers – Computador, software ou material dedicado que serve para interligar duas ou mais redes efectuando automaticamente o redireccionamento correcto dos pacotes de informação de uma rede para outra.

Servidor – um computador (ou um programa num computador) que fornece ou direcciona informação para outros computadores numa rede (ex. um servidor de e-mail ou de web). Um dispositivo (hardware ou software) que gere os recursos numa rede (ex. impressoras).

Sistema – vários componentes diferentes a trabalharem em conjunto. Por exemplo, um sistema de computadores inclui tanto o hardware como o software.

Site – é um endereço na world wide web (www). Cada site contém uma *home page* que é normalmente a primeira página a ser apresentada. Um site também pode conter outros documentos e ficheiros. Cada site é gerido por um indivíduo, organização ou companhia. Podem existir vários sites num só *servidor*.

Sniffer – programa que é posto a correr numa máquina e que “fareja” toda a informação que por ela passa à procura de dados com certas características (ex. números de contas bancárias).

SSH - Secure Shell – programa utilizado para nos ligarmos a um outro computador numa rede, para executar comandos, programas e mover ficheiros para outro computador. O SSH tem como característica a sua componente de elevada segurança que permite comunicações seguras a partir de ligações com baixa segurança. Toda a informação é *encriptada* e a ligação poderá ser autenticada. Poderá ser utilizada como VPN e eventualmente para fazer passar tráfego por por firewalls que o restringem às portas 80 e 443.

SSL – um protocolo desenvolvido pela Netscape para transmitir informação privada via Internet. Muitos web *sites* utilizam este protocolo para obter informação confidencial do utilizador (ex. números de cartão de crédito). O seu endereço inicia com https: em vez de http:.

Trojan – ver cavalo de Tróia.

Vírus – fragmento de código que se coloca dentro de um programa e que o altera. O vírus só é activado quando o programa é executado, podendo afectar outras aplicações.

Worms – talvez a ameaça mais perigosa. É um programa “inteligente” que se propaga pela rede e que pode bloquear os recursos de um sistema.

XML – *Extensible Markup Language* – permite que o programador defina as suas próprias instruções, permitindo a transmissão, validação e a interpretação de dados entre aplicações e organizações diferentes. O xml torna mais dinâmica a troca, comparação e interacção de dados e informações vindas de diferentes locais.

BIBLIOGRAFIA

Ackerman, Robert, *Computer Security Experts Warn of Growing System Vulnerabilities*, SIGNAL, Agosto de 2000.

Arquilla, John J. and Ronfeldt, David F, in *Comparative Strategy*, Vol. 12, pp. 141-165, 1993. Excerpted from Cyber War Is Coming.

Borland, John, *Analysing the Threat of Cyberterrorism*, 1998 CMP Publications Inc., TECHWEB NEWS 23/09/98.

Breton, Philippe, *A utopia da guerra tecnológica mascara a natureza histórica das situações de conflito*, in Cordellier, Serge (dir.), *O novo estado do mundo*, Porto, Campo das Letras, 2000, pp. 77-79.

- Church, William, *Kosovo and the Future of Information Operations*, Centre for Infrastructural Warfare Studies.
- Denning, Dorothy E., *Activism, Hacktivism, and cyberterrorism: The Internet as a Tool for influencing foreign Policy*, Georgetown University, 1999.
- Devost, Matthew G. e outros, *Information Terrorism: Can you trust your Toaster?*, The Terrorism Research Center, April 1996.
- Dunlap, Charles, *Sometimes the Dragon Wins: A Perspective on Information-Age Warfare*, In Schwartau, 1996, pp.436-453.
- Erbschloe, Michael, *Information Warfare: How to Survive Cyber Attacks*, Osborne/McGraw-Hill, 2001.
- Figueiredo, Dias de, *A revolução está nas redes*, in Amaral, Francisco, (org.) *Os desafios do Milénio*, Lisboa, Quarteto, 2000, pp. 41-51.
- Guisnel, Jean, *Espionagem na Internet, As Guerras no Ciberespaço*, Lisboa, Difusão Cultural, 1997.
- Hart, Liddel, *Strategie: The Indirect Approach*, Praeger, 2.^a edição, 1968.
- Kopp, Carlo, *Information Warfare - A Fundamental Paradigm of Infowar*, Technical Report , posted on infowar.com, April 2000.
- Lev, Izhar, *E-Intifada: political disputes cast shadows in cyberspace*, Novembro, 2000. Disponível em: www.janes.com/security/international_security/news/jir/jir001103_1_n.shtml
- McLendon, James W., *Battlefield of the Future - 21st Century Warfare Issues*, Capítulo 7. Disponível em: <http://www.airpower.maxwell.af.mil/airchronicles/battle/bftoc.html>
- Molander, Roger C. e outros, *Strategic Information Warfare: A New Face of War*, research performed by RAND (Research and Development) for the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), 1996. Disponível em: <http://www.rand.org/publications/MR/MR661/>.
- Regan, Tom, *When Terrorists Turn To The Internet*, The Christian Science Monitor, January 1999.

Whitaker, Brian, *War games on the Net: But this time is for Real*, 30 Novembro de 2000, The Guardian. Disponível em: <http://www.guardian.co.uk/online/story/0,,404673,00.html>.

Alguns sites consultados:

Center for Army Lessons Learned: <http://call.army.mil/>

CNN: <http://www.cnn.com>

Computer Emergency Response Team Coordination Center: <http://www.cert.org>

Global Security: <http://globalsecurity.org>

Google!: <http://www.google.com>

Infowar: <http://www.infowar.com>

Institute for the Advanced Study of Information Warfare: <http://www.psycom.net/iwar.1.html>

Slashdot: <http://slashdot.org>

The Terrorism Research Center: <http://www.terrorism.com/infowar/index.shtml>