

# A Guerra de Informação: Perspectivas de Segurança e Competitividade - 2.ª Parte

Coronel  
José António Henriques Dinis



## 2ª PARTE

*“Na guerra, de modo geral, a melhor política é tomar um Estado intacto. Arruinando-o, diminui-se o valor”.*

*“Dominar o inimigo sem o combater é o cúmulo da habilidade”.*

*“Na guerra é de suprema importância atacar a estratégia do inimigo”.*

*“Um exército confuso conduz o adversário à vitória”.*

*“Sai vitorioso aquele que sabe quando pode combater e quando não pode alcançar a vitória”.*

Sun Tzu, in “A Arte da Guerra”

## 4. O Futuro Prospectivo

A explosão do conhecimento, em associação com a globalização e as características de descontinuidade dos diversos percursos profissionais, alguns deles de natureza forçada, “obrigam” as pessoas a terem de fazer face e a conviver com novas ideias e tecnologias, e a integrarem-se em novas culturas e práticas de gestão, tornando cada vez mais relativo e difícil a sua percepção da realidade. Nestas condições actuais e porventura com a sua pertinência no futuro, é com certeza um imperativo e um desafio para todos em encontrar novos meios e oportunidades para uma aprendizagem permanente, a fim de permitir a descoberta de novos horizontes e soluções para os desafios da vida.

Qual será o futuro das novas formas de trabalho e de emprego? Hoje já se conhecem algumas realidades que no futuro próximo serão cada vez mais acentuadas. Um emprego para toda a vida! Este desiderato é algo que começa a ter menos significado, nomeadamente nos diversos sectores económicos privados. E o que se passará com o

sector da Administração Pública, onde ainda hoje se pode dizer que o emprego tem alguma segurança, muito embora por vezes à custa de menores retribuições e outras condições estatutárias.

Tentando perspectivar o futuro a médio prazo, é necessário ter-se a consciencialização de que se vive um tempo de mudança e de transformações profundas, no qual parece assistir-se a uma brusca aceleração da história. Hoje tudo se passa muito depressa, e o pensamento filosófico em que se afirma “este momento presente já é passado”, tem uma realidade cada vez mais acentuada, podendo-se talvez extrapolar a outras dimensões da vida, e não exclusivamente à variável “tempo”. Uma novidade pode tornar-se obsoleta no dia seguinte, ou mesmo, no momento seguinte. Toffler, apresentou o “conceito de transitoriedade” como “o ritmo de movimentação das diferentes espécies de relações da vida do indivíduo”; e, refere que este ritmo, para algumas pessoas, apresenta-se com uma cadência de movimentação muito mais lenta o que para outras (Toffler: 1970: 50-51).

Perante o “conceito de transitoriedade”, o autor referia, em 1970, que:

As pessoas do passado e do presente levam vidas de «baixa transitoriedade», as suas conexões tendem a durar muito. Mas as pessoas do futuro vivem [viverão] num estado de «alta transitoriedade» e, por isso, a duração das suas conexões é [será] reduzida, o seu movimento de afinidades é [será] rapidíssimo. Nas suas vidas, coisas, lugares, pessoas, ideias e estruturas organizacionais são «consumidos» mais depressa (Toffler: 1970: 51).

Ainda segundo Toffler, “à medida que o ritmo geral de mudança se acelera, na sociedade, a economia da permanência é - tem mesmo de ser - substituída pela economia da transitoriedade”, em que: (1) “o progresso da tecnologia tende a baixar o custo da manufactura<sup>1</sup> muito mais depressa do que o custo do trabalho de reparação, pois enquanto aquela é automatizada, esta continua a ser, em grande parte, manual”; (2) “o progresso da tecnologia torna possível aperfeiçoar o objecto à medida que o tempo passa. A segunda geração de computadores é melhor do que a primeira, e a terceira é melhor do que a segunda”; e, (3) à medida que a mudança se acelera e chega a cantos cada vez mais remotos da sociedade, aumenta a incerteza acerca das necessidades do futuro. Reconhecendo-se a inevitabilidade da mudança, mas indecisos quanto às exigências que nos imporá (...)” (Toffler: 1970: 61).

As constatações e previsões anteriores, consideram-se uma realidade na actualidade, onde a “Guerra de Informação” se insere como uma consequência dos factos relatados e uma substância da “economia da transitoriedade”.

Segundo o mesmo autor anterior, “A fronteira entre «moda» e o produto comum tornar-se-á progressivamente mais difusa. Estamos [nos anos 70 do Sec. XX] a entrar rapidamente na era do produto temporário, feito por métodos temporários para satisfazer necessidades temporárias”, levando a uma “proliferação de produtos de usar e deitar fora e de estruturas temporárias” (Toffler: 1970: 63, 77).

Neste tempo de mudança, em que a incerteza é o que temos mais certo, o imobilismo já

não é possível, tal como a estabilidade sinónimo de segurança.

O lema “inovar ou desaparecer”, tem cada vez mais acuidade, e muito em particular ao nível empresarial, onde a concorrência é feroz. Manter nestas circunstâncias níveis de segurança e competitividade aceitáveis, é muito mais difícil, mas imprescindível para se conseguir sobreviver neste mundo como uma “Aldeia Global”.

De facto, as formas de vida do Homem e das Organizações que dirige, estão em permanente mutação. A informação e o seu controlo tornaram-se vitais para a sua sobrevivência. A informação e o conhecimento são activos cada vez com mais importância na gestão e avaliação das Organizações. A introdução de métodos e técnicas para contabilidade do Capital Intelectual, pode ser um factor diferenciador entre organizações, pela mais-valia dos seus recursos intangíveis, inerentes ao valor do respectivo conhecimento que constituem, e que não é fácil visualizar.

A Guerra de Informação tem um âmbito cada vez mais alargado, e no contexto do seu conceito, em sentido lato, apresenta-se com uma envolvente global, alargada a toda a sociedade, sem esquecer o vector militar, e com incidência particular e muito importante na Segurança e Defesa.

## **5. Conclusões**

Neste trabalho pretendeu-se analisar um tema emergente, sobre diversos assuntos com uma importância, à partida, determinante em diversos sectores da Sociedade, em que se vive uma nova era - a era da Sociedade da Informação.

A Segurança e a Defesa são dois conceitos, que na actualidade se consideram indissociáveis, e, assim, devem ser analisados em conjunto, o que se justifica por diversas razões, e que do ponto de vista conceptual, em Portugal, está bem patente no actual Conceito Estratégico de Defesa Nacional.

O sector da Defesa continua a ter como um dos seus pilares fundamentais as Forças Armadas (FFAA), que devem inserir-se no conceito global de Segurança e Defesa. As FFAA com a sua missão e especificidade própria, devem constituir-se como um meio de garantir a preservação de determinados princípios e valores nacionais e internacionais, com a necessária adaptação às situações e circunstâncias envolventes mais recentes, nomeadamente os novos tipos de conflitos, em particular provocados por actos de terrorismo.

A Guerra de Informação, à partida, poderia pensar-se como um assunto essencialmente de natureza militar. No entanto, se em sentido restrito esse desiderato se pode aplicar, já em sentido lato, considera-se que o termo “Guerra de Informação” abrange toda a sociedade, onde todos os sectores (económico, social, político, cultural e naturalmente o militar) têm a sua quota parte de actividade, neste Mundo cada vez mais uma “Aldeia Global”.

A Informação e o Conhecimento são cada vez mais objecto de conflitualidade e de competitividade, onde a segurança é essencial, mas as FFAA apenas em circunstâncias muito particulares têm condições para actuar, neste novo tipo de Guerra. Todas as organizações devem estar preparadas para se defender dos ataques a que estão sujeitas, perante as ameaças permanentes e que se desenvolvem num meio muito difuso - o Ciberespaço.

O tradicional “Campo de Batalha” está a ser substituído pelo “Espaço de Batalha”, onde os limites são imponderáveis e indefinidos, e mesmo o “potencial relativo de combate” é difícil, senão impossível, de estimar.

O espaço de batalha da Guerra de Informação, pode dizer-se que se confina essencialmente com o Ciberespaço, onde os meios e as condições de fazer este tipo de Guerra são caracterizados por uma assimetria aos diversos níveis. A utilização de determinadas “armas” contra as quais os meios de defesa convencionais não são adequados, e também perante a imprevisibilidade do tipo de operações possíveis e os efeitos da respectiva surpresa associada, permitem que uma diversidade de actores dispendo de meios relativamente limitados, tenham uma capacidade superior para provocar danos.

A Informação é a nova moeda da economia mundial, mas apresenta duas faces, a da conflitualidade e a da competitividade. Os agentes económicos que melhor consigam conduzir estas duas faces da Informação, que em muitas situações se confundem e se sobrepõem, talvez se permitam alcançar resultados favoráveis, nalguns casos positivos para a sociedade, e noutras situações negativos, perante determinados princípios éticos e de valores societais.

A Guerra de Informação pressupõe a utilização de meios relativamente extensos. Alguns elementos especialistas em tecnologias de informação, poucos computadores ligados à Internet e algumas aplicações informáticas adequadas, permitem levar a efeito acções de ataque cibernético, quer a um simples computador individual, quer a computadores servidores de redes informáticas de empresas ou de outras instituições, públicas ou privadas, incluindo as infra-estruturas críticas do Estado, relativas aos serviços de primeira necessidade dos cidadãos.

É necessário que os responsáveis das organizações, públicas e privadas, aos diversos níveis da sociedade, reunam esforços e maximizem as sinergias, para em conjunto e em parceria consigam uma estratégia global de segurança do ciberespaço, onde circula grande parte da informação que comanda esta “Aldeia Global”.

É necessário estar alerta, mas os nossos olhos agora são imensamente impotentes para monitorizar o que se passa no ciberespaço, e muito em particular na cabeça das pessoas, que podem facilmente aproveitar este espaço difuso e provocar ataques “perigosos”, com efeitos potencialmente catastróficos, através do hipotético comandamento de determinadas redes de computadores, que “comandam” e “controlam” serviços

nevrálgicos, nomeadamente as redes de produção e de distribuição de energia eléctrica, e de água, de controlo de tráfego aéreo, e por absurdo que pareça, nalguns casos até de sistemas de armas militares.

Embora se refira que os conflitos entraram na era mediática, de forma a tirar partido da gestão da opinião pública, no entanto, dos conflitos e das operações de Guerra de Informação, muito pouco se sabe, e não chega de uma maneira geral ao grande público. Neste caso, uma empresa ou outro tipo de organização, por norma não publicita os ataques de que é alvo, e muito menos quais os prejuízos sofridos. Esta situação, justifica-se porventura pelas consequências ainda mais negativas, que traria a divulgação de factos resultantes de vulnerabilidades atacadas, com deterioração da respectiva imagem e redução da eventual notoriedade no sector. Neste caso, pensa-se que em particular podem estar as instituições bancárias, que devem constituir-se num dos “alvos mais apetecidos”, mas naturalmente não serão as únicas, pois dependerá dos objectivos a alcançar com os ataques, em que a Informação, pode ser a própria arma e o objecto a atingir.

A Internet, a rede das redes, é hoje um meio sem regulação, onde se maximizam ameaças e oportunidades, e se tira partido das forças e fraquezas, ao nível dos diversos actores da Sociedade da Informação. A Guerra de Informação abrange actividades com incidência em todos os sectores da sociedade, e consequências potencialmente negativas em actividades de interesse público ou privado, onde a Segurança e Defesa assume particular importância.

Depois dos estudos e reflexões sobre este tema - “A Guerra de Informação, Perspectivas de Segurança e Competitividade”, - fica a percepção de que a ignorância conduz à despreocupação, e ambas devem ser condição necessária e suficiente, para que se criem condições de sensibilização sobre a Segurança no Ciberespaço.

Em Portugal, parece haver um longo caminho a percorrer, quanto à Segurança no Ciberespaço, em particular quanto ao seu enquadramento legal e coordenação das estratégias a definir. Neste caso, é necessário pensar que todas estas questões têm incidências ao nível individual, no meio empresarial, nas infra-estruturas críticas nacionais, no Estado de uma maneira geral, e na sua inter-relação com os outros actores da cena internacional.

Como conclusão e proposta final, considera-se imprescindível tomar medidas, a todos os níveis da sociedade, e, muito em particular nos sectores com maior incidência no âmbito da Segurança e Defesa, sobre a **Segurança no Ciberespaço**. Neste sentido, seria necessário estudar processos de “Mudança nas Organizações”, e, criar condições para a implementação de “**Projectos de Transformação**”, associados a “**Projectos de Modernização**”<sup>2</sup>, que se considerem adequados à situação da transformação prevista para o Futuro.

## Bibliografia

ABREU, Francisco (2002). *Fundamentos de Estratégia Militar e Empresarial - Obter Superioridade em Contextos Conflituais e Competitivos*. Lisboa: Edições Sílabo. ISBN: 972-618-275-1.

AIP - Associação Industrial Portuguesa (23Jul2003). *Carta Magna da Competitividade*. Lisboa: Associação Industrial Portuguesa - CCI/Câmara de Comércio e Indústria ([www.aip.pt](http://www.aip.pt) - acedido: 26Ago2003).

ALBERTS, David, S., GARSTKA, John J., HAYES, Richard E., SIGNORI, David A. (2001). *Understanding Information Age Warfare*. USA: CCRP Publication Series (DoD C4ISR Cooperative Research Program, ([www.dodccrp.org](http://www.dodccrp.org)). ISBN: 1-893723-04-6 (pbk).

ALBERTS, David, S., GARSTKA, John J., STEIN, Frederick, P. (1999). *Network Centric Warfare - Developing and Leveraging Information Superiority*. 2nd Edition (Revised) August 1999/Second printing February 2000. USA: CCRP Publication Series (DoD C4ISR Cooperative Research Program, ([www.dodccrp.org](http://www.dodccrp.org)). ISBN: 1-57906-019-6.

ARQUILLA, John, RONFELDT, David (editors) (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*.

(<http://www.rand.org/publications/MR/MR1382/> - acedido: 16Mar2003) (RAND: MR-1382-OSD) ISBN: 0-8330-3030-2.

BELLINGER, Gene (2000). *Knowledge Management - Emerging Perspectives, OutSights*. (<http://www.outsights.com/systems/kmgmt/kmgmt.htm> - acedido: 01Jun2000).

BISPO, António Jesus (2002). "A Sociedade de Informação e a Segurança Nacional". *Separata da Estratégia, Vol. XIII - IPCE - Lisboa - 2002*. Lisboa: Instituto Português da Conjuntura Estratégica.

BONIBACE, Pascal (2003). *Guerras do Amanhã*. Mem Martins: Editorial Inquérito. ISBN: 972-670-407-3.

BROWNING, John (1998). *Tecnologias de Informação - O Essencial das Tecnologias de Informação de A a Z*. Linda-a-Velha: Abril/Controljornal Editora, Lda (Biblioteca de Gestão EXAME n.º 4 - *The Economist Books, Essencial*). ISBN: 972-611-365-2.

BUSH, President George W. (USA) (February 2003a). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington: The White House.

([http://www.whitehouse.gov/pcipb/physical\\_strategy.pdf](http://www.whitehouse.gov/pcipb/physical_strategy.pdf) - acedido: 27Abr2003).

BUSH, President George W. (USA) (February 2003b). *The National Strategy to Secure Cyberspace*. Washington: The White House.

([http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf) - acedido: 27Abr2003).

BUSH, President George W. (USA) (July 16, 2002a). *National Strategy for Homeland Security*. Washington: The White House, Office of Homeland Security. ([http://www.whitehouse.gov/homeland/book/nat\\_strat\\_hls.pdf](http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf) - acedido: 27Abr2003).

BUSH, President George W. (USA) (September 17, 2002b). *The National Security Strategy of the United States of America*. Washington: The White House, SEAL of the President of the United States.

(<http://www.whitehouse.gov/nsc/nss.pdf> - acedido: 04Jan2003).

BUSH, President George W. (USA) (September 2002c). *The National Strategy to Secure Cyberspace for Comment (Draft)*. Washington: The White House, The President's Critical Infrastructure Protection Board.

(<http://www.whitehouse.gov/> - acedido: 04Jan2003).

CALDERA, Jose (2000). *Survivability Requirements for the U.S. Health Care Industry - A Thesis Submitted to the Information Networking Institute in Partial Fulfillment of the Requirements for the degree Master of Science in Information Networking*. Pittsburgh, Pennsylvania: Carnegie Mellon University. (<http://www.cert.org/archive/pdf/surv-us-health-thesis.pdf> - acedido: 10Set2003).

CAMPBELL, Duncan (2001). *O Mundo Sob Escuta - As capacidades de Intercepção no Sec XXI*, Tradução: Jorge P. Pires, Lisboa: FRENESI.

CASTELLS, Manuel (2002). *A Era da Informação: Economia, Sociedade e Cultura (Volume I) - A Sociedade em Rede*. Lisboa: Fundação Calouste Gulbenkian. ISBN: 972-31-0984-0.

CEDN - Conceito Estratégico de Defesa Nacional (2003). "Resolução do Conselho de Ministros n.º 6/2003, de 20Jan". *Diário da República - I Série-B, N.º 16, 20Jan2003*, pp. 279-287. Lisboa: Imprensa Nacional - Casa da Moeda.

CHO, George (Lt Col, USAF), JERRELL, Hans J. (Lt Col, USAF), LANDAY, William E. (Capt, USN) (2000, Jan). *Program Management 2000: Know the Way, How Knowledge Management Can Improve DoD Acquisition*. Fort Belvoir, Virginia 22060-5565: Defense Systems Management College Press. ([www.dsmc.dsm.mil/pubs/mfrpts/mrflist.htm](http://www.dsmc.dsm.mil/pubs/mfrpts/mrflist.htm) - acedido: 30Mar2000).

COELHO, José Dias et al. (1997). *Livro Verde para a Sociedade da Informação em Portugal*. Lisboa: Missão para a Sociedade da Informação - Ministério da Ciência e da Tecnologia. (<http://www.aceso.mct.pt/docs/lverde.htm> - acedido: 06Abr2003).

CRONIN, M. J. Lieutenant Colonel INT CORPS (1996). "Command and Control Warfare: Intelligence Support". *Army Doctrine and Training News*, Nr 5, May 1996. (Restricted).

DANIELS, N. Caroline (1997). *Estratégias Empresariais e Tecnologias da Informação*. Lisboa: Editorial Caminho. ISBN: 972-21-1128-0.

DINIS, José A. Henriques (1997, Dezembro). *A Gestão de Projectos de I&D, o Caso do Projecto de um Sistema C3I, no âmbito dos Projectos de I&D da Defesa Nacional*. Lisboa: Universidade Aberta (Dissertação de Mestrado - Não Publicado).

DINIS, José A. Henriques (2000). "A Gestão de Projectos de I&D no Âmbito da Defesa Nacional". *X Encontro da Associação das Universidades de Língua Portuguesa (AULP)*, pp.317-335. AULP: Ponta Delgada, Abril 2000.

DLCP - Dicionário de Língua Portuguesa Contemporânea (2001). Lisboa: Academia das Ciências de Lisboa e Editorial Verbo (2 Volumes).

EU - European Union (2001). "Working Document in preparation on the existence of a global system for intercepting private and commercial communications (ECHELON intercepting system)". Brussels: European Parliament, Temporary Committee on the ECHELON Interception System (4May2001).

Executive Digest (2002). "Supergestores". *Executive Digest*, Maio 2002, n.º 91, pp. 92-97. Linda-a-Velha: Abril/Controljornal-Editora, Lda.

FOGLEMAN, Ronald R. (General USAF, Chief of Staff), WIDNALL, Sheila E. (Secretary of the Air Force). *Cornerstones of Information Warfare*. (<http://www.af.mil/lib/corner.html> - acedido: 17Jul2003).

FRANKE, Ulrich J. (2001). "The Concept of Virtual Web Organizations and its Implications on Changing Market Conditions", *Virtual Organization Net*, Vol 3, No. 4 (ISSN: 1422-9331), *Electronic Journal of Organizational Virtualness*, eJOV 3 (2001) 4,

(<http://www.virtual-organization.net> - acedido: 23Nov2001).

GATES, Bill (1999). *Negócios @ Velocidade do Pensamento - com um Sistema Nervoso Digital*. Lisboa: Temas e Debates - Actividades Editoriais, Lda.

HOPKINS, Terence K., WALLERSTEIN, Immanuel, et al (1996). *The Age of Transition Trajectory of the World-System, 1945-2025*. London: Zed Books, Ltd. (N.º IDN: 9640).

IHEDN - Institut des Hautes Études de Defense Nationale (2002). *Comprendre La Defense*, pp. 57-63. Paris: Ed. Economica. ISBN: 2-7178-4473-2 (2e édition). ([www.ihedn.fr](http://www.ihedn.fr)).

JOINT PUB 1-02 (2003). *Department of Defense Dictionary of Military and Associated Terms*. USA: Joint Chiefs of Staff (Joint Publication 1-02, 12April2001, As Amended Through 5June2003).

JOINT PUB 2.0 (2000a). *Doctrine for Intelligence Support to Joint Operations*. USA: Joint Chiefs of Staff (Joint Publication 2-0, 9March2000).

JOINT PUB 2-01.3 (2000b). *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*. USA: Joint Chiefs of Staff (Joint Publication 2-01.3, 24May2000).

JOINT PUB 3-13 (1998). *Joint Doctrine for Information Operations*. USA: Joint Chiefs of Staff (Joint Publication 3-13, 9October1998).

LAUDON, Kenneth C., LAUDON, Jane P. (2002). *Management Information Systems, Managing The Digital Firm, Seventh Edition*. USA, New Jersey: Prentice-Hall International.

MILLER, Jerry P. et al. (2000). *Millennium Intelligence - Understanding and Conducting Competitive Intelligence in the Digital Age*. Medford, New Jersey: CyberAge Books ([www.infotoday.com](http://www.infotoday.com)).

MITNICK, Kevin D., SIMON, William L. (2002). *The Art of Deception- Controlling the Human Element of Security*. Indianapolis: Wiley Publishing. ISBN: 0-471-23712-4.

MOLANDER, Roger C., RIDDLE, Andrew S., WILSON, Peter A. (1996). *Strategic Information Warfare: A New Face of War*. Santa Monica: RAND (<http://www.rand.org/>).

NBSO - NIC BR Security Office (2003). *Cartilha de Segurança para Internet*. Versão 2.0, 11 de Março de 2003 (<http://www.nbso.nic.br/docs/cartilha/> - acedido: 27Ago2003).

NEGROPONTE, Nicholas (1996). *Ser Digital*. Lisboa: Editorial Caminho.

NONAKA, Ikujiro, TAKEUCHI, Hirotaka (1995). *The Knowledge Creating Company: How Japanese Companies Create The Dynamics of Innovation*. Oxford University Press.

OLIVEIRA, Luís Alcide d' (1995). "O C3I e a Informática". *Jornal do Exército*, Ano XXXVI, N.º 425, Maio, pp. 20-22. Lisboa: Estado-Maior do Exército.

OLIVEIRA, Luís Alcide d' (1996). "O Projecto RRING". *Jornal do Exército*, Ano XXXVII, N.º 435, Março, pp. 32-34. Lisboa: Estado-Maior do Exército.

PEREIRA, Alexandre, POUPA, Carlos (2003). *Como Escrever uma Tese, Monografia ou Livro Científico usando o Word*. Lisboa: Edições Sílabo. ISBN: 972-618-290-5.

PFALTZGRAFF, Robert L., SHULTZ, Richard H. (Ed.) (1997). *War in the Information Age: New Challenges for U. S. Security*. Virginia: Brassey's Editorial. ISBN: 1-57488-118-3 (IDN: N.º 9757).

POLLOCK, Neal J. (2002). *Knowledge Management and Information Technology (Know-IT Encyclopedia), First Edition September 2002*. Virginia (Fort Belvoir): Defense Acquisition University Press.

(<http://www.dau.mil/pubs/pubs-main.asp> - acedido: 26Abr2003).



RAMONET, Ignacio (2002). *Guerras do Seculo XXI - Novos Medos, Novas Ameaças*. Porto: Campo das Letras - Editores. ISBN: 972-610-570-6.

RODRIGUES, Fernando Carvalho (1999). "Ciência e Tecnologia da Guerra da Informação". *Jornal do Exército, Ano XL, N.º 474, Junho, pp. 26-27*. Lisboa: Estado-Maior do Exército.

RODRIGUES, Maria João (coord.), BOYER, Robert, CASTELLS, Manuel, ESPING-ANDERSEN, Gosta, LINDLEY, Robert, SOETE, Luc (2000). *Para Uma Europa da Inovação e do Conhecimento - Emprego, Reformas Económicas e Coesão Social (Documento de base da Presidência Portuguesa da União Europeia)*. Oeiras: Editora Celta.

ROGEIRO, Nuno (2002). *Guerra em Paz - A Defesa Nacional na Desordem Mundial*. Lisboa: Hugin Editores (<http://hugin.shopping.sapo.pt>). ISBN: 972-794-140-0.

ROGERS, C. T. (1995). "HQ Training and Doctrine Command - The Architect of the Future". *Army Doctrine and Training News, Nr 4, Nov 1995*. (Restricted).

SANTOS, José Rodrigues dos (2002). *A Verdade da Guerra - da Subjectividade, do Jornalismo e da Guerra*. Lisboa: Gradiva - Publicações.

SERRANO, António, FIALHO, Cândido (2003). *Gestão do Conhecimento - O Novo Paradigma das Organizações*. Lisboa: FCA - Editora de Informática. ISBN: 972-722-353-2.

SIEBER, Pascal (1.10.1998). "Virtual Organization". *Virtual Organization Net, Resources - Definitions*, (<http://www.virtual-organization.net> - acedido: 14Mar2002).

SIEBER, Pascal, GRIESE, Joachim (Eds.) (1999). *Organizational Virtualness and Electronic Commerce*. Proceedings of 2nd International VoNet - Workshop, September 23-24, 1999, Institute of Information Systems, Department of Information Management, University of Bern. Bern: Simowa Verlag Bern, (<http://www.virtual-organization.net/files/articles/vonet.99.pdf> - acedido: 19Jul2000).

SOUSA, Célio (2000). *Gestão do Conhecimento*. Lisboa: Editora RH.

STEWART, Thomas A. (Maio, 1999). *Capital Intelectual - A Nova Riqueza das Organizações*. Lisboa: Edições Sílabo.

TABORDA, João Pedro, FERREIRA, Miguel Duarte (2002). *Competitive Intelligence - Conceitos, Práticas e Benefícios*. Cascais: Editora Pergaminho, Lda.

TAPSCOTT, Don; CASTON, Art (1993). *Paradigm Shift: the new promise of information technology*. New York: McGraw-Hill Inc..

TOFFLER, Alvin (1970). *Choque do Futuro*. Lisboa: Edição Livros do Brasil.

TOFFLER, Alvin (1984). *A Terceira Vaga*. Lisboa: Edição Livros do Brasil.

TOFFLER, Alvin; TOFFLER, Heidi (1991). *Os Novos Poderes*. Lisboa: Edição Livros do Brasil.

TOFFLER, Alvin; TOFFLER, Heidi (1994). *Guerra e Antiguerra*. Lisboa: Edição Livros do Brasil.

TOFFLER, Alvin; TOFFLER, Heidi (1995). *Criando Uma Nova Civilização, A Política da Terceira Vaga*. Lisboa: Edição Livros do Brasil.

TZU, Sun (1993). *A Arte da Guerra*. Mem Martins: Publicações Europa-América (2ª Edição, Tradução de Ricardo Iglésias- "The Art of War").

UE - União Europeia (1996). *Livro Verde sobre a Inovação, Documento elaborado com base no documento COM (95) 688 final*. Bruxelas: Serviço das Publicações Oficiais das Comunidades Europeias.

UE - União Europeia (2000a). "O Conselho Europeu de Lisboa - Uma Agenda de

Renovação Económica e Social para a Europa, Contribuição da Comissão Europeia para o Conselho Europeu Especial de Lisboa, 23-24 de Março de 2000. Bruxelas: Comissão Europeia (01Mar2000).

UE - União Europeia (2000b). *Documento de trabalho da Comissão: Relatório sobre a implementação do Plano de Acção para Promover o Espírito Empresarial e a Competitividade, SEC(2000) 1825 - Vol. I*. Bruxelas: CCE - Comissão das Comunidades Europeias (27.10.2000).

UE - União Europeia (2000c). *Documento Interno da Comissão: Quais os progressos necessários para uma política empresarial ao serviço da competitividade da Europa, SEC (2000) 1942*. Bruxelas: CCE - Comissão das Comunidades Europeias (9/11/2000).

University of Texas (Jan, 2001). Measuring the Internet Economy. University of Texas/Cisco Systems. ([www.internetindicators.com](http://www.internetindicators.com) - acedido: 23Nov2001).

University of Texas (Jun 6, 2000). Measuring the Internet Economy. University of Texas/Cisco Systems. ([www.internetindicators.com](http://www.internetindicators.com) - acedido: 07Jun2000).

WALTZ, Edward (1998). *Information Warfare: Principles and Operations*. Boston: Artech House, Inc. ISBN: 0-89006-511-X.

WEST-BROWN, Moira J., et al. (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh: Carnegie Mellon University, Software Engineering Institute (Handbook CMU/SEI-2003-HB-002), (First release: December 1998, by West-Brown/Stikvoort/Kossakowski. 2nd updated edition April 2003).

(<http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html> - acedido: 10Set2003).

WICKHMAN, John A. (1989). "Why C4I is Right for AFCEA Today". *Signal*, Nov 1989, pp. 25-26.

## **Anexo A**

Conceitos sobre os termos:

"Dados", "Informação" e "Conhecimento"

### **Dados**

"Dados" são conjuntos de elementos discretos, não organizados, compostos por números, palavras, sons ou imagens independentes, e que podem ser facilmente estruturados.

Exemplo: os números 100 ou 5%, completamente fora de contexto, são apenas peças de dados, (sem significado). Estas peças de dados, fora de um contexto, não são mais do que "dados", e cada um pode apresentar-se com múltiplos significados, dependentes dos diversos contextos em que se enquadrem.

### **Informação**

"Informação" é um conjunto de dados organizados, padronizados, agrupados e/ou categorizados que dizem respeito a uma descrição, definição ou perspectiva. A Informação responde às questões: "o quê?", "quem?", "quando?", "onde?".

Exemplo: Se se criar uma conta bancária como base de um contexto, então uma determinada quantidade alocada de capital e uma taxa de juro anual de depósitos a prazo, passam a ter um significado nesse contexto com interpretações específicas. Em

relação aos “dados” anteriores, neste caso a quantidade amealhada do capital seria 100e, e a taxa de juro anual de depósitos a prazo teria o valor de 5%, sobre o capital da conta a prazo, durante um ano.

### **Conhecimento**

“Conhecimento” é Informação associada a uma experiência, que compreende uma estratégia, uma prática, um método ou uma abordagem. O Conhecimento responde à questão: “como?”.

Segundo Nonaka e Takeuchi (1995: 59), “uma organização não pode criar conhecimento sem indivíduos”.

Exemplo: Se se depositar 100e numa conta bancária, e o Banco pagar uma taxa de juro anual de 5%, então no final de um ano o Banco contabiliza 5e de juros e soma-os ao capital inicial depositado, e fica-se com 105e na conta bancária. Este modelo representa conhecimento, o qual, quando se entender, permite-se perceber quais os resultados que o modelo produz ao longo de um determinado período de tempo. Se se perceber o modelo, conhece-se, e o que se conhece é conhecimento. Se se depositar mais dinheiro numa conta bancária, obtém-se mais dinheiro dos juros, enquanto se se retirar dinheiro da conta, ganham-se menos juros.

Tipos de Conhecimento:

- Conhecimento Explícito: é o conhecimento documentado em livros, manuais, bases de dados, e outros suportes de informação.

- Conhecimento Tácito: é o conhecimento que está na cabeça das pessoas.

Segundo Nonaka e Takeuchi (1995: 60-61) o conhecimento explícito é objectivo e diz respeito a acontecimentos passados, enquanto o conhecimento tácito é subjectivo, e para a sua partilha entre indivíduos através da comunicação é um processo analógico, e necessita de um processamento simultâneo entre os respectivos indivíduos que pretendem partilhar o seu conhecimento.

Segundo Miller *et al.* (2000: 158), estima-se que cerca de 75-80% do que uma empresa/organização precisa de conhecer, para poder competir de forma mais eficiente, pode existir e residir na cabeça dos seus empregados e outros colaboradores, fornecedores e clientes-chave. Assim, a apreensão do conhecimento tácito ou não-articulado, considera-se um activo extremamente valioso, e constitui um dos objectivos das actividades da Gestão do Conhecimento. Desta forma, há que apostar no potencial humano e no seu desenvolvimento, através da valorização dos seus conhecimentos, saber/sabedoria e respectivas competências, como factores de alavanca para a melhoria das condições de competitividade.

A figura seguinte apresenta os Tipos de Conhecimento - Explícito e Tácito - e a sua complementaridade, em termos da sua relação com os “Dados”, a “Informação” e o “Conhecimento” propriamente dito.

Segundo Nonaka e Takeuchi (1995: 56-94), a criação do conhecimento organizacional faz-se através de um processo interactivo contínuo e dinâmico, em espiral, entre o

Conhecimento Tácito (CT) e o Conhecimento Explícito (CE), com base em quatro modos de conversão do respectivo conhecimento: (1) “socialização” - CT $\rightarrow$ CT; (2) “externalização” - CT $\rightarrow$ CE; (3) “combinação” - CE $\rightarrow$ CE; e, (4) “internalização” - CE $\rightarrow$ CT.

### **Saber/Sabedoria**

O “Saber/Sabedoria” exprime um princípio, discernimento, costume ou arquétipo, correspondendo a uma determinada “Competência”. O Saber/Sabedoria responde à questão: “porquê?”.

### **Figura 1 - Tipos de Conhecimento (Explícito e Tácito)**

A obtenção de “saber/sabedoria” é de certa forma um pouco complicado, e é baseada em princípios de sistemas. O princípio é que qualquer acção que produz um resultado, que encoraja outras acções do mesmo tipo, produz uma característica emergente denominada crescimento. Mas nada cresce de forma contínua sem ter em conta os seus limites de crescimento. O conhecimento e a capacidade de armazenamento têm os seus limites, que quando se refere à cabeça das pessoas, considera-se haver a necessidade de aprender a esquecer, para garantir a capacidade de adquirir novos conhecimentos.

A caracterização dos quatro conceitos anteriores - “dados”, “informação”, “conhecimentos” e “saber/sabedoria” - resume-se na figura seguinte.

O nível da estruturação dos dados e da respectiva informação, aumenta com a intervenção do ser humana, sobre esses dados e informação. No entanto, se se estiver perante máquinas “inteligentes”, através de técnicas de inteligência artificial, também poderemos, em determinadas circunstâncias e condições, ter o mesmo efeito, mas devemos pensar que essas próprias máquinas ditas “inteligentes”, foram estudadas e fabricadas pelo Homem. Haverá seres mais inteligentes que o ser humano?!...



Figura 2 – Caracterização de “Dados”, “Informação”, “Conhecimento” e “Saber/Sabedoria”<sup>4</sup>

## Anexo B

A “Guerra Centrada em Rede” - Relatório ao Congresso dos EUA

Em Março de 2001, o Departamento de Defesa, dos EUA, apresentou ao Congresso um Relatório sobre “Network Centric Warfare”<sup>5</sup>, onde se referiam as perspectivas iniciais daquele Departamento sobre o que é a “Guerra Centrada em Rede” na actualidade e quais os seus caminhos no futuro. Um documento subsequente, apresentado ao Congresso em Julho de 2001<sup>6</sup>, contém o mesmo assunto mais desenvolvido, segundo os capítulos seguintes:

- Introdução
- Transformação no Departamento de Defesa
- Conceitos e Teoria da Guerra Centrada em Rede (GCR)
- Pontos de Vista das Visões e Conceitos sobre GCR do Exército, Marinha, Corpo de Marines e Força Aérea

- Pré-requisitos da GCR
- Formas de Capacitar a GCR
- Estratégia de Implementação da GCR no
- Avaliação e Análise da GCR, incluindo a Evidência do Impacto da GCR
- Grelha Global da Informação
- A GCR e o Departamento de Defesa - Políticas e Processos
- A GCR Actual e Planeada - Iniciativas e Programas Relacionados
- Constatções e Conclusões

Este último documento, apresenta as definições para os termos “Transformação” e “Modernização”, que se considera útil e oportuno referir. Assim, “Transformação” é “a evolução e desenvolvimento de capacidades de combate que proporcionem vantagens revolucionárias ou assimétricas para as nossas forças [armadas]”, e, “Modernização” é “a substituição de equipamentos, sistemas de armas, e instalações de forma a manter ou melhorar a capacidade de combate, actualização de instalações, ou redução de custos de operação” (27Jul2001: 2-2).

Nos termos das definições anteriores, a implementação do conceito de GCR é uma “Transformação”, em que segundo o mesmo relatório, “envolve uma nova forma de pensar acerca de como se cumpre a nossa missão, como se organizamos e se interrelacionamos, e como adquirimos e colocamos em campo os sistemas que nos apoiam”. Por outro lado, a “GCR representa um conjunto de potencialidades de conceitos de combater e capacidades militares associadas que permitem aos combatentes tirar uma vantagem completa de toda a informação disponível e poder utilizar todos os equipamentos de forma rápida e flexível” (27Jul2001: i).

As formas de guerra tomam as características da era em que se desenvolvem. A GCR pode considerar-se como uma resposta às mudanças e oportunidades criadas pela Era da Informação.

Assim, “os termos ‘Operações Centradas em Rede’ (OCR) e ‘GCR’ são utilizados para descrever vários tipos de operações militares da mesma forma que os termos ‘e-business’ e ‘e-commerce’ são utilizados para descrever uma classe alargada de actividades de negócios que a Internet<sup>7</sup> possibilita”. Fazendo um paralelismo, então também a GCR é muito mais do que restringida ao combate - acerca do emprego dos conceitos da Era da Informação para aumentar o potencial de combate na guerra, e a eficácia na missão em operações diferentes da guerra<sup>8</sup> (27Jul2001: 3-1).

Tal como “os competidores que foram capazes, em primeiro lugar, de identificar correctamente o espaço de oportunidades proporcionado pela Internet, e com o negócio (comércio) electrónico permitirem-se procurar lucros desproporcionados. [Também,] o Departamento de Defesa [dos EUA] procura vantagens desproporcionadas em conflitos futuros, assim que se desenvolva e implemente uma estratégia de transformação centrada em rede” (27Jul2001: 3-1).

Como já se referiu no texto, no parágrafo sobre a Guerra Centrada em Rede, o termo “NCW”, não é ainda aceite universalmente na comunidade do Departamento de Defesa dos EUA, tal como os conceitos de GCR não são entendidos universalmente.

“O termo NCW” foi introduzido pela primeira vez numa larga audiência em 1998, no artigo “Network Centric Warfare: Its Origins and Future”, publicado nos “Proceedings of the Naval Institute”<sup>9</sup>. “Este artigo descreveu uma nova forma de pensar acerca de operações militares na Era da Informação e destacou a relação entre vantagem de informação e vantagem competitiva”. Entre dezenas de outros artigos e centenas de comunicações, sobre o tema da GCR, destaca-se porém o livro, “Network Centric Warfare: Developing and Leveraging Information Superiority”<sup>10</sup>, com dezenas de milhares de cópias distribuídas, incluindo a possibilidade de “download” da Internet<sup>11</sup>, em todo o mundo, e a sua tradução em japonês e coreano. Assim, este livro constitui-se na obra de referência principal sobre o assunto de GCR<sup>12</sup> (27Jul2001: 3-2).

O Relatório de 27Jul2001, apresentado ao Congresso dos EUA, sobre GCR, põe em evidência que os combatentes que utilizem os conceitos de GCR, podem obter um domínio da situação e um aumento substancial em sobrevivência, letalidade, rapidez, oportunidade em tempo e sensibilidade. A transformação do potencial de combate através do emprego destes conceitos, só se entendem através do foco centrado nas relações da guerra que têm lugar simultaneamente e entre os domínios “físico”, informacional” e “cognitivo”. O domínio físico é o domínio tradicional da guerra. O domínio informacional é o domínio onde a informação se cria, se manipula e se partilha. O domínio cognitivo é o domínio da mente dos combatentes e da população que os apoia (27Jul2001: iv).

Embora o conceito da GCR se apresente como muito facilitador para uma força militar tirar partido das condições inerentes à Sociedade da Informação, no entanto apresenta ainda alguns impedimentos que podem reduzir o avanço e limitar a capacidade para alcançar o potencial completo deste conceito emergente e que se considera inovador. O Relatório referido, apresenta como impedimentos principais já identificados, para o avanço do conceito da GCR, de natureza técnicos, culturais, organizacionais e administrativos, e incluem (27Jul2001: iii):

- Falta de segurança, conectividade robusta e interoperabilidade;
- Intolerância à inovação disruptiva;

- Falta de entendimento dos aspectos chave sobre o comportamento humano e organizacional;
- Falta de investimentos em tecnologia relacionada com a GCR.

O Relatório, apresenta como conclusões, as seguintes(27Jul2001: vii-viii):

- No futuro, as redes serão a forma mais simples e importante que contribui para o potencial de combate;
- Existe uma urgência considerável e crescente associada à eliminação dos impedimentos do avanço da GCR;
- A eliminação em tempo oportuno (ou mitigação) dos impedimentos, será facilitada por um Gabinete de Transformação ao nível do Gabinete do Secretário da Defesa;
- É necessário definir uma data para se alcançar a capacidade específica centrada em rede;
- A GCR (NCW) oferece promessas sem precedentes, para se alcançarem capacidades desejadas a longo prazo, sem um correspondente aumento em recursos para o mesmo período. Neste caso espera-se conseguir melhores resultados sem aumento de recursos.
- A GCR e as OCR serão a pedra de toque do plano estratégico do Departamento de Defesa para levar a efeito a transformação das forças (militares).

Como remate deste Anexo, permita-se a reflexão sobre a importância que estes conceitos apresentam para os investimentos a efectuar nos sectores da Segurança e Defesa, nas próximas décadas. É necessário distinguir e equacionar qual o empenhamento em processos e actividades de “Transformação” e/ou de “Modernização”, o que se aplica, também ao caso de Portugal, sem deixar de se enquadrar no âmbito das envolventes em que se inserimos, nomeadamente quanto às Organizações com quem se têm compromissos assumidos, em particular com a NATO e a União Europeia.

## **Anexo C**

### **Serviços de Resposta a Incidentes de Segurança Informática Europeus**

A lista seguinte contém os “Serviços de Resposta a Incidentes de Segurança Informática”<sup>13</sup> (SRISI) (CSIRT/CERT) Europeus, conhecidos e ordenados por países<sup>14</sup>. O livro “Handbook for Computer Security Incident Response Teams (CSIRTs)” constitui uma referência bibliográfica sobre este assunto, publicado pela “Carnegie Mellon University”<sup>15</sup>, dos EUA.



**Austria**

n ACOnet-CERT - "accredited" (28 March 2003)

**Belgium**

n BE-CERT

**Croatia**

n CARNet-CERT - "accredited" (9 September 2002)

**Cyprus**

n CYPRUS

**Denmark**

n CSIRT.DK - "accredited" (20 April 2001)

n DK-CERT - "accredited" (5 February 2002)

n KMD IAC - "accredited" (21 March 2002)

**Europe**

n Cisco PSIRT - "accredited" (1 May 2003)

n IBM ERS

**Finland**

n Funet CERT - "accredited" (21 April 2002)

n CERT-FI

**France**

n CERT-Intexxia - lost its Accredited Team (former "accredited") Status (28 February 2003)

n CERT-LEXSI

n CERTA - "accredited" (25 March 2002)

n certIST

n Renater CERT - "accredited" (30 September 2001) - also known as Le CERT Renater

**Germany**

n BSI-CERT changed its name to CERT-Bund

n CERT-Bund - formerly known as BSI-CERT

n CERT-VW

n CERTBw

n ComCERT

n dCERT

n DFN-CERT - "accredited" (14 November 2001)

n PRE-CERT - "accredited" (12 June 2002)

n RUS-CERT - "accredited" (15 March 2002)

n S-CERT - "accredited" (10 October 2002)

n secu-CERT

n SIEMENS-CERT - "accredited" (23 March 2001)

n *T-NETWORK-CERT* changed its name to T-Com-CERT

n T-Com-CERT - formerly known as T-NETWORK-CERT

n Telekom-CERT

**Greece**

n GRNET-CERT - "accredited" (7 April 2003)

**Hungary**

n HUNGARNet-CERT

**Iceland**

n ISNet CERT

**Ireland**

n HEANET-CERT

**Israel**

n ILAN CERT

**Italy**

n CERT-IT

n GARR-CERT - "accredited" (1 January 2001)

**Lithuania**

n LITNET CERT - formerly known as LITNET NOC-CERT

n *LITNET NOC-CERT changed its name to LITNET CERT*

**Luxembourg**

n LUX-CERT

**The Netherlands**

n AMC-CERT

n CERT-IDC

n CERT-KUN

n CERT-NL - "accredited" (1 January 2001)

n *CERT-RO changed its name to GOVCERT.NL*

n CERT-RUG - "accredited" (13 August 2002) - formerly known as seckern

n CERT-UU

n GOVCERT.NL - "accredited" (10 June 2002) - formerly known as CERT-RO

n KCSIRT - "accredited" (18 December 2002)

n *seckern changed its name to CERT-RUG*

n UNI-CERT

n UvA-CERT

**Norway**

n UniNett CERT - "accredited" (1 April 2001)

**Poland**

n Abuse TP S. A.

n *CERT-NASK changed its name to CERT POLSKA*

n CERT POLSKA - "accredited" (22 November 2001) - formerly known as CERT-NASK

n POL34-CERT

**Portugal**

n CERT.PT - formerly known as RCCN CERT

n *RCCN CERT changed its name to CERT.PT*

**Russia**

n RU-CERT

n WebPlus ISP

**Scandinavia**

n NORDUNET CERT - "accredited" (6 April 2001)

**Slovenia**

n SI-CERT - "accredited" (3 July 2001)

**Spain**

n esCERT-UPC - “accredited” (30 September 2001)

n IRIS CERT - “accredited” (23 March 2001)

n SI-API-CERT - “accredited” (13 November 2001)

### **Sweden**

n SITIC

n SUNet CERT - “accredited” (23 May 2002)

n TeliaCERT - “accredited” (12 July 2001)

n UU-IRT

### **Switzerland**

n CC-SEC

n CERN CERT

n IP+ CERT

n OS-CIRT

n SWITCH-CERT - “accredited” (20 September 2001)

### **United Kingdom**

n BTCERTCC - “accredited” (1 June 2001)

n BT SBS - “accredited” (1 June 2001)

n *CCTA changed its name to OGCBS*

n CITIGROUP

n DAN-CERT

n *DERA became Q-CIRT*

n E-CERT

n EUCS-IRT

n JANET-CERT - “accredited” (1 January 2001)

n MLCIRT

n MODCERT

n OGCBS - formerly known as CCTA

n OxCERT

n Q-CIRT - derived from DERA

n UNIRAS - “accredited” (21 April 2002)

## **Anexo D**

“CERT/Coordination Center” e “US-CERT”

- Estatísticas 1988-2003

O “CERT<sup>16</sup> Coordination Center” (CERT/CC)<sup>17</sup> é um centro de especialização em segurança da Internet, que faz parte do “Networked Systems Survivability (NSS) Program”<sup>18</sup> do “Software Engineering Institute” (SEI), um centro de investigação e desenvolvimento da “Carnegie Mellon University”, dos EUA.

O CERT/CC foi formado pela “Defense Advanced Research Projects Agency” (DARPA), em Novembro de 1988, em resposta a necessidades identificadas durante um incidente de segurança na Internet. Tem uma função de trabalhar com a comunidade da Internet na detecção e resolução de incidentes de segurança de computadores, tal como em tomar

medidas para prevenir futuros incidentes.

A missão específica do CERT/CC é:

- Fornecer uma visão abrangente de métodos de ataque, vulnerabilidades e o impacto de ataques nas redes e sistemas de informação; fornecer informação acerca de tendências e características de incidentes e vulnerabilidades.
- Construir uma infra-estrutura de profissionais de segurança cada vez mais competentes que responda rapidamente aos ataques aos sistemas ligados à Internet e que sejam capazes de proteger os seus sistemas contra compromissos de segurança.
- Fornecer métodos para avaliar, melhorar e manter a segurança e sobrevivência dos sistemas ligados em rede.
- Trabalhar com vendedores para melhorar a segurança dos produtos conforme vendidos.

Em 15 de Setembro de 2003, o “Department of Homeland Security”, em conjunção com o CERT/CC da “Carnegie Mellon University”, anunciou a criação do “US-CERT”<sup>19</sup>. O “US-CERT” trabalha com a “National Cyber Security Division” (NCSD) para prevenir e mitigar ataques e reduzir vulnerabilidades no ciberespaço.

O “US-CERT” é também o elemento central no “Cyber Security Tracking Analysis and Response Center” da “National Cyber Security Division” (NCSD), que inclui o “Federal Computer Incident Response Center” (FedCIRC).

A iniciativa de criação do “US-CERT” foi no sentido de utilizar as capacidades do “CERT/CC”, para ajudar a acelerar resposta da nação aos ataques e vulnerabilidades no ciberespaço. Esta iniciativa também pretende que o “Department of Homeland Security” permita uma melhor coordenação da análise, avisos e respostas das ameaças no ciberespaço.

O “CERT/CC” publica estatísticas<sup>20</sup>, sobre a sua actividade, que se apresentam nas tabelas seguintes (de acordo com a respectiva fonte indicada).

Tabela 1 – Número de incidentes relatados

**1988-1989**

Ano	1988	1989
<b>Incidentes</b>	6	132

**1990-1999**

Ano	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
<b>Incidentes</b>	252	406	773	1.334	2.340	2.412	2.573	2.134	3.734	9.859

**2000-2003**

Ano	2000	2001	2002	1Q-2Q 2003
<b>Incidentes</b>	21.756	52.658	82.094	76.404

Total de incidentes relatados (1988-2Q 2003): **258.867**

*Note-se que um incidente pode envolver um site ou centenas (ou mesmo milhares) de sites. Também, alguns incidentes podem envolver actividades de rotina por longos períodos de tempo.*

Tabela 2 – Vulnerabilidades relatadas

**1995-1999**

Ano	1995	1996	1997	1998	1999
<b>Vulnerabilidades</b>	171	345	311	262	417

**2000-2003**

Ano	2000	2001	2002	1Q-2Q 2003
<b>Vulnerabilidades</b>	1.090	2.437	4.129	1.993

Total de vulnerabilidades relatadas (1995-2Q 2003): **11.155**

Tabela 3 – Alertas de segurança publicados

**1988-1989**

Ano	1988	1989
“Advisories”	1	7
“Vendor Bulletins”		
“Summaries”		
<b>Totais</b>	<b>1</b>	<b>7</b>

**1990-1999**

Ano	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
“Advisories”	12	23	21	19	15	18	27	28	13	17
“Vendor Bulletins”					2	10	20	16	13	
“Summaries”						3	6	6	8	5
<b>Totais</b>	<b>12</b>	<b>23</b>	<b>21</b>	<b>19</b>	<b>17</b>	<b>31</b>	<b>53</b>	<b>50</b>	<b>34</b>	<b>22</b>

**2000-2003**

Ano	2000	2001	2002	1Q-2Q 2003
“Advisories”	22	37	37	13
“Summaries”	4	4	4	2
<b>Totais</b>	<b>26</b>	<b>41</b>	<b>41</b>	<b>15</b>

Total de alertas de segurança publicados (1988-2Q 2003): **413**

Tabela 4 – Notas de segurança publicadas

**1998-1999**

Ano	1998	1999
<b>Notas de Incidentes</b>	<b>7</b>	<b>8</b>
<b>Notas de Vulnerabilidades</b>	<b>8</b>	<b>3</b>
<b>Total de notas</b>	<b>15</b>	<b>11</b>

**2000-2003**

Ano	2000	2001	2002	1Q-2Q 2003
<b>Notas de Incidentes</b>	<b>10</b>	<b>15</b>	<b>6</b>	
<b>Notas de Vulnerabilidades</b>	<b>47</b>	<b>326</b>	<b>375</b>	<b>144</b>
<b>Total de notas</b>	<b>57</b>	<b>341</b>	<b>381</b>	<b>144</b>

Total de notas de segurança publicadas (1998-2Q 2003): **949**

Tabela 5 – Mensagens de mail manuseadas

**1988-1989**

<b>Ano</b>	1988	1989
<b>Mail</b>	539	2,869

**1990-1999**

<b>Ano</b>	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999*
<b>Mail</b>	4,448	9.629	14.463	21.267	29.580	32.084	31.268	39.626	41.871	34.612

**2000-2003**

<b>Ano</b>	2000	2001	2002	1Q-2Q 2003
<b>Mail</b>	56.365	118.907	204.841	146.291

Total de Mensagens de mail manuseadas (1988-2Q 2003): **788.660**

Tabela 6 – Chamadas “hotline” recebidas

**1992-1999**

<b>Ano</b>	1992	1993	1994	1995	1996	1997	1998	1999
<b>Chamadas</b>	1.995	2.282	3.665	3.428	2.062	1.058	1.001	2.099

**2000-2003**

<b>Ano</b>	2000	2001	2002	1Q-2Q 2003
<b>Chamadas</b>	1.280+	1.417+	880+	380+

Total de chamadas “hotline” recebidas (1992-2Q 2003): **22.275+**

## Anexo E

Termos e Conceitos sobre a segurança na internet

Este Anexo tem a finalidade de apresentar alguns conceitos sobre segurança de computadores, nomeadamente ligados em rede e à Internet.

A compilação de termos e conceitos aqui apresentada, baseou-se em partes (respectivamente adaptadas) do documento “Cartilha de Segurança para Internet”, cuja versão completa pode ser obtida no endereço da Internet em: <http://www.nbso.nic.br/docs/cartilha/>, onde, segundo a versão 2.0, de 11 de Março de 2003, é periodicamente actualizado.

### Segurança de Computadores

Um computador, ou uma rede de computadores, considera-se segura se satisfizer aos três requisitos básicos: “Disponibilidade”, “Integridade” e “Confidencialidade”.

A “Confidencialidade” permite que a informação só está disponível para os utilizadores devidamente autorizados; a “Integridade” permite que a informação não é destruída ou corrompida e o sistema tem um desempenho correcto; e, a “Disponibilidade” permite que os serviços/recursos do sistema estão disponíveis sempre que forem necessários.

Violações de cada um dos requisitos anteriores são apresentadas nos exemplos seguintes:

- “Confidencialidade”: alguém obtém acesso não autorizado ao computador pessoal de outra pessoa, e lê todas as informações contidas na sua Declaração de Imposto de Rendimentos (IRS/IRC);

- “Integridade”: alguém obtém acesso não autorizado ao computador pessoal de outra pessoa, e altera informações da sua Declaração de Imposto de Rendimentos (IRS/IRC), momentos antes de a enviar para a Direcção-Geral de Impostos, do Ministério das Finanças;

- “Disponibilidade”: a Direcção-Geral de Impostos, do Ministério das Finanças, sofre uma grande sobrecarga de dados ou um ataque de negação do serviço e por este motivo fica-se impossibilitado de enviar a Declaração de Imposto de Rendimentos (IRS/IRC).

### ***Que motivos leva alguém a querer invadir o meu computador?***

A resposta para esta pergunta não é simples. Os motivos pelos quais alguém tentaria invadir o seu computador são inúmeros. Alguns destes motivos podem ser:

- Utilizar o seu computador em alguma actividade ilícita, para esconder a sua real identidade e localização;

- Utilizar o seu computador para lançar ataques contra outros computadores;

- Utilizar o seu disco rígido como repositório de dados;

- Destruir meramente informação (vandalismo);

- Disseminar mensagens alarmantes e falsas;

- Ler e enviar *e-mails* em seu nome;

- Propagar vírus de computador;

- Furtar números de cartões de crédito e códigos bancários;

- Furtar o código da conta do seu fornecedor de Internet, para se ligar à Internet em seu



nome;

- Furtar dados do seu computador, como, por exemplo, informação do seu Imposto de Rendimentos (IRS/IRC).

### ***Códigos de Acesso (Passwords)***

Um código de acesso ou senha (*password*) na Internet, ou em qualquer sistema de computadores, serve para autenticar o utilizador, ou seja, é utilizada no processo de verificação da identidade do utilizador, assegurando que este é realmente quem diz ser.

Se alguém fornece a sua senha a outra pessoa, esta poderá utilizá-la na Internet para se passar pelo dono da senha. Alguns dos motivos pelos quais uma pessoa poderia utilizar a senha de outra pessoa são:

- Ler e enviar *e-mails* em seu nome;

- Obter informações sensíveis dos dados armazenados no seu computador, tais como números de cartões de crédito;

- Esconder a sua real identidade e então desferir ataques contra computadores de terceiros.

Portanto, a senha merece uma consideração especial, afinal ela é da inteira responsabilidade de cada pessoa utilizadora de sistema com segurança de acesso.

### ***O que não se deve usar na elaboração de um código de acesso ou senha (password)?***

O sobrenome, números de documentos, matrículas de carros, números de telefones e datas (qualquer data que possa estar relacionada o utilizador, como, por exemplo, a data do seu aniversário ou de familiares) deverão estar fora da lista de códigos de acesso ou senhas. Esses dados são muito fáceis de se obter e qualquer pessoa poderia utilizar este tipo de informação para tentar autenticar-se por outra pessoa.

Existem várias regras de criação de senhas, sendo que uma regra muito importante é jamais utilizar palavras que façam parte de dicionários. Existe *software* que tenta descobrir senhas, combinando e testando palavras em diversos idiomas, e geralmente possuem listas de palavras (dicionários) e listas de nomes (nomes próprios, músicas, filmes, etc.).

### ***O que é um bom código de acesso ou boa senha (password)?***

Uma boa senha deve ter pelo menos oito caracteres (letras, números e símbolos) (existem serviços que permitem utilizar senhas maiores do que oito caracteres; quanto maior for a senha, mais difícil será descobri-la, portanto procure utilizar a senha com o maior número de caracteres possível), deve ser simples de digitar e, o mais importante, deve ser fácil de lembrar.

Normalmente os sistemas diferenciam letras maiúsculas das minúsculas, o que já ajuda na composição da senha. Por exemplo, “pAraleLepiPedo” e “paRaLElePipEdo” são senhas diferentes. Entretanto, estas são senhas fáceis de descobrir utilizando software para quebra de senhas, pois não possuem números e símbolos e contém muitas repetições de letras.

### ***Quantos códigos de acesso ou senhas (password) diferentes se devem usar?***

Procurar identificar o número de locais onde se necessita utilizar uma senha. Este número deve ser equivalente à quantidade de senhas distintas a serem mantidas por cada utilizador. Utilizar senhas diferentes, uma para cada local, é extremamente importante, pois pode atenuar os prejuízos causados, caso alguém descubra uma das senhas.

Para ressaltar a importância do uso de senhas diferentes, imagine que é responsável por realizar movimentações financeiras num conjunto de contas bancárias, e todas estas contas possuem a mesma senha. Então, procure responder às seguintes perguntas:

- Quais seriam as consequências se alguém descobrisse esta senha?
- E se elas fossem diferentes, uma para cada conta, caso alguém descobrisse uma das senhas, um possível prejuízo teria a mesma proporção?

### ***Com que frequência se devem mudar os códigos de acesso ou senhas (passwords)?***

Devem trocar-se as senhas regularmente, procurando evitar períodos muito longos. Uma sugestão é que se realizem tais trocas em cada dois ou três meses.

Procurar identificar se os serviços que se utilizam e que necessitam de senha, quer seja o acesso ao fornecedor de Internet, *e-mail*, conta bancária, ou outro, disponibilizam funcionalidades para alterar as senhas e usar regularmente tais funcionalidades.

Caso não se possa escolher a senha na hora em que se contratar o serviço, procurar trocá-la com a maior urgência possível. Procurar utilizar serviços em que se possa escolher a senha.

Lembrar-se que trocas regulares são muito importantes para se assegurar a integridade das senhas.

### ***Quais os cuidados especiais que se devem ter com os códigos de acesso ou senhas?***

De nada adianta elaborar uma senha bastante segura e difícil de ser descoberta, se ao se usar a senha alguém puder vê-la. Existem várias maneiras de alguém poder descobrir a senha. Dentre elas, alguém poderia:

- Observar o processo de digitação da senha;

- Utilizar algum método de persuasão, para tentar convencer a entrega da senha;
- Capturar a senha enquanto ela é transmitida pela rede.

Em relação a este último caso, existem técnicas que permitem observar dados, à medida que estes são transmitidos entre redes. É possível que alguém extraia informações sensíveis desses dados, como, por exemplo, senhas, caso não estejam criptografados.

Portanto, alguns dos principais cuidados que se devem ter com as senhas são:

- Certificar-se de não estar a ser observado ao digitar a senha;
- Não fornecer a senha a qualquer pessoa, em hipótese alguma;
- Certificar-se que o fornecedor de Internet disponibiliza serviços criptografados, principalmente para aqueles que envolvam o fornecimento de uma senha.

### **Certificado Digital**

O certificado digital é um arquivo electrónico que contém dados de uma pessoa ou instituição, utilizados para comprovar a sua identidade.

Contém um conjunto de informações que identificam uma pessoa ou alguma autoridade garantindo a sua validade.

Algumas das principais informações encontradas num certificado digital são:

- Dados que identificam o dono (nome, número de identificação, estado, etc.);
- Nome da Autoridade Certificadora (AC) que emitiu o certificado;
- O número de série do certificado;
- Período de validade do certificado;
- Assinatura digital da AC.

O objectivo da assinatura digital no certificado é indicar que uma outra entidade (a Autoridade Certificadora) garante a veracidade das informações nele contidas.

### ***O que é uma Autoridade Certificadora (AC)?***

Autoridade Certificadora (AC) é a entidade responsável por emitir certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc.

Os certificados digitais possuem uma forma de assinatura electrónica da AC que o emitiu. Graças à sua idoneidade, a AC é normalmente reconhecida por todos como confiável, fazendo o papel de “Cartório Electrónico”.

### ***Que exemplos podem ser citados sobre o uso de certificados?***

Alguns exemplos típicos do uso de certificados digitais são:

- Quando se liga a um *site* com ligação segura, como, por exemplo, o acesso à conta bancária pela Internet, é possível verificar se o *site* apresentado é realmente da instituição que diz ser, através da verificação do seu certificado digital;
- Quando se consulta o banco pela Internet, este tem que assegurar-se da sua identidade antes de fornecer informações sobre a conta;
- Quando se envia um *e-mail* importante, a aplicação de *e-mail* pode utilizar o certificado para assinar “digitalmente” a mensagem, de modo a assegurar ao destinatário que o *e-mail* é remetente e que não foi adulterado entre o envio e a recepção.

### **Cookies**

*Cookies* são pequenas informações que os *sites* visitados podem armazenar no *browser*. Estes são utilizados pelos *sites* de diversas formas, tais como:

- Guardar a identificação e a senha quando se vai de uma página para outra;
- Manter listas de compras ou listas de produtos preferidos em *sites* de comércio electrónico;
- Personalizar *sites* pessoais ou de notícias, quando se escolhe o que quer que seja mostrado nas páginas;
- Manter a lista das páginas visitadas num *site*, para estatística ou para retirar as páginas que não têm interesse dos *links*.

### **Engenharia Social**

O termo Engenharia Social é utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do utilizador, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

### ***Que exemplos podem ser citados sobre este método de ataque?***

O primeiro exemplo seguinte, apresenta um ataque realizado por telefone. Os outros dois exemplos, apresentam casos onde foram utilizadas mensagens de *e-mail*.

Exemplo 1: algum desconhecido liga para sua casa e diz ser do suporte técnico do seu

fornecedor de Internet. Nesta ligação o desconhecido diz que a sua ligação com a Internet apresenta algum problema e, então, pede a sua senha para corrigi-lo. Caso entregue a sua senha, este suposto técnico poderá realizar uma infinidade de actividades maliciosas, utilizando a sua conta de acesso à Internet e, portanto, relacionando tais actividades com o seu nome.

Exemplo 2: recebe uma mensagem de *e-mail*, dizendo que o seu computador está infectado por um vírus. A mensagem sugere que instale uma ferramenta disponível num *site* da Internet, para eliminar o vírus do seu computador. A real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.

Exemplo 3: recebe uma mensagem de *e-mail*, onde o remetente diz ser o gerente ou o gestor de conta do seu banco. Na mensagem ele diz que o serviço de *Internet Banking* apresenta algum problema e que tal problema pode ser corrigido se executar a aplicação que está anexada à mensagem. A execução desta aplicação apresenta um ecrã análogo àquela que utiliza para ter acesso à conta bancária, aguardando que digite a sua senha. Na verdade, esta aplicação está preparada para roubar a sua senha de acesso à respectiva conta bancária e enviá-la para o atacante.

Estes casos mostram ataques típicos de engenharia social, pois os discursos apresentados, nos exemplos, procuram induzir o utilizador a realizar alguma tarefa e o sucesso do ataque depende única e exclusivamente da decisão do utilizador em fornecer informações sensíveis ou executar programas.

## **Vírus**

Vírus é um programa capaz de infectar outros programas e arquivos de um computador.

Para realizar a infecção, o vírus coloca uma cópia de si mesmo num programa ou arquivo, que quando executado, executa também o respectivo vírus, dando continuidade ao processo de infecção.

Normalmente o vírus tem controlo total sobre o computador, podendo fazer de tudo, desde mostrar uma mensagem de “feliz aniversário”, até alterar ou destruir programas e arquivos do disco.

### ***Como é que um computador é infectado por um vírus?***

Para que um computador seja infectado por um vírus, é preciso que de alguma maneira um programa previamente infectado seja executado. Isto pode ocorrer de diversas maneiras, tais como:

- Abrir arquivos anexados aos *e-mails*;
- Abrir arquivos do *Word*, *Excel*, etc.;
- Abrir arquivos armazenados em outros computadores, através da partilha de recursos;

- Instalar programas de procedência duvidosa ou desconhecida, obtidos pela Internet, de disquetes, ou de CD-ROM;

- Esquecer uma disquete no drive A: quando o computador é ligado.

Novas formas de infecção por vírus podem surgir. Portanto, é importante manter-se informado através de jornais, revistas e dos *sites* dos fabricantes de antivírus.

Existem vírus que procuram permanecer ocultos, infectando arquivos do disco e executando uma série de actividades sem o conhecimento do utilizador. Ainda existem outros tipos que permanecem inactivos durante certos períodos, entrando em actividade em datas específicas.

### ***O que é um vírus propagado por e-mail?***

Um vírus propagado por *e-mail* (*e-mail borne virus*) normalmente é recebido como um arquivo anexado a uma mensagem de correio electrónico. O conteúdo dessa mensagem procura induzir o utilizador ao clicar sobre o arquivo anexado, fazendo com que o vírus seja executado. Quando este tipo de vírus entra em acção, além de infectar arquivos e programas, envia cópias de si mesmo para todos os contactos encontrados nas listas de endereços de *e-mail* armazenadas no computador.

É importante ressaltar que este tipo específico de vírus não é capaz de se propagar automaticamente.

O utilizador precisa executar o arquivo anexado que contém o vírus, ou o programa de *e-mail* precisa estar configurado para auto-executar arquivos anexados.

### ***O que é um vírus de macro?***

Uma macro é um conjunto de comandos que são armazenados em algumas aplicações, e utilizados para automatizar algumas tarefas repetitivas. Um exemplo, seria num editor de textos, definir uma macro que contenha a sequência de passos necessários para imprimir um documento com a orientação de "portrait" (retrato) e utilizando a escala de cores em tons de cinza.

Um vírus de macro é escrito de forma a explorar esta facilidade de automatização e é a parte de um arquivo que normalmente é manipulado por alguma aplicação que utiliza macros. Para que o vírus possa ser executado, o arquivo que o contém precisa de ser aberto e, a partir daí, o vírus pode executar uma série de comandos automaticamente e infectar outros arquivos no computador.

Existem algumas aplicações que possuem arquivos base (modelos) que são abertos sempre que a aplicação é executada. Caso este arquivo base seja infectado pelo vírus de macro, todas as vezes que a aplicação for executada, o vírus também será.

Arquivos nos formatos gerados pelo *Microsoft Word*, *Excel*, *Powerpoint* e *Access* são os mais susceptíveis a este tipo de vírus. Arquivos nos formatos RTF, PDF e PS são menos

susceptíveis, mas isso não significa que não possam conter vírus.

### **Worm**

*Worm* é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

Difere do vírus, o *worm* não necessita de ser explicitamente executado para se propagar, a sua propagação executa-se através da exploração de vulnerabilidades existentes ou falhas na configuração de *software* instalado em computadores.

Geralmente o *worm* não tem como consequência os mesmos danos gerados por um vírus, como, por exemplo, a infecção de programas e arquivos ou a destruição de informações. Isto não quer dizer que não represente uma ameaça à segurança de um computador, ou que não cause qualquer tipo de dano.

Os *Worms* são notadamente responsáveis por consumirem muitos recursos. Degradam sensivelmente o desempenho de redes e podem ocupar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar. Além disso, podem gerar grandes transtornos para aqueles que estão a receber tais cópias.

### **Backdoors**

Normalmente um atacante procura garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão. Na maioria dos casos, a intenção do atacante é poder retornar ao computador comprometido sem ser notado.

A esses programas de retorno a um computador comprometido, utilizando-se serviços criados ou modificados para este fim, dá-se o nome de *Backdoor* ("porta do fundo").

### **Cavalo de Tróia**

Conta a mitologia grega que o "Cavalo de Tróia" foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso à cidade de Tróia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Tróia. Daí surgiram os termos "Presente de Grego" e "Cavalo de Tróia".

Na informática, um Cavalo de Tróia (*Trojan Horse*) é um programa que além de executar funções para as quais foi aparentemente projectado, também executa outras funções normalmente maliciosas e sem o conhecimento do utilizador.

Algumas das funções maliciosas que podem ser executadas por um Cavalo de Tróia são:

- Alteração ou destruição de arquivos;
- Furto de senhas e outras informações sensíveis, como números de cartões de crédito;
- Inclusão de *backdoors*, para permitir que um atacante tenha total controlo sobre o computador.

Por definição, o Cavalo de Tróia distingue-se de vírus e *worm*, por não se replicar, infectar outros arquivos, ou propagar cópias de si mesmo automaticamente.

Normalmente um Cavalo de Tróia consiste num único arquivo que necessita ser explicitamente executado.

Podem existir casos onde um Cavalo de Tróia contenha um vírus ou *worm*. Mas mesmo nestes casos é possível distinguir as acções realizadas como consequência da execução do Cavalo de Tróia propriamente dito, daquelas relacionadas ao comportamento de um vírus ou *worm*.

É necessário que o Cavalo de Tróia seja executado para que ele se instale num computador.

Geralmente um Cavalo de Tróia vem anexado a um *e-mail* ou está disponível em algum *site* na Internet.

É importante ressaltar que existem programas de *e-mail*, que podem estar configurados para executar automaticamente arquivos anexados às mensagens. Neste caso, o simples facto de ler uma mensagem é suficiente para que qualquer arquivo (executável) anexado seja executado.

### **Negação de Serviço (*Denial of Service*)**

Nos ataques de negação de serviço (*DoS - Denial of Service*) o atacante utiliza um computador para tirar de operação um serviço ou computador ligado à Internet.

Exemplos deste tipo de ataque são:

- Gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o utilizador não consiga utilizá-lo;
- Gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível;
- Retirar serviços importantes de on-line, de um determinado acesso importante da Internet (Serviço Público, por exemplo), impossibilitando o acesso dos utilizadores às suas caixas de correio no servidor de *e-mail* ou ao servidor *Web*.



### ***Negação de Serviços Distribuídos (Distributed Denial of Service)***

A Negação de Serviços Distribuídos (*DDoS - Distributed Denial of Service*) constitui um ataque de negação de serviços distribuídos, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores ligados à Internet.

Normalmente estes ataques procuram ocupar toda a banda disponível para o acesso a um computador ou rede, causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede.

O objectivo de tais ataques é indisponibilizar o uso de um ou mais computadores, e não invadi-los.

É importante notar que, principalmente em casos de *DDoS*, computadores comprometidos podem ser utilizados para desferir os ataques de negação de serviço.

Um exemplo deste tipo de ataque ocorreu no início de 2000, onde computadores de várias partes do mundo foram utilizados para indisponibilizar o acesso aos *sites* de algumas empresas de comércio electrónico. Estas empresas não tiveram os seus computadores comprometidos, mas sim ficaram impossibilitadas de vender os seus produtos durante um longo período de tempo.

### **Incidentes de Segurança e Abusos**

#### ***O que é um incidente de segurança?***

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

São exemplos de incidentes de segurança:

- Tentativas de ganhar acesso não autorizado a sistemas ou dados;
- Ataques de negação de serviço;
- Uso ou acesso não autorizado a um sistema;
- Modificações num sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;
- Desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou fornecedor do acesso.

#### ***O que é política de segurança?***

A política de segurança atribui direitos e responsabilidades às pessoas que trabalham com os recursos computacionais de uma instituição e com as informações neles

armazenadas. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham.

Uma política de segurança também deve prever o que pode ou não ser feito na rede da instituição e o que será considerado inaceitável. Tudo o que não cumprir a política de segurança é considerado um incidente de segurança.

Na política de segurança também são definidas as penalidades às quais estão sujeitos aqueles que não cumprirem a respectiva política de segurança.

### ***O que é política de uso aceitável (AUP)?***

A política de uso aceitável (*AUP - Acceptable Use Policy*) é um documento que define como os recursos computacionais de uma organização podem ser utilizados. Também é ela quem define os direitos e responsabilidades dos utilizadores.

Os fornecedores de acesso à Internet normalmente deixam as suas políticas de uso aceitável disponíveis nas suas páginas. As empresas costumam dar conhecimento da política de uso aceitável no momento da contratação ou quando um funcionário ou colaborador começa a utilizar os recursos computacionais da empresa.

### ***O que pode ser considerado uso abusivo de uma rede?***

Não existe uma definição exacta do que possa ser considerado um uso abusivo de uma rede.

Internamente às empresas e instituições, as situações que caracterizam o uso abusivo da sua rede estão definidas na política de uso aceitável. Na Internet como um todo, os comportamentos listados abaixo são geralmente considerados como uso abusivo:

- Envio de “SPAM”;
- Envio de correntes da felicidade e de correntes para ganhar dinheiro rápido;
- Cópia e distribuição não autorizada de material protegido por direitos de autor;
- Utilização da Internet para fazer difamação, calúnia e ameaças;
- Tentativas de ataques a outros computadores;
- Comprometimento de computadores ou redes.

Glossário

**AC** Autoridade Certificadora

**AFCEA** The Armed Forces Communications and Electronics Association

**AIP** Associação Industrial Portuguesa

**AIP/CCI** Associação Industrial Portuguesa/Câmara de Comércio e Indústria

**C2** Comando e Controlo; *Command and Control*

**C3I** Sistemas integrados de Comando, Controlo, Comunicações e Informações; *Command, Control, Communications and Intelligence (Systems)*

**C3IIS** *Command, Control, Communications, Intelligence and Information Systems* (ver C3ISI)

**C3ISI** Sistemas integrados de Comando, Controlo, Comunicações, Informações e Sistemas de Informação (ver C3IIS)

**C4I** Sistemas integrados de Comando, Controlo, Comunicações, Computadores e Informações; *Command, Control, Communications, Computers and Intelligence (Systems)*

**C4ISR** *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*; Comando, Controlo, Comunicações, Computadores, Informações, Vigilância e Reconhecimento (C4IVR)

**C4IVR** Comando, Controlo, Comunicações, Computadores, Informações, Vigilância e Reconhecimento; *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR)*

**CCE** Comissão das Comunidades Europeias

**CDN** Curso de Defesa Nacional

**CDN2003** Curso de Defesa Nacional 2002-2003

**CDNA** Conferência de Directores Nacionais de Armamento; *Conference of National Armaments Directors (CNAD)*

**CE** Conhecimento Explícito

**CEDN** Conceito Estratégico de Defesa Nacional

**CEM** Chefe(s) de Estado Maior

**CEM** Conceito Estratégico Militar

**CERT** *Computer Emergency Response Team; Computer Security Incident Response Team(s) (CSIRT)*; Serviço(s) de Resposta a Incidentes de Segurança Informática (SRISI)

**Ciberespaço (Cyberspace)** Espaço onde um sistema nervoso composto por centenas de milhares (ou mesmo milhões) de computadores pessoais, servidores, *routers*, *switches*, cabos de fibra óptica e outras tecnologias de informação, permite o funcionamento de todas as infra-estruturas, de instituições públicas e privadas, baseadas em rede, através de comunicação electrónica e realidade virtual (ver Cibernética).

**Cibernética** Ciência que investiga os mecanismos de comunicação e de controlo nos organismos vivos e nas máquinas

**CNPCE** Conselho Nacional de Planeamento Civil de Emergência

**COMPUSEC** *Computer Security*; Segurança de Computadores

**COMSEC** *Communications Security*; Segurança de Comunicações

**COTEC Portugal** COTEC Portugal - Associação Empresarial para a Inovação

**CPE** Comissão(ões) de Planeamento de Emergência

**CSDN** Conselho Superior de Defesa Nacional

**CSIRT** *Computer Security Incident Response Team(s), Computer Emergency Response Team(s) (CERT)*; Serviço(s) de Resposta a Incidentes de Segurança Informática (SRISI)

**CSM** Conselho Superior Militar

**CT** Conhecimento Tácito

**DL** Decreto Lei

**DLPC** Dicionário de Língua Portuguesa Contemporânea

**DN** Defesa Nacional  
**DoD** *Department of Defense (USA)*; Departamento de Defesa dos EUA  
**DR** Diário da República  
**EM** Estado Maior  
**EME** Estado Maior do Exército  
**EMES** Estabelecimento(s) Militar(es) de Ensino Superior  
**EMEU** Estabelecimento(s) Militar(es) de Ensino Universitário  
**EMFAR** Estatuto dos Militares das Forças Armadas  
**EP** *European Parliament*; Parlamento Europeu (PE)  
**EU** *European Union*; União Europeia (UE)  
**EUA** Estados Unidos da América; *United States of America (USA)*  
**EW** *Electronic Warfare*; Guerra Electrónica (GE)

**Extranet** Uma rede utilizada como extensão da *intranet* de uma organização, através da mesma tecnologia utilizada pela *Internet (World Wide Web)*, implementada para facilitar a comunicação com fornecedores, clientes e colaboradores dessa organização. Pretende-se com uma *extranet* aumentar a rapidez e a eficiência das relações comerciais e outras actividades afins. O acesso a alguma informação não é público, é restringido a determinados utilizadores pré-definidos, com perfis associados de acesso e segurança conforme a necessidade da sua função.

**FFAA** Forças Armadas  
**GCR** Guerra Centrada em Rede; *Network-Centric Warfare (NCW)*  
**GE** Guerra Electrónica; *Electronic Warfare (EW)*  
**GI** Guerra de Informação; *Information Warfare (IW)*  
**GU** Grande(s) Unidade(s)  
**HF** *High Frequency*; HF é a banda de radiofrequências de 2 MHz a 30 MHz  
**I&D** Investigação e Desenvolvimento  
**IDN** *Instituto da Defesa Nacional*  
**IHEDN** Institut des Hautes Études de Defense Nationale

**In** Inimigo

**INFOSEC** *Information Security*; Segurança de Informação

**Internet** A maior REDE de computadores do mundo, também designada como “Rede das Redes”. A Internet teve a sua origem na década de 60, numa iniciativa da Agência de Projectos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos da América (DARPA), cuja arquitectura de rede designada por ARPANET, tinha como finalidade impedir a posse ou destruição do sistema norte-americano de comunicações pelos soviéticos. Em 2000 ligava mais de 300 milhões de utilizadores, enquanto em 1996 não ultrapassavam os 20 milhões (CASTELLS, 2002: 7-8).

**Intranet** Uma rede destinada a organizar e partilhar informação e a efectuar procedimentos de negócios por via digital no interior de uma organização. Uma *intranet* utiliza tecnologias e aplicações comuns às da *Internet (browsers, páginas Web, e-mail, mailing lists, newsgroup)*, mas que foi concebida primariamente para ser utilizada apenas por pessoas que trabalhem dentro da organização, constituindo-se como uma rede privativa de computadores.

**IW** *Information Warfare*; Guerra de Informação (GI)

**JIT** *Just-in-Time (Method)*; método de “zero stock”

**LDNFA** Lei de Defesa Nacional e das Forças Armadas  
**LPM** Lei(s) de Programação Militar  
**MDN** Ministério/Ministro da Defesa Nacional  
**NATO** *North Atlantic Treaty Organization*; Organização do Tratado do Atlântico Norte (OTAN)  
**NCO** *Network Centric Operations*; Operações Centradas em Rede (OCR)  
**NCW** *Network-Centric Warfare*; Guerra Centrada em Rede (GCR)  
**NID** Núcleo de Indústrias de Defesa da Associação Industrial Portuguesa (AIP)  
**NSS** *Networked Systems Survivability*  
**NT** Nossas Tropas  
**NTIC** Novas Tecnologias de Informação e Comunicação  
**NTSI** Novas Tecnologias e Sistemas de Informação  
**OCR** Operações Centradas em Rede; *Network Centric Operations* (NCO)  
**OODA** Observar, Orientar, Decidir, Agir  
**OOG** Objectivos Operacionais Gerais  
**OpInfo** Operações de Informação  
**OPSEC** Operações de Segurança; *Operations Security*  
**OTAN** Organização do Tratado do Atlântico Norte; *North Atlantic Treaty Organization* (NATO)  
**PC** *Personal Computer*; Computador Pessoal  
**PE** Parlamento Europeu; *European Parliament* (EP)  
**PEDN** Planeamento Estratégico de Defesa Nacional  
**PESC** Política Externa e de Segurança Comum (Europeia)  
**PIDDAC** Programa de Investimentos e Despesas do Desenvolvimento da Administração Central  
**RCTS** Rede Ciência, Tecnologia e Sociedade  
**REDIS** Rede Digital com Integração de Serviços (voz, dados, imagens e vídeo); *Integrated Services Digital Network* (ISDN)  
**RTP** *Research and Technology Projects*; Projecto(s) de Investigação e Tecnologia  
**SCIP** Society of Competitive Intelligence Professionals  
**SEI** Software Engineering Institute  
**SF** Sistema de Forças  
**SI** Sistema(s) de Informação  
**SICOM** Sistema Integrado de Comunicações Militares (das Forças Armadas)  
**SITEP** Sistema Integrado de Telecomunicações do Exército Português  
**SNCT** Sistema Nacional de Ciência e Tecnologia  
**SNI** Sistema Nacional de Inovação  
**SNPCE** Sistema Nacional de Planeamento Civil de Emergência  
**SRISI** Serviço(s) de Resposta a Incidentes de Segurança Informática; *Computer Security Incident Response Team(s)* (CSIRT); *Computer Emergency Response Team(s)* (CERT)  
**STANAG** *Standardisation Agreement* (NATO); Acordo de Normalização da NATO  
**SWOT** *Strenght, Weaknesses, Oportunities, Treats*; Forças e Fraquezas (envolvente interna), Oportunidades e Ameaças (envolvente externa). Uma análise SWOT é o estudo da envolvente interna e externa de uma organização, nomeadamente de uma sociedade

comercial (empresa).

**TERENA** Trans-European Research and Education Networking Association

**TI** Tecnologia(s) de Informação

**TIC** Tecnologias de Informação e Comunicação

**TLP** Telefones de Lisboa e Porto

**TSI** Tecnologias e Sistemas de Informação

**U/E/O** Unidade(s)/Estabelecimento(s)/Órgão(s)

**UE** União Europeia; *European Union (EU)*

**UEO** União Europeia Ocidental, ou União da Europa Ocidental; *Western European Union (WEU)*

**USA** *United States of America*; Estados Unidos da América (EUA)

**VHF/FM** *Very High Frequency/Frequency Modulate*; VHF é a banda de radiofrequências de 30 MHz a 300 MHz; FM é um tipo de Modulação de Frequência

**WEAG** *Western European Armaments Group*; Grupo de Armamento da Europa Ocidental (Groupe Armement de l'Europe Occidentale) (GAEO), composto pelos países europeus da NATO: Alemanha, Bélgica, Dinamarca, Espanha, França, Grécia, Holanda, Itália, Luxemburgo, Noruega, Portugal, Turquia e Reino Unido

**WEU** *Western European Union*; União da Europa Ocidental (UEO)

**WS** Workstation

**WWW** *World Wide Web*

\* Trabalho de investigação individual elaborado no âmbito do Curso de Defesa Nacional 2003, no Instituto de Defesa Nacional.

\*\* Coronel de Transmissões (Engenheiro). Comandante do Regimento de Transmissões.

1 O termo “custo da manufactura” considera-se equivalente a “custo do fabrico”.

2 Ver definições dos termos “Transformação” e “Modernização”, referidos anteriormente neste trabalho.

3 Cho et al. (2000: p. 2-4/Figure 2-3) (adaptado).

4 Bellinger (2000), Serrano e Fialho (2003: 53/Figura 3.3) (adaptado).

5 Report on Network Centric Warfare - Sense of the Report, Submitted to the Congress in partial fulfillment of Section 934 of the Defense Authorization Act for FY01 (Public Law 106-398), March 2001; Arthur L. Money, Assistant Secretary of Defense (C3I).

(www.c3i.osd.mil/NCW, acedido: 31Ago2003).

6 Network Centric Warfare, Department of Defense, Report to Congress, 27 July 2001. (www.c3i.osd.mil/NCW, acedido: 31Ago2003).

7 Citando o Relatório referido a 27Jul2001, relativo à fonte: Amir Hartman, John Sifonis, John Kador, Net Ready: Strategies for Success in the E-conomy, McGraw Hill, 2000, p. xvii-xviii.

8 Por exemplo, Operações de Manutenção de Paz” ou “Operações de Imposição de Paz”.

9 Citando o Relatório referido a 27Jul2001, relativo à fonte: VADM Arthur K. Cebrowski, USN, and John J. Garstka, “Network Centric Warfare: Its Origin and Future,”

Proceedings of the Naval Institute 124:1 (January 1998), p. 28-35.

10 ALBERTS, David, S., GARSTKA, John J., STEIN, Frederick, P. (1999). Network Centric Warfare - Developing and Leveraging Information Superiority. 2nd Edition (Revised) August 1999/Second printing February 2000. USA: CCRP Publication Series (DoD C4ISR Cooperative Research Program, [www.dodccrp.org](http://www.dodccrp.org)). ISBN: 1-57906-019-6.

11 Fonte: <http://www.dodccrp.org/publicat.htm>.

12 Embora o livro referido de Alberts et al. (1999), constitua a obra principal de referência de base teórica para o Relatório apresentado ao Congresso, o livro “Understanding Information Age Warfare” da mesma série de publicações CCRP, também de Alberts et al. (2001), encontra-se listado no sítio da Internet onde se encontram os documentos do respectivo Relatório ([www.c3i.osd.mil/NCW](http://www.c3i.osd.mil/NCW), acedido: 31Ago2003).

13 Esta designação é utilizada pelo CERT.PT ([www.cert.pt](http://www.cert.pt)), equivalente à terminologia inglesa “Computer Security Incident Response Teams” (CSIRT).

14 Fonte: <http://www.ti.terena.nl/teams/country.html> (TERENA - Trans-European Research and Education Networking Association).

15 Este “Handbook” foi publicado em Dezembro de 1998, e actualizado em Abril de 2003, e, está disponível na Internet em: <http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html> (West-Brown et al.: 2003).

16 “CERT - Computer Emergency Response Team”.

17 Fonte: [http://www.cert.org/annual\\_rpts/cert\\_rpt\\_02.html#incident](http://www.cert.org/annual_rpts/cert_rpt_02.html#incident).

18 A meta principal do Programa “Networked Systems Survivability” é assegurar que tecnologias adequadas e práticas de gestão de sistemas, sejam utilizadas, para resistir a ataques aos sistemas baseados em redes e limitar danos e prejuízos, e, assegurar a continuidade dos serviços críticos em vez de os ataques terem sucesso.

19 Fonte: <http://www.us-cert.gov/>.

20 Fonte: [http://www.cert.org/stats/cert\\_stats.html#vulnerabilities](http://www.cert.org/stats/cert_stats.html#vulnerabilities), (Last updated July 15, 2003).