A Guerra de Informação: Perspectivas de Segurança e Competitividade

Coronel
José António Henriques Dinis

1ª 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"*

Agradecimentos

Este é o culminar do Curso de Defesa Nacional 2002-2003 (CDN2003), no Instituto da Defesa Nacional (IDN), que muito me apraz referir, pelo imenso prazer que tive na sua frequência e da possibilidade de poder elaborar este trabalho neste contexto.

Na impossibilidade de me referir a todos que me prestaram algum do seu melhor esforço e facilidades, para que fosse possível a elaboração deste trabalho, apresento de forma impessoal o meu melhor apreço e devido reconhecimento a todas as pessoas que, de uma forma directa ou indirecta, contribuíram para a sua concretização. No entanto, cabe-me destacar algumas dessas pessoas que, em determinados momentos, constituíram factores-chave para a sua execução.

Ao Comando da Academia Militar, na pessoa do seu Comandante, Excelentíssimo Senhor Tenente-General Silvestre Salgueiro Porto, a minha mais elevada gratidão, pela possibilidade concedida para concorrer à frequência deste Curso de Defesa Nacional; e, a

Sua Excelência o General Chefe do Estado-Maior do Exército, o meu mais elevado reconhecimento por me ter sido atribuída a vaga institucional do Exército, em Lisboa.

Aos diversos Conferencistas, que ao longo do Curso se predispuseram compartilhar os seus saberes e experiências, a todos o meu reconhecimento pelo seu elevado valor e mérito, que me permitiu a aquisição de novos conhecimentos e mais-valias de nível superior, em diversas áreas do saber, de caracter multidisciplinar e multisectorial, no âmbito da Segurança e Defesa.

Aos diversos Assessores do IDN, que mais directamente estiveram ligados ao funcionamento deste Curso, o meu mais sentido apreço pelo seu trabalho e dedicação, que em muito contribuiu para o êxito deste CDN2003.

À Directora do Curso de Defesa Nacional 2002-2003, na pessoa da Excelentíssima Senhora Arquitecta Rita Martins Cabral, o meu sentido reconhecimento, por ter aceite a minha proposta para desenvolver este tema no Trabalho de Investigação Individual, o que me apraz registar com muito agrado, e pela sua disponibilidade contínua para acompanhar e apoiar o desenvolvimento das diversas actividades ao longo do Curso, o meu bem haja.

Ao Subdirector do Curso de Defesa Nacional 2002-2003, na pessoa do Excelentíssimo Senhor Comandante-de-Mar-e-Guerra Cervaes Rodrigues, os meus melhores agradecimentos pelo esforço inexcedível que dedicou ao funcionamento deste Curso, sendo ainda de destacar a sua permanente disponibilidade demonstrada.

Não posso também deixar de expressar, a minha melhor gratidão, ao conjunto de todos os Auditores deste Curso (de Lisboa e Porto), quer pela partilha dos seus conhecimentos e reflexões, acerca dos diversos assuntos analisados ao longo do curso, quer pelo convívio e pelas novas relações humanas criadas, em prol da Segurança e Defesa.

Não posso deixar de agradecer à minha família (à Isabel, à Marta e ao Nuno) o apoio e incentivo que me deu, e a compreensão por alguns sacrifícios que lhe fiz passar, inerentes a diversas situações da frequência deste Curso, e em particular, no processo de elaboração deste Trabalho.

Finalmente desejo expressar à Direcção do IDN, na pessoa do seu Director, Excelentíssimo Senhor Tenente-General Garcia Leandro, os melhores agradecimentos e o mais profundo reconhecimento, pela elevada qualidade na organização e funcionamento deste Curso, o que permitiu novos conhecimentos e perspectivas diversas sobre temas emergentes e abrangentes, e criou outros horizontes, no âmbito da Segurança e Defesa.

1. Introdução

1.1 Finalidade

Este estudo pretende analisar a utilização da "Informação" e do "Conhecimento"[1] (*Intelligence*), nos seus aspectos de natureza conflitual e competitiva, aplicada às actividades civis e militares, com incidência no âmbito da Segurança e Defesa, a desenvolver em três partes fundamentais.

Na primeira parte, aborda-se a caracterização dos diversos conceitos relacionados com o tema proposto, estabelecendo o "*state-of-art*" deste domínio, à luz da Sociedade da Informação e do Conhecimento - a Sociedade Centrada em Rede.

Na segunda parte, desenvolver-se-ão os aspectos relacionados com a utilização da "Informação" e do "Conhecimento", aplicados no âmbito do conceito de "Guerra de Informação", no sentido lato do termo, onde a "Segurança" e a "Competitividade" são temas abordados. Pretende-se estabelecer um paralelismo entre a sua aplicação a actividades civis e militares, baseado em estudos considerados referência nestes domínios científicos, e, em análises e reflexões a elaborar no âmbito deste trabalho.

Na terceira parte, faz-se uma reflexão integradora dos aspectos mais relevantes relacionados com o tema em estudo, sobre o seu "Futuro Prospectivo" e apresentam-se algumas "Conclusões" e propostas consideradas pertinentes, numa perspectiva de enquadramento no âmbito da Segurança e Defesa.

1.2 Enquadramento

A Sociedade da Informação[2] e do Conhecimento, que a humanidade tem vindo a desenvolver, traduz-se em substituir os "átomos" e as "moléculas" por "bits"[3] e "bytes"[4], através de uma "revolução digital", a que Alvin Toffler designou por "terceira vaga"[5]. O trabalho tem, cada vez mais, a "informação" como matéria prima, levando na actualidade que os equipamentos e os diversos produtos e serviços incorporem muito mais "conhecimento", e possam satisfazer novas necessidades sociais, económicas e culturais.

Na era da informação, em que se vive nos países mais desenvolvidos, a informação considera-se um "factor de produção", aliada ao "capital" e ao "trabalho" da era industrial. No contexto de uma economia e uma sociedade baseada na inovação e no conhecimento, a informação tem um valor vital[6].

A informação apresenta-se numa realidade, como fazendo parte das faces de uma mesma moeda. Numa das faces mostram-se as suas características de natureza competitiva, e na outra os aspectos que pode tomar quanto a aspectos de natureza conflitual, onde a segurança assume uma importância relevante.

A quantidade de "informação" e de "conhecimento" apresentam cada vez mais valor, no tipo de sociedade actual referida aos países mais desenvolvidos tecnologicamente. Nestes países, a "guerra de informação", analisada em sentido lato[7], afecta de uma forma geral todas as actividades centradas em rede[8], desde o nível individual ou doméstico até ao

nível transnacional, num contexto de internacionalização e globalização em que se vive.

A "guerra de informação" pode influenciar de uma forma geral toda a sociedade, e apresenta-se como uma nova forma de "guerra", que ultrapassa as próprias operações essencialmente militares, e, tem implicações de uma forma significativa e nível global, nas actividades das diversas áreas e sectores sócio-económicos, e muito em particular no âmbito da Segurança e Defesa.

Assim, considera-se que a "guerra de informação", em sentido lato, se enquadra, por um lado, em aspectos de segurança que devem preservar os interesses de cidadãos, estados e organizações nacionais e supranacionais de interesse público, contra acções que os pretendam prejudicar; e, por outro lado, no campo económico pode abranger alguns aspectos no âmbito da competitividade, de forma a levar o tecido empresarial a obter superioridade na utilização da informação e assim poder maximizar os respectivos factores críticos de sucesso das suas actividades.

O conceito de "Guerra de Informação" (*information warfare*) propriamente dita, numa análise em sentido restrito do termo, corresponde à utilização da "informação" que apresente aspectos de conflitualidade entre actores de uma sociedade. O uso da "informação" num contexto em que os aspectos legais e éticos são (devem ser) garantidos, para atingir objectivos de melhoria da competitividade empresarial, pode enquadrar-se em actividades de "Gestão do Conhecimento" (*Knowledge Management*), "Business Intelligence", "Competitive Intelligence"[9] ou em outros contextos ou conceitos, inerentes a aspectos da gestão organizacional. Neste caso, em particular na gestão empresarial, a melhoria da produtividade e do desempenho são em geral objectivos necessários alcançar, neste mundo cada vez mais competitivo.

A "Guerra de Informação", a "Gestão do Conhecimento", a "Business Intelligence" e a "Competitive Intelligence" são hoje assuntos emergentes que abrangem um amplo conjunto de processos e técnicas com características de multidisciplinaridade, que pela sua dimensão e importância merecem ser estudadas e carecem de reflexão, com especial incidência e merecida atenção e nas áreas relacionadas com a Segurança e Defesa.

No novo "Conceito Estratégico de Defesa Nacional" (CEDN)[10], considera-se que:
Embora (...) [o] novo ambiente estratégico tenha atenuado as ameaças[11] tradicionais de cariz militar, fez surgir factores de instabilidade traduzidos em novos riscos[12] e potenciais ameaças, de que os trágicos acontecimentos de 11 de Setembro de 2001 são o paradigma. (…) Com aquela acção, o terrorismo transnacional parece, assim, não considerar sequer limites éticos, nem de qualquer natureza, assumindo uma possibilidade de actuação à escala global, conjugando a violência tradicional, decorrentes de atentados a acções bombistas, com a utilização do ciberespaço[13] e de meios de destruição maciça.

Como a utilização do Ciberespaço está directamente relacionado com o meio onde se realizam actividades de Guerra de Informação, naturalmente que este novo tipo de guerra tem incidência particular no âmbito da Segurança e Defesa.

Em Portugal, começaram a dar-se já alguns passos estruturantes na divulgação e formação académica nestas áreas do conhecimento, através de algumas instituições de ensino superior. Como exemplo, refere-se a Academia Militar[14] que criou recentemente um Curso de Pós-Graduação em "Guerra de Informação/*Competitive Intelligence*"[15], que pela primeira vez é frequentado no ano lectivo de 2002-2003[16], por alunos civis e militares. Alguns dos Objectivos deste Curso de Pós-Graduação são: (1) "Criar e desenvolver competências avançadas na área emergente do acesso e utilização conflitual e competitiva da Informação, no contexto das actividades civis e militares"; (2) "Fomentar a reflexão sobre o binómio fluxo de informação - segurança, tendo em conta, nomeadamente, os requisitos de domínio, a complexidade das organizações e o papel do cidadão numa sociedade vincadamente interactiva"; (3) "Analisar metodologias para avaliação de ameaças, vulnerabilidades e riscos na Sociedade da Informação, Comunicação e Conhecimento"; (4) "Desenvolver actividades e iniciativas de forma a melhorar o intercâmbio entre a instituição militar e a sociedade civil, através da análise de assuntos emergentes de interesse mútuo, onde a Segurança e Defesa Nacional se apresentam como temas privilegiados de análise".[17]

As tecnologias associadas aos sistemas de informação tiveram um desenvolvimento sem precedentes durante as últimas décadas, e em particular no início deste Século XXI. Em especial, os países mais desenvolvidos introduziram na Sociedade uma dependência cada vez maior daqueles mesmos sistemas. Hoje, a necessidade de utilizar diversos sistemas de informação é uma realidade, por vezes por necessidade propriamente dita, mas noutras situações por necessidades criadas e até impostas. A privacidade e a segurança são outras necessidades e condições que devem estar associadas à utilização dos sistemas de informação. Assiste-se assim a importantes alterações que afectam a sociedade de forma global.

Os principais sistemas, em que cada cidadão, cada empresa, cada instituição, cada Estado, baseiam as suas actividades diárias, nomeadamente associadas às redes de telecomunicações e às redes de energia eléctrica, que são geridos por sistemas informáticos, e constituem actualmente as auto-estradas da informação e da comunicação, carecem de especial atenção e medidas de segurança e protecção adequadas.

As infra-estruturas que suportam os sistemas de segurança e defesa de um Estado, dependem em maior ou menor grau, das suas redes de computadores, aplicações informáticas e transmissão de dados, que devem permitir o seu funcionamento com um elevado grau de fiabilidade, segurança e confiança.

As novas formas de conflito que emergem no dia a dia, trazem novas necessidades no âmbito dos sectores da segurança e defesa, e fazem com que as tarefas de identificar os riscos e as ameaças (que potencialmente podem afectar os diversos sistemas informáticos) tenham hoje um caracter com uma dimensão e envolvimento muito superior ao passado.

Os sistemas informáticos e de telecomunicações, estão potencialmente sujeitos a ataques de informação, onde a sua protecção e segurança, em especial aqueles que permitem a segurança e defesa de um Estado, são actividades que se inserem no âmbito da guerra de informação.

Considera-se pois que a guerra de informação pertence ao marco das operações militares modernas e consequentemente à Segurança e Defesa do Estado, que deve estar preparado para reagir a este novo tipo de conflito.

2. A Sociedade Centrada Em Rede

2.1 Tempos de Mudança e Novas Perspectivas

Nas últimas décadas tem-se assistido a uma grande aceleração quanto aos ritmos das mudanças em diversos aspectos técnicos e tecnológicos, com repercussões a nível social, económico e cultural da sociedade actual.

No final do Sec. XX e no limiar do Sec. XXI, enquanto as novas tecnologias se desenvolveram de forma exponencial, os ciclos de vida dos produtos reduziram-se numa base logarítmica (Dinis, 2000: 332). Enquanto antes, as pessoas passavam e as tecnologias ficavam, mais recentemente (em particular nas duas últimas décadas), face à rapidez da evolução da ciência e tecnologia a nível mundial, as pessoas começaram a ficar e as tecnologias a passar por elas. Estes factos tornam-se muito mais evidentes e com mais incidência perante o aumento da esperança de vida das pessoas e da velocidade com que operam as respectivas mudanças tecnológicas.

Cada vez é mais difícil ou mesmo impossível, acompanhar os mais recentes progressos do conhecimento, com incidência particular em algumas áreas do saber, mais emergentes. Se, por um lado, as nossas capacidades têm limites, por outro lado, existe informação e conhecimento que passa a não ter utilidade ou perde importância, perante as necessidades do momento. Era normal dizer-se que o "saber não ocupa lugar", mas actualmente tem que se integrar uma nova realidade. Está-se perante um dilema, se por um lado se tem de *aprender-a-aprender* novos conhecimentos, por outro lado, deve também assumir-se, com frontalidade, que se tem de *aprender-a-esquecer* algumas coisas, que se considerem já obsoletas ou sem utilidade para a respectiva função que desempenham. Tem-se uma nova realidade, a qual não se pode ignorar e se deve estar predisposto para um processo de "aprendizagem ao longo da vida". A flexibilidade e a própria polivalência são hoje factores críticos para se assegurar um posto de trabalho, ou mudar para um outro melhor.

As teorias de Alvin Toffler, caracterizam a evolução da sociedade em três vagas[18]: (1) a agrícola, (2) a industrial e (3) a sociedade da informação[19], (Toffler, 1984, 1991, 1994, 1995). Cada uma destas vagas relaciona-se, de certa forma, com o respectivo tipo de

meio de produção que a caracteriza. Em cada época, o respectivo meio de produção emergente, constitui-se num dos factores facilitadores de forma a permitir atingir-se, em cada um desses períodos, os objectivos do "progresso" económico, social e mesmo cultural. Mesmo assim, constata-se que estes desideratos, não têm sido atingidos na sua plenitude, e, presume-se que no futuro também não serão conseguidos de forma uniforme e equitativa a nível internacional, mesmo tendo em consideração a realidade da globalização mundial, onde as desigualdades e desequilíbrios sócio-económicos são ainda evidentes em algumas das regiões do Globo.

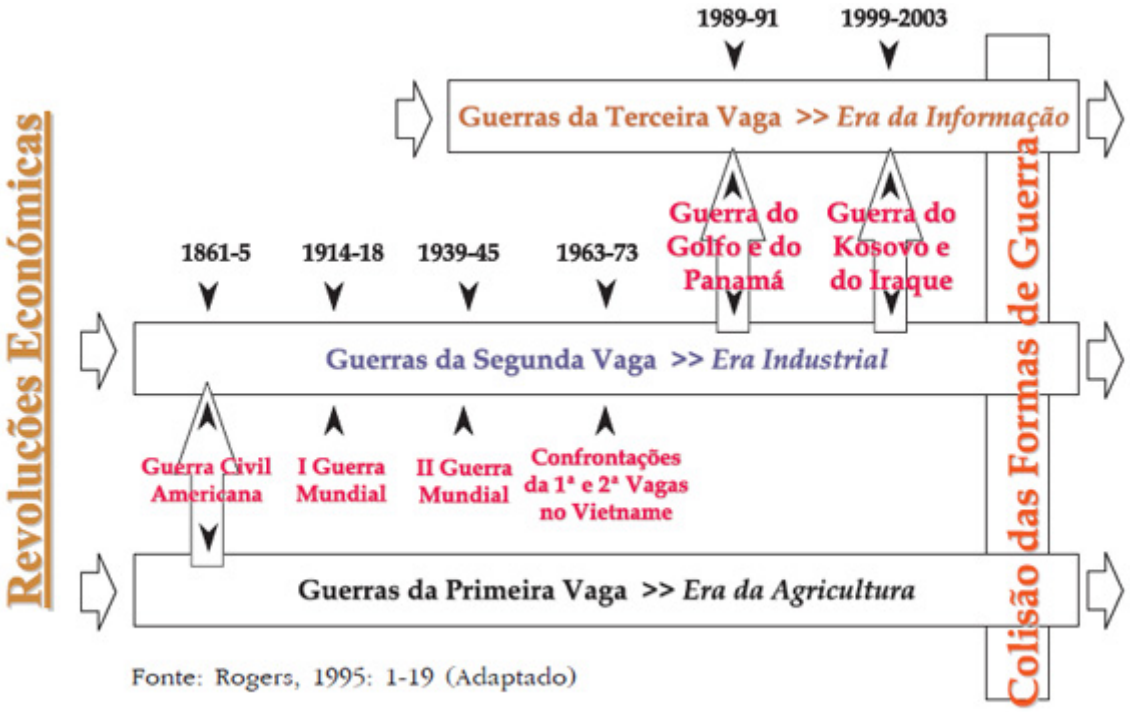

Figura 1 – As Três Vagas *versus* as Três Formas de Guerra[20]

A sociedade actual baseia-se em teorias económicas onde a economia está cada vez mais baseada em produtos intangíveis, onde a informação e o conhecimento são factores preponderantes. Assim, pode dizer-se que se vive numa economia baseada no conhecimento, onde as pessoas cada vez "pesam" mais, através do seu potencial humano.

O Conhecimento está intimamente relacionado com o Capital Intelectual. Segundo Setwart (1999: 14) "é composto por material intelectual (...) que pode ser usado para criar riqueza. É a inteligência colectiva". Stewart (1999: 228) refere ainda que "nas empresas em que a riqueza é constituída por capital intelectual, as redes, mais do que as hierarquias, representam o *design* organizacional adequado". Por outro lado, refere o mesmo autor (1999: 230) que "o maior desafio para o gestor da Idade da Informação é criar uma organização capaz de partilhar conhecimento". Embora as organizações necessitem, cada vez mais, de se organizarem em rede, isto não quer dizer que deixem

completamente de ter uma hierarquia instalada, que embora baseada em procedimentos diferentes dos tradicionais, considera-se dever existir na base de uma forte liderança.

Bill Gates, reconhecido como o "patrão" da MicroSoft, no seu livro "Negócios @ Velocidade do Pensamento, com um Sistema Nervoso Digital", refere que "o mundo digital está simultaneamente a obrigar as empresas a reagir à mudança e a fornecer-lhes os instrumentos que lhes permitem antecipar-se a essa mudança" (Gates, 1999: 363). E, por outro lado, "se nos limitarmos a reagir e deixarmos que a mudança nos passe ao lado, teremos dela uma percepção negativa. Se optarmos por uma abordagem activa, procurarmos compreender o futuro no presente e encararmos a mudança de modo optimista, a ideia do inesperado pode ser positiva e animadora" (Gates, 1999: 365).

Nas circunstâncias apresentadas, tem-se a necessidade de configurar uma posição mais proactiva e considerar que o Presente deve ser mais influenciado pelo Futuro do que pelo Passado, sem deixar de se pensar que o conhecimento anterior é também importante e deve ser considerado, mas apenas na medida da sua adequação e adaptação à realidade do momento.

2.2 Organizações Virtuais

No limiar do século XXI, perante o ambiente mundial da globalização e os desafios de uma nova economia digital baseada no conhecimento, necessita-se de novas perspectivas de solução para os problemas que se apresentam neste mundo. Com a "mudança em aceleração"[21], cada vez mais rápida, onde a incerteza tem grande acuidade, torna-se necessário flexibilizar as organizações e a forma como os seus colaboradores nelas participam.

Na União Europeia (UE) e em Portugal, em particular, nesta década têm de se levar a cabo transformações no sentido de consolidar um espaço económico mais dinâmico e competitivo, à luz das novas tecnologias da informação e do conhecimento, com capacidades de poder garantir um crescimento económico sustentável, onde se consigam mais e melhores empregos, sem deixar de atingir, em paralelo, uma maior coesão social.

O tipo de trabalho e as diversas formas de emprego ter-se-ão de desenvolver numa perspectiva cada vez mais centradas em rede, onde as tecnologias e respectivos sistemas de informação serão a respectiva base de sustentação. A coerência e os meios adequados ao seu desenvolvimento, consoante a diversidade das necessidades e oportunidades, serão de ter em consideração aos diversos níveis políticos, económicas, sociais e culturais.

O tipo de emprego actual tem de ser encarado com características bem diferentes do que foi no passado, e com certeza será no futuro próximo. Um emprego para toda a vida começa a ser utopia, tal como ser baseado exclusivamente nos conceitos clássicos dos tipos de Organizações que lhes deram suporte no passado recente. Há que desenvolver novas formas de trabalho, e, novos e diversos tipos de emprego, de acordo com as

necessidades económicas, sociais e mesmo culturais baseados em novas perspectivas e tipos de Organizações. As Tecnologias a seleccionar devem constituir um factor facilitador para melhorar as capacidades e condições de execução do Trabalho, nomeadamente aplicadas no âmbito do conceito de "Organização Virtual", onde a Gestão da Informação e do Conhecimento é algo muito importante a ter em consideração.

Hoje não é necessário ser-se um especialista ou um técnico de informática para se poder utilizar um computador. Com a massificação e a democratização das diversas tecnologias de informação e de comunicação, aparecem outras formas de estar na vida e de viver, e criam-se novas necessidades e alguns negócios para as satisfazer.

Diz-se que se vive actualmente na era da Internet, e até se tem uma juventude da geração Web (ou WWW), com novas facilidades, novos desafios, embora com outras dificuldades e mesmo contrariedades sociais e humanas, que urge identificar e encontrar uma eventual terapia se for necessário. As novas tecnologias não trouxeram apenas realidades positivas.

As pessoas utilizam as novas e mais modernas tecnologias, quase sem se darem por isso. O telemóvel teve uma aceitação exuberante pelo mercado. A nível pessoal e profissional o telemóvel é utilizado como uma ferramenta de apoio. Os doentes são submetidos, nas unidades de saúde, a diversos testes e análises onde as tecnologias são cada vez mais sofisticadas, permitindo-se diagnósticos e mesmo intervenções cirúrgicas a distância, através de técnicas e métodos de telemedicina. As crianças em vez dos brinquedos tradicionais, alguns antes fabricados pelos pais e amigos e outros até pelas próprias crianças, brincam hoje com produtos onde a tecnologia impera e absorve a sua atenção para novas realidades, incluindo o mundo da realidade virtual[22].

Alguns trabalhadores que antes tinham de deslocar-se diariamente da sua residência para o seu local de trabalho, nas instalações da sua empresa ou outro tipo de entidade empregadora, hoje podem trabalhar em casa, tirando partido das mais modernas Tecnologias de Informação e de Comunicação (TIC).

Em todos os domínios socio-económicos, o conceito de "lugar", relacionado com a localização física, está a ser substituído pelo conceito de "espaço", independente da localização física e do tempo. Assim, temos actualmente o conceito de "Marketspace"[23] em vez de "Marketplace"[24], onde o Ciberespaço[25] (*Cyberspace*) se apresenta como meio envolvente de suporte relevante, com novas oportunidades, mas também novas ameaças. Nos EUA considera-se que o funcionamento "saudável" do Ciberespaço é essencial para a sua economia e para a sua segurança nacional[26], por constituir um sistema nervoso como sistema de controlo do país, e muito em particular as suas infra-estruturas críticas nacionais[27].

O desenvolvimento do trabalho empresarial, seja em actividades de gestão de operações normaisou em gestão de projectos, deve enquadrar-se num ambiente de trabalho colaborativo e cooperativo. Com o apoio das Tecnologias de Informação e Comunicação,

podem executar-se tarefas inseridas em determinadas actividades de alguns Projectos, durante 24 horas sobre 24 horas, sem que haja necessidade de horas extraordinárias, pois uns trabalham num local enquanto outros dormem noutro ponto do globo. Esta situação pode enquadrar-se, por exemplo, em projectos de desenvolvimento de software, tendo equipas de trabalho situadas em regiões do globo terrestre que permitam um trabalho sequencial de forma colaborativo e cooperativo remoto. Face à localização geográfica adequada, as actividades podem executar-se durante o período diurno local, sem interrupções e com continuidade e troca de experiências entre as diversas equipas de trabalho[28]. Nestes casos, no trabalho executado através de equipas internacionais, permite-se trocar conhecimentos, verificar e melhorar soluções de outros elementos do grupo e aumentar as sinergias, sempre vantajosas para obter o melhor rácio custo/eficácia do trabalho desenvolvido, e melhorar os factores de competitividade, desde que sejam garantidas as medidas de segurança adequadas.

Um dos aspectos importantes de uma Rede de suporte a um Sistema de Informação (SI) "é poder fornecer informação na altura exacta, e não quando é possível" (Stewart, 1999: 231). Assim, o Trabalho centrado em Rede, em princípio, permitirá ter a informação certa para a pessoa que dela necessita num dado instante, independente do local e da hora, o que flexibiliza a sua utilização e melhora com certeza os resultados e os objectivos a alcançar daí decorrentes.

A utilização das tecnologias "Web" permitem desenvolver aplicações de rede, baseados em "sistemas abertos" (não-proprietários), a custos relativamente reduzidos e reconhecidos a nível quase global. Podem assim, criar-se e utilizar-se ambientes de trabalho em redes tipo "Intranet" e "Extranet", a nível privativo das organizações, ou a nível da "Internet", em regime aberto e público. Estas tecnologias permitem criar "equipas virtuais", constituídas por um Chefe ou Director e por determinados profissionais de acordo com as necessidades das suas valências técnicas e não com a localização física dos postos de trabalho. Esta situação permite utilizar o regime de trabalho a distância, por exemplo o denominado Teletrabalho. Toda esta envolvente, de trabalho centrado em rede, tem aspectos muito positivos, mas não é imune a preocupações de segurança, que permitam fazer um trabalho com toda a confiança nos respectivos resultados a obter.

O conceito de "Organização Virtual" foi introduzido no âmbito da discussão académica por Mowshowitz, na década de 80 do século XX (Franke, 2001: 44). A "realidade" do aparecimento da "Organização Virtual", deve-se por um lado às condições de mudança dos Mercado e das necessidades do Consumidor, e, por outro lado pelo desenvolvimento rápido das Novas Tecnologias de Informação e Comunicação (NTIC).

Mowshowitz citado por Sieber (1999: 11), define "organização virtual" como uma "empresa" (*enterprise*) que opera na base de uma gestão de tarefas organizadas virtualmente. Nesta definição considera-se que o significado de "empresa" não é sinónimo de companhia (*company*) ou negócio (*business*). Neste caso, "empresa" pode referir-se a uma unidade (de negócios) ou uma função no interior de uma companhia.

Assim, algumas das actividades no seio de uma organização podem ser processadas de forma virtual e outras através de um modo convencional.

Segundo Sieber (1998) define-se "organização virtual" como sendo "caracterizada primariamente como uma rede de organizações dispersas geograficamente e independentes, com uma sobreposição parcial da sua missão. No seio da rede, todos os parceiros proporcionam as suas competências próprias principais e a respectiva cooperação é baseada em relações semi-estáveis. Os produtos e os serviços fornecidos por uma organização virtual são dependentes da inovação e estão fortemente baseados no cliente". Nesta definição apresenta-se uma forma mais desenvolvida do conceito de "organização virtual".

Entretanto foram criados e apareceram outros termos, conceitos e definições, que se enquadram neste novo paradigma organizacional, inserido no Mundo digital. Assim, temos a "Companhia Virtual" (*Virtual Company*), a "Empresa Virtual" (*Virtual Enterprise*) e a "Fábrica Virtual" (*Virtual Factory*) (Franke, 2001: 44), entre outras, tal como o "Escritório Virtual" (*Virtual Office*). Todos estes conceitos identificam as TIC como uma base comum que permite a concretização deste novo paradigma emergente que é a "Organização Virtual". Estamos na era da Internet e é com naturalidade que se pode admitir também o conceito de "Virtual Web Organization"[29], apresentado por Franke (2001).

Tal como uma organização, qualquer que ela seja, nas teorias ditas clássicas, não se confina apenas à sua estrutura organizacional, também este novo conceito de organização não se deve reduzir à sua estrutura. Neste caso, haveria ainda o perigo de se poder confundir a sua estrutura com a respectiva plataforma tecnológica de sustentação e suporte.

A figura seguinte apresenta um modelo conceptual de enquadramento do Trabalho Virtual.

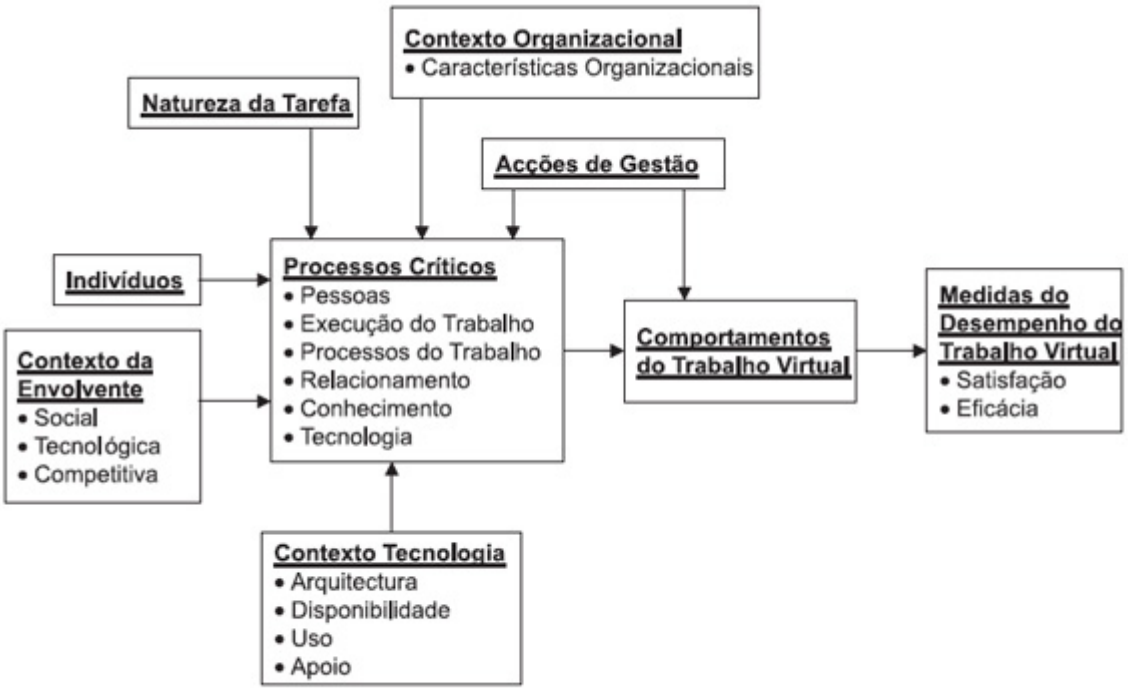

Figura 2 – Modelo Conceptual de Enquadramento do Trabalho Virtual[30]

Nos conceitos tradicionais, uma "vizinhança era simplesmente definida pela disponibilidade física e pela [respectiva] adjacência", e, assim "toda a nossa história está ligada ao espaço e ao local, à geometria e à geografia" (Negroponte, 1996: 250). No entanto, no mundo digital de hoje, e porque não no mundo virtual em que se vive, a realidade é bem diferente. O ciberespaço apresenta-se com novos conceitos de "vizinhança", "proximidade" e de "fronteira". Os princípios de espaço, local, geometria e geografia mantêm-se, mas as suas novas formas e representações são bem diferentes. Hoje qualquer computador ligado em rede, está tão próximo de qualquer outro (da mesma rede), independentemente da sua localização física geográfica. A "vizinhança" e a "fronteira" podem apresentar-se com sentidos opostos aos conceitos tradicionais. Dois computadores podem estar colocados sobre a mesma secretária, mas a distância funcional que os separa pode tender para o infinito, por estarem a funcionar em redes independentes que não permitam troca de informação digital. Por outro lado, dois computadores podem estar situados a uma distância de milhares de quilómetros e a respectiva "vizinhança" equivaler a uma "proximidade" quase nula, por fazerem parte de uma mesma rede de computadores, interligados por sistemas operativos e de telecomunicações interoperáveis. Assim é o "Mundo Virtual" dos nossos dias e das nossas vidas, onde "não devemos apenas interpretá-lo - a questão é mudá-lo".

Na estrutura de toda a sociedade existe uma "zona central", a que se pode designar por "centro". A pertença a uma determinada Sociedade, mais do que localizada num determinado território limitado a adaptar-se a um meio circundante, e afectado ou constituído por pessoas e outros seres localizados dentro das mesmas fronteiras geográficas, constitui-se pela relação com a referida "zona central". Esta zona central,

contudo, não é um fenómeno espacialmente localizado. A sua centralidade não tem nada a ver com uma dada geometria ou a própria geografia. O centro é um fenómeno na esfera dos valores e das crenças. É o centro da ordem de símbolos, de valores e de crenças que governam a sociedade a que se pertence. O centro é também um fenómeno na esfera da acção. É uma estrutura de actividades, de papéis e de pessoas dentro da rede de instituições. É nestes papéis que os valores e as crenças que são centrais se incorporam e se oferecem.

A procura de uma autonomia seria desta forma a diluição destes centros em cada indivíduo. Os valores não seriam função de uma crença central, de uma imagem de mundo corporificada numa instituição ou tradição predefinida. A extensão desta formulação implicaria a superação dos mecanismos de mercado como mecanismos básicos de interacção na sociedade. Tendo como pressuposto que apenas através da interacção na sociedade, é dado ao homem ultrapassar os obstáculos à razão, ou seja, obter o conhecimento da sua condição, um pressuposto mais forte tem que ser introduzido: a superação das desigualdades significativas entre os Homens é condição básica de uma livre interacção, que permita essa busca da autonomia. Mas a utilização da noção de que o percurso dos indivíduos em busca da sua liberdade, implica o crescimento do acesso dos indivíduos aos centros e à sua diluição na sociedade, e não implica apenas utopias, mas é antes um excelente instrumento para a análise do caminho até agora percorrido pelas instituições políticas.

Este é um ponto associado a alguma utopia, no entanto, numa reflexão repensada porque não poder levar-se a acreditar que as comunidades virtuais são os locais onde as desigualdades diminuem a sua relevância. O acesso dos indivíduos aos centros e a sua diluição pode ser compreendido como o acesso ao conhecimento, e a possibilidade da sua difusão e construção colectiva, mas também podem ficar muito mais vulneráveis em alguns aspectos, por viverem simultaneamente num “Mundo Virtual” e num “Mundo Real”, onde as respectivas interacções são substancialmente diferentes.

2.3 O Trabalho Centrado em rede

As sociedades capitalistas e comunistas, cuja terminologia pode deixar de ter sentido face aos mecanismos da globalização, operados no final do Sec. XX, estão a sofrer de certa forma, no limiar deste Sec. XXI, um impacto de mudanças que se manifestam a todos os níveis: políticos, socio-económicos, culturais, éticos e religiosos. Cada vez se revela mais a importância que os recursos intangíveis têm no dia a dia das pessoas e das organizações.

A sociedade da informação e do conhecimento está a mudar as economias, as culturas e as formas de viver e de estar na vida a nível individual, familiar, de grupo, das organizações, das instituições e dos próprios estados.

O conhecimento como um novo estágio da apresentação da informação, é um meio e um recurso que se pode considerar inesgotável. O mesmo conhecimento pode ser utilizado, em simultâneo, por muitas e diversas pessoas, ou mesmo máquinas, para se obter

resultados que criem riqueza e possam também produzir muito mais conhecimento.

A vida de hoje não é igual à de ontem e será, com certeza, muito diferente num futuro próximo, face às inúmeras e rápidas alterações que se manifestam no quotidiano.

As três vagas de Toffler tiveram durações bem diferentes. A Primeira Vaga - a revolução agrária - perdurou por um período de milhares de anos. A Segunda Vaga - a civilização industrial - não durou mais que cerca de uns trezentos anos. A Terceira Vaga - a sociedade da informação - terá uma duração muito mais curta e estima-se que não vá além de algumas décadas, permitindo a algumas pessoas verificar do seu impacto ainda durante o período da sua vida (Toffler, 1995: 27, 28). A mudança tem de ser encarada como um estado de espírito permanente. O que ontem era novo, hoje pode tornar-se obsoleto, e constata-se que, por vezes, nem sempre em prol de uma melhor qualidade de vida. Quem não conseguir acompanhar a evolução tecnológica, social, cultural e económica, pode tornar-se num elemento excluído da sociedade, por rejeição ou auto-exclusão. Há que se estar atento às mudanças e tentar a melhor adaptação às diversas circunstâncias do meio envolvente. A flexibilidade das mentalidades pode ser um factor importante, no entanto, nem sempre os mecanismos socio-económicos se adaptam às novas realidades e condições do trabalho e do emprego, o que seria desejável e um dos factores críticos de sucesso neste mundo em mutação constante.
Segundo palavras de Negroponte (1996: 240), "À medida que o mundo dos negócios se globaliza e a Internet cresce, começaremos a ver um local de trabalho digital sem descontinuidades". Assim, novas formas de trabalho são possíveis, através da circulação de bits num espaço sem fronteiras reais, sendo guardados e utilizados sem respeito pelas fronteiras geopolíticas. Neste contexto, os fusos horários terão um papel mais importância do que as zonas comerciais. Embora nestas circunstâncias, com a utilização da Internet se intensifique um tipo de comércio de bits[31], no entanto, é bom não subestimar o comércio de átomos[32], pois considera-se que necessariamente continuará a ser a base de sustentação da economia.

O trabalho centrado em rede, tira partido da utilização das Novas Tecnologias de Informação e Comunicação, para estabelecer comunicações em tempo real, tipo síncronas[33], e/ou em tempo diferido, tipo assíncronas[34], que permitem novas funcionalidades e facilidades. Com a utilização da mesma tecnologia pode permitir-se uma ou outra forma de comunicação, consoante a necessidade e a oportunidade do momento e da situação.

2.4 A Guerra Centrada em Rede

O conceito de "Guerra Centrada em Rede" (GCR) (*Network-Centric* Warfare)-(*NCW*) insere-se no contexto da sociedade centrada em rede e em particular no trabalho centrado em rede.

Segundo Alberts *et al.* (1999), pode fazer-se um paralelismo entre as operações militares e as actividades empresariais tirando partido do valor que as redes emprestam a cada

uma das situações. O modelo que Alberts *et al.* apresenta para "A Organização Militar como uma Empresa Centrada em Rede"[35], "relaciona os elementos básicos necessários para gerar poder de combate [comparado] com o modelo de Empresa Centrada em Rede"[36] onde "Tal como no sector comercial, tudo começa na info-estrutura" o que "permite a criação de uma consciencialização e conhecimento do espaço de batalha[37] compartilhado" (1999: 88-89)

Segundo o conceito de GCR apresentado por Pollock:
A GCR é baseada em adoptar uma nova forma de pensar e aplicá-la às operações militares. A GCR focaliza-se no poder de combate que pode ser gerado através da conexão ou rede efectiva da organização combatente. É caracterizada pela capacidade de ter forças dispersas geograficamente para criar um elevado nível de consciencialização do espaço de batalha compartilhado que pode ser explorado por via de auto-sincronismo ou auto-organização para levar a cabo tarefas urgentes no tempo e outras operações centradas em rede para realizar as intenções dos comandantes. A GCR não é apenas tecnologia, mas um conceito mais alargado acerca de uma resposta militar emergente face à era da informação. (...) A GCR é uma aplicação de sistemas de pensamento e de sistemas de engenharia, para as operações militares. Através de sinergia, o todo é maior do que a soma das partes. (...) A GCR permite uma alternativa ao combate da guerra tradicional, melhor, mais rápida e mais barata (2002: 258-259).

O valor e a eficácia de uma rede prova-se ser dependente do número de nós que a constituem. A "Lei de Metcalfe" descreve o valor do potencial de uma rede, na medida em que, se o número de nós aumentar linearmente o "valor" ou "eficácia" do seu potencial aumenta com o quadrado do número de nós da respectiva rede[38]. Assim, "o mecanismo para criar e explorar a superioridade de informação é uma função das dinâmicas de competição num domínio de concorrência". Logo, a dinâmica de algumas empresas[39], em diversos sectores da economia global, de utilizarem estratégias baseadas na utilização da informação, permite-lhes criar uma vantagem competitiva que lhe possibilita serem líderes ou concorrentes principais no domínio dos seus respectivos negócios (Alberts *et al.*, 1999: 32-35).

Com a implementação do conceito de guerra centrada em rede considera-se poder aumentar o ritmo das operações e reduzir a sua duração, ter menores riscos, menores custos e um aumento de eficácia do combate, podendo pensar-se em reduções drásticas do número de baixas (mortes) devido ao combate, podendo mesmo atingir o nível mínimo de "zero baixas"[40]. Se o princípio de "zero baixas" não for atingido, haverá com certeza um número muito mais reduzido, quando comparado com estimativas calculadas na base de estatísticas de algumas das últimas guerras. Naturalmente que se excluem as guerras, onde as armas ditas "inteligentes" foram já utilizadas em larga escala, protagonizadas pelos EUA e pela NATO. A Guerra do Golfo foi reconhecida como a primeira guerra da era da informação. Nesta guerra, segundo as palavras de Toffler, "Saddam gabava-se de que os aliados seriam feitos em pedaços, na «Mãe de Todas as Guerras»", mas contrariamente às previsões de mais de 30.000 mortos, afinal as baixas, do lado dos Aliados, não ultrapassaram a meia centena[41] (Toffler, 1994: 81; Dinis, 1997: 94).

Cada vez mais, uma baixa devido a uma operação militar, tem um factor muito negativo na opinião pública, tendo mesmo em consideração que as operações militares têm esse risco inerente à sua actividade[42]. Do ponto de vista político é reconhecida a importância do princípio de "zero baixas", em particular, nos países ocidentais. Assim, há a necessidade de criar condições, que levem a novas formas de fazer a Guerra (que não seja possível evitar e resolver por meios diplomáticos), que preservem a vida humana, a todo o custo e sem fanatismos[43]. As novas tecnologias associadas a novas doutrinas militares são factores potenciadores para concretizar tais desideratos, como o têm provado os últimos conflitos armados.

Figura 3 – Modelo de Soluções de Problemas (Tecnologia *vs* Doutrina)

A figura anterior apresenta uma metodologia com dois caminhos para resolver deficiências num sistema de apoio à concretização da missão. Nem sempre a solução dos problemas se pode encontrar em hipóteses tecnológicas, através da aquisição de material. Em primeiro lugar, deve interrogar-se se a solução pode encontrar-se através de mudanças na doutrina, nas tácticas, no treino e formação ou em alterações da própria organização. Assim, deve avaliar-se antes de tomar outras medidas, se com o mesmo material se pode fazer mais e melhor, apenas com a introdução de alterações noutros aspectos organizacionais.

Regressando ao conceito de GCR. Ainda segundo Alberts *et al.*, existem vários conceitos chave na sua definição, que merecem destaque e se descrevem a seguir.
O primeiro conceito chave é a utilização de uma força *geograficamente dispersa*. No passado, devido a limitações da nossa capacidade para se: 1) comunicar, 2) movimentar, e 3) projectar efeitos, as forças (e os seus elementos de apoio) necessitavam de ser co-localizadas, ou relativamente próximo do inimigo ou do alvo a defender. Como resultado, uma força geograficamente dispersa era relativamente fraca, e era incapaz de responder prontamente ou levar a efeito um ataque concentrado. Constrangimentos de localização têm influenciado uma capacidade de as forças se movimentarem com rapidez e ao mesmo tempo manterem a coesão e o apoio logístico. As tecnologias da Era da Informação têm permitido a liberdade de acção da fonte de poder de combate face à localização física dos meios ou entidades do espaço de batalha e poderão, no futuro, fazer com que as forças sejam mais eficazes "na movimentação". A eliminação de constrangimentos de geo-localização associados ao combate tem várias vantagens inerentes.
Permite-nos evoluir de um conceito baseado na concentração de forças para um de concentração de efeitos. (...)
O segundo conceito chave é o facto de se conseguir uma força *que possua conhecimento*[44]. Potenciado pelo conhecimento, derivado de uma consciencialização do espaço de batalha compartilhado e de um entendimento compartilhado das intenções do comandante, as nossas forças serão capazes de auto-sincronismo, de operarem com dissimulação, e de serem mais eficazes quando em operações desenvolvidas autonomamente. Uma força com conhecimento depende de uma alimentação adequada com informação oportuna e precisa, assim como de poder de processamento, de ferramentas e de especialistas necessários a fim de colocar a informação do espaço de batalha dentro de um contexto, e transformá-lo num espaço de batalha informado (que se conhece).
O terceiro conceito chave refere-se à existência de uma *ligação efectiva* entre as entidades do espaço de batalha. Isto significa que:

- entidades dispersas e distribuídas podem gerar sinergias;

- a responsabilidade e o trabalho podem ser reatribuídos dinamicamente por forma a se adaptarem à situação.
Uma ligação efectiva requer uma infra-estrutura de informação robusta e de elevado desempenho, ou *info-estrutura*, que forneça acesso a serviços de informação de elevada qualidade a todos os elementos do esforço de guerra. (Alberts *et al.*, 1999: 90-92)[45].

Tem sido difícil chegar a um consenso geral para arranjar uma designação para descrever a natureza da guerra na Era da Informação. Segundo Alberts *et al.* (1999), a terminologia de "Guerra Centrada em Rede", como definida anteriormente é a mais apropriada, visto que directa ou indirectamente reconhece as características essenciais da revolução, que se tem manifestado ao nível dos sectores empresariais, na economia do conhecimento e da globalização. Constata-se que a terminologia de "Guerra Centrada em Rede" (*Network Centric* Warfare)-(*NCW*) não consta no "Dicionário de Termos Militares e

Associados do Departamento de Defesa"[46], dos EUA, corrigido e publicado recentemente, com a "terminologia para uso geral por todas as componentes do Departamento de Defesa" dos EUA (Joint Pub 1-02, 2003: i). Assim, se se tiver como pressuposto que a respectiva doutrina militar se reflecte no documento oficial referido anteriormente, então este conceito ainda não é aceite oficialmente no âmbito da doutrina conjunta do Departamento de Defesa dos EUA[47].
No entanto, este assunto é um tema emergente[48], muito em particular nos EUA, onde existem já diversas fontes bibliográficas sobre o assunto, mas é também reflectido em outros fóruns internacionais[49].

Como já foi referido, o conceito de "Network-Centric Warfare" (*NCW*) (Guerra Centrada em Rede) ainda não constitui um elemento de doutrina do Departamento de Defesa dos EUA. No entanto, constata-se que este Departamento já apresentou relatórios circunstanciados ao Congresso dos EUA, a fim de que a Guerra Centrada em Rede seja aceite como uma realidade, e um mecanismo inserido na "Transformação do Departamento de Defesa".

Em Anexo B, apresenta-se alguma informação dos Relatórios sobre "Network-Centric Warfare", enviados ao Congresso dos EUA, pelo respectivo Departamento de Defesa.

3. A Guerra de Informação

3.1 Conceitos e Definições

Na era da Internet, da globalização e do trabalho centrado em rede, a actividade humana tende a inserir-se mais em "espaços" do que em "locais" físicos. Neste novo contexto, a Informação e o Conhecimento tendem a difundir-se e a dispersar-se num determinado "espaço", ainda que associado a "pessoas", "processos" e "tecnologias", o que necessariamente suscita um novo tipo de gestão adequada e específica - por exemplo, a Gestão do Conhecimento.

Considera-se importante e necessário, do ponto de vista conceptual, distinguir os conceitos associados aos termos "Sistema de Informações" e "Sistema de Informação". Assim, na nossa perspectiva, um "Sistema de Informações" processa informação classificada, sendo o seu acesso permitido apenas a pessoas "credenciadas" para o efeito, que face às funções que exercem também se deve cumprir rigorosamente a regra de "necessidade de conhecer". Por outro lado, um "Sistema de Informação", constitui a plataforma de processamento da informação, composto por determinadas "tecnologias de informação", um tipo de "gestão" e uma "organização" adequada[50] (Laudon, 2002), e, regra geral, refere-se a um Sistema que processa informação não-classificada, embora o seu acesso possa ser restringido a determinados utilizadores da informação, através de um perfil adequado, e correspondente à respectiva função numa determinada organização. Nestes termos, um "Sistema de Informações" necessita obviamente de um "Sistema de Informação" adequado, onde a segurança da informação deve ser um

requisito essencial.

Qualquer operação militar é caracterizada por um Comando bem definido, com Controlo das acções que se vão desenvolvendo, e, é indispensável um Sistema de Informações (*Intelligence*), apto a responder com informação adequada e oportuna sobre a situação, e de apoio aos seus diversos níveis - táctico, operacional e estratégico. Por outro lado, um Sistema de Comunicações fiável, de confiança e com segurança adequada, é outra componente imprescindível na composição de um Sistema Integrado de Comando, Controlo, Comunicações e Informações, que em gíria militar se designa pelo termo abreviado de "Sistema C3I". Um Sistema C3I, que também se designa por "Sistema C4I"[51] ou por outras siglas complementares[52], deve possibilitar o melhor desempenho do respectivo Sistema de Forças. Com base nos seus meios disponíveis, um Sistema C4I deve permitir a integração do Conhecimento[53] a todos os níveis do dispositivo da força, e em particular aos seus elementos fundamentais, de modo a conseguir-se alcançar o sucesso das operações.

Os conceitos de "Sistema de Informação" e de "Sistema Integrado C3I/C4I", apresentam-se nas figuras seguintes. Um Sistema C3I/C4I considera-se um tipo particular e específico de um "Sistema de Informação".

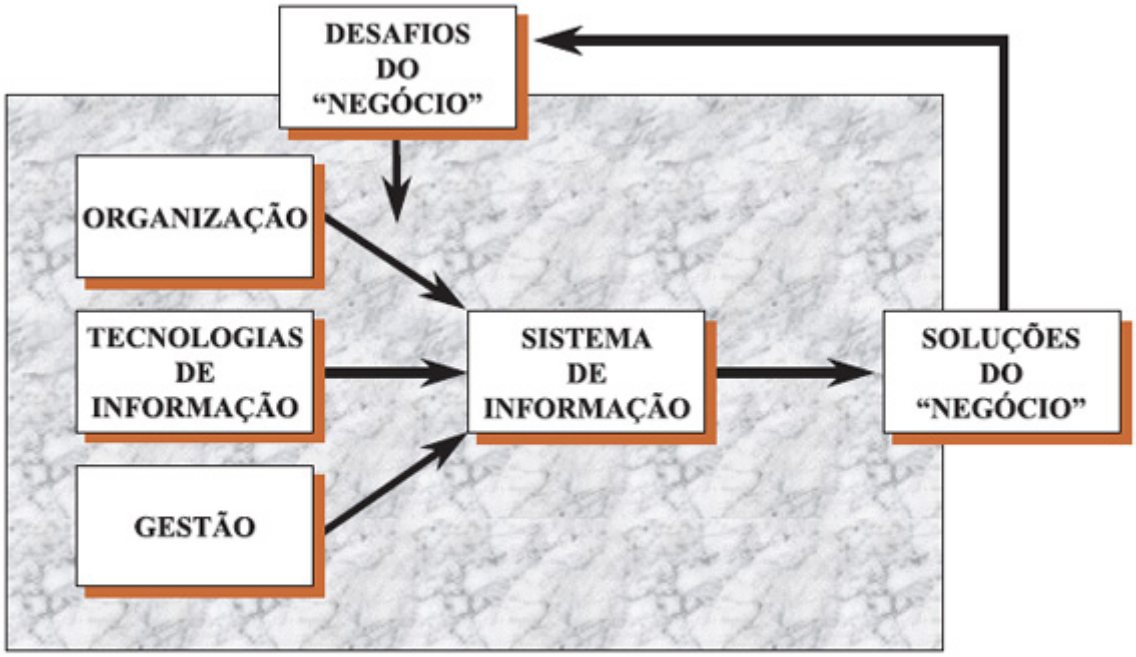

Figura 4 – Modelo de um Sistema de Informação[54]

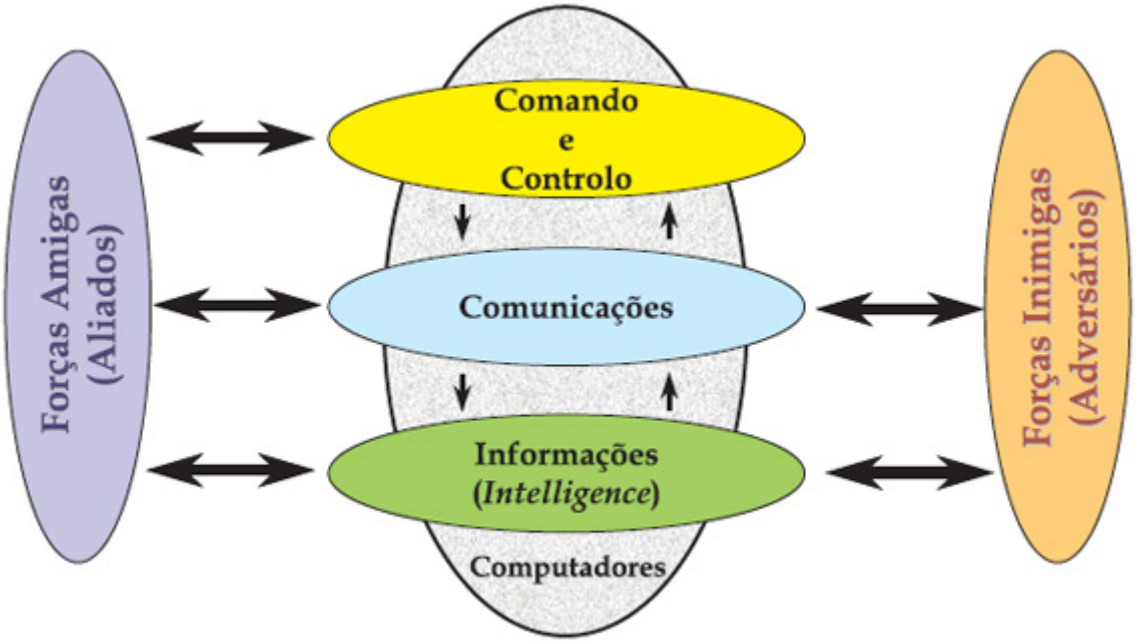

Figura 5 – Modelo de um Sistema Integrado C3I/C4I[55]

A concepção do modelo de um Sistema Integrado C3I/C4I[56], embora se aplique, em particular, no âmbito das Forças Armadas (FFAA), considera-se no entanto poder adaptar-se também às actividades e circunstâncias do tecido empresarial, onde a "Informação" se considera como um novo factor de produção.

Segundo Bill Gates, um "Sistema Nervoso Digital" compreende "os procedimentos digitais que permitem que uma empresa [organização] entenda e reaja ao seu ambiente, se aperceba dos desafios da concorrência e das necessidades dos clientes e organize respostas oportunas. Um sistema nervoso digital distingue-se de uma simples rede de computadores pelo rigor, imediatismo e abundância de informação que proporciona aos *knowledge workers* [trabalhadores do conhecimento] e pela compreensão e colaboração que a informação permite" (Gates, 1999: 393).

A Informação pode considerar-se como a seiva de uma árvore que corre por todas as suas partes, servindo-lhe de alimentação, o que permite a sua sobrevivência. Numa organização, a Informação constitui a alimentação do respectivo "Sistem@ Nervoso Digital", sem o qual uma organização fica desprotegida e com dificuldade para sobreviver e fazer face às mudanças operadas no seu meio envolvente.

A competitividade de uma empresa passa por tirar partido das forças e das oportunidades, no sentido de minimizar as suas fraquezas e reduzir as ameaças, de forma adequada e em tempo oportuno. Neste termos, qualquer empresa ou outro tipo de organização que pretenda ser competitivo no seu sector de actividade, tem necessidade de possuir um Sistema de Informação eficiente e eficaz, que permita implementar o que Bill Gates designa por um "Sistem@ Nervoso Digital". No entanto, um "Sistem@ Nervoso Digital" não se cria apenas com tecnologias, é também imperioso criar as condições de reacção à mudança, o que, em certa medida para por criar uma nova cultur@ organizacional.

As mudanças tecnológicas que tiveram lugar nas últimas décadas deram um lugar de destaque à utilização da informação no nosso dia a dia, quer a nível profissional e mesmo familiar. A informação passou a ser um elemento fundamental na nossa vida, e, deve pensar-se e não deixar de reflectir-se a sua importância, quanto aos diversos aspectos e sectores que influencia, e neste caso particular, no âmbito da Segurança e Defesa.

A amplitude e o valor da informação, hoje, numa sociedade globalizante, têm impacto aos seus diversos níveis - económico, político, cultural, social e também militar. Há que considerar e reflectir os aspectos conflituais da informação, e que se enquadram no tipo de Guerra de Informação.

Figura 6 – Sistem@ Nervoso Digital *versus* Competitividade

A definição de guerra de informação, com base na doutrina militar conjunta[57] americana, configura-se com "operações de informação conduzidas durante tempo de crise ou conflito para alcançar ou promover objectivos específicos sobre um adversário específico ou [vários] adversários"[58] (Joint Pub 3-13, 1998; Joint Pub 1-02, 2003). Considera-se que, se se fizer uma extensão deste conceito para além do âmbito essencialmente militar, com a sua aplicação a um nível mais alargado aos diversos sectores económicos, então toda esta doutrina se poderá expandir e aplicar ao tecido empresarial e a outras organizações, para além das militares, com as necessárias configurações circunstanciais, e respectivas adaptações a cada realidade particular.

A guerra de informação, como se refere na sua definição anterior, está associada a "operações de informação" que são "acções tomadas para afectar a informação e os sistemas de informação do adversário enquanto se defende a nossa informação e os nossos sistemas de informação". Neste contexto, falta definir o conceito de "sistema de informação" que, segundo a mesma doutrina americana, "é a infra-estrutura completa, organização, pessoal, e componentes que recolhem, processam, armazenam, transmitem, mostram, disseminam, e actuam na informação. O sistema de informação também inclui os processos baseados em informação" (Joint Pub 3-13, 1998; Joint Pub 1-02, 2003).

O novo "Conceito Estratégico de Defesa Nacional"[59] português, no âmbito do seu "Enquadramento internacional", identifica que "os fenómenos de desestruturação dos Estados e da globalização vieram contribuir para aumentar os riscos de (...) uso indevido de novas tecnologias", onde a utilização do Ciberespaço se inclui, o que está

directamente relacionado com actividades de Guerra de Informação, e, naturalmente com incidência no âmbito da Segurança e Defesa.

Este novo tipo de guerra apresenta-se num ambiente algo difuso, mas onde se revelam algumas características, nomeadamente: (1) "é grande a dificuldade de identificar o autor da agressão"; e, (2) "a evolução rápida do arsenal da guerra de informação desenrola-se em particular à velocidade da dos computadores" (IHEDN, 2002: 57).

A disseminação e a utilização cada vez mais maciça das Novas Tecnologias de Informação e Comunicação (NTIC) leva à sua explosão e vulgarização, dando uma supremacia ao uso da informação, com incidência particular, por parte dos que dominam estes meios tecnológicos.

A Guerra de Informação tem como elemento de base a informação, em que esta se apresenta com três aspectos complementares: (1) "Para a Informação" - sobre a exploração da informação disponível, proveniente de fontes quer sejam públicas ou secretas, de meios humanos ou meios técnicos; (2) "Contra a Informação" - consistindo na protecção da nossa informação e destruição da do adversário (inimigo), incluindo a contra-espionagem, a sabotagem de infra-estruturas ou de suportes da informação; e, (3) "Pela Informação" - no sentido de ganhar a batalha mediática, de agir psicologicamente, com necessidade de recurso à desinformação e à propaganda (IHEDN, 2002: 58-59).

3.2 Enquadramento e Âmbito

A Guerra de Informação enquadra-se no âmbito do "Espectro dos Conflitos", apresentando, no entanto, determinadas especificidades perante os tipos de guerra convencionais.

A Guerra de Informação está hoje muito associada à utilização do Ciberespaço, e diz respeito a questões internacionais numa sociedade caracterizada pela globalização, mas que afecta também o simples cidadão, na actual Sociedade da Informação, nas suas interacções efectuadas, quer a nível profissional quer a nível individual ou familiar. A informação para satisfazer às necessidades actuais, deve circular com toda a facilidade que permita o seu acesso e disponibilidade efectuar-se em tempo quase real. No entanto, as condições de acesso e de disponibilidade ficam em determinadas circunstâncias "prejudicadas" pelas necessárias e adequadas medidas de segurança e protecção a implementar.

A informação tem cada vez mais importância, não só ao nível estratégico, mas também operacional e táctico, no entanto, a informação por si só não tem um valor absoluto primordial, face aos dados que a constituem. É necessário que a informação se utilize em tempo oportuno e de forma coordenada, tirando partido do conhecimento que se pode retirar da mesma (informação), para se conseguir obter melhores tomadas de decisão.

A Guerra de Informação enquanto disputa, por vezes muito intensa, sobre o controlo e a

utilização dos sistemas de informação, tem um campo de análise alargado, e numa perspectiva de Segurança e Defesa, agrega-se à segurança dos cidadãos e das instituições, e mais estritamente associa-se às próprias operações militares.

Na figura seguinte apresenta-se um enquadramento global da Guerra de Informação, onde se verificam as componentes de natureza militar, mas também meios e interesses de natureza económicos, financeiros, comerciais, políticos e diplomáticos.

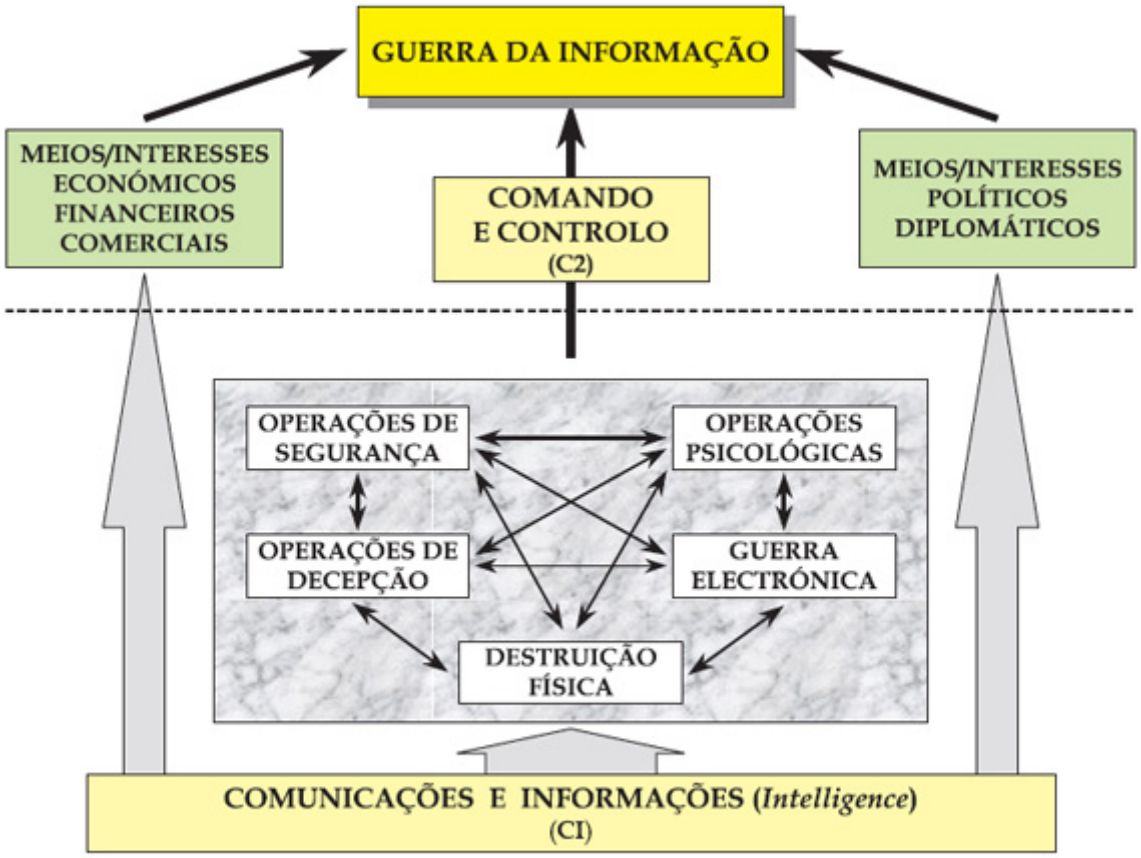

Figura 8 – Envolvente Global da "Guerra da Informação"[60]

Este novo tipo de guerra, tem características particulares quando comparada com os tipos de guerra convencional. É uma forma de guerra que existe desde o tempo de paz, e, é uma guerra que não se declara, embora este facto se considere extensivo, quase como uma norma, a outros conflitos modernos. Muito embora os Estados estejam a perder, na cena internacional, algumas das suas características próprias, em particular os Estados-Membros da União Europeia, nomeadamente em questões de soberania, mesmo assim pensa-se que deverão ter uma palavra a dizer, quanto aos limites da sua intervenção no âmbito das actividades da Guerra de Informação. Por outro lado, face às circunstâncias peculiares e à caracterização específica deste tipo de guerra, os interesses dos agentes privados, a segurança dos cidadãos e mesmo a segurança nacional, não se conseguirão

alcançar apenas com medidas tomadas no contorno e controlo das fronteiras geográficas dos respectivos Estados individualizados, ou mesmo das Organizações e/ou Tratados Internacionais, de âmbito regional, de que fazem parte. É necessário tomar medidas a nível global, com parcerias para a paz, contra o terrorismo e outras formas de ameaças, face aos diversos tipos e níveis de vulnerabilidades[61].

A envolvente da Guerra de Informação apresenta-se perante um dilema. Por um lado, a segurança da informação carece hoje de um espectro de medidas tomadas ao nível internacional, de forma coordenada e em cooperação com diversas instituições públicas[62] e privadas[63], mas por outro lado, cada uma destas próprias instituições (públicas e privadas) necessitam de preservar a sua informação, muitas vezes incompatível com a colaboração e cooperação externa. Assim, é necessário que cada instituição, e mesmo cada Estado, preserve a informação (crítica), que faz parte da sua sobrevivência, muito embora as parcerias sejam hoje necessárias, por vezes até imprescindíveis, e compatíveis com a competitividade, e mesmo com a segurança e defesa. A troca de informação tal como de conhecimento (*intelligence*) pode ser necessária para se garantir uma melhor segurança ou mais competitividade. Hoje, o segredo já não é sempre a alma do negócio.

Segundo o Instituto de Altos Estudos da Defesa Nacional Francesa, a Guerra de Informação pode apresentar diversos modos de acção, onde se realçam os seguintes:

- "A manipulação da informação" - com a finalidade de obrigar o adversário a tomar medidas da nossa vontade sem que se aperceba desse facto.

- "A destruição da informação" - que consiste em destruir a informação de que o adversário (inimigo) depende, por exemplo através de vírus informáticos, bombas lógicas, radiações electromagnéticas da guerra electrónica, etc..

- "A desorganização da informação" - com ataques concebidos para atingir um dado objectivo táctico, por exemplo o ataque a um sistema bancário de um país inimigo.

- "O ataque semântico" - em que o sistema integrado de Comando do inimigo parece funcionar normalmente, mas que está a ser controlado por um operador da guerra de informação. (IHEDN, 2002: 60-61).

A Guerra de Informação tem como objectivo levar a efeito actividades que permitam dominar a informação e impedir que potenciais adversários (inimigos) a possam utilizar, podendo mesmo usar-se a informação e empregar-se como a própria arma, para tirar partido da situação informacional associada.

Quanto maior for a sofisticação de um Sistema de Informação, mais alargado será o seu âmbito de aplicação, e maior a dependência da sua utilização. Nestes casos, então, maiores serão as respectivas vulnerabilidades e eventuais ameaças, visto que nestas condições passa a verificar-se uma maior remuneração do objectivo a alcançar, por parte

de potenciais adversários ou inimigos. As vulnerabilidades e eventuais ameaças impõem que se analisem respostas a dar aos riscos, que coloquem em perigo a respectiva situação. A protecção dos SI pode passar por investimentos, que devem avaliar-se quanto à sua relação custo/benefício esperada, sem deixar de equacionar as vulnerabilidades e os riscos associadas aos três elementos componentes do respectivo SI: (1) as Tecnologias de Informação (TI); (2) a Gestão; e, (3) a Organização. No âmbito da análise e gestão de riscos há que identificar os bens que possam apresentar vulnerabilidades e estejam sujeitos a ameaças, podendo optar-se por aceitar os riscos, proceder à sua transferência, ou adoptar contra-medidas, para os poder evitar ou minimizar.

Um SI deve constituir um conjunto de elementos coerentes e de articulação coordenada, de forma que as medidas de protecção a implementar sejam adequadas e permitam maximizar os resultados, face aos investimentos a utilizar[64].

Quando se analisa a protecção e segurança, no âmbito de um SI, deve considerar-se que a Guerra de Informação tem cada vez mais acuidade, e que cada SI constitui-se apenas numa ínfima componente do universo em que este se integra - o ciberespaço. Hoje, o principal problema da segurança e da respectiva protecção, insere-se numa realidade com contornos muito pouco definidos e inseridos no contexto de uma única Rede. A Internet é a base de sustentação de praticamente todos os SI, onde cada Organização, de uma forma ou de outra, necessita de ter uma porta de acesso ao respectivo mundo Web. Neste caso, cada Organização deve preparar-se para se confrontar com os aspectos negativos desta realidade, a fim de estar preparada para tirar partido das possibilidades que a Internet permite.

3.3 Operações de Guerra de Informação

Segundo a doutrina militar de referência, dos EUA, conforme se referiu anteriormente, a guerra de informação, está associada a “Operações de Informação” (OpInfo) que são “acções tomadas para afectar a informação e os sistemas de informação do adversário enquanto se defende a nossa informação e os nossos sistemas de informação” (Joint Pub 3-13, 1998; Joint Pub 1-02, 2003).

Os apoios das “Informações” (*Intelligence*)[65] e das “Comunicações” consideram-se essenciais e mesmo críticos para se poder executar OpInfo, quer de natureza ofensiva ou defensiva. Por outro lado, para se obterem os melhores resultados globais, as OpInfo “devem integrar-se com os outros tipos de operações (ar, terra, mar, espaço e especiais) e assim contribuir para atingir os objectivos nacionais e militares” (Joint Pub 3-13, 1998: vii), que porventura não se consigam alcançar com a exclusividade da Guerra de Informação.

As OpInfo ofensivas incluem “operações de segurança” (OPSEC)[66], “decepção militar”, “operações psicológicas”, “guerra electrónica” (GE)[67], “ataque/destruição física”, e “operações especiais de informação”, podendo também incluir “ataques a redes de computadores”.

As OpInfo defensivas são conduzidas através de "garantia da informação"[68], "segurança física", "segurança de operações", "contra-decepção", "contra-propaganda"[69], contra-informações, "guerra electrónica" (GE)[70] e "operações especiais de informação".

Diversos autores, citados numa compilação de Waltz (1998), apresentam vários modelos para caracterizar a guerra de informação, que se resumem a seguir.

Assim, nas palavras de Waltz, John Arquilla e David Ronfeld, "distinguem quatro categorias básicas de guerra de informação baseada no desenvolvimento das infra-estruturas de informação globais expandidas: (1)"guerra em rede" (*net warfare*); (2) "guerra política" (*political warfare*); (3) "guerra económica" (*economic warfare*); e (4) "guerra de comando e controlo" correspondente a "guerra no ciberespaço" (*cyber warfare*)[71] (Waltz, 1998: 16-17).

De acordo com Martin Libicki, propôe-se sete categorias de guerra de informação, que conforme Waltz apresenta são: (1) "guerra de comando e controlo" (*command and control warfare*); (2) "guerra baseada nas informações" (*intelligence-based warfare*); (3) "guerra electrónica" (*electronic warfare*); (4) "guerra psicológica" (*psychological warfare*); (5) "guerra dos hackers" (hacker warfare); (6) "guerra de informação económica" (economic information warfare); e "guerra do ciberespaço" (cyber warfare) (Waltz, 1998: 18).

Segundo Winn Schwartau, a terminologia da guerra de informação, nas palavras de Waltz, aplica-se a três domínios da sociedade: (1) pessoal; (2) corporativo (ou institucional); e (3) nacional (ou global), cujos tipos de agressões aos diversos níveis se apresentam na tabela seguinte.

Domínio de Conflito	Exemplos Representativos de Agressões de Informação
1. Nacional (Global, sector público)	– Guerra na rede – Guerra económica – Guerra política – Guerra de Comando e Controlo
2. Corporativo (institucional, sector privado)	– Espionagem, sabotagem, e fontes de informações (intelligence), de informação baseada em rede – Espionagem ou sabotagem de agentes internos [da organização] – Destruição de meios magnéticos – Roubo de Computador Portátil – Análise de exploração de empregados formadores e produtos concorrentes – Captura e análise de lixo do concorrente – Incêndio premeditado, outros ataques sem precisão nos sistemas de informação
3. Pessoal (sector pessoal)	– Fraude de comércio electrónico – Difamação na rede, "spoofing", envio de e-mails com preocupações, "spamming" – Escutas telefónicas e intercepção de telemóveis – Imitação de cartão bancário, roubo de cartão de crédito e cartão bancário – Telefonemas com preocupações, captura de PIN – Roubo de bases de dados e cartão de crédito – Destruição de computador

Tabela 1 – Domínios de Conflito e Exemplos de Agressões de Informação[72]

O conceito de GI apresenta três aspectos principais: (1) domínio da informação; (2) protecção da informação; e, (3) ataque à informação.

O objectivo central da GI é obter a superioridade de informação, mas esta condição é necessária para alcançar o sucesso em qualquer operação, no âmbito de quaisquer outros tipos de guerra. Neste caso, qualquer guerra moderna deve ser baseada na informação. A informação contribui para se ter uma consciência e conhecimento dominantes do "campo de batalha", através da sua aquisição, processamento, distribuição e exploração.

Uma força militar com controlo dominante da informação, marca a diferença perante os seus adversários, através de um melhor conhecimento que tem sobre o "espaço de batalha" em que opera.

O controlo da informação consegue-se através de operações defensivas (defesa) e operações ofensivas (ataque) de informação. Com operações defensivas de informação, permite-se obter garantia e confiança na respectiva informação, através de medidas de protecção, detecção e recuperação da própria informação. Através de operações

ofensivas (de ataque) de informação tem-se como objectivo atacar, com acções de contra-informação, para negar, perturbar ou explorar a possibilidade de utilização da informação, ou destruir a informação, do adversário.

Objectivo Info >>>>>>	**SUPERIORIDADE DE INFORMAÇÃO**									
Contribuição Da Informação	**Domínio sobre Consciência/Conhecimento do Espaço de Batalha**			**Domínio sobre Controlo da Informação**						
	Consciência/Conhecimento			Garantia/Confiança			Contra-informação			
Componentes das Operações de Informação	Exploração da Informação			Defesa da Informação			Ataque da Informação			
Funções	Adquirir	Explorar	Distribuir	Proteger	Detectar	Recuperar	Negar	Perturbar	Explorar	Destruir
	↑									↓
	Domínio			**Defesa**			**Ofensiva**			
	Guerra Baseada na Informação									
	GUERRA DE INFORMAÇÃO									

Figura 9 – Componentes e Meta das Operações da Guerra de Informação[73]

A guerra de informação apresenta três propriedades essenciais de segurança, para uma infra-estrutura de informação (info-estrutura), e os respectivos objectivos das contra-medidas para cada uma delas. A info-estrutura deve apresentar tais características e propriedades de segurança adequadas, para que se obvie aos efeitos dos objectivos da GI, e, assim se permita a "disponibilidade", a "integridade" e a "confidencialidade" da informação, aos órgãos que necessitam de a utilizar de forma eficiente e com eficácia.

Um computador, ou uma rede de computadores, considera-se segura se satisfizer aos três requisitos básicos anteriores: 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: (1) "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); (2) "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; e, (3) "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).[74]

Os ataques da GI pretendem perturbar o funcionamento de determinados órgãos e alterar o conteúdo da própria informação. Para cada objectivo de ataque de estar-se preparado para tomar contra-medidas específicas, cujo alvo permita dar uma resposta adequada. A resposta do alvo pode ser de natureza passiva (não detectável pelo adversário) - para detectar apenas que houve um ataque -, por exemplo, através de um sinal de alerta de um ataque; ou, de natureza activa (detectável pelo adversário) - para responder com medidas de segurança -, por exemplo, iniciar medidas de auditoria do sistema, iniciar medidas de protecção, ou recuperar e reconstituir a situação interferida com os ataques.

Figura 10 – Esquema Funcional da Guerra de Informação[75]

Como já se referiu anteriormente, a guerra de informação pode apresentar-se numa perspectiva de âmbito restrito militar, ou alargado à sociedade em geral, num sentido lato do termo. Com a aplicação do ciclo de Observar, Orientar, Decidir, Agir (OODA)[76], desenvolvido pelo Coronel John Boyd, da Força Aérea dos EUA, como modelo de Comando e Controlo, permite-se fazer uma análise do âmbito restrito e alargado da GI, conforme se mostra na figura seguinte.

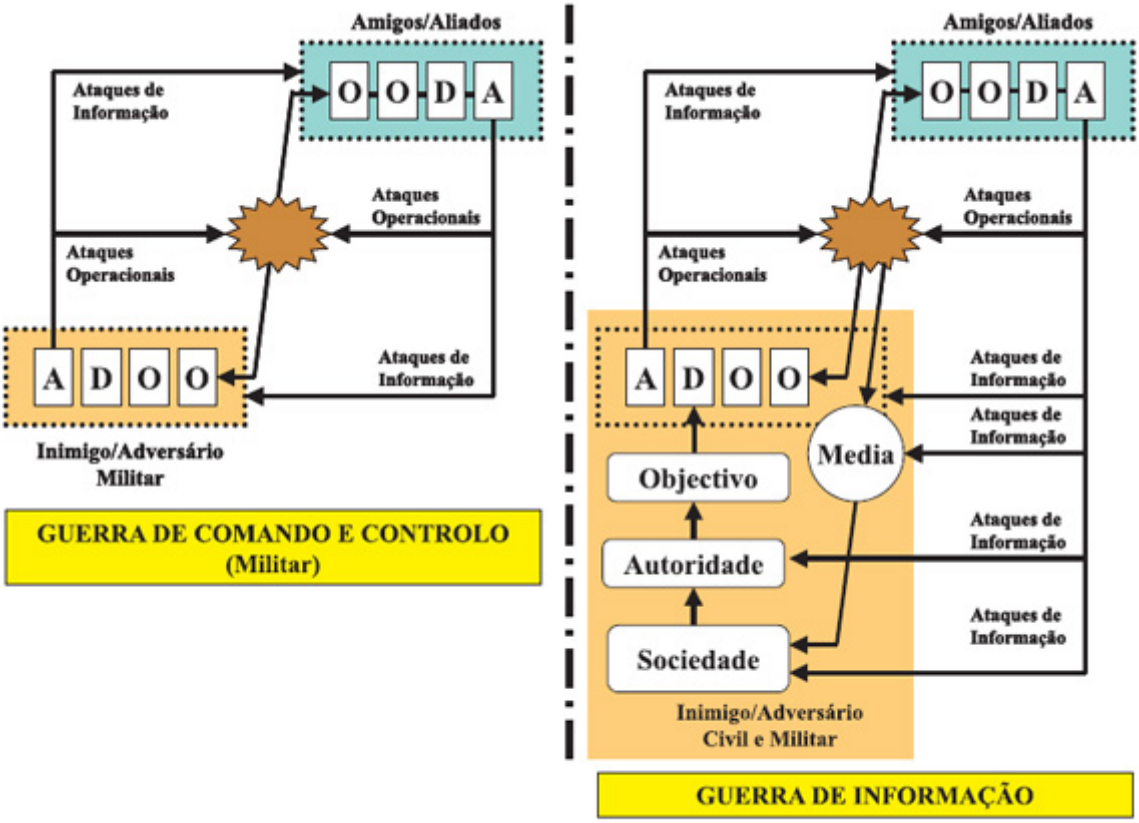

Figura 11 – Extensão do Espaço de Batalha da Guerra de Informação[77]

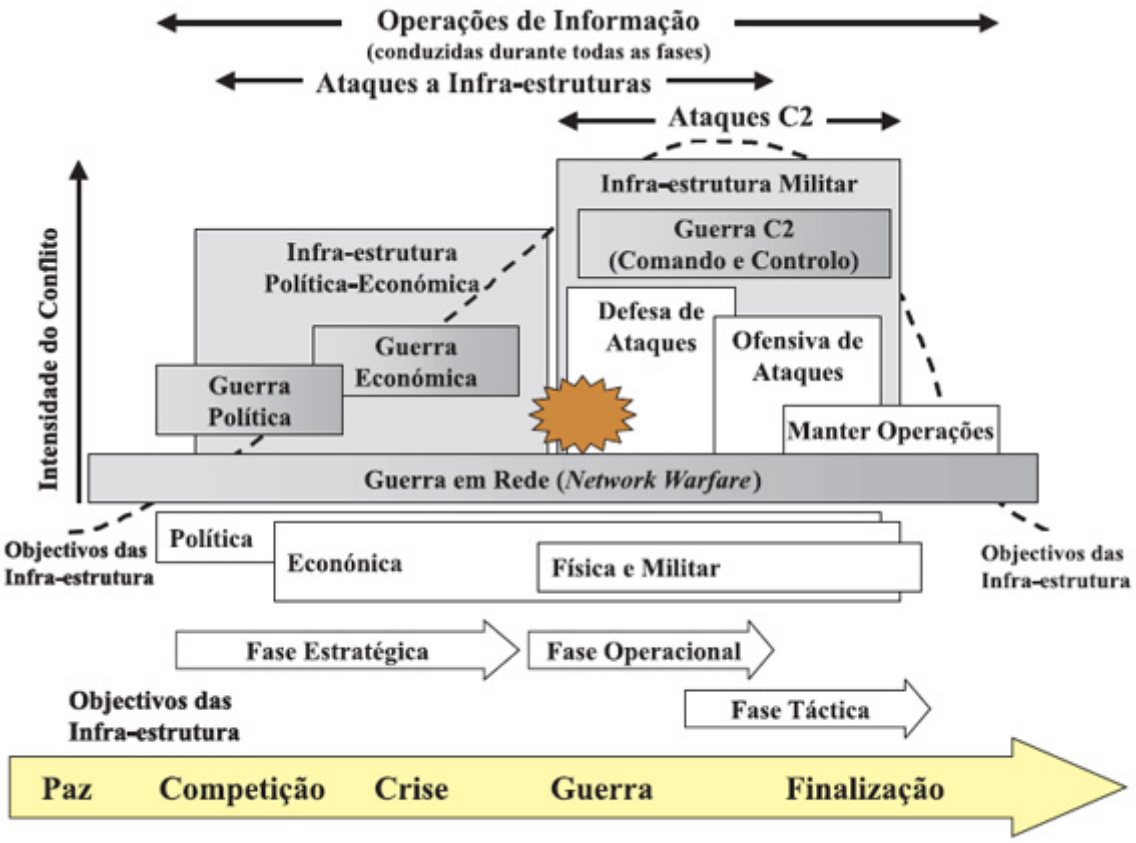

Figura 12 – Extensão das Actividades da Guerra de Informação[78]

Numa perspectiva operacional, no sentido do conceito alargado de guerra de informação esta "pode ser aplicada ao longo de todas as fases de operações" que abrangem a competição, o conflito até à guerra propriamente dita[79], conforme se representa na figura anterior.

É de tomar nota que as infra-estruturas políticas, económicas e físicas de muitos países, pertencem ao sector privado. A defesa dos bens que não sejam públicos (ou militares) considera-se ser uma responsabilidade conjunta e partilhada entre o sector público e o sector privado. É muito importante referir-se este facto, pois que "enquanto os militares protegem os bens do sector privado em tempo de guerra, isso não é sua responsabilidade durante o tempo de paz. Uma vez que os ataques à informação, ocorrem [também] em tempo de paz, os sectores público e privado devem desenvolver uma nova relação para executar as funções de indicação e aviso, segurança e resposta" (Waltz, 1998: 29). Este assunto, nos EUA, está bem explícito, num documento sobre a segurança do ciberespaço, publicado recentemente pela Casa Branca, em que "num esforço nacional" então o "governo federal convida a criação de parcerias entre o sector público e privado, e a sua participação, para aumentar a consciência da segurança do ciberespaço, formar pessoal, estimular as forças do mercado, melhorar a tecnologia, identificar a remediar vulnerabilidades, troca de informação, e planear operações de recuperação" (Bush, 2003b: xiii).

A guerra de informação é um tipo de " guerra" especial que:

- Se desenvolve num "espaço de batalha" quase virtual, em vez de ter lugar num "campo de batalha" de natureza físico. Neste caso, existe alguma dificuldade em definir os seus níveis e diversas categorias, correspondentes a outro tipo de guerra clássica, e inerentes aos respectivos conflitos - crime ou guerra, espionagem pública ou privada, ataques de nível táctico ou estratégico.

- Tem limites que não se distinguem entre os níveis de agressão e os tipos de ataques, provocados pelo anonimato na rede, que complicam as funções de alerta e a capacidade de distinguir os ataques internos dos estrangeiros.

- É considerada como uma ajuda potencial às ameaças transnacionais[80], proporcionando apoio para levar a cabo ataques físicos, por exemplo, com armas de destruição maciça. As operações de informação, espera-se que neste caso, sejam empregues para elevar o impacto psicológico do ataque físico, aumentar o pânico, e impedir a resposta dos serviços de emergência (Waltz, 1998: 30).

Na figura seguinte apresenta-se o relacionamento, ao longo do tempo, das diversas fases de desenvolvimentos de operações de informação, com a Garantia e Confiança de Informação, com as Operações de Informação Especiais, e com a própria Guerra de Informação, desde a situação de paz, passando pelo estado de crise e conflito, até ao regresso novamente à situação de paz.

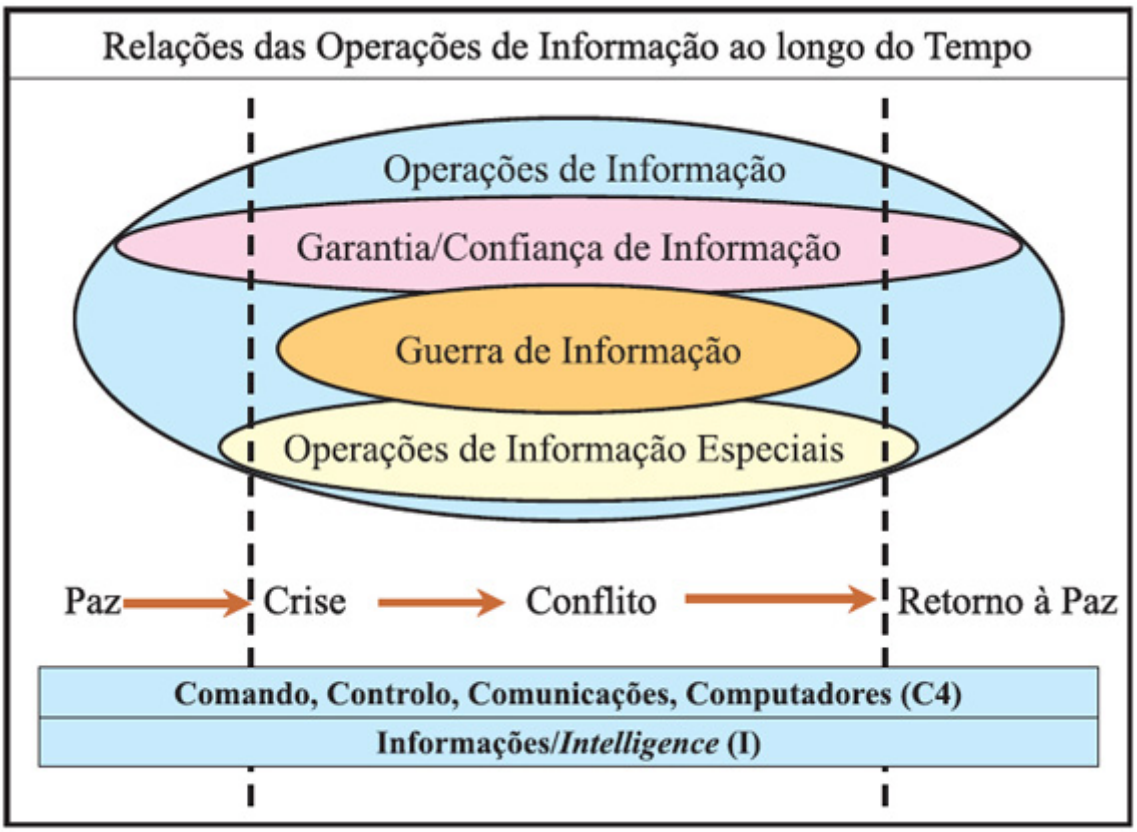

Figura 13 – Relações das Operações de Informação ao Longo do Tempo[81]

Será que em termos de Guerra de Informação se poderá pensar ou falar em tempo de paz? Uma questão difícil de responder, mas importante para reflectir.

3.4 Segurança

A economia e a segurança nacional a nível global, estão criticamente dependentes das tecnologias e das infra-estruturas de informação, que controlam determinadas infra-estruturas críticas, não só a nível dos sectores públicos como também dos privados. O controlo das redes de produção e distribuição de energia eléctrica, das bombas de *pipelines*, dos depósitos de produtos químicos, dos sistemas de radares e dos stocks de mercadorias, apenas para enumerar alguns exemplos, estão dependentes do bom funcionamentos dos sistemas electrónicos que os supervisionam.

Por outro lado, existem diversos "actores" que podem conduzir ataques contra as infra-estruturas de informação crítica e respectivos sistemas de informação, pondo assim em perigo o seu funcionamento, e em determinadas circunstâncias a prestação de serviços de primeira necessidade aos cidadãos, como, por exemplo, a distribuição de energia eléctrica e de água.

As ameaças à informação e aos sistemas de informação têm crescido e provenientes de diversas origens, podendo identificar-se como mais relevantes, as seguintes: (1)

utilizadores internos e autorizados (das organizações); (2) *hackers*; (3) espionagem industrial e económica; (4) países estrangeiros; (5) terroristas; (6) criminosos e crime organizado (Joint Pub 3-13: III-6/Figure III-4).

Face às ameaças e vulnerabilidades conhecidas e associadas à prestação de serviços à comunidade, por entidades públicas ou privadas, é necessário reunir as condições para garantir com eficiência e eficácia o funcionamento dos referidos sistemas de informação, baseados fundamentalmente em complexas redes de computadores, inseridas no ciberespaço, através de políticas e procedimentos de protecção adequados.

A Segurança de Informação, cujo acrónimo inglês utilizado é "INFOSEC"[82], consiste na "protecção e defesa de informação e sistemas de informação contra acessos não autorizados ou modificação de informação, quer em armazenamento, processamento ou trânsito e contra a negação do serviço a utilizadores autorizados". Para contrariar as ameaças a que a informação e os sistemas de informação estão arriscados, com a INFOSEC permite-se tomar "as medidas necessárias para detectar, documentar e contrariar tais ameaças" (Joint Pub 3-13: III-9).

As NTSI baseiam-se em meios multimedia[83] e hipermedia[84], que cada vez tiram mais partido das potencialidades conjuntas das tecnologias dos computadores e das comunicações[85]. Embora o termo "telemática" não seja aceite por todos os autores[86], é no entanto utilizada esta terminologia para significar a junção da utilização conjunta das tecnologias das telecomunicações (comunicações) e da informática[87] (computadores). Se por um lado, é cada vez mais difícil distingui-las ao nível da sua integração e aplicação nos sistemas que as utilizam, por outro lado, considera-se que cada uma destas disciplinas apresenta aspectos muito específicos, do ponto de vista técnico e científico, que é bom não confundir. No entanto, é uma realidade que ambas estão cada vez mais relacionadas, apresentando funções e aplicações complementares[88] imprescindíveis.

Face às especificidades técnicas, funcionais, organizacionais, de gestão e outras da INFOSEC, esta é composta por duas componentes, a Segurança de Computadores (COMPUSEC)[89] e a Segurança de Comunicações (COMSEC)[90], tendo cada um destes tipos de segurança de informação a respectiva definição seguinte:
A COMPUSEC envolve as medidas e controlos para assegurar confidencialidade, integridade e disponibilidade da informação processada e armazenada por um computador. Estas medidas incluem políticas, procedimentos, e as ferramentas de hardware e software necessárias para proteger e defender os sistemas de computadores e a informação (Joint Pub 3-13, 1998).
A COMSEC consiste no resultado de todas as medidas designadas para negar informação de valor a pessoas não autorizadas que possa ser derivada da posse e estudo de telecomunicações, ou para desencaminhar pessoas não autorizadas na sua interpretação dos resultados de tal posse e estudo. A COMSEC inclui a segurança criptográfica, a segurança de transmissão, a segurança de emissão, e a segurança física dos materiais e informação da segurança das comunicações (Joint Pub 3-13, 1998; Joint Pub 1-02, 2003).

A segurança de redes, nomeadamente em redes de computadores, consiste em tomar medidas a seis níveis: (1) administrador da rede; (2) segurança física; (3) monitorização; (4) software; (5) ferramentas de segurança; e, (6) auditorias de segurança.

Existe um aumento dos riscos na sociedade actual, a todos os níveis, face às vulnerabilidades inerentes aos diversos sistemas de informação que necessariamente se utilizam. Por este facto e por existirem ameaças, e, não se conseguirem abordagens, completamente eficientes e eficazes, de segurança, que consigam proteger os diversos sistemas distribuídos de grandes dimensões, então, existe uma necessidade premente para desenvolver sistemas que estejam preparados para sobreviver, limitar os perigos, recuperar, e funcionar mesmo sujeitos a ataques que não se podem evitar completamente.

No âmbito do ciberespaço, a gestão das ameaças e a redução das vulnerabilidades, é um desafio particularmente complexo face à quantidade e extensão dos seus diferentes tipos de utilizadores. A segurança do ciberespaço implica uma acção em múltiplos níveis através de diversos actores, face à existência de centenas de milhões de equipamentos interligados numa rede das redes. Neste sentido, identificou-se nos EUA que as ameaças e vulnerabilidades no âmbito da Segurança do Ciberespaço, se apresentam como um problema com os cinco níveis de actuação seguintes (Bush, 2003b):

- Nível 1: Utilizador Doméstico;

- Nível 2: Grandes Empresas;

- Nível 3: Sectores e Infra-Estruturas Críticas;

- Nível 4: Consequências e Vulnerabilidades Nacionais;

- Nível 5: Global.

Face ao exposto, nos EUA encara-se o problema da Segurança do Ciberespaço como um assunto de Estratégia de Segurança Nacional, estratificado nos cinco níveis de actuação anteriores, para uma melhor identificação dos problemas específicos e das respectivos prioridades e neste contexto, definiram-se cinco prioridades (Bush, 2003b):

- Prioridade I: Um Sistema de Resposta à Segurança Nacional do Ciberespaço;

- Prioridade II: Um Programa de Redução de Ameaças e Vulnerabilidades da Segurança Nacional do Ciberespaço;

- Prioridade III: Um Programa de Consciencialização e Formação de Segurança Nacional do Ciberespaço;

- Prioridade IV: Segurança Governamental do Ciberespaço;

- Prioridade V: Cooperação de Segurança Nacional e Segurança Internacional do Ciberespaço.

Em Portugal, o "Sistema Nacional de Planeamento Civil de Emergência" (SNPCE)[91], compreende:

- O Conselho Nacional de Planeamento Civil de Emergência (CNPCE); e,

- As Comissões de Planeamento de Emergência (CPE).

A legislação mais recente sobre o SNPCE[92], identifica "a necessidade reforçada e imperiosa de dar resposta às novas ameaças, ainda mais patentes após os atentados de 11 de Setembro de 2002, através do reforço da capacidade e eficácia do sistema de planeamento civil de emergência nas áreas do ambiente e do ciberespaço". Neste sentido, foram criadas duas Comissões de Planeamento de Emergência específicas do ambiente e do ciberespaço[93]. Reconhece-se que os Estados, indivíduos e empresas sentem diariamente os efeitos, benéficos ou não, da revolução da informação e como consequência a necessidade de segurança na Internet.

Constata-se que a regulamentação das "Comissões de Planeamento de Emergência" sectoriais, conforme previsto na legislação da sua criação, não foi até à data objecto de decreto regulamentar.

A legislação sobre o SNPCE está em fase final de revisão. Em princípio, será publicado, em breve, novo enquadramento jurídico, sobre esta matéria, de forma a actualizar o seu conteúdo e os respectivos mecanismos de funcionamento.

Nas condições anteriores, sabe-se da intenção de propor a criação de uma "Comissão de Planeamento de Emergência das Comunicações e do Ciberespaço", que por hipótese virá a reunir as funções das duas CPE congéneres anteriores. Neste caso, se isto acontecer, considera-se um retrocesso, relativo ao conteúdo do Decreto-Lei n.º 128/2002, de 11 de Maio, que actualizou o Decreto-Lei n.º 153/91, de 23 de Abril (onze anos depois), que pela importância actualmente reconhecida às actividades do ambiente e do ciberespaço, se criaram duas Comissões de Planeamento de Emergência, específicas, em cada um destes assuntos, dando-se particular relevo ao ciberespaço neste caso.

Naturalmente que as "Comunicações" e o "Ciberespaço" estão intimamente relacionadas, mas do ponto de vista de segurança, apresentam-se com aspectos relativamente diferenciados, ao ponto de se identificar a Segurança de Computadores (COMPUSEC) e a Segurança de Comunicações (COMSEC) como dois conceitos distintos, já referidos anteriormente neste documento.

Assim, sob o ponto de vista conceptual, e perante a importância que o Ciberespaço tem vindo a ganhar actualmente, parecia-nos mais adequado manter as duas CPE separadas. Esta opção justifica-se pela dimensão, especificidade e importância de cada uma em

particular, e porque as atribuições do CNPCE permitem a coordenação das diversas CPE. Face à dimensão e à importância que a utilização do Ciberespaço tem actualmente, a Casa Branca dos EUA publicou em Fevereiro de 2003 um documento sobre a "Estratégia Nacional para a Segurança do Ciberespaço"[94], considerando-se este mais um factor que justifica a opção de manter o Ciberespaço numa CPE específica.

A resposta a incidentes de segurança na Internet é a missão central de um Serviço de Resposta a Incidentes de Segurança Informática (SRISI), designado tradicionalmente, a nível internacional, pela sigla "CERT"[95], e mais recentemente associada à abreviatura "CSIRT"[96].

Em Portugal existe o CERT.PT (que substituiu o FCCN CERT), cuja missão é:
Prestar apoio a utilizadores de sistemas informáticos na resolução de incidentes de segurança, aconselhando procedimentos, analisando artefactos e coordenando acções com as entidades envolvidas.
Reunir e disseminar um conjunto de informação autoritativa sobre vulnerabilidades e recomendações referentes a potenciais riscos de segurança e actividades maliciosas em curso.
Receber, de fontes acreditadas, informação relacionada com novos incidentes de segurança, e actuar no sentido de minimizar danos a nível Nacional.
O âmbito de actuação do CERT.PT é comunidade utilizadora da RCTS - Rede Ciência, Tecnologia e Sociedade. Se o seu caso não se enquadra nos pressupostos atrás descritos, por favor consulte a lista de CERTs disponíveis na Internet, como por exemplo no FIRST ou TI-CSIRT.[97]

Os serviços prestados pelo CERT.PT são:
Resposta a incidentes de segurança: é a missão central de um CERT. Este serviço é composto pelas actividades de triagem, análise e resposta sobre cada incidente particular. A análise de uma solicitação determina a existência ou não de um incidente de segurança, a sua extensão e impacto, e caso seja possível, a vulnerabilidade explorada. Face a este apuramento inicial, é efectuado um aconselhamento das medidas correctivas a tomar em cada caso particular. Em caso de necessidade, o CERT.PT efectuará a coordenação do incidente com outros CERT.
Coordenação de incidentes de segurança: No caso de um incidente particular envolver simultaneamente entidades ou indivíduos dentro do âmbito de actuação do CERT.PT e fora deste, é efectuado um serviço de coordenação entre CERTs.
Classificação e disseminação de recomendações e alertas: Este serviço implica a recolha, de fontes bem conhecidas, de informação relativa a recomendações e alertas de vulnerabilidades; a sua classificação relativamente ao grau de risco e extensão e posterior disseminação para utilizadores interessados. Para alertas considerados muito críticos, como por exemplo um vírus com elevado grau de propagação, à parte dos canais de divulgação electrónica, é elaborado um *press-release* para difusão pelos media.
Tradução de recomendações e alertas: Para recomendações e alertas considerados críticos ou relativos a plataformas muito usadas, onde o risco de exploração de uma vulnerabilidade é elevado, é publicada e difundida uma versão em português dos

mesmos.[98]

Em Anexo C, apresenta-se uma lista de CSIRT/CERT europeus, onde consta o respectivo CERT de Portugal (CERT.PT).

Em Anexo D, referem-se as actividades e funções de dois Serviços de Resposta a Incidentes de Segurança Informática (CERT) dos EUA, relacionados com a segurança do Ciberespaço, incluindo-se algumas estatísticas publicadas pelo "CERT/Coordination Center" (CERT/CC)[99].

Em Anexo E, apresentam-se alguns termos e conceitos sobre a Segurança na Internet.

3.5 Competitividade

As actividades sociais, económicas, políticas, culturais e em particular as da segurança e defesa, têm a informação como base de apoio à maior parte das tomadas de decisão, aos diversos níveis de responsabilidade. A estrutura informacional baseia-se em sistemas de informação que não se devem resumir às tecnologias de informação, que muito embora constituam uma das suas componentes principais, no entanto, a gestão e a respectiva organização em que se integram são também fundamentais. Um SI não é apenas o conjunto das respectivas Tecnologias de Informação (TI) que o compõem, como muitas vezes é considerado, e de forma errada, talvez por falta de uma percepção holística do assunto, por parte de alguns responsáveis, e, por vezes, talvez mesmo por parte dos próprios gestores de topo. Hoje considera-se necessário, até por razões do conteúdo anterior, que os gestores possam ter uma formação abrangente em diversas áreas do saber, cujos conhecimentos são fundamentais para exercerem uma gestão empresarial integrada.

Segundo Daniels (1997: 210-211), "Os gestores com aptidão para compreender tanto a orientação da empresa como as potencialidades tecnológicas têm muito valor. Peter Keen inventou a teoria do gestor «híbrido»[100] para se referir a alguém que tenta combinar as duas competências".
De acordo com a perspectiva do Dr. John Spackman, director de *Computing and Information Services* da *British Telecom*, refere-se na obra de Daniels (1997: 67) que:
Tanto os gestores das empresas como os das tecnologias devem ser gestores híbridos, capazes de compreender a área dos outros. (…) Somente os gestores dotados de capacidades híbridas serão capazes de detectar as oportunidades emergentes das novas formas de gerir a informação e de conseguir a maior rendibilidade dos objectivos empresariais integrados, utilizando tanto a tecnologia como as capacidades humanas. (...) Hoje, competimos num mundo em mudança. O segredo da gestão é gerir num ambiente em mutação permanente. Uma solução que hoje é eficaz será, quase certamente, um constrangimento no futuro. (...) Os nossos principais objectivos estratégicos são possuir uma rede de informação integrada, para que a informação seja um recurso partilhado.

Ainda segundo Daniels (1997: 185), "Os gestores modernos deveriam ser perspicazes em

relação à empresa e às tecnologias" e "necessitam de dominar as tecnologias e de manter relações de cooperação com os outros utilizadores da informação da empresa".

Assim, pode considerar-se que a competitividade das organizações, e muito em particular a das empresas, pode passar pelas práticas de gestão associadas ao conceito de "gestor híbrido"[101].

Outro conceito associado à economia do conhecimento é o de "gestor T". Este conceito tem por base um novo tipo de gestor que "deve saber desenvencilhar-se da hierarquia da empresa tradicional e partilhar o conhecimento". A barra horizontal do T representa a capacidade de compartilhar livremente o conhecimento com toda a organização, mas sem deixar de descurar as suas responsabilidades relativo ao desempenho da sua unidade de negócio, representado pelo segmento vertical do T (Executive Digest, 2002).

A Associação Industrial Portuguesa/Câmara de Comércio e Indústria (AIP/CCI) apresentou, recentemente, a "Carta Magna da Competitividade"[102], para Portugal, onde se identificam como "novas estratégias empresariais", entre outras, (AIP, 2003: 11-12) as seguintes:
A internacionalização, como condição para a competitividade das empresas, compreende o crescimento exponencial dos fluxos comerciais entre Portugal e o exterior e depende da capacidade de orquestrar as maiores oportunidades e os melhores recursos, estejam onde estiverem.
Ultrapassar a fase de "arquipélago" que caracteriza a actuação das empresas no seu relacionamento e desenvolver verdadeiras redes de partilha de informação e de capacidades entre empresas e entre estas e outros parceiros (universidades, centros de investigação e tecnologia, etc.).

Se por um lado, se recomenda o crescimento de práticas de "internacionalização", por outro lado, considera-se necessário "desenvolver verdadeiras redes de partilha de informação", como forma de melhorar os indicadores de competitividade das empresas nacionais. Com estas duas estratégias, em conjunto, vai-se necessariamente ter um crescimento exponencial dos fluxos de informação transnacionais. Logicamente que como consequência haverá um aumento das ameaças e riscos de ataque às respectivas infra-estruturas e conteúdos associados a Novas Tecnologias e Sistemas de Informação (NTSI), no âmbito da utilização requerida do Ciberespaço. Para a implementação destas estratégias considera-se necessário desenvolver uma análise *SWOT* [103], e tomar as medidas adequadas perante a situação identificada, a fim de se poder tirar partido da utilização da informação como uma vantagem competitiva, face à situação de cada empresa ou outro tipo de organização, no âmbito de uma "nova economia"[104] baseada na informação e no conhecimento.

O "Relatório sobre a Competitividade" apresenta, entre outros "Indicadores de Input"[105], a "Sociedade da Informação" e a "I&D e Inovação", que se consideram os que mais se relacionam com o tema em análise. Em relação ao indicador "Sociedade da Informação", este subdivide-se nos aspectos de: "Taxa de Penetração de Banda Larga"; "Taxa de

Penetração Telefónica"; Nível de Acesso à Internet - Empresas e Família"; e, "Despesas em TIC". Quanto ao indicador "I&D e Inovação", neste analisam-se os aspectos de: "Licenciados em Ciência e Tecnologia"; "Despesas em I&D"; "Despesas Públicas em I&D"; "Despesas Privadas em I&D (Indústria)"; e, "Patentes Europeias".

Nos dois "Indicadores de Input", referidos anteriormente, face aos aspectos que os compõem, revela-se que a Competitividade está intimamente relacionada com a utilização da Internet e os investimentos em TIC, onde se inclui a formação superior em Ciência e Tecnologia, a fim de ter pessoas formadas com competências para dar resposta aos desafios da utilização do Ciberespaço, nas melhores condições.

Segundo o Professor Carvalho Rodrigues, "Com superioridade de informação ganha-se aos competidores, com supremacia de informação não existem competidores" (Rodrigues, 1999: 26). Desta forma, poderia concluir-se que existe a possibilidade de criar novas formas de monopólio, através da "supremacia de informação". No entanto, em determinadas circunstâncias, a longevidade destes estados de "supremacia de informação" e "superioridade de informação" pode ser relativamente curta.

Há que tomar medidas constantes de protecção, para minimizar o risco das consequências de permanentes ameaças dos respectivos competidores[106] potenciais, mas, tais medidas nem sempre são eficazes. Perante a ubiquidade que caracteriza a informação[107], a forma da sua utilização é que pode dar mais valia à respectiva organização, através do conhecimento que com ela cria e aplica num determinado contexto.

A nova economia, baseada no conhecimento, em termos de gestão de recursos, pode dizer-se que está fundamentada numa teoria de abundância, ao contrário das economias anteriores, a agrícola e a industrial, em que eram caracterizadas pela teoria da escassez. A teoria da abundância é válida para os recursos informacionais, enquanto que para os bens de consumo, continua válida a teoria da escassez. A teoria da abundância justifica-se porque o conhecimento ao ser partilhado, cresce e não diminui, podendo mesmo utilizar-se em diversos locais ou espaços simultaneamente. O conhecimento quanto mais se utiliza mais valor se cria com novos conhecimentos.

Foi recentemente criada em Portugal[108], sob a iniciativa de Sua Excelência o Presidente da República, Dr. Jorge Sampaio[109], a COTEC Portugal - Associação Empresarial para a Inovação, com a missão[110] de:
Promover o aumento da produtividade e competitividade das empresas localizadas em Portugal, através de uma nova atitude e prática da inovação empresarial assente, nomeadamente, na investigação, no conhecimento, desenvolvimento e aproveitamento das tecnologias, estruturas organizacionais e processos relevantes.
Prestar o contributo empresarial, desafiando as entidades públicas e não públicas com responsabilidades na área da inovação em Portugal, por forma a garantir a criação de um ambiente favorável e estimulador do desenvolvimento da inovação no nosso país, influenciando a correspondente tomada das necessárias medidas e acções concretas.

Na apresentação do Projecto da COTEC Portugal, em 27Nov2002[111], considerou-se que: (1) o fim do modelo tradicional de competitividade, baseado em baixos custos; (2) a orientação da procura (escassa) para a oferta mais competitiva (diferenciação, qualidade); (3) as Empresas como agentes da Inovação); e, (4) o Estado como catalizador/facilitador da inovação, leva à "Competitividade baseada na Inovação", através de tecnologias, processos, organizações, gestão, qualidade e internacionalização.

Considera-se esta iniciativa, como mais um caminho para tentar quebrar uma realidade que parece existir em Portugal, de sermos um povo de inventores, mas sermos pouco inovadores, e, nestes termos colocar-se a nossa criatividade ao serviço da comunidade, através de actividades empreendedoras.

Se com o propósito de cumprir a missão da "COTEC Portugal", for possível aumentar a produtividade e competitividade das empresas, e, desafiar as entidades públicas e não públicas com responsabilidade na área da inovação[112] em Portugal, para melhorar as condições do nosso país. É necessário, no entanto, que cada actor consiga conciliar o espírito de cooperação com o espírito de concorrência[113], que não sendo contraditórios são por vezes pouco conciliadores.

Termina no próximo número

---

* 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 Segundo Waltz (1998: 2) o conceito de "Conhecimento" (Knowledge), no contexto militar, é equivalente ao termo "Intelligence". Neste trabalho, o conceito inglês de "Intelligence" considera-se também equivalente à terminologia portuguesa de "Informações". A terminologia brasileira utiliza o termo "Inteligência" como sinónimo de "Intelligence".

2 Castells (2002: 25) faz a distinção entre "Sociedade da Informação e "Sociedade Informacional", cuja análise e reflexão se aborda mais tarde.

3 A palavra "bit" resulta da contracção das palavras "binary digit" (dígito binário), cuja expressão tem origem no facto de se poder utilizar um código binário simbólico, representado por "zeros" e "uns" para identificar cada um dos estados de um "bit", assim representados por 0 (zero) ou 1 (um).

4 Um "byte" é um conjunto de oito "bits", em código binário, em que se permite

representar (28=256) 256 símbolos diferentes, suficientes para identificar qualquer letra, algarismo ou outro símbolo de escrita.

5 Toffler (1994).

6 Ver o "Anexo A" sobre a caracterização dos conceitos de "dados", informação" e "conhecimento".

7 Nesta situação considera-se o âmbito da guerra de informação para além das actividades essencialmente militares.

8 Internet, Intranet e Extranet (ver Glossário).

9 Nos EUA o conceito de "competitive intelligence" tornou-se numa ferramenta de gestão standard (European Parliament, 2001), onde existe a "Society of Competitive Intelligence Professionals" (SCIP, www.scip.org) que teve, entre 1995 e 1999, um aumento de 3.260 nos seus membros, que embora corresponda a um aumento de 100% neste período de quatro anos (Miller, 2000: 239), considera-se pouco significativo em termos absolutos, face ao país e à sua extensão a nível internacional, talvez explicável pela emergência, apenas nos últimos dez anos, deste tipo de actividade profissional. Este conceito, traduzido para português como "inteligência competitiva", tem incidência muito em particular a nível micro-económico, do interesse empresarial, enquanto que a exploração da "Inteligência" para fins macro-económicos "constitua matéria exclusiva dos governos, e não dos produtores ou comerciantes singulares, embora possam ser estes os seus beneficiários finais" (Campbell, 2001: 96).

10 O actual CEDN foi aprovado pela Resolução do Conselho de Ministros n.º 6/2003, de 20Jan (DR - I Série-B, N.º 16, pp. 279-287).

11 "Uma ameaça é o perigo que uma vulnerabilidade [fraqueza] pode conduzir a consequências indesejáveis - por exemplo, que pode ser explotado intencionalmente ou accionado acidentalmente" (Caldera, 2000: 7).

12 "Um risco é um problema potencial, com causas e efeitos" (Caldera, 2000: 7).

13 O itálico é nosso.

14 A Academia Militar é um Estabelecimento Militar de Ensino Universitário, do Exército Português, de acordo com o DL n.º 88/2001, de 23Mar.

15 Este Curso de Pós-Graduação constitui o primeiro marco, em Portugal, no âmbito da Formação Pós-Graduada em Estabelecimentos Militares de Ensino Superior, realizado pela Academia Militar (www.exercito.pt/am/).

16 O Autor deste trabalho, à data da sua elaboração, é o Chefe do Departamento de Ciências e Tecnologia de Engenharia, da Academia Militar, órgão de enquadramento científico deste Curso de Pós-Graduação, e, em acumulação faz parte da sua Coordenação.

17 Fonte: www.exercito.pt/am/.

18 Toffler (1984) refere-se a "três vagas" como sinónimo de "três eras" ou "três civilizações".

19 Segundo Castells (2002) existe uma distinção analítica entre os conceitos de "sociedade da informação" e de "sociedade informacional", e, como consequência para a terminologia "economia da informação" e "economia informacional". Este autor faz esta distinção por considerar que "a informação, num sentido mais lato, por exemplo, a comunicação do conhecimento, tem sido crítica em todas as sociedades (...). Ao contrário o termo "informacional" indica o atributo de uma forma de organização social na qual a produção da informação, o seu processamento e transmissão se tornam nas fontes

principais da produtividade e do poder em virtude das novas condições tecnológicas emergentes no actual período da história." Assim pretende "estabelecer um paralelo com a distinção entre indústria e industrial" e considera que "Uma sociedade industrial (...) não é somente uma sociedade onde existe indústria, mas uma sociedade na qual as formas sociais e tecnológicas da organização industrial permeiam todas as esferas da actividade, começando pelas actividades dominantes, localizadas no sistema económico e na tecnologia militar, e atingindo os objectos e hábitos do quotidiano". Deste modo considera que no "emprego dos termos "sociedade informacional" e "economia informacional" procura uma caracterização mais precisa das transformações actuais, indo além da observação do senso comum de que a informação e o conhecimento são importantes nas nossas sociedades", e, "uma das características principais da sociedade informacional é a lógica de rede da sua estrutura básica que explica o uso do conceito "sociedade em rede" tal como é definido e especificado na conclusão" da sua obra de referência (2002: 25).

20 Toffler (1984, 1994).

21 Toffler (1991: 11).

22 A título anedótico, na era da sociedade da informação, e num mundo cada vez mais virtual, "poderia" dizer-se às crianças que nascem por download, em vez das "mentiras" tradicionais, em que é a cegonha que as traz de França.

23 Mercado baseado em espaços com "localizações" virtuais.

24 Mercado baseado em lugares com "localizações" físicas.

25 "Ciber" é um "elemento de formação de palavras que exprime as noções de comunicação electrónica e realidade virtual (DLPC, 2001).

26 Nos EUA, foi publicado pela Casa Branca (White House) um documento sobre a "A Estratégia Nacional para a Segurança do Ciberespaço", como enquadramento para a protecção das infra-estruturas que são essenciais para a sua economia, segurança e forma de vida normal (Bush, February 2003b). Este documento esteve em discussão pública desde Setembro de 2002 (Bush, September 2002c), e faz parte de um conjunto de outros estudos publicados também pela Casa Branca, num esforço global para protecção da Nação Americana (Bush, July 16, 2002a, September 17, 2002a, Februrary, 2003b), de certa forma como resposta aos acontecimentos do 11 de Setembro de 2001.

27 Nos EUA, considera-se que as suas infra-estruturas críticas nacionais, são compostas por instituições públicas e privadas, nos sectores da agricultura, alimentação, água, saúde pública, serviços de emergência, governo, base industrial de defesa, informação e telecomunicações, energia, transportes, sistema bancário e financeiro, materiais químicos e perigosos, o sistema postal e o sistema de navegação, cuja segurança é necessário assegurar-se com a participação do sector privado no âmbito de uma "Parceria para a Segurança de Infra-Estruturas Críticas" (Bush, February 2003b: VII, XIII).

28 Nestas condições, por exemplo, "A Microsoft terá que criar gabinetes em Londres e em Tóquio para o desenvolvimento de software, com o objectivo de produzir em três turnos" (Negroponte, 1996: 240).

29 "Organização Virtual Web", ou "Organização Virtual Baseada na Web", ou "Organização Virtual Baseada na Internet".

30 Fonte: Sieber e Griese (Eds.), 1999: 23/Figure 1 (adaptado), incluído no artigo (paper) "Managing Virtual Work: Integrating Reflection and Action through Appropriate

Software Support", de Marvin L. Manheim & Mary Beth Watson-Manheim.

31 Considera-se que o comércio de bits se baseia em trocas comerciais de informação e conhecimento, que se efectuam através das "auto-estradas de informação", por processos de transmissão electrónica, por exemplo, o comércio de capitais, o comércio de produtos multimedia (livros, filmes, música, software), em formato digital, efectuando-se também o respectivo pagamento através de um processo electrónico.

32 O comércio de átomos constitui-se com produtos físicos, por exemplo, alimentos, combustíveis, materiais de construção e outros produtos necessários à vida quotidiana das pessoas, cujas trocas comerciais se efectuam por canais de distribuição adequados aos produtos a entregar pelo fornecedor ao cliente. Neste caso, o pagamento dos produtos poderá ser efectuado por transferência de valor em formato digital transmitido através de bits.

33 Exemplos de comunicações síncronas: conversação telefónica, comunicação por chats na internet.

34 Exemplos de comunicações assíncronas: voicemail, e-mail, carta postal.

35 "The Military as a Network-Centric Enterprise" (Alberts et al., 1999: 89/Figure 9).

36 "The Network-Centric Enterprise" (Alberts et al., 1999: 36/ Figure 6).

37 Realça-se a terminologia empregue de "espaço de batalha" (Battlespace) em vez de "campo de batalha" (battlefield). Na verdade as NTSI permitem que as operações militares se desenvolvam dando mais relevância ao "espaço" em detrimento do "local". Para exemplificar, as diferenças do passado com as possibilidades do presente, refere-se que "Os comandantes de Corpo de Exército e de Divisão viajavam ao longo do campo de batalha [battlefield] para se encontrarem no mesmo local ao mesmo tempo para planear as operações terrestres", enquanto que com as NTSI permite-se que "Os comandantes interajam através de VTC [videoteleconferência], de onde resulta uma redução significativa no tempo de planeamento e a eliminação do tempo de viagens" (Alberts et al., 1999: 109).

38 Cada nó numa rede de "N" nós é capaz de estabelecer "N-1" interacções (conexões). O número total de interacções (conexões) potenciais entre nós numa rede com N nós é dado por N*(N-1)=N2-N. Para valores grandes de N o valor do potencial aumenta com N2 (N ao quadrado). Exemplificação: (1) uma rede com N=2, tem (2*1=2) 2 interacções de informação potenciais; (2) uma rede com N=3, tem (3*2=6) 6 interacções de informação potenciais. Assim, o acrescentar 1 nó, neste caso, equivale a um aumento de (6-2=4=22) 4 possibilidades de interacções.

39 Segundo Alberts et al., a "Dell Computer Corporation" e a "Cisco Systems" (tecnologias de informação), a "Federal Express" e a "American Airlines" (transportes), a "Charles Schwab", a "Deutsche Morgan Grenfell" e a "Capital One" (serviços financeiros), e, a "Wal-Mart" e a "Amazon.com" (retalho), são empresas de referência.

40 Nas palavras de Ramonet, o "conflito dos Balcãs [guerra do Kosovo em 1999] foi (...), na sua condução, uma guerra de novo tipo. Nunca, na história militar, nenhum confronto foi dirigido como fez o general Wesley Clark, comandante supremo da NATO. O princípio de "zero baixas" tornou-se num imperativo absoluto. Após dois meses de bombardeamentos, nem um único militar da Aliança encontrou a morte em acção de guerra. Nunca se tal tinha visto" (Ramonet, 2002: 117).

41 Segundo Toffler, "as perdas reais foram aproximadamente 340 - mais ou menos um centésimo das previsões" (1994: 81).

42 A fórmula do Juramento de Bandeira pelos Militares Portugueses refere "(...) Juro defender a minha Pátria e estar sempre pronto para lutar pela sua liberdade e independência, mesmo com o sacrifício da própria vida" (EMFAR, DL n.º 236/99, de 25Jun, Diário da República n.º 146/99 - I Série-A; alterado pela Lei n.º 25/2000, de 23Ago, Diário da República n.º 194/2000 - I Série-A).

43 Acontece porém que, por razões de utilizar novas formas de fazer terrorismo, ou novas formas de fazer a guerra, com outros meios, cada vez é mais frequente a utilização do "Homem-Bomba". Considera-se que estes casos, a maior parte das vezes, praticam-se por valores ideológicos, religiosos ou outros, em troca de recompensas sobrenaturais, mas que à luz de princípios da civilização ocidental se consideram anti-naturais.

44 "A second key concept is the fact that our force is knowledgeable".

45 Optou-se por uma tradução livre extensiva destes conceitos, para se apresentarem da forma mais explícita possível, face à sua importância e especificidade.

46 A publicação Joint Pub 1-02 (2003) foi corrigida e publicada em 05Jun2003, e não contém o termo "Network Centric Warfare", que é objecto do livro "Network Centric Warfare - Developing and Leveraging Information Superiority" de Alberts et al. (1999), cuja obra é referência de Pollock (2002) para este conceito de "Network Centric Warfare", com a abreviatura ou acrónimo "NCW". Na mesma publicação da doutrina dos EUA, a abreviatura ou acrónimo "NCW" aparece como correspondente ao termo "Naval Coastal Warfare" (Joint Pub 1-02, 2003: 259).

47 Segundo Alberts et al. (1999) as "opiniões, conclusões e recomendações expressas no [seu] livro são apenas dos autores [e] não representam necessariamente os pontos de vista do Departamento de Defesa, ou qualquer outra agência do Governo" dos EUA, de onde se pode compreender que este assunto emergente pode ainda não estar suficientemente consolidado, para ser utilizado em termos de doutrina oficial.

48 Numa pesquisa efectuada, em 31Ago2003, na Internet (www.google.pt) sobre o termo "Network Centric Warfare" apareceram 14.500 links, para consulta de informação sobre este assunto.

49 Segundo um destacável da Revista "Signal" da AFCEA, de Agosto 2003 (Volume 57, No. 12), realiza-se um conjunto de Conferências sobre o tema "Network Centric Warfare", de 29Set a 01Out2003, em Londres, com a participação de diversos especialistas (civis e militares) internacionais (NATO, EUA, UK, Canadá, Austrália, Holanda, Suécia), com informação on-line, na Internet, em www.smi-online.co.uk/networkcentric.asp. A mesma edição desta Revista contém diversos artigos relacionados com o tema "Network Centric Warfare" (Guerra Centrada em Rede).

50 Neste conceito apresentado por Laudon (2002), considera-se explicitamente que um "Sistema de Informação" não é composto apenas por "Tecnologias de Informação".

51 Um "Sistema C3I" designa-se mais recentemente por "Sistema C4I" (Sistema integrado de Comando, Controlo, Comunicações, Computadores e Informações), dando-se, neste caso, relevância à importância que os "Computadores" têm, na actualidade, para o funcionamento eficiente e eficaz de um Sistema C3I. É de notar que o "FM 100-6" "Informations Operations", do Exército dos EUA, publicado em 27Ago1996, apenas inclui no respectivo texto, exclusivamente a sigla C4I (equivalente a C4I) omitindo a sigla original de C3I ou C3I.

52 Exemplo: C4ISR - Command, Control, Communications, Computers, Intelligence,

Surveillance and Recoonaissance (C4IVR - Comando, Controlo, Comunicações, Computadores, Informações, Vigilância e Reconhecimento).

53 Segundo Waltz (1998) o conceito de "Conhecimento" é equivalente ao termo "Intelligence". Neste trabalho o conceito inglês de "Intelligence" considera-se também equivalente à terminologia portuguesa de "Informações".

54 Segundo Laudon (2002), "Sistemas de Informação" são mais do que computadores. A utilização efectiva de "Sistemas de Informação" (SI) requer um entendimento da "Organização", da "Gestão" e das "Tecnologias de Informação" (TI), que constituem estes "Sistemas de Informação". Todos os SI podem descrever-se como soluções organizacionais e de gestão para fazer face às mudanças colocadas pela envolvente das respectivas actividades. Assim, não deve confundir-se a componente das TI com o respectivo SI, de que aquelas fazem parte. As mesmas TI podem ter um desempenho diferente consoante o tipo de "Gestão" e "Organização" a que se associam, para se conseguir uma "Solução da Actividade" de uma Instituição.

55 Dinis, 1997: 90/Figura 5.1 (adaptado).

56 A sigla C3I e C4I também se representam por C3I e C4I, correspondentes ao número de potências de base "C" e de expoente 3 e 4 respectivamente, das componentes do Sistema cujas designações são iniciadas por "C".

57 A doutrina militar "conjunta" americana é a doutrina utilizada em comum pelo Exército, Marinha, Força Aérea, Corpo de Marines e Guarda Costeira, dos EUA.

58 Considera-se interessante verificar que no âmbito da definição de guerra de informação apresentada, e, em outros assuntos e conceitos com ela relacionados, utiliza-se o termo "adversário" em vez de "inimigo". Isto não deixa de ter algum significado quanto a este novo tipo de guerra e operações militares afins. Neste caso, o opositor pode não ser necessariamente um inimigo, mas até pode configurar-se com um "amigo", que em determinadas circunstâncias considera necessário utilizar "operações de informação", para vir a garantir a obtenção de superioridade quanto à posse e utilização de informação.

59 O actual CEDN foi aprovado pela Resolução do Conselho de Ministros n.º 6/2003, de 20Jan (DR - I Série-B, N.º 16, pp. 279-287).

60 Cronin (1996: 1-28).

61 "Uma vulnerabilidade é uma fraqueza que pode levar a consequências indesejáveis" (Caldera, 2000: 7).

62 Por exemplo: os Serviços de Informações de diversos Países Amigos.

63 Por exemplo: as firmas fornecedoras de software, de aplicações e de ferramentas de segurança (firewalls, antivírus).

64 Considera-se que, por mais e maiores investimentos se façam, não se consegue alcançar níveis de protecção que permitam garantir o pleno de fiabilidade do sistema, em termos de 100% de segurança. Há que identificar quais os riscos que se correm, e destes quais se devem evitar e quais se podem admitir, sendo neste caso estudados planos de contingência para lhes dar respostas, de forma a minimizar os seus efeitos negativos.

65 O termo inglês "Intelligence" considera-se neste trabalho equivalente ao termo "Informações" da língua portuguesa, de Portugal, e que no Brasil se utiliza com o termo "Inteligência".

66 "Operations security" (OPSEC).

67 "Electronic warfare" (EW). Neste caso, através de "contra-medidas de GE",

nomeadamente “empastelamento”.
68 “Information assurance”.
69 “Contra-operações psicológicas”.
70 Neste caso, através de “Medidas de Apoio de GE” e “Medidas de Protecção de GE”.
71 O termo “cyberwar” apresentado em “Cyberwar is Coming!” por Arquilla e Ronfeld, em 1993, tinha um âmbito ao nível de conflitos militares (Arquilla e Ronfeld, 2001: 2). Nestes termos, Waltz fez corresponder o conceito de “cyberwar/cyber warfare” à “guerra de comando e controlo” (command and control warfare - C2W), para o alinhar com a terminologia militar correspondente.
72 Waltz, 1998: 20/Table 1.5.
73 Waltz, 1998: 21/Figure 1.2 (adaptado).
74 Fonte: http://www.nbso.nic.br/docs/cartilha/ (adaptado) (acedido: 11Março2003).
75 Waltz, 1998: 22/Figure 1.3 (adaptado).
76 “Observe”, “Orient”, “Decide”, “Act”.
77 Waltz, 1998: 28/Figure 1.4 (adaptado).
78 Waltz, 1998: 29/Figure 1.5 (adaptado).
79 Segundo Waltz, “lamenta-se a nomenclatura de “guerra de informação” porque as suas operações são desenvolvidas durante todas as fases da tradicional “paz”. Na verdade, a guerra em rede [net warfare] não é de todo pacífica, mas não tem as características de aparência de guerra” (Waltz, 1998: 28).
80 As ameaças do terrorismo podem ser maximizadas através de actividades de GI, não só para acções de ciberterrorismo, mas também para apoio de outras acções terroristas. Nas palavras de Boniface, “Em muito poucos anos, o terrorismo informático tornou-se numa fonte de grandes preocupações para os responsáveis políticos e militares ocidentais, nomeadamente nos Estados Unidos. Em Maio de 1998, o presidente Bill Clinton anunciou a nomeação de um coordenador nacional para a segurança, a protecção das infra-estruturas e o contra-terrorismo” (Boniface, 2003: 16).
81 Joint Pub 3-13, 1998: 1-4/Figure I-2.
82 Este acrónimo é utilizado como abreviatura da expressão inglesa “Information Security”. Esta terminologia talvez seja mais conhecida e utilizada a nível militar, no entanto, com certeza que cada vez será mais utilizada noutros sectores, e, em particular pelos profissionais relacionados com as NTSI.
83 Considera-se um meio multimedia aquele que permite utilizar dados, texto, som/voz e imagem, no mesmo equipamento, sendo o computador pessoal (PC) o meio mais elucidativo para dar como exemplo. O PC actual permite substituir outros equipamentos que anteriormente se utilizavam cada qual para seu fim. O PC substituiu, em certa medida, o computador central único com terminais “estúpidos” para processamento de “dados”, a máquina de escrever para escrita de “texto”, o telefone para comunicação da “voz”, e, a televisão para utilizar “imagens”.
84 Considera-se um meio hipermedia aquele que tem características multimedia, mas em que o acesso à informação se pode efectuar de forma não sequencial, em tempo real, através de cliques sobre palavras, imagens ou outros símbolos. Permite-se “navegar” através da informação à vontade do utilizador, consoante o seu gosto, desejo ou necessidade, dentro dos parâmetros de formatação associados aos links da respectiva informação a consultar. O “hipertexto” foi a primeira aplicação de tecnologia deste tipo.
85 É comum utilizar-se o termo “telecomunicações” com o mesmo significado que

“comunicações”, embora aquele se refira etimologicamente apenas a “comunicações a distância”.

86 Segundo o autor Alcide d´Oliveira “A existência da palavra Telemática, que é utilizada para sugerir que “hoje em dia” lembra uma só disciplina que engloba o que “antigamente” eram as Telecomunicações e a Informática”, é “um erro grosseiro esse, porque se se associasse às Telecomunicações todas as entidades que têm o radical “Tele” na sua constituição, elas absorveriam metade das tecnologias e até das funções em geral.” (Oliveira, 1995).

87 Em termos funcionais, e em particular a nível militar, há que distinguir dois conceitos sobre informática: “informática de gestão” e “informática operacional”. A “informática de gestão” traduz-se em aplicações do tipo de gestão empresarial, e, a “informática operacional” relaciona-se com a gestão das operações militares através do C2 e na operação dos sistemas de armas.

88 Uma rede de computadores é constituída por tecnologias de computadores (hardware e software), mas também por tecnologias de comunicações (fibras ópticas, satélites, feixes hertzianos, equipamentos wireless, modems). As redes de computadores com tecnologia wireless (sem fios) (que se prevê tenham a curto prazo cada vez mais utilização, face à sua flexibilidade e facilidade de instalação), apenas são possíveis implementar pelo desenvolvimento que teve este tipo de tecnologias de comunicações. A gestão de uma rede de um qualquer operador de telecomunicações (PT Comunicações, Novis, TMN, Vodafone, etc), seria com certeza impossível, sem a utilização de um sistema de informação baseado em tecnologias de computadores, pois já lá vai o tempo (das décadas de 70 e 80, do Sec. XX) em que a facturação dos TLP passava por uma fase de fotografar os contadores das chamadas dos clientes nas respectivas centrais telefónicas electromecânicas.

89 Este acrónimo é utilizado como abreviatura da expressão inglesa “Computer Security”.

90 Este acrónimo é utilizado como abreviatura da expressão inglesa “Communications Security”.

91 Aprovado pelo Decreto-Lei n.º 153/91, de 23 de Abril, e, alterado pelo Decreto-Lei n.º 128/2002, de 11 de Maio.

92 Decreto-Lei n.º 128/2002, de 11 de Maio.

93 “O presidente da Comissão de Planeamento de Emergência do Ciberespaço é uma individualidade de reconhecida competência na matéria em causa, a nomear por despacho do Ministro da Ciência e da Tecnologia” (actualmente do Ministro da Ciência e do Ensino Superior).

94 Ver Bush (2003b).

95 “CERT - Computer Emergency Response Team”.

96 “CSIRT - Computer Security Incident Response Teams”.

97 Fonte: www.cert.pt.

98 Fonte: www.cert.pt.

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

100 Daniels refere-se ainda que, “O professor Michael Earl, da London Business School, e

o Dr. David Skyrme, do Templeton College, em Oxford, enriqueceram ainda mais a definição de gestor híbrido como sendo «pessoas dotadas de grandes competências técnicas e de adequados conhecimentos da empresa, ou vice-versa… os híbridos são aqueles que, possuindo competências técnicas, são capazes de trabalhar em áreas de utilizador a desempenhar um trabalho de line ou funcional, mas são adeptos do desenvolvimento e do incremento de ideias da aplicação das TI»" (Daniels, 1997: 211).
101 Um "gestor híbrido" será um gestor que para além de ter bons conhecimentos na área científica da gestão propriamente dita, deve ter outros conhecimentos que complementem essa formação de base, nomeadamente na área das tecnologias de informação, a fim de permitir tomadas de decisão mais fundamentadas na base do seu conhecimento próprio, e assim evitar decidir sem questionar as hipóteses de solução que o respectivo "staff" lhe propõe.
102 Este documento apresentado publicamente, em 23Jul2003, pela AIP/CCI, no âmbito da competitividade em Portugal, é constituído por duas partes, a "Carta Magna da Competitividade" e o "Relatório sobre a Competitividade" (www.aip.pt) (AIP, 2003: 3). A "Carta Magna da Competitividade compreende dois pontos fundamentais": (a) "A visão estratégica tem o propósito de concentrar e mobilizar as atenções de forma constante para que em Portugal exista um enquadramento político e económico "amigo" da competitividade, o que passa por: (1) - estabelecer prioridades a nível do posicionamento e das alianças estratégicas nacionais; (2) - pela assunção de um novo modelo económico e (3) - pela referência aos recursos essenciais"; e, (b) "Os grandes objectivos e princípios orientadores ao nível das estratégias empresariais e das políticas públicas representam escolhas (por vezes difíceis) entre opções válidas em termos de competitividade, com a finalidade de estabelecer prioridades de actuação para os "agentes" privados e públicos" (AIP, 2003: 3). O "Relatório sobre a Competitividade inclui": (a) "diversos indicadores sobre competitividade em Portugal comparada com um conjunto de parceiros internacionais (benchmarking) (...) [e] consiste na análise de cada um desses indicadores (enquadramento) com uma metodologia comum e na definição de objectivos sobre a evolução desses indicadores em termos comparados e, sempre que possível, em termos absolutos"; e (b) "estabelece, finalmente, uma metodologia de avaliação periódica da performance em matéria de competitividade incluindo propostas de intervenção ao nível das políticas e das práticas, dirigidas aos decisores privados e públicos" (AIP, 2003: 3).
103 Uma análise SWOT é um estudo de gestão estratégica que inclui, a análise da Envolvente Interna, sobre as Forças e Fraquezas (Strenghts, Weaknesses), e a análise da Envolvente Externa, sobre as Oportunidades e Ameaças (Oportunities, Treats), de uma organização (empresa).Em documentos da União Europeia (UE, 2000a) refere-se a este conceito como "economia do conhecimento". A terminologia de "economia digital" é, por vezes, também utilizada, no entanto, neste caso, considera-se que seria mais adequado utilizar "economia baseada na internet", ou simplesmente "economia da internet" (Internet Economy) (University of Texas, 2000, 2001), pois que este é um factor preponderante que veio revolucionar a nova economia com incremento do negócio e comércio electrónicos (e-Business, e-Commerce).
104
105 Os outros "Indicadores de Input" são: "Custos Laborais"; "Preços e Custos"; "Fiscalidade"; "Educação e Formação"; "Transportes"; "Ambiente e Energia"; "Capital; Investimento"; e, "Produtividade".

106 Considera-se o termo “competidor” inserido no conceito de “adversário”, “inimigo”, “opositor” ou “concorrente”, consoante a situação e circunstâncias da sua aplicação.
107 A mesma informação pode ser utilizada em diversos locais ao mesmo tempo, sem que se consuma, e, quanto mais se utiliza mais conhecimento pode produzir.
108 A cerimónia de criação da COTEC Portugal, realizou-se em 30 de Abril de 2003, no Palácio da Ajuda, com a presença de Sua Excelência o Presidente da República, Dr. Jorge Sampaio, e de Sua Majestade o Rei de Espanha. Neste local e nesta data foi também assinado um Protocolo de Acordo entre a COTEC de Espanha, de Itália e de Portugal.
109 Segundo o n.º 6, do Art. 5º dos Estatutos da “COTEC Portugal”, “O Presidente da República, Dr. Jorge Sampaio, como principal promotor e dinamizador da criação da Associação, assumirá a qualidade de Presidente da Mesa da Assembleia Geral da Associação” (www.cotec.pt, Estatutos).
110 Fonte: www.cotec.pt, Sumário Executivo.
111 Fonte: www.cotec.pt, Sumário Executivo.
112 Em Portugal e na Europa de uma maneira geral, as entidades “não públicas”, em particular as empresas, são as entidades que menos investem em I&D, e por consequência em actividades directamente relacionadas com a inovação, se comparado com situações idênticas dos EUA e do Japão.
113 No texto da apresentação do Projecto da “COTEC Portugal”, em 27Nov2002, a conjunção dos termos “Cooperação” e “Concorrência” designa-se pelo termo “Coopetição” (www.cotec.pt, Sumário Executivo). Este último, é um termo onde se aliam dois conceitos que em separado se podem considerar contrários, mas que num contexto de parceria para a competitividade se podem aliar; veja-se o exemplo do Projecto Auto-Europa que resultou de uma parceria Ford-Volkswagen, constituindo-se numa coopetição no sector automóvel.