Mundos Virtuais, Riscos Reais: Fundamentos para a Definição de uma Estratégia da Informação Nacional

Brigadeiro-general
Paulo Fernando Viegas Nunes

Evolução Tecnológica e a Sociedade em Rede

A evolução tecnológica e a utilização alargada da Internet contribuíram para a formação de uma grande "aldeia global" onde a interacção entre os homens deixa de ser influenciada por barreiras geográficas e passa a ser condicionada pelo tempo de acesso e pela disponibilidade dos recursos de informação. Entendendo a evolução tecnológica como um desafio e uma oportunidade de convergência para padrões mais elevados de desenvolvimento económico e social, os Estados procuram estimular a inovação e fomentar a adopção de novas plataformas tecnológicas.

Num contexto onde o conhecimento determina os modelos de interacção que permitem potenciar a exploração da informação, a conectividade desempenha também um papel relevante, constituindo um pré-requisito para a evolução em comunidade e para a democratização do acesso à informação.

Assistimos à alteração do paradigma social, onde novas formas de comunicação emergiram e acabaram por se massificar, transportando do físico/presencial para o virtual muitos dos tradicionais processos de interacção social. A assumpção plena de uma

identidade digital por um número crescente de utilizadores, estimulada por um certo deslumbramento e pela mais-valia de construir uma ligação quase permanente com outros utilizadores, marca o sucesso dos *Blogs* e das Redes Sociais[1]. No entanto, apesar do inquestionável valor associado ao funcionamento em rede[2], a exploração da Internet adiciona muitas vezes um elevado grau de entropia às relações sociais, que se reflecte, nomeadamente, no surgimento de novos actores de intermediação. A adesão a novos processos e modelos de interacção em rede, é também marcada por alguma "ingenuidade tecnológica" que leva os utilizadores a partilhar, por vezes sem restrições, os seus dados pessoais. Motivada em grande parte por deficiente formação tecnológica mas sobretudo por um falso sentimento de confiança, esta situação é responsável pelo surgimento de novos riscos sociais.

A estruturação das sociedades mais desenvolvidas em rede e a própria construção do ciberespaço constituem características fundamentais da conjuntura estratégica deste novo Século. Numa economia em rede, o actor que apre-sentar melhores ligações às diversas fontes de conhecimento possui uma grande vantagem competitiva, resultante do facto de estar posicionado no "lugar certo" numa rede de troca de informação.

A capacidade de exploração das redes, tanto no contexto de complexos sistemas económicos como das restantes áreas de actividade das modernas sociedades, demonstra a "força" que alguns actores exibem sobre outros, influenciando a cadeia de valor das organizações, condicionando o exercício do poder e delimitando as fronteiras do espaço estratégico em que estas podem competir. Dentro deste contexto, constata-se que a forma como os diferentes actores utilizam a informação pode ser simultaneamente geradora de novas oportunidades e de novas ameaças no ciberespaço, apresentando importantes implicações na condução da Política e da Estratégia dos Estados.

Geopolítica e Geoestratégia do Ciberespaço

A utilização da informação encontra-se hoje intrinsecamente associada à forma como se processa tanto a sua difusão como a sua apropriação. O ciberespaço oferece uma difusão global e uma apropriação localizada, apresentando muitos aspectos tangíveis que justificam uma análise geográfica focalizada num determinado território. A utilização da Geografia[3] e da Geopolítica[4] como instrumentos de análise, abrirá caminho para a melhor compreensão deste mundo digital, da forma como ele se estrutura fisicamente e como está a ser utilizado, permitindo desta forma perspectivar os seus impactos no mundo real e na sociedade contemporânea. A promoção do desenvolvimento sustentado e da competitividade nacional, dá sentido e torna necessária a análise da localização das infra-estruturas de informação à luz da consecução dos objectivos da Política. É através da Geopolítica que entendemos e perspectivamos o mundo e o País em que vivemos, capacitando-nos para enfrentar os desafios que as novas realidades colocam.

A estruturação de uma autêntica "rede de redes" e a emergência de uma interacção em tempo-real, através da Internet, tem contribuído para impor a compressão do "espaço-tempo", construindo um espaço de comunicação virtual de cobertura mundial. A este espaço virtual, não físico ou territorial, atribui-se a designação de Ciberespaço[5]. Paradoxalmente, a sensação de "abolição do espaço" e a consequente desterritorialização do estudo das relações sociais assume agora novos contornos, uma vez que a localização das infra-estruturas de informação e as "novas acessibilidades" desempenham um papel determinante para a compreensão desta "Geografia do Ciberespaço". Podemos assim constatar que as redes de comunicações que compõem o ciberespaço, não se situam apenas no espaço virtual dos fluxos de informação que transportam, elas constituem o próprio espaço (Negroponte, 1996), originando a consequente inclusão e exclusão geográfica de lugares e pessoas da rede global. Face às diferentes visões sociológicas que o ciberespaço suscita, é nossa convicção, que o seu estudo poderá ser sistematizado segundo duas perspectivas:

- como infra-estrutura tecnológica de informação, composta pela interligação física de redes de computadores que constitui a *World Wide Web*;
- como espaço virtual, palco de interacções sociais, económicas, políticas e culturais.

Num ambiente aberto e sem fronteiras físicas, a defesa dos interesses nacionais[6] assume contornos relativamente latos. Em resposta a este desafio, existe hoje uma evidente preocupação e uma aposta dos responsáveis políticos na percepção das interdependências e das áreas envolventes deste espaço virtual, como fundamento para a tomada de decisões estratégicas mais informadas. Tendo por base dados estatísticos e documentais disponíveis (AC, 2010; ISOC, 2010), é possível constatar que o ciberespaço pode ser "mapeado" de forma a facilitar a sua compreensão, obviando desta forma à existência de eventuais problemas decorrentes da sua utilização não criteriosa. Se considerarmos que este tipo de análise pode também ser utilizada para efeitos militares, nomeadamente, para planear ciberataques destinados a impedir a utilização das infra-estruturas de informação de um adversário, estamos também a lançar as bases para o estudo do que podemos designar por "Geoestratégia do Ciberespaço".

Em aberto, por enquanto, encontra-se a formulação de uma teoria Geopolítica do Ciberespaço, numa perspectiva global do poder mundial. Face à crescente dependência da Economia mundial e do próprio Sistema Internacional relativamente às interacções e aos fluxos de informação estabelecidos através da Internet, não tardará muito até que apareça alguém que defenda que "quem dominar o ciberespaço domina o mundo". Não pretendendo desenvolver uma teoria destinada a justificar este silogismo, que reputamos de difícil e complexa concretização prática, antes procuraremos apresentar alguns aspectos que julgamos relevantes para a compreensão do seu impacto estratégico.

À medida que a matriz tecnológica da sociedade vai permitindo novas formas de comunicação, um número cada vez maior de actores (indivíduos, organizações e Estados) passa a estar ligado e a interagir através de uma Infra-estrutura de Informação Global (IIG)[7]. Face à indefinição dos limites físicos e à dificuldade em estabelecer princípios de jurisdição territorial sobre as redes de comunicações transnacionais, os Estados são confrontados com a existência de um ambiente de informação à escala planetária, onde não é possível definir de forma clara o que representa a Infra-estrutura de Informação Nacional (IIN).

Pensando nos recursos materiais que permitem levantar esta infra-estrutura[8], constata-se que ela integra todas as estruturas de suporte à nossa vivência diária. Neste âmbito, se considerarmos o funcionamento da Rede Nacional de Emergência (112), do sistema de distribuição de águas ou mesmo do sistema de distribuição de energia eléctrica, verificamos que se geram "cascatas de interdependências" decorrentes das suas interacções e do funcionamento dos seus subsistemas. A quebra dos fluxos de informação, necessários ao funcionamento de qualquer um destes sistemas, poderá ter consequências catastróficas.

Organizações como a União Europeia (EU) (COM, 2002) e alguns países como os Estados Unidos da América (EUA) (NSHS, 2002; Lewis, 2002) e a Holanda (Luiijf, 2003), têm vindo a identificar a vulnerabilidade das sociedades ocidentais relativamente à ruptura das suas infra-estruturas críticas. Mesmo em Portugal, têm surgido sinais de preocupação relativamente ao facto de existirem "infra-estruturas de risco" que, quando afectadas, comprometem o bem-estar e a satisfação das necessidades básicas das populações (Caetano & Garcia, 2003). Seguindo as linhas gerais de estudos existentes sobre esta temática (Anderson, 1999; Lewis, 2002), podemos mesmo chegar a um modelo vertical de dependências funcionais. De acordo com este modelo, constatamos que no topo das dependências do funcionamento das Infra-estruturas Críticas Nacionais (ICN) se encontra a Rede Eléctrica Nacional. À semelhança do que se passou durante a última década noutros países[9], uma falha prolongada do abastecimento de energia eléctrica pode colocar em causa o funcionamento de todas as ICN.

A infra-estrutura de informação, constituída pela rede de telecomunicações, dependerá também da rede eléctrica. No entanto, no caso das restantes infra-estruturas críticas do Estado, existe uma dupla dependência uma vez que estas só funcionarão se puderem dispor, simultaneamente, de energia eléctrica (dependência estrutural) e das infra-estruturas de informação que suportam o seu funcionamento (dependência funcional)[10]. Só a completa compreensão da extensão das interdependências de uma infra-estrutura

(verticais e/ou horizontais) permite levantar as necessárias medidas correctivas, destinadas a controlar este efeito.

A protecção da IIN, passa inevitavelmente pela identificação dos recursos-chave que se pretendem defender ou preservar e pela realização de uma adequada análise e gestão do risco, destinada a reduzir as vulnerabilidades[11] existentes. Na análise do risco social associado à IIN, temos que ter em atenção que este resulta do efeito conjugado de três factores importantes: dos recursos a proteger (alvos potenciais), da detecção das vulnerabilidades da IIN e das ameaças que, explorando essas vulnerabilidades, podem afectar os recursos que pretendemos proteger.

Após a sua análise e avaliação, a gestão do risco social pode assumir diversas formas, nomeadamente, através da sua redução (adopção de contra-medidas), aceitação (manutenção do risco) ou transferência para terceiros. A escolha de cada uma destas três opções está intimamente relacionada com o valor que atribuímos ao recurso a proteger[12]. Quanto mais crítico for o recurso, maior será a necessidade de adoptar as contra-medidas necessárias para reduzir o nível do risco que se lhe encontra associado. Exemplos recentes como os ciberataques lançados contra a Estónia (Abril/Maio de 2007) e contra a Geórgia (Agosto de 2008), vieram provar a necessidade de salvaguardar o fluxo de informação vital entre as estruturas governamentais e os diversos Órgãos/Sectores considerados críticos para a sobrevivência do Estado.

Se Portugal pretender ocupar um lugar no grupo das "Sociedades de Informação"[13], torna-se necessário garantir a segurança e a protecção contínua da IIN, encarando esta necessidade como um processo contínuo e sistémico que passa pela análise e gestão dos riscos sociais emergentes do ciberespaço. Devendo estes aspectos ser tidos em conta na definição de uma Estratégia da Informação Nacional, importa agora caracterizar a vulnerabilidade estratégica e o espectro da ameaça no ciberespaço.

Vulnerabilidade Estratégica e a Ciberameaça

A utilização do ciberespaço como vector privilegiado de acções terroristas e a sua crescente exploração militar, tem um impacto profundo no ambiente estratégico internacional, obrigando os Estados a rever os fundamentos da sua Segurança e Defesa. No entanto, a utilização de uma nova arma ou de uma inovação tecnológica para explorar uma vulnerabilidade estratégica não poderá ser considerada como inovadora. Para além da incontornável referência aos princípios da guerra assimétrica e aos fundamentos do pensamento estratégico de Sun Tzu (1993), constata-se que já na 1ª Guerra Mundial, alguns pensadores como Douhet[14] e Trenchard[15] defendiam ser possível afectar a capacidade inimiga para conduzir a guerra, através do lançamento de ataques aéreos contra as suas infra-estruturas críticas, normalmente situadas em áreas distantes da

linha da frente. No decurso da 2ª Guerra Mundial, estas teorias foram também levadas à prática através da condução de bombardeamentos estratégicos destinados a destruir as centrais eléctricas, os centros industriais e os sistemas de transportes que suportavam o esforço de guerra inimigo.

De acordo com a teoria desenvolvida por Alvin Toffler (1991), a Era industrial deu lugar à Era da informação. Face às bases em que se fundamentam tanto a geração de riqueza como a natureza das relações de poder, os recursos-alvo a atingir deixaram de ser as instalações fabris e as matérias-primas, passando os recursos intangíveis (a informação) a constituir o alvo privilegiado desses ataques[16]. As ciberameaças (Denning, 1999; NSSC, 2003), podem assumir a forma de intervenção social ("ciber-activismo", "ciber-hacktivismo", "ciber-vandalismo" ou "ciber-graffiti"), a forma de acções criminosas (*hacking*, c*racking*, cibercrime ou ciberterrorismo) ou mesmo a forma de actos de guerra (ciberguerra).

Independentemente de acreditarmos ou não na iminência de um ciberataque, não podemos ignorar que a sua ocorrência poderá provocar um efeito disruptivo na nossa sociedade. No actual ambiente de informação, um ciberataque (ataque de informação) poderá ser considerado de nível estratégico se o seu impacto for tão importante que afecte (ou possa vir a afectar) a capacidade de um Estado para assegurar as suas funções vitais (segurança e bem-estar da sua população). Dentro deste contexto, tendo por base os seus efeitos, também as armas da guerra baseada na informação (Guerra de Informação[17]), poderão ser consideradas como armas de "disrupção massiva" (Libicki, 1995; Morris, 1995), apresentando a sua utilização um enquadramento estratégico semelhante ao das armas nucleares de destruição massiva. Os fundamentos associados ao lançamento de ciberataques, apresentam assim grandes semelhanças com os princípios do bombardeamento estratégico, permitindo-nos este paralelismo uma melhor percepção da forma como os ataques às infra-estruturas críticas de um Estado afectam a sua sociedade.

Devido à incerteza das consequências e ao potencial impacto de um ciberataque nas populações civis e na sociedade em geral, os Estados terão inevitavelmente de realizar uma avaliação dos riscos sociais decorrentes da utilização de armas de informação por parte de actores hostis, nomeadamente por parte de grupos terroristas e até de outros Estados. Assim, a avaliação da ameaça terá forçosamente que passar por uma análise tanto da sua probabilidade de ocorrência como da sua severidade ou grau de disrupção. Dentro deste contexto, assume também particular importância analisar a forma como os Estados e a comunidade internacional poderão, de forma integrada e concertada, desenvolver políticas e implementar estratégias de prevenção e combate às ameaças emergentes no ciberespaço.

Conforme refere o General Loureiro dos Santos (2001), a Sociedade de Informação fez surgir o ciberespaço como um novo espaço de confronto estratégico. Neste contexto, é legítimo assumir-se que se desenvolvem, em permanência, actividades em que a informação desempenha, simultaneamente, o papel de alvo e de arma. O desenvolvimento de uma capacidade defensiva é, dentro deste enquadramento, encarada como aceitável ou mesmo como justificável, sendo por muitos países classificada como uma actividade de Guerra de Informação "legítima". Contudo, o levantamento de uma capacidade de análise de vulnerabilidades, a simulação de ataques e a realização de jogos de guerra, implica necessariamente o desenvolvimento de acções de contornos agressivos. Desta forma, se nos referirmos apenas à Guerra de Informação defensiva, excluindo a sua componente ofensiva, estamos a desprezar a sinergia existente entre elas, comprometendo a necessária manutenção da superioridade no ambiente da informação.

Desenvolvimento de Cenários e Análise Estratégica

A análise do risco social associado ao ciberespaço, que todas as sociedades tecnologicamente desenvolvidas hoje enfrentam, passa pela identificação dos seus parâmetros influenciadores mas impõe também uma análise de cenários que permita perceber, face a determinadas condicionantes, qual a variação dos parâmetros que lhes está associada. Este tipo de análise, permite assim perspectivar o impacto da imposição de uma determinada escolha/pressuposto, facilitando uma avaliação concorrente das diferentes opções estratégicas disponíveis.

A Análise Morfológica[18] constitui um método de análise ajustado tanto para o levantamento de cenários como para o desenvolvimento sustentado de opções estratégicas. Esta metodologia, consiste na representação do problema a resolver através da identificação de diversos parâmetros (fase de análise) e na criação de configurações consistentes a partir desses parâmetros (fase de síntese). Com base nestes pressupostos, partindo das condicionantes a analisar, construiu-se a matriz representada na Figura 1. Esta matriz, representa os diversos estados/opções que cada uma das variáveis pode assumir, construindo desta forma o "espaço-solução" que permite apoiar a análise morfológica do problema. A partir desta matriz, foi possível avaliar de forma concorrente diversas soluções.

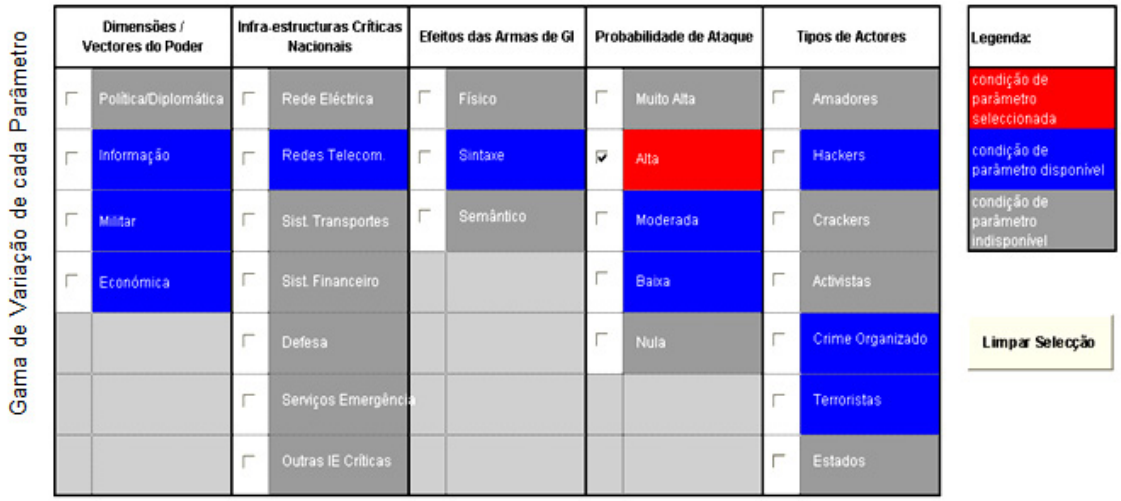

Figura 1 - Matriz de Análise do Risco Social no Ciberespaço

- Cenário "Mais Provável"

Neste contexto, após a consolidação do modelo de inferência, foi desenvolvida uma aplicação de *software* especialmente orientada para a análise do risco social decorrente da utilização do ciberespaço[19]. Assumindo que o risco social é determinado não só com base na severidade (nível de impacto) mas também pela probabilidade de ocorrência de um ataque, importa essencialmente fazer face à situação "mais provável e acautelar a situação mais perigosa". A partir da ferramenta computacional desenvolvida, foi possível visualizar graficamente os parâmetros associados a todos os cenários e obter a intersecção destes dois "espaços-solução". De acordo com os dados obtidos, a estratégia mais consistente e eficaz passa por uma aposta na protecção das redes de telecomunicações (IIN) do Estado. Este passo, constituiu o culminar de todo o processo de análise morfológica desenvolvido, permitindo definir a "melhor estratégia possível" para reduzir o risco social na exploração do ciberespaço.

Fundamentos do Poder da Informação

O Poder de uma Unidade Política[20] pode ser caracterizado como "a revelação da sua força, numa situação específica, para prossecução de fins determinados" (IAEM, 1999). Esta força, resultante dos meios que um Estado consegue mobilizar para fazer face a outros Estados ou mesmo a outro tipo de actores que se lhe opõem, constitui o que se designa por Potencial Estratégico[21]. Um actor só pode avaliar o seu Poder relativamente a outro actor quando o exerce[22]. Verifica-se também que o Poder, para além de relativo e situacional é também multidimensional e não conversível. Desta forma, o Poder é multifacetado e deve ser analisado em todas as suas dimensões, sendo ilógico considera-lo de forma isolada, apenas segundo determinado tipo/vector de Poder (Militar, Económico, etc.). Também não é possível converter um tipo de Poder noutro, pois não

existindo um factor ou unidade comum que assegure essa conversão, não se afigura como viável utilizar mecanismos de compensação de um tipo de Poder face a outro. Procurando "fazer a ponte" com o tema do presente trabalho, a título de exemplo do que aqui se refere, constata-se que se um actor utilizar o domínio da informação (ciberespaço) para exercer Poder sobre outro actor, este último só pode compensar a existência de eventuais assimetrias, se desenvolver "forças" ou capacidades neste domínio. Quer isto dizer que se um País for alvo de um ataque cibernético a forma mais eficaz de limitar o seu impacto e evitar possíveis efeitos destrutivos é o levantamento de uma capacidade de ciberdefesa.

Tendo em vista a sua aplicação, podemos afirmar que o Poder se organiza em três bases diferentes: objectiva, subjectiva e relativa (Couto, 1988). Por definição, a base objectiva integra todos os recursos materiais (tangíveis) que, encontrando-se à disposição de determinado actor, podem ser objectivamente quantificados e avaliados. A base subjectiva, integra todos os factores intangíveis ou de difícil materialização, mas que se revelam decisivos para o exercício do Poder. Quanto à base relativa, verifica-se que esta inclui um conjunto de factores que só fazem sentido no contexto de uma interacção com outrém, reflectindo a dialéctica do "eu" com o "outro" (Dias, 2005, p.221). Associado a este conjunto de factores, encontra-se o inevitável circunstancialismo da eventual aplicação do Poder, tanto ao nível do local, como da distância e dos meios a serem aplicados.No que se refere ao "Poder da informação", conforme se tem vindo a demonstrar ao longo deste estudo, podemos dizer que as infra-estruturas de informação constituem a sua base objectiva, a capacidade para gerir as percepções no domínio da informação materializa a sua base subjectiva e o conjunto de interacções que se estabelecem no ciberespaço, através da troca dos diferentes fluxos de informação, representa a sua base relativa.

Uma vez que se pretende estabelecer a lógica das dinâmicas de Poder associadas ao domínio da informação e do ciberespaço, considera-se também importante a sua interpretação à luz dos princípios da teorização do potencial estratégico. Também aqui, é possível reconhecer que as infra-estruturas de informação, enquanto elemento caracterizador das forças materiais de uma Unidade Política, influenciam e contribuem para a avaliação do seu potencial estratégico. Por outro lado, o ciberespaço, enquanto elemento mediador das interacções sociais, económicas e políticas, também influência a aplicação das forças morais, constituindo-se como elemento caracterizador do "potencial dinâmico". De acordo com esta visão, que pretende evidenciar o incontornável contributo do ciberespaço para a definição dos diversos tipos de forças (tangíveis e intangíveis) de uma Unidade Política, constatamos que o potencial estratégico de qualquer Estado depende e pode ser influenciado por este novo espaço de informação e comunicação. Este pressuposto, abre caminho para a constatação, cada vez mais consistente e estruturada, que a informação constitui um factor de Poder de importância crescente, capaz de funcionar como elemento multiplicador do Potencial, condicionando a posição e o espaço estratégico que qualquer País pode atingir.

Estratégia da Informação Nacional: Enquadramento e Definição

A História tem vindo a provar que, sempre que surgem relações de conflito e se perspectiva a utilização da coacção, existe a necessidade de definição de uma Estratégia, fruto da dinâmica conflitual das relações sociais ou mesmo da actual evolução científico-tecnológica, como se tem vindo a demonstrar. No domínio do conflito, o conceito de Estratégia pode ser aplicado aos diferentes níveis de planeamento e condução dos meios utilizados para a sua resolução. No entanto, importa referir que todas as aplicações do termo, apesar de revelarem um mesmo sentido genérico, são claramente diferenciáveis nos instrumentos, cenários e formas de emprego dos meios, de modo a procurarem atingir os seus fins específicos.

Sendo a Estratégia Global[23] dos Estados tradicionalmente influenciada tanto por aspectos estruturais como conjunturais, onde a Teoria Geral dos Conflitos, a dinâmica das Relações Internacionais e até o pensamento Geopolítico e Geoestratégico exercem inevitável influência, é possível constatar que o ciberespaço toca todos estes domínios e interpenetra-os, dando-lhes uma nova dimensão num ambiente de informação global. Reflexo desta realidade, em consonância com a visão expressa pelo General Beaufre (1965), parece existir uma verdadeira "pirâmide de Estratégias distintas e interdependentes, que se torna necessário definir com clareza, para as combinar da melhor maneira num conjunto de acções que vise a mesma finalidade de conjunto" (Couto, 1988, p.227). Atendendo ao princípio de que a cada forma de coacção[24] corresponde uma Estratégia Geral[25], a utilização conflitual da informação como forma de coacção faz surgir uma nova Estratégia Geral, a Estratégia da Informação.

Conforme se procura evidenciar, a Estratégia da Informação apresenta características muito especiais, no âmbito da qual se desenvolve um tipo de conflitualidade específico (Guerra de Informação) mas a partir da qual também é possível influenciar as restantes Estratégias Gerais, uma vez que a informação constitui um recurso necessário ao desenvolvimento da acção estratégica nos domínios Diplomático/Político, Económico, Militar e Psicológico[26]. A Estratégia da Informação assume, assim, um papel determinante em todos os domínios da conflitualidade reflectindo-se ao nível da utilização dos sistemas de armas (Estratégia Militar), na globalização da Economia e das transacções digitais (Estratégia Económica), na influência que Media e ciberespaço detêm na gestão das percepções (domínio psicológico da própria Estratégia da Informação) e nas redes de influência social e diplomática criadas com base na Internet (Estratégia Diplomática/Política).

Enquadrada a Estratégia da Informação no âmbito das Estratégias do Estado, importa agora definir o objecto do nosso estudo. Assim, como uma das componentes da Estratégia Total e a esta subordinada, a Estratégia da Informação, pode ser definida como:

- A ciência[27] e a arte[28] de desenvolver capacidades e explorar o ambiente de informação[29], com vista à consecução dos objectivos fixados pela Política.

Quanto ao estilo ou modo de acção, podemos constatar que a Estratégia da Informação constitui o suporte para a condução tanto de uma Estratégia indirecta como directa. A Estratégia da Informação dá sentido à acção conduzida no plano material (físico), fornecendo-lhe um contexto e contribuindo para maximizar os seus efeitos, completando-a (**Francart, 2000)**. Ela própria é acção porque modela o ambiente da informação (não físico), tendo em vista a concretização/materialização da situação futura que se pretende obter, nomeadamente, antes, durante e após a ocorrência de uma crise ou conflito.

A Estratégia da Informação situa-se assim na charneira entre a concepção e a execução (nível das Estratégias Gerais). Pelo seu carácter transversal e pela natureza específica do tipo de conflitualidade envolvida, a Estratégia da Informação deve ser coordenada ao nível da Estratégia Total do Estado, sendo considerada uma das áreas prioritárias do planeamento e condução da sua acção estratégica. Atendendo à natureza dos meios empregues e aos diferentes sectores a que se dirige, é possível considerar a existência de duas Estratégias Particulares: uma Estratégia da Informação iminentemente militar e uma Estratégia da Informação iminentemente não-militar. Dentro deste contexto, são conduzidas respectivamente Operações de Informação (OI) de âmbito militar e civil, que procuramos enquadrar posteriormente de forma mais precisa.

O desenvolvimento da Estratégia da Informação Nacional passa, assim, pela definição dos seus aspectos operacionais (relacionados com a utilização dos recursos), genéticos (ligados à obtenção, geração e criação de novos meios) e estruturais (relativos à organização e articulação desses meios). De acordo com o objectivo proposto no âmbito deste estudo, a definição conceptual da Estratégia da Informação Nacional só faz sentido se perspectivarmos também o seu âmbito e a finalidade a atingir com a sua implementação.

Modelo de Implementação: Âmbito, Finalidade e Operacionalização

Contrariamente ao que defende a teoria "mecanicista" da informação[30] postulada por Hartley Shannon, a informação não deve ser só utilizada como aspecto residual no seu contexto (Waltz, 1998). Ela participa no próprio contexto, fá-lo evoluir e não se distingue da acção em geral, a não ser devido ao facto de visar directamente o plano das representações que permitem influenciar a nossa realidade. A informação, factor-chave para o processo de tomada de decisão aos vários níveis das Estratégias do Estado, pode ser representada como uma "info-esfera" que inclui o somatório de toda a informação proveniente das diversas fontes disponíveis. Dentro deste entendimento, é possível definir um processo de aquisição, protecção e exploração da informação (CFIOM,

1998)[31].

A Estratégia da Informação Nacional tem como âmbito a info-conflitualidade resultante das relações de competição e conflito geradas entre a nossa info-esfera, definida com base nos interesses nacionais, e a info-esfera de outros actores (Estado ou não-Estado). Atendendo ao âmbito da Estratégia da Informação, considera-se que esta pode apresentar três finalidades principais: Garantia da Informação (*Information Assurance*)[32], Superioridade da Informação (*Information Superiority*)[33] e Domínio da Informação (*Information Dominance*)[34]. Tendo por base as capacidades nacionais, consideramos que Portugal deve orientar a sua Estratégia da Informação de acordo com a prioridade de satisfação da primeira finalidade apresentada (curto prazo) e perspectivar a segunda (médio/longo prazo). Não se considera como objectivo realista o levantamento das capacidades necessárias à consecução da terceira finalidade (Domínio da Informação). Verifica-se, assim, que os domínios envolvidos no desenvolvimento de uma Estratégia da Informação, dependem essencialmente do ciclo de tomada de decisão das lideranças do País, das funções mobilizadas, dos meios técnicos utilizados, dos campos de acção e dos vectores do Poder que se pretendem explorar. No âmbito da condução da Estratégia definida, a identificação destes elementos é indispensável para assegurar uma atribuição coerente de responsabilidades. São os domínios de competência.

A lógica da confrontação dos interesses económicos, fez deslocar o epicentro da moderna conflitualidade do campo de aplicação estritamente militar para um campo de aplicação geoeconómico e transnacional (Toffler & Toffler, 1995). Neste âmbito, também se tem vindo a assistir à aplicação crescente das actividades de Guerra de Informação no âmbito não-militar, constituindo o *Echelon*[35] e o *Carnivore*[36], bons exemplos do que aqui se refere. A Guerra de Informação constitui, como verificamos, um conceito cuja abordagem se torna incontornável no contexto da Era da informação. Neste âmbito, reiterando uma ideia-chave antes expressa, arriscamos dizer que a competição no domínio da informação deve ser vista cada vez mais como excepção de uma situação de permanente conflito, onde se exige uma resposta concertada por parte de cada Estado. A Guerra de Informação pode assim desenvolver-se com base em diversas actividades específicas e permitir, ao Estado que melhor a conduzir, o domínio do ambiente de informação. Só a percepção das dinâmicas das actividades que afectam este domínio e o acompanhamento da evolução do conceito, nos diferentes Países e Forças Armadas do mundo, pode permitir o desenvolvimento de defesas mais eficazes.

O estudo dos conceitos e domínios de utilização das actividades ligadas à Guerra de Informação, assume assim uma especial importância para a construção do nosso quadro conceptual. Com o intuito de identificar que elementos doutrinários, estruturas, procedimentos e meios são utilizados para a operacionalização da Estratégia da Informação noutros países, analisou-se o modelo de enquadramento doutrinário da Guerra de Informação nos EUA, OTAN, Rússia e Alemanha, reflectindo o enquadramento

das OI desenvolvidas no seu âmbito. Adicionalmente, analisaram-se também os sistemas de protecção e segurança da infra-estrutura de informação dos EUA e da Suécia. Desta forma, foi possível enquadrar a utilização conflitual da informação e perspectivar a melhor forma de promover a realização do conjunto de actividades que permitem implementar a Estratégia da Informação no âmbito nacional. Tendo sido definida a Garantia da Informação como a finalidade primária a atingir, importa agora realizar o levantamento das actividades a desenvolver ao nível operacional para a sua consecução.

Como ponto comum das diferentes Doutrinas analisadas[37], podemos verificar que as OI, que materializam a condução da Estratégia da Informação, apresentam uma aplicação transversal. De acordo com os efeitos a atingir, este tipo de operações pode ser de âmbito Político-Estratégico, Estratégico-Militar ou Operacional. A conflitualidade da informação, na sua vertente táctica, materializa-se através da condução de acções de Guerra de Comando e Controlo.Com base no enquadramento doutrinário norte-americano e no modelo adoptado pela Suécia, também se considera que a Segurança da Informação Nacional só pode ser garantida através de um conceito alargado de Protecção da Infra-estrutura de Informação Crítica[38] e que a condução de OI defensivas é decisiva para garantir essa protecção. Partindo do princípio que existe, no contexto do actual ambiente estratégico e económico, uma natural sinergia entre as actividades de Guerra de Informação e a condução de OI, constata-se que, ao nível da sua implementação, a Estratégia da Informação Nacional apresenta duas componentes fundamentais: a condução de Operações de Informação e a Segurança da Informação Nacional.

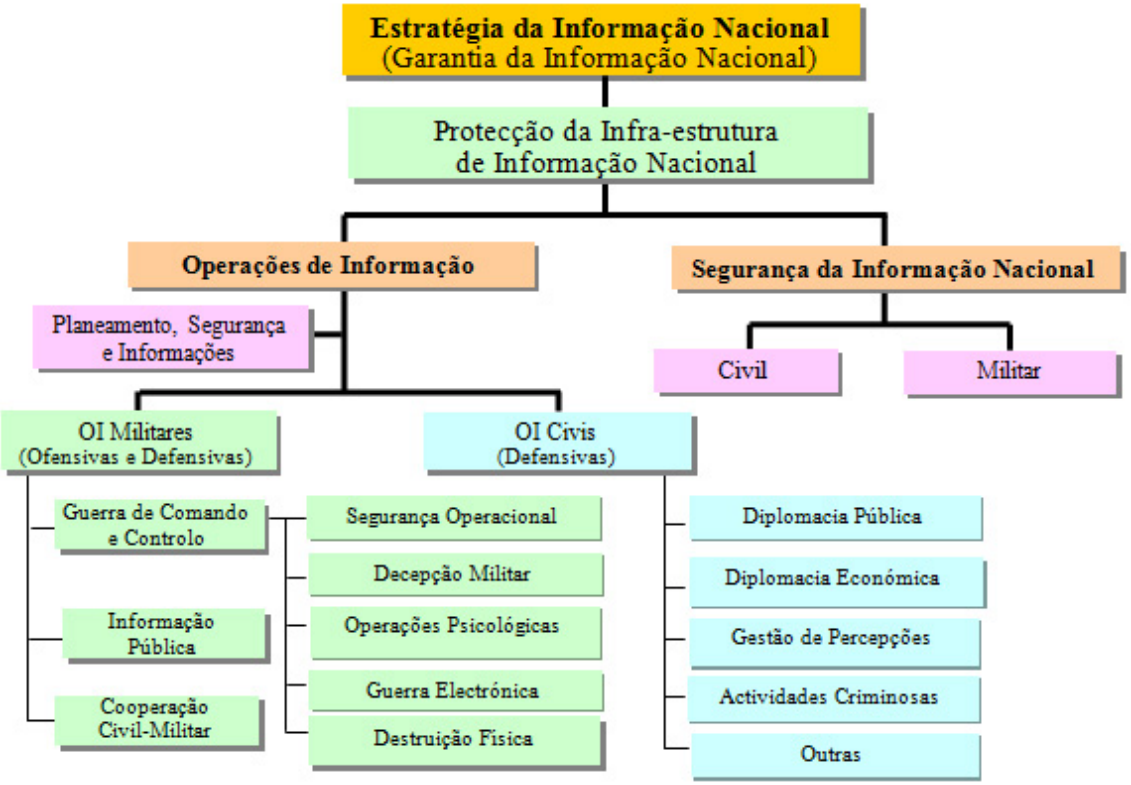

Figura 2 - Modelo de Implementação da Estratégia da Informação Nacional

Conforme se procura ilustrar na Figura 2, face à natureza dos meios empregues e aos diferentes sectores a que se dirige a Estratégia da Informação, são conduzidas respectivamente OI e actividades de Segurança das Infra-estruturas de Informação de âmbito civil e militar. Ainda que a fronteira entre o ambiente da informação civil e militar seja muito ténue, não podemos deixar de constatar que, se a Estratégia da Informação for desenvolvida em cada um destes contextos (nível das suas Estratégias Particulares), também as OI que a materializam (nível Operacional) podem ser do tipo civil ou militar. Face a este enquadramento e atendendo à transversalidade do domínio da informação, a Estratégia Militar conduz OI Militares (ofensivas e defensivas) e as restantes Estratégias Gerais, OI Civis (defensivas). As actividades de Planeamento, Segurança e de obtenção de Informações assumem também um papel importante para o sucesso de todos os tipos de OI, revelando-se essencial promover a sua correcta articulação civil-militar.

Resposta Estrutural

Os fundamentos do pensamento estratégico permitem definir sinergias e orientá-las no sentido da obtenção de uma resultante estrutural sustentada numa organização coerente, capaz de definir uma resposta articulada e pensada ao nível nacional. Procuramos assim delinear uma possível estrutura organizacional, susceptível de assegurar a condução operacional da Estratégia da Informação Nacional.

Os dados recolhidos da actual situação Portuguesa reflectem que a segurança dos sistemas de informação é por vezes ainda encarada como um conceito relativamente estático, muito associado à tradicional "guarda" da informação e dirigido à protecção hermética e institucional das diversas infra-estruturas de informação. Uma vez que existem diversas instituições e organizações que implementam autonomamente, e de forma por vezes desenquadrada, as suas Políticas de Segurança, não existe uma estrutura integradora e normalizadora de âmbito nacional[39]. Analisadas também as capacidades nacionais na área da condução de OI, constatou-se que, de momento, não existem estruturas e doutrinas operacionais vocacionadas para a condução de OI defensivas ao nível estratégico. A estrutura existente, não se revela por isso a mais adequada para garantir a Protecção da IIN, uma vez que não reflecte, de forma coerente e global, a adopção de mecanismos de protecção, nem introduz funções específicas no âmbito da prevenção, da detecção, da reacção e da dissuasão num ambiente de informação caracterizado por novas ameaças e riscos.

A Protecção da IIN apresenta desafios únicos para as entidades responsáveis pela Segurança Nacional, exigindo também soluções únicas e inovadoras. Existe assim um

forte argumento para o desenvolvimento de um Sistema de Protecção da Infra-estrutura de Informação Nacional (SPIIN) que, partindo de uma visão clara da situação actual e do conhecimento dos princípios orientadores do funcionamento do sistema, permita perspectivar o levantamento da sua estrutura organizacional. De acordo com esta orientação, considera-se que a estrutura do SPIIN pode ser criada com base no levantamento de uma Autoridade Nacional de Informação (ANI)[40], Células de Segurança e Operações de Informação (CSOI)[41], um Centro de Segurança e Operações de Informação Militares (CSOIM)[42], Órgãos Sectoriais de Alerta e Registo (OSAR)[43] e na colaboração e acção coordenada de Entidades e Organizações Públicas e Privadas que possam contribuir para a Protecção da IIN.

O SPIIN, consubstanciando a definição de uma estrutura de enquadramento, pode ser visto como uma aproximação holística ao problema. Tendo por base esta estrutura organizacional, assume especial importância a definição de doutrinas e processos que permitam assegurar a efectiva coordenação das acções envolvidas, tanto ao nível das actividades de Segurança da Informação como na área da condução das OI Civis e Militares. Podem assim evitar-se conflitos de interesses e estimular a cooperação, quer no âmbito nacional quer internacional, delimitando os problemas policiais dos que afectam a Segurança e Defesa Nacional. A resposta estrutural apresentada também exige a criação de legislação específica que, garantindo o difícil equilíbrio entre direitos individuais e responsabilidades institucionais, permita clarificar o objectivo, as atribuições e as competências dos diversos Órgãos da estrutura do SPIIN.

Resposta Genética

No quadro do Planeamento Estratégico, as decisões de investimento dos Estados traduzem escolhas entre diversas opções que, quando os recursos são limitados, se tornam por vezes mutuamente exclusivas. Decorrente das decisões políticas, a tradução destes investimentos nos seus diversos domínios de aplicação depende essencialmente da Estratégia adoptada e tem por base o estabelecimento criterioso de prioridades para o desenvolvimento de capacidades.

Inspirados por uma visão genética, associada à produção de novos equipamentos ou para a reconversão de outros que já existem, a maior parte dos processos de desenvolvimento de capacidades ou de geração de forças apresenta, numa fase inicial, tendência para adoptar uma aproximação essencialmente quantitativa. No entanto, no quadro das iniciativas analisadas (OTAN, UE, Reino Unido e EUA), a geração e o desenvolvimento de capacidades é já considerada no seu sentido mais lato, nomeadamente, é assumido que uma capacidade resulta do produto de três diferentes factores (Capacidade = Possibilidades x Meios x Vontade)[44].

Face às restrições e constrangimentos políticos, económicos e militares que caracterizam este tipo de iniciativas, parece existir vantagem em que Portugal articule os esforços a empreender no domínio do desenvolvimento de capacidades ligadas à Segurança e Defesa com aqueles que decorrem em paralelo em Organizações Internacionais de que o País faz parte. Neste contexto, faz sentido referir o desenvolvimento de capacidades (civis e militares) da UE[45] que, inspirado em alguns dos princípios seguidos pela OTAN, não apresenta um foco exclusivamente militar[46]. Considera-se assim que o processo de desenvolvimento de capacidades da UE pode constituir uma referência para a reflexão que nos propomos desenvolver uma vez que, mantendo o foco no domínio da Segurança e Defesa, permite perspectivar a implementação de uma Estratégia em vários domínios complementares das actividades do Estado. Aplicando este princípio ao contexto deste estudo, considera-se que a definição de uma resposta genética, enquanto elemento mais visível da forma como se pretende levantar a Estratégia da Informação Nacional, envolve um processo/mecanismo específico que se deve objectivar segundo um Plano de Desenvolvimento de Capacidades (PDC).

Sem a pretensão de traçar uma solução definitiva, antes procurando apresentar uma proposta credível ao desafio de levantar um PDC, importa agora caracterizar de forma sumária este processo/mecanismo. Explorando a experiência do autor, adquirida no âmbito do processo de desenvolvimento de capacidades da UE, considera-se especialmente importante que o PDC se estruture com base em três preocupações principais:
- determinação das necessidades no domínio da Protecção da IIN[47], de forma a garantir a salvaguarda dos interesses nacionais e satisfazer os compromissos internacionais assumidos por Portugal, no quadro do desenvolvimento de esforços cooperativos neste domínio;
- identificação e gestão das lacunas de capacidades existentes, com o objectivo de mitigar o risco social que se coloca ao País no domínio do ciberespaço em geral e no das ICN em particular;
- acompanhamento e avaliação periódica dos progressos efectuados, tanto no âmbito da gestão das lacunas de capacidades como do próprio processo de desenvolvimento de capacidades.

Tendo por fundamento as preocupações enunciadas, considera-se que o “ciclo” de desenvolvimento de capacidades a implementar pode ser genericamente ilustrado e explicado através da Figura 3. Conforme se observa, considerando o nível de ambição estratégica e as directivas/orientações estabelecidas neste âmbito, são identificadas as necessidades em termos das capacidades destinadas a garantir a Protecção da IIN. Com base na identificação global dessas necessidades, consolidada com as lições recolhidas da experiência operacional e pela análise das tendências de evolução futura de cada área de capacidades, é possível desenvolver um planeamento estratégico consistente. Tendo em atenção tanto os projectos actuais e planeados como as capacidades existentes, será

possível avaliar o impacto operacional das necessidades e identificar as lacunas de capacidades.

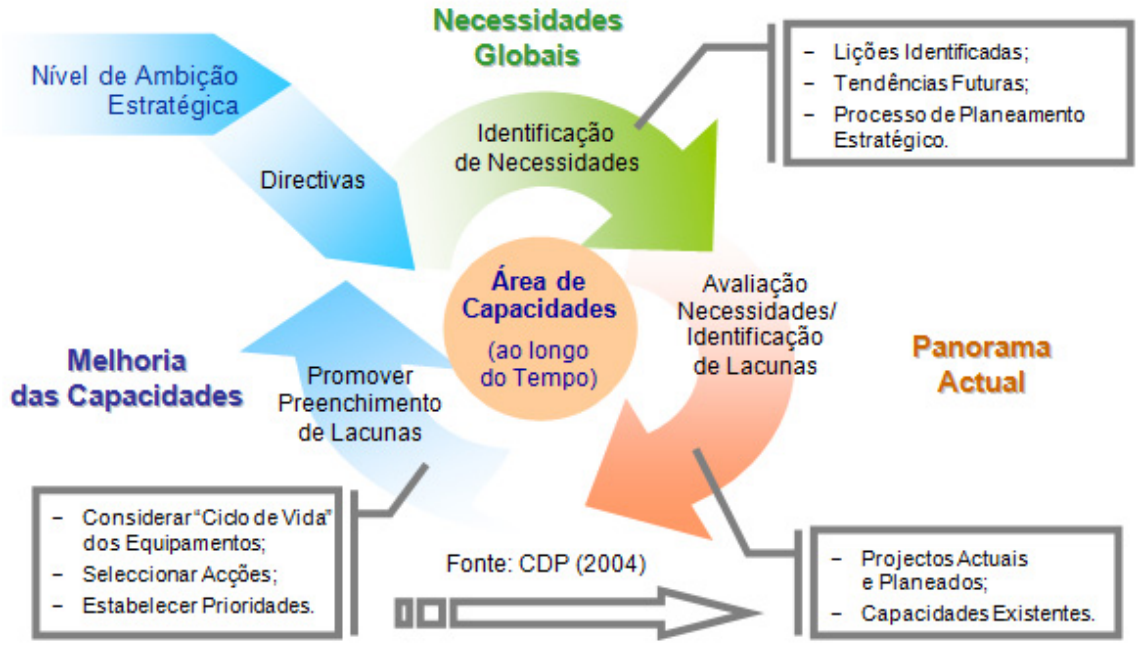

Figura 3 - Processo Genérico de Desenvolvimento de Capacidades

Caracterizada a situação e traçado o panorama actual, o passo seguinte é o de promover o preenchimento das lacunas, tendo em vista a melhoria das capacidades existentes. Para tal, torna-se necessário seleccionar acções e estabelecer prioridades, considerando o "ciclo de vida" dos equipamentos e outros factores (materiais e não materiais), não só a curto mas também a médio e longo prazo. Estas acções vão influenciar a situação actual e as capacidades existentes, realimentando o "ciclo de desenvolvimento de capacidades" com novos dados de planeamento que, inevitavelmente, acabam também por influenciar as tarefas a desenvolver no âmbito operacional. O PDC, encontrando-se alinhado com a Estratégia da Informação Nacional, vai permitir enquadrar e dirigir o esforço colectivo de desenvolvimento de capacidades de forma estruturada, identificar oportunidades de cooperação, orientar tanto as actividades de Investigação e Desenvolvimento (I&D) apoiadas pelo Estado como as desenvolvidas pela própria Indústria Nacional, fornecendo métricas que permitam avaliar o progresso relativo de todo o processo.

Aplicação e Validação do Modelo

Sentindo o autor a importância de criar um processo de validação da forma como se procuraram perspectivar e edificar as diversas componentes da Estratégia da Informação Nacional, decidiu-se ir um pouco mais longe e "fechar o ciclo" através da sua aplicação a

situações o mais realistas possível. Tendo em mente este desafio, com o objectivo de avaliar a coerência e validade da sua implementação, optou-se pela aplicação dos fundamentos e princípios enformadores desta Estratégia no contexto de um Exercício de Gestão de Crises no Ciberespaço[48].

Promovendo a adaptação e exploração de ferramentas de análise e apoio ao planeamento, o Exercício incluiu uma fase prévia de construção de cenários e de análise do risco social associado ao ciberespaço, explorando para esse efeito a ferramenta de análise morfológica antes apresentada. Para além da informação referente aos princípios de elaboração de cenários e à forma como são planeados e executados este tipo de Exercícios, os participantes receberam um enquadramento teórico relativamente à forma como se desenvolve o processo de gestão de crises no âmbito da OTAN e UE. No contexto da preparação do Exercício foi também incluída uma ferramenta adicional de análise dos actores do cenário (incluindo a determinação dos seus Centros de Gravidade) e uma ferramenta de apoio ao planeamento de Operações Baseadas em Efeitos (OBE). Explorando na caracterização dos actores os fundamentos das OBE, procurou-se associar estas duas ferramentas de forma a criar as condições necessárias ao planeamento integrado de OI ao mais alto nível (Estratégico/Operacional).

Antes de se passar à execução do Exercício, procurou-se ainda obter a percepção do impacto que a decisão em rede pode ter na condução das operações planeadas. Nesse sentido, para além dos fundamentos teóricos das Operações Centradas em Rede transmitidos aos participantes, foi planeada a utilização de uma ferramenta computacional (ELICIT[49]) que permitisse simular a interacção e o processo de decisão em rede[50].

Para que seja possível caracterizar com clareza o enquadramento da aplicação do modelo de Estratégia desenvolvido, importa agora detalhar as duas fases associadas à execução do Exercício. Entendendo a 1ª fase do Exercício como a fase da "tomada de consciência" das implicações e dos diferentes aspectos ligados ao surgimento e à gestão de uma crise no ciberespaço, a 2ª fase constituiu essencialmente a fase do "realismo e do pragmatismo" consubstanciando aquela onde tem lugar a formulação de uma visão Política/Estratégica relativa à forma como se pode mitigar o risco social no ciberespaço.

Tendo por base o conjunto de acções a desenvolver no curto prazo, destinadas essencialmente a limitar os efeitos dos ataques/incidentes registados, no final da 1ª Fase foi possível identificar algumas das áreas críticas onde intervir e clarificar os aspectos operacionais das capacidades a activar. No âmbito das áreas críticas onde intervir, foi identificada a necessidade de isolar sistemas críticos, detectar a ocorrência de ataques/situações anómalas e de criar uma Infra-estrutura de Informação Crítica Mínima. Na 2ª Fase do Exercício, reflectindo um conjunto de opções Políticas/Estratégicas a

explorar no futuro, foram registadas diversas propostas de iniciativas de I&D a lançar no longo-prazo. Estas propostas, centraram-se essencialmente na redução das vulnerabilidades nacionais e no aumento da segurança da exploração do ciberespaço.

Atendendo à forma como decorreu a execução do Exercício e aos resultados que foi possível recolher no seu final, constatou-se que a fase de preparação constituiu um elemento fundamental para a concretização dos objectivos propostos. Muitas das ideias e valiosos contributos, consubstanciados em propostas inovadoras recebidas na fase conclusiva do Exercício, apontaram também para a mais-valia de ter sido possível conjugar os vários elementos/instrumentos do Poder dos Estados no processo de planeamento. Segundo a lógica expressa nestes comentários, a sistematização das ideias aqui apresentadas pode ser explorada na estruturação de um "Exercício Nacional de Gestão de Crises no Ciberespaço".

Conclusões

As infra-estruturas de informação e o ciberespaço são reconhecidamente indispensáveis para a vida da "Sociedade de Informação". O seu correcto funcionamento assume importância vital para a livre circulação da informação e para os processos e serviços dependentes desse fluxo. Não sendo a IIN absolutamente segura, pode ser alvo de ataques que procuram explorar as vulnerabilidades e insuficiências estruturais existentes, facto que impõe a necessidade de assegurar a sua protecção e defesa. As melhores práticas ao nível da cibersegurança e a adopção eficaz dos princípios da ciberdefesa, obrigam as organizações e os Estados a estabelecer mecanismos de protecção, aconselhando a que esta seja encarada segundo uma perspectiva de gestão do risco social: protecção, detecção e reacção.

O ciberespaço, enquanto espaço de defesa de interesses, impõe novas formas de interacção e de relacionamento entre as Unidades Políticas. As estratégias prosseguidas centram-se no valor dos recursos de informação e em operações destinadas a afectar esse valor, onde se privilegia o princípio da economia de meios e a acção indirecta. Estamos perante uma situação paradigmática da relação bem-estar/desenvolvimento e segurança das sociedades onde um mundo sem fronteiras como o ciberespaço cria tantas oportunidades como riscos. A percepção de que os processos e mecanismos de segurança existentes dificilmente acompanham a dinâmica das vulnerabilidades, levanta a necessidade de uma forte sensibilização nacional para a importância da defesa e protecção das infra-estruturas e recursos de informação nacionais, obrigando a uma revisão dos actuais conceitos de Segurança e Defesa.

Ainda que relativamente complexa na sua concepção e planeamento, não será possível ignorar a necessidade de uma Estratégia da Informação Nacional, sob pena de, no

quadro das relações internacionais, Portugal correr o risco de ser remetido para um papel de mero executante das Estratégias ditadas pelas Nações lideres neste domínio, ou, no quadro de um empenhamento bilateral ou nacional, das organizações que desenvolvem actividades de Guerra de Informação.

Para além da premência e urgência de que se reveste a definição da Estratégia da Informação Nacional, importa referir que esta só fará sentido se perspectivarmos de forma articulada os seus aspectos operacionais, uma estrutura organizacional e o conjunto de capacidades que se lhe encontram associadas. Para o levantamento desta Estratégia, torna-se ainda necessária a revisão e actualização do actual quadro legal, nomeadamente, no que diz respeito à utilização conflitual da informação. Dentro deste contexto, deve ser criado e institucionalizado um SPIIN, onde importa clarificar, nomeadamente, as responsabilidades e atribuições das Forças Armadas e das Forças de Segurança. Existindo uma intenção genuína de assumir o compromisso de garantir a Segurança Nacional no ciberespaço, este é um passo que, em nosso entender, deve ser dado o mais rapidamente possível.

Finalmente, assumindo que lidamos com mundos virtuais onde os riscos se revelam reais, importa chamar à atenção para os extraordinários benefícios sociais e culturais associados ao ciberespaço, referindo que é preciso ver além dos perigos emergentes da Era da informação e perceber que, eventualmente, o levantamento de uma Estratégia é apenas um degrau do caminho a percorrer, quiçá talvez não o mais importante. Desta forma, sem descurar o Interesse Nacional, ao invés de promover uma visão meramente securitária e isolacionista, justificada pelo aumento dos riscos sociais e pelo receio de comprometer a Segurança Nacional, importa sobretudo aproveitar a oportunidade para explorar a existência de uma rede global e, de forma informada e consciente, alavancar a modernização e promover o desenvolvimento nacional. A conectividade e a virtualização do real, que permitem perspectivar a emergência de uma rede semântica e cognitiva, desde que acompanhadas por uma consciência colectiva dos riscos emergentes, conduzem-nos inevitavelmente para o próximo patamar civilizacional, em que todos e cada um de nós desempenhará, como nunca antes, um papel activo.

Referências Bibliográficas

Alves, José (1998). *Estratégia - Panorama Geral e sua Teoria*, Publicações Dom Quixote, Lisboa. Beaufre, Andre (1965). *Introduction a la Stratégie.* Librarie Armand Colin, Paris. Bispo, António (2002). *A Sociedade de Informação e a Segurança Nacional*. Instituto Português da Conjuntura Estratégica, Lisboa. Caetano, Paulo e Garcia, Rita (2003). "Portugueses em Perigo", em *Revista FOCUS*, 27Ago03, pp.96-100. CDP (2004). "*Capability Development Plan"*, Documento da União Europeia, Bruxelas, 01Mar04. CFIOM (1998). "*Canadian Forces Information Operations Manual",* Documento Doutrinário do Estado Maior de Defesa do Canadá, B-GG-005-004/AF-010, 14 de Abril.

Couto, Abel (1988). *Elementos de Estratégia - Apontamentos para um Curso,* Volume I, IAEM, Lisboa. Denning, Dorothy (2000). *Activism, Hacktivism and Cyberterrorism: The Internet as Tool for Influencing Foreign Policy*, Nautilus Institute. Dias, Carlos (2005). *Geopolítica: Teorização Clássica e Ensinamentos,* Editora Prefácio, Lisboa. Douhet, Giulio, (1942). *The Command of the Air,* tradução de Dino Ferrari (nova reimpressão, Washington, D.C.: Office of the Air Force History, 1983). Galeano, Ernesto (1997). *Modelos de Comunicacion*, Edições MACCHI, 2ª Edição, Buenos Aires. GibsoN, William (1984). *Neuromancer*, Ace Brooks, Canadá. Herzfeld, Charles (1999). "The Defence of Infrastructure", em *Information Impacts Magazine*, Setembro. IAEM (1999). *Elementos de Análise Geopolítica e Geoestratégica,* ME 71-00-08, Edições do Instituto de Altos Estudos Militares, Lisboa. Lewis, James (2002). "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", Artigo do *Center for Strategic and International Studies (CSIS),* Washington D.C., Dezembro. Libicki, Martin (1995). "*What is Information Warfare?*", National Defense University Press, Washington D.C. Manso, Marco e Nunes, Paulo (2008). "*ELICIT and the Future C2: Theoretical Foundations for the Analysis of ELICIT Experiments*"", Student Paper in 13th International Command and Control Research and Technology Symposium: C2 for Complex Endeavors", Seattle, 17-19 Junho. Negroponte, Nicholas (1996). *Ser Digital*, Editorial Caminho, Lisboa. Nunes, Paulo (2003). "A Geopolítica do Ciberespaço", Número Especial da *Revista Militar* subordinado ao tema "Guerra na Idade da Informação", Outubro, Lisboa. Nunes, Paulo (2004). "A Conflitualidade da Informação: da Guerra de Informação à Estratégia da Informação", TILD do CEM 2002/04, *Boletim do Instituto de Altos Estudos Militares*, Maio, Pedrouços. Santos, Loureiro dos (2001). *Segurança e Defesa na Viragem do Milénio: Reflexões sobre Estratégia II,* Publicações Europa-América, Mem Martins. Toffler, Alvin (1991). *The Third Wave*, New York Bantam Books, New York. Toffler, Alvin e Toffler, Heidi (1995). *War and anti-War*: *Survival at the Dawn of the 21 Century*, Warner Books, New York. Tzu, Sun (1993). *A Arte da Guerra*, Publicações Europa-América, 2ª Edição, Mem Martins. Waltz, Edward (1998). *Information Warfare: Principles and Operations*, Artech House.

Referências Electrónicas

AC (2010). *An Atlas of Cyberspaces,* em http://www.cybergeography.org/atlas/, 14Mai10/22H12. Anderson, R. et al (1999). *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*, Relatório MR-993, RAND, em http://www.rand.org/publications/MR/MR993, 04Set03/15H45. Brito, Paula (2009). "Portugal é o terceiro país da Europa nas redes sociais", em edição do Diário de Notícias de 22 Fev09, em http://dn.sapo.pt/inicio/tv/interior.aspx?content_id=1151669, 23Fev09/16H15. CEL (2000). "*Definição da Estratégia de Lisboa",* Conclusões da Presidência do Conselho Europeu de Lisboa, em http://www.eurocid.pt/pls/wsd/wsdwcot0.detalhe?p_cot_id=968&p_est_id=2654, 15Jun08/11H55. EB (2010). Versão electrónica da *Enciclopédia Britânica*, em http://www.britannica.com/, 13Mai10/11H40. FM 100-6, (1996). *Information Operations*, Documento Doutrinário do Exército dos EUA, 27Ago, disponível em http://www.jya.com/fm100/fm100-6.htm**, 15Set05**/10H50. Francart**, Loup (2000).** ***La Maitrise de l'Information,*** Artigo de Site Francês sobre Guerra de Informação, em www.Infoguerre.com, 23Fev10/16H38. ISOC (2010). Site da Internet Society, em

http://www.isoc.org, 18Mai10/22H50. **JP 3-**13 **(2006). *"Joint Doctrine for Information Operations Publication"*, Joint Chiefs of Staff, em** http://www.carlisle.army.mil/DIME/documents/jp3_13.pdf**, 25Jan10/0H55.** Luiijf, Ir et al. (2003). *In Bits and Pieces,* Estudo sobre a vulnerabilidade da Infra-estrutura de Informação e Comunicações da Holanda e as suas consequências para a Sociedade da Informação, INFODROME, em http://www.infodrome.nl/, 02Set2003/15H35. Morris, Chris et al. (1995). "*Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos"*, *Airpower Journal*, Primavera, em http://www.cdsar.af.mil/air-chronicles.html, 18Mai03/19H34. NSHS (2002). "*National Strategy for Homeland Security,* White House Office of Homeland Security, em http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf, 03Set03/09H47. NSSC (2003). "*National Strategy to Secure Cyberspace",* White House Office of Homeland Security, Janeiro, em http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf, 03Set03/09H50. POSI (2005). Programa Operacional para a Sociedade da Informação, em http://www.posi.pcm.gov.pt/documentos/pdf/, 20Jan05/17H10. PT (2008). Documento de Apresentação do *Plano Tecnológico (PT)*, em http://www.planotecnologico.pt/document/OPlanoTecnologico.pdf, 11Mai08/12H30.

---

* Comunicação apresentada no I Congresso Nacional de Segurança e Defesa (24-25 Junho 2010).

** Tenente-coronel de Transmissões. Chefe da Repartição de Sistemas e Tecnologias de Informação da DivCSI/EME. Sócio Efectivo da Revista Militar.

[1] Como exemplo, refere-se que Portugal é hoje o terceiro País da Europa no *ranking* dos utilizadores de Redes Sociais com 2,5 milhões de aderentes - 84,4% do total de utilizadores nacionais (Brito, 2009). Redes Sociais como o *Facebook*, *HI5*, *Twitter* ou *Netlog*, têm elevadas taxas de utilização.
[2] De acordo com esta perspectiva, se tomarmos a rede telefónica como exemplo, verificamos que por cada novo subscritor que adere à rede, esta, para além de aumentar o seu número de assinantes, torna-se mais atractiva em relação a novos subscritores uma vez que lhes permitirá ligarem-se a mais pessoas. A mecânica deste efeito de "bola de neve", esteve na base do processo de expansão da rede telefónica e, eventualmente, do da maior parte das redes e sistemas de comunicações actuais de que a Internet poderá certamente ser considerada um dos casos de maior sucesso.
[3] De acordo com a Enciclopédia Britânica (EB, 2010), a Geografia "descreve e analisa a variação espacial dos fenómenos físicos, biológicos e humanos que ocorrem na superfície do globo e avalia as suas interrelações e padrões regionais mais significativos".
[4] A Geopolítica pode ser definida como o "estudo das constantes e das variáveis do espaço acessível ao Homem que, ao objectivarem-se na construção de modelos de

dinâmica do Poder, projectam o conhecimento geográfico na actividade da Ciência Política" (IAEM, 1999, p.61).

[5] A palavra "ciberespaço" surge da aglutinação dos termos "cibernética" e "espaço". Avançada inicialmente pelo escritor canadiano William Gibson, no seu livro "Neuromencer" (1984), a sua utilização viria a generalizar-se para descrever o espaço virtual associado à Internet.

[6] Estes materializam os objectivos teleológicos do Estado, constituindo os seus fins últimos e a razão de ser do próprio Estado.

[7] A IIG é muitas vezes vista como incluindo a Internet e as infra-estruturas de informação dos diversos Países (JP 3-13, 2006, p.GL-8).

[8] Poderemos encarar esta infra-estrutura como um simples conjunto de sistemas independentes, integrados e interoperáveis (Herzfeld, 1999).

[9] Os cortes prolongados de energia eléctrica, ocorridos nos EUA, Canadá, Reino Unido e Itália, durante os meses de Agosto e Setembro de 2003, conduziram a uma indisponibilidade prolongada das infra-estruturas críticas destes países.

[10] Em muitos casos, as infra-estruturas críticas (incluindo a IIN) apresentam ainda dependências horizontais e/ou verticais, formando cadeias de infra-estruturas vitais. Uma cadeia de dependências deste tipo, pode produzir um "efeito de dominó", de consequências não previsiveis, em que a ruptura de uma infra-estrutura pode estender-se a outras de forma sequencial e quase imediata.

[11] A "vulnerabilidade social", que aqui se procura identificar, pode ser definida como a "susceptibilidade do funcionamento da Sociedade relativamente à falha de determinadas funções específicas" (Luiijf, 2003). Apesar de ser obrigatório garantir a sua disponibilidade, se pretendermos analisar a vulnerabilidade de sistemas e infra-estruturas críticas, terá que se equacionar também a sua capacidade de sobrevivência. Dentro deste contexto, a sobrevivência de um sistema ou infra-estrutura pode ser vista como a capacidade de restabelecer a sua disponibilidade em condições extremas (falhas graves).

[12] A dimensão do risco está ligada ao valor/dependência que um actor apresenta e às consequências negativas que a não disponibilidade de um recurso pode implicar. Segundo alguns autores, é possível determinar o risco através de métodos qualitativos/quantitativos que permitem a sua avaliação, podendo a sua quantificação ser realizada através da seguinte expressão: R= (A.V/ Ms).I, onde: R é o valor do risco, A é o valor da ameaça, V é o valor da vulnerabilidade, Ms é o valor da medida de salvaguarda e I é o valor do impacto previsto (Bispo, 2002).

[13] De acordo com os objectivos traçados na Estratégia de Lisboa (CEL, 2000), vertidos no Programa Operacional para a Sociedade de Informação (POSI, 2005) e mais recentemente reforçados no âmbito do Plano Tecnológico (PT, 2008).

[14] No rescaldo da 1ª Grande Guerra, o General Giulio Douhet sugeria já que a solução para obter a vitória em futuros conflitos, teria de passar pela exploração de uma superioridade tecnológica antes que o oponente pudesse responder: "A Vitória sorri aqueles que anteciparem as alterações dos princípios de condução da guerra, não aos que aguardam para se poderem adaptar às alterações que entretanto vierem a ocorrer" (Douhet, 1942, p.30). Ainda que alguns responsáveis pelo planeamento militar contemporâneo tenham ignorado os princípios enunciados por Giulio Douhet, o seu

contributo para o estudo do fenómeno da guerra tem sido notório na introdução dos seus ensinamentos nas bases do planeamento da estratégia militar dos Estados Unidos ao longo dos últimos anos.

[15] O Major-general Hugh Trenchard ajudou a fundar e comandou a Royal Air Force durante a 1ª Guerra Mundial. Trenchard, foi um fervoroso defensor do bombardeamento estratégico, organizando diversos ataques aéreos aos caminhos-de-ferro e centros industriais da Alemanha.

[16] Face à intangibilidade dos dados que materializam a informação, a maior parte das acções desenvolvidas no âmbito da guerra baseada na informação são do tipo não violento, não implicando, na maior parte dos casos, a necessidade de utilização de armas de destruição física.

[17] O conceito que aqui se apresenta é deduzido a partir da definição apresentada no FM 100-6 (1996, p.GL-8). Esta publicação, define Guerra de Informação como "as acções desenvolvidas para obter a superioridade de informação, afectando a informação, processos baseados em informação, sistemas de informação e redes baseadas em computadores de um adversário enquanto se defendem os nossos sistemas afins".

[18] A Análise Morfológica foi desenvolvida pelo suiço Fritz Zwicky (1898-1974). Constituindo uma técnica de raciocínio orientada para a resolução de problemas multidimensionais e não quantificáveis, este método é especialmente utilizado em casos onde os tradicionais processos de modelação e de simulação não funcionam ou não podem ser directamente aplicados. Utilizando uma matriz, onde são representados os valores das variáveis independentes do problema, Zwicky concluiu que é possível reduzir a complexidade sem reduzir o número de variáveis envolvidas. Desta forma, reduz-se o número de soluções possíveis através da eliminação de combinações de soluções ilógicas para o problema.

[19] Esta ferramenta, revelou-se particularmente útil tanto para apoiar a revisão e validação da metodologia seguida, como para a preparação do Exercício de Gestão de Crises no Ciberespaço que a Academia Militar conduz anualmente no âmbito do Curso de Pós-Graduação/Mestrado em Guerra de Informação/*Competitive Intelligence*.

[20] Ainda que segundo os princípios do Direito Internacional todos os Estados sejam iguais (igualdade de jure), na prática estes apresentam uma capacidade (Poder) diferente para promover a satisfação dos seus interesses. Existe, na realidade, uma desigualdade "de facto" entre os diversos Estados, reflexo da sua capacidade de criação e projecção de Poder na cena internacional.

[21] O Potencial Estratégico pode ser definido como "o conjunto das Forças Materiais e Morais de qualquer natureza que um Estado ou Coligação pode utilizar na sua Acção Estratégica" (Alves, 1998, p. 131).

[22] Neste âmbito, o Poder não deve ser considerado absoluto, apenas potencial, revelando-se sempre subjectiva a sua aplicação.

[23] Quando falamos em Estratégia Global, estamos a referir-nos ao emprego coordenado de todos os instrumentos do Poder Nacional, com o objectivo de alcançar os efeitos políticos pretendidos através da manobra Político-Estratégica, planificada e conduzida ao mais alto nível. Surge desta forma reforçada a subordinação da Estratégia à Política, decorrente da sequência lógica do processo de decisão/governação do Estado.

[24] As formas de coacção relacionam-se com "os recursos e capacidades

operacionalmente disponíveis", podendo ser exercidas de acordo com os meios empregues e não com os efeitos obtidos (Couto, 1988).

[25] O General André Beaufre (1965) sistematizou o conceito de Estratégia Global, definindo-o como Estratégia Total e agrupando todos os instrumentos de acção política do Estado em campos/áreas afins, de forma a facilitar a sua condução. A estas diferentes áreas, Beaufre atribui a designação de Estratégias Gerais, diferenciando-as em diferentes campos de acção: Interno (Político), Externo (Diplomático), Psicológico, Económico e Militar.

[26] Com a criação de uma Estratégia da Informação, a acção estratégica no domínio psicológico tende a ser integrada no conjunto das actividades conduzidas no domínio da informação. Desta forma, a concepção autónoma de uma Estratégia Psicológica perde significado.

[27] Relacionada com os aspectos tangíveis, metodológicos e científicos da utilização da informação.

[28] Essencialmente ligada aos aspectos intangíveis da utilização da informação. Dentro deste âmbito, não poderemos deixar de referir a importância crescente da gestão das percepções no contexto da conflitualidade da informação, facto que justifica plenamente a importância dos aspectos empíricos, intuitivos e emocionais contidos neste termo.

[29] A informação assume, dentro deste contexto, o duplo papel de recurso/alvo e de arma.

[30] Shannon e Weaver lançaram em 1948 uma Teoria Matemática da Comunicação, pensada em função da Cibernética, área científica que materializa o estudo do funcionamento das máquinas electrónicas. A informação, segundo Shannon, constitui uma unidade quantificável que não tem em conta o conteúdo da mensagem (Galeano, 1997, p.23).

[31] A aquisição da informação constitui o processo através do qual a nossa "info-esfera" procura captar tanto a informação amiga como a de eventuais adversários. A protecção da informação materializa o processo que permite garantir a segurança deste ambiente, quer face a um adversário declarado, quer face a entidades consideradas amigas ou neutrais. Finalmente, a exploração da informação constitui o processo através do qual a informação é apresentada ao decisor, servindo de base ao seu processo de tomada de decisão.

[32] Neste âmbito, o principal desafio que os Estados e a generalidade das organizações têm que enfrentar é a protecção da sua infra-estrutura de informação (JP 3-13, 2006, p.GL-9). Este desiderato requer tanto a implementação de mecanismos de Segurança como de Defesa da IIN.

[33] Uma vez garantida a disponibilidade e a integridade dos sistemas de informação de um Estado, uma opção futura que se coloca é a expansão da sua info-esfera de influência em direcção a outros ambientes mais alargados, dentro dos quais a organização ou o Estado pretende intervir (JP 3-13, 2006, p.GL-9).

[34] Após estabelecido um certo grau de superioridade no ambiente de informação, um actor estará em posição para lançar uma campanha orientada para a obtenção de uma vantagem operacional, se assim o desejar. A condução com sucesso desta campanha requer o domínio do ambiente de informação adversário por aqueles que necessitem dessa informação (FM 100-6, 1996, p.GL-7).

[35] O *Echelon* constitui uma rede cooperativa de intercepção e vigilância de

comunicações, unindo Agências dos EUA, Canadá, Reino Unido, Austrália e Nova Zelândia. Nascido durante o período da Guerra-Fria, com o intuito de identificar e interceptar as comunicações do antigo Pacto de Varsóvia, este sistema continuou a funcionar mesmo após a queda do Muro de Berlim. Em Outubro de 2000, o Echelon foi alvo de uma investigação conduzida por uma comissão de inquérito do Parlamento Europeu (presidida pelo Eurodeputado Carlos Coelho), tendo sido provado que este sistema foi utilizado para conduzir acções de espionagem sobre empresas europeias.

[36] O *Carnivore* constitui um sistema de vigilância electrónica utilizado pelo FBI para identificar e interceptar comunicações via Internet. Este sistema possibilita não só a análise de endereços visitados como também a análise de conteúdos.

[37] O motivo que nos levou a escolher estes Países e Organizações Internacionais como objecto de análise, prende-se com o facto de estes revelarem uma maior maturidade conceptual e doutrinária, razão que os permite eleger como referência incontornável nos domínios de estudo identificados. A comparação das Doutrinas de diferentes países que realizámos permitiu deduzir um modelo de aplicação à realidade Portuguesa.

[38] Neste contexto, a Protecção da Infra-estrutura de Informação Nacional pode ser entendida como o conjunto de actividades que permitem assegurar a Garantia da Informação do Estado face a acções hostis desenvolvidas tanto no interior como no exterior do País. As OI e a Segurança da Informação Nacional constituem os mecanismos que determinam a Protecção da IIN.

[39] Ainda que a Fundação para a Computação Científica Nacional (FCCN) assuma já algumas das funções atribuídas a um *Computer Emergency Response Team* (CERT) Nacional como sejam a gestão de endereços de rede (domínio.pt), a implementação de Políticas de Segurança e o desenvolvimento de acções de sensibilização para a necessidade de garantir a protecção das redes e sistemas de informação nacionais, esta Fundação possui uma capacidade limitada para articular uma reacção ajustada a todo o espectro de ameaças e, assim, puder afirmar-se como um factor dissuasor de potenciais ciberataques de larga escala à IIN.

[40] Face à transversalidade das implicações da Protecção da IIN e à necessidade de garantir a coordenação e unidade dos objectivos políticos a atingir, julgamos que este Órgão deverá ser colocado na directa dependência hierárquica do 1º Ministro. Para conduzir as suas actividades, a ANI deve integrar os seguintes órgãos: Um Centro de Planeamento e Coordenação (CPC), um Centro de Operações (COp), um Centro Nacional de Alerta e Registo (CNAR), um Gabinete Técnico e Equipas Independentes Especializadas (*Red Teams*).

[41] Considera-se desejável a existência de uma CSOI em cada Ministério que, sendo constituída por um núcleo de especialistas em segurança da informação e em OI, através de uma acção coordenada, facilite o alerta e registo de incidentes e a condução de OI civis. As CSOI, devem ser colocadas na directa dependência dos Ministros com assento no Conselho Nacional de Planeamento Civil de Emergência (CNPCE), exceptuando o caso do Ministro da Defesa em que esta Célula é substituída por um outro Órgão com funções mais específicas.

[42] Este Centro deve ser colocado na dependência do Ministro da Defesa Nacional. Face à especificidade das OI Militares, a Célula responsável pela Segurança da Informação e pela coordenação das OI com os outros Ministérios, deve ser substituída por um Centro

de Operações de Informação Militares que, mantendo essas atribuições, possua também responsabilidades ao nível do planeamento e condução das OI Militares. Este Órgão deve manter uma forte dependência funcional ao mais alto nível hierárquico das Forças Armadas, ou seja, ao nível do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA). O Director do CSOIM pode, dentro deste contexto, ser designado por Autoridade de Informação Militar.

[43] Situado na dependência das diversas CSOI e do CSOIM, este Órgão funciona como CERT Sectorial, comunicando ao Centro Nacional de Alerta e Registo (CERT Nacional) indicações e alertas de nível táctico, informações sobre a ameaça e dados sobre a situação corrente.

[44] Desta forma, constata-se que o levantamento de uma Capacidade deve ter em conta as possibilidades de resolução de determinado problema/tarefa, os meios disponíveis, e, até a própria vontade para realizar/desenvolver uma acção nesse sentido.

[45] No âmbito da definição de uma Política Europeia de Segurança e Defesa (PESD), o Conselho Europeu definiu em Junho de 2004 o "*Headline Goal 2010 (HG 2010)*", estabelecendo os fundamentos e os objectivos estratégicos a atingir com o desenvolvimento de uma futura capacidade militar conjunta da UE. Mais recentemente, esta iniciativa conheceu também a sua versão "não militar" com a definição de um *Headline Goal* Civil em Novembro de 2007. Apresentando grandes semelhanças com o esforço desenvolvido na área militar, esta iniciativa poderá vir a aproximar estes dois domínios e a contribuir no futuro para uma visão estratégica integrada do desenvolvimento de capacidades.

[46] Na UE é evidente a influência transversal das áreas Político/Diplomática, Económica e até da própria Sociedade de Informação neste processo.

[47] Conforme referido anteriormente, a Protecção da IIN permite assegurar a Garantia da Informação, identificada como materializando o objectivo a atingir pela Estratégia da Informação Nacional no curto prazo.

[48] Para este efeito, tendo por base o trabalho desenvolvido pela Academia Militar no âmbito da sua Pós-Graduação/Mestrado em Guerra de Informação/*Competitive Intelligence,* foi utilizada uma adaptação do Exercício "*Day After in … Cyberspace*" (da *RAND Corporation* dos EUA), onde o ciberespaço e as acções de Guerra de Informação assumem um papel central.

[49] O Projecto *Experimental Laboratory for Investigating Collaboration, Information-sharing and Trust (ELICIT)* foi desenvolvido para investigar o impacto cognitivo e social da adopção de diferentes estruturas organizacionais e de diferentes aproximações à tomada de decisão.

[50] Apesar de até ao momento ainda não ter sido possível adaptar e integrar este tipo de ferramentas no Exercício "O Dia seguinte … no Ciberespaço", está já prevista a criação de um desenvolvimento aplicacional especialmente orientado para esse efeito (Manso & Nunes, 2008).