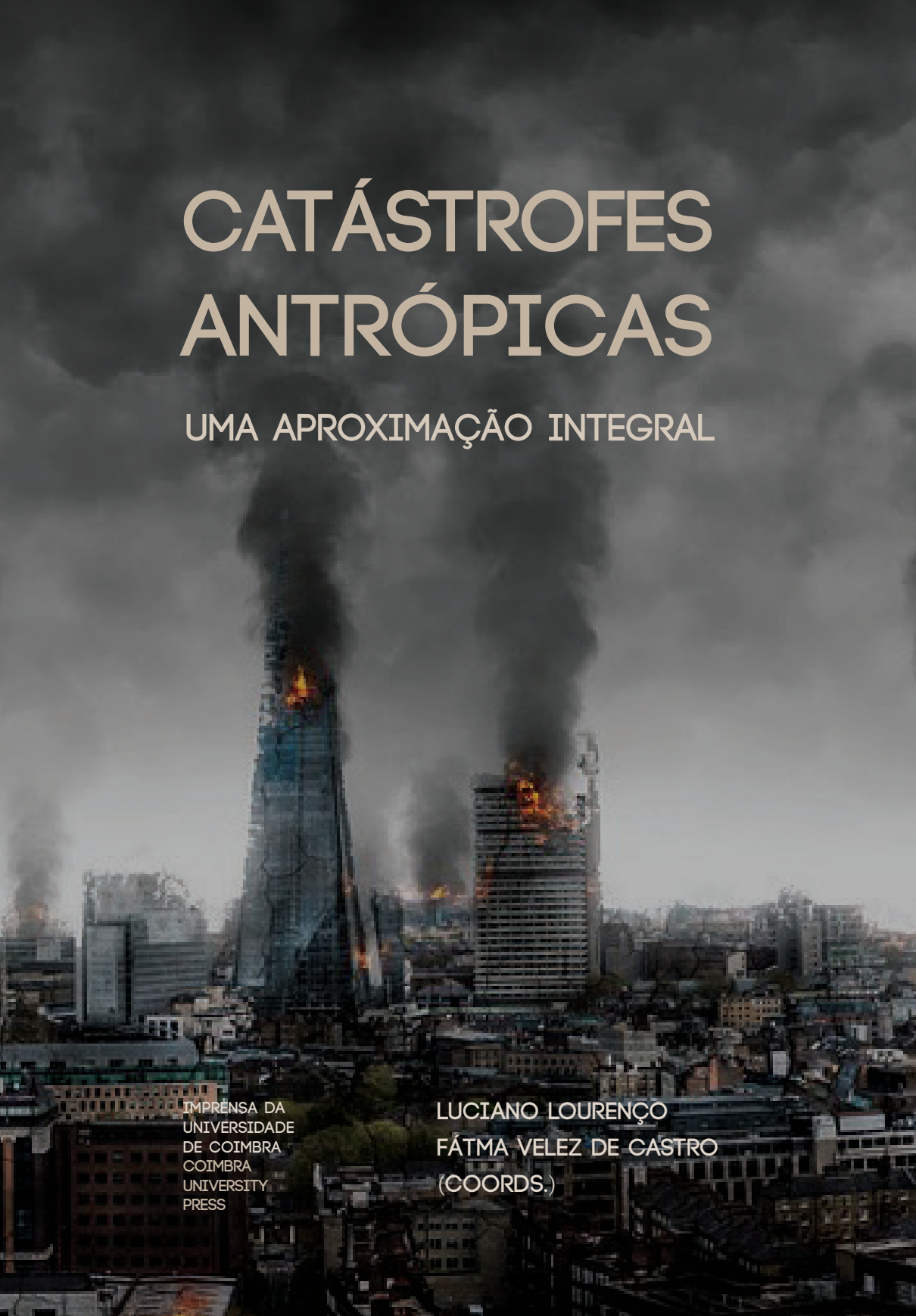

CATÁSTROFES ANTRÓPICAS

UMA APROXIMAÇÃO INTEGRAL

LUCIANO LOURENÇO
FÁTMA VELEZ DE CASTRO
(COORDS.)

IMPRENSA DA UNIVERSIDADE DE COIMBRA
COIMBRA UNIVERSITY PRESS

CONFLITOS DA ERA DA INFORMAÇÃO: GUERRAS CIBERNÉTICAS

INFORMATION AGE CONFLICTS: CYBER WARS

Paulo Fernando Viegas Nunes
Cor Tm (Eng)
Centro de Investigação da Academia Militar, CINAMIL, Portugal
nunes.pfv@mail.exercito.pt

Sumário: A "Sociedade de Informação" constrói-se hoje num novo espaço global (ciberespaço), estruturado através da Internet, com base em redes e fluxos de informação, cujas regras e modos de operação se encontram em permanente construção. A conectividade em rede desempenha um papel relevante neste contexto, constituindo um pré-requisito para a evolução em comunidade e para a democratização do acesso à informação.

Face a um ritmo elevado de desenvolvimento tecnológico, tornou-se cada vez mais difícil conciliar a crescente oferta de serviços de telecomunicações e aplicações informáticas com o ritmo relativamente mais lento do desenvolvimento de mecanismos de segurança. Os riscos associados aos desafios que a Sociedade de Informação encerra, não podem por isso ser ignorados ou negligenciados.

O aprofundamento de uma cultura de cibersegurança e a tomada de consciência coletiva das sociedades, relativamente à importância do desenvolvimento de políticas e estratégias cooperativas, levam os Estados a desenvolver sistemas e processos de combate a todas as

DOI: http://doi.org/10.14195/978-989-26-1867-8_13

formas de ataque cibernético. A emergência de novas ameaças não tipificadas, que exploram cada vez mais o ciberespaço como vetor de ataque, tem originado um amplo debate relativo à natureza híbrida dos modernos conflitos, obrigando muitas vezes a uma alteração dos conceitos associados à Segurança e Defesa Nacional.

Atentos ao tema central deste artigo, procuraremos avaliar o impacto do ciberespaço no Sistema Político Internacional, analisar as tendências de evolução da moderna conflitualidade e os desafios que o ciberespaço coloca à gestão do risco social. Neste âmbito, só a formulação de um conceito de ação estratégica consistente permitirá aos Estados edificar uma capacidade de cibersegurança e ciberdefesa coerente e devidamente estruturada, de acordo com o nível de ambição definido.

Palavras-chave: Sociedade de informação, ciberespaço, gestão do risco social, ação estratégica, cibersegurança e ciberdefesa.

Abstract: The "Information Society" is building and developing itself within a new global common (cyberspace). This global space, based on the Internet, is built upon a set of networks and information exchanges wich rules are permanently changing. Within this framework, network connectivity is a pre-requisite to communitarian progress and to the free and democratic access to information.

Due to the growing pace of technological evolution, it became harder and harder to conciliate the growing offer of Information and Communications Technologies (ICT) with the slower process of developing the necessary security mechanisms. Therefore, due to this asymmetry, the Information Society associated risks cannot be neither ignored nor neglected.

The emerging of non-typified threats that, more and more, uses cyberspace as an attack vector, originated a large international debate about the hybrid nature of modern conflicts and the need

to rethink the traditional approaches and concepts associated with National Security and Defence. The increasing level of cyber security collective awareness of modern societies highlighted the importance of developing and adopting cooperative policies and strategies in order to face all kinds of cyber-attacks.

In line with this paper's main subject, we analyze the impact of cyberspace on the International Political System, the trends of modern conflicts and the social risks' management challenges raised by cyberspace. Within this scope, only a consistent strategic action concept, aligned with the appropriate level of ambition, will allow the formulation of a coherent and structured approach towards the development of a National Cyber Security and Cyber Defence capability.

Keywords: Information society, cyberspace, social risk management, strategic action concept, cyber security and cyber defence.

Introdução

Assistimos à emergência e afirmação de uma "sociedade em rede" em que redes, sistemas e aplicações permitem assegurar o acesso permanente aos recursos de informação. Neste âmbito, importa referir que a informação, enquanto recurso base da sociedade em que vivemos, constitui a força motora de todas as atividades que aí se desenvolvem.

Apesar de existir uma relação natural entre o ambiente da informação e o ciberespaço, decorrente do facto de o ciberespaço constituir um dos seus principais vetores estruturantes, importa salientar o facto de o ambiente de informação ser algo mais do que o Ciberespaço. Para além da informação que se encontra acessível *on-line*, requerendo para tal o acesso prévio a um fornecedor de serviços Internet, existem várias das suas componentes que têm uma natureza não digital. A título de exemplo do que aqui se refere, se quisermos caracterizar a Sociedade de Informação, teremos de ter também em linha de conta toda a informação analógica que, mercê

da progressiva digitalização e de um verdadeiro "apagão analógico", está hoje apenas disponível fora do ciberespaço. Esta é a razão pela qual a nossa reflexão tem por foco o domínio da informação e não apenas o ciberespaço.

Dentro deste universo, não se integram apenas redes físicas e sistemas de comunicação, uma vez que também novos modelos e regras de interação social têm vindo a surgir à escala mundial. A própria aplicação da "teoria dos jogos" à atual conjuntura internacional, onde as modernas sociedades se organizam em redes, demonstra que estes deixaram de poder ser considerados de soma nula[1]. Neste novo contexto, aquilo que um ator perde, nas dinâmicas que caracterizam os vários tipos de interação no ambiente da informação (cooperação, competição e conflito), poderá não ser ganho por outro ou outros dos atores presentes.

Tal como acontece com os sistemas biológicos, se qualquer computador for ligado à Internet sem ter pelo menos a proteção de um *software* antivírus ou de uma firewall, em poucos segundos será infetado. Por esta razão, face ao crescente número de ciberataques e à sua natureza cada vez mais disruptiva e destrutiva, os indivíduos, as organizações e as sociedades da Era da Informação são cada vez mais confrontadas com a necessidade de assegurarem permanentemente a sua proteção e defesa. Para além da constatação dos enormes benefícios associados à crescente utilização deste espaço de acesso livre e aberto, o Ciberespaço deverá ser assim perspetivado como um ambiente naturalmente hostil.

Entendendo o ciberespaço como um vetor instrumental, através do qual circulam múltiplos fluxos de informação, importa agora caracterizar o ambiente de informação como um novo espaço de confrontação e competição à escala global. Neste contexto, o ciberespaço, caracterizado por novas acessibilidades físicas (infraestruturas de informação) e não físicas (interação virtual), obriga-nos cada vez mais a estudar as relações e fatores de poder que permitem a sua análise estratégica.

---

[1] O Prémio Nobel da Economia foi em 2005 atribuído a Thomas Schelling e Robert Aumann, dois investigadores da Teoria dos Jogos. No seu trabalho, est*es autores estudaram diversos modelos de conflito e cooperação, refletindo o seu efeito sobre o "jogo da informaçã*o" que se gera entre a informação que cada ator possui e a informação sobre o conhecimento que a outra parte detém.

O Sistema Político Internacional na Era da Informação

O ambiente estratégico internacional, a natureza das ameaças e os desafios que se colocam aos Estados na Era da Informação, sofreram uma alteração profunda ao longo das últimas décadas. Para além da turbulência e instabilidade que caracterizam o Sistema Político Internacional[2], existe uma revolução tecnológica em curso que, devido ao seu forte impacto, origina uma espiral de mudança social, económica e militar.

A revolução industrial e principalmente a revolução tecnológica tornaram os Estados interdependentes. Estes, deixaram de poder considerar-se autossuficientes e sofreram o impacto da criação de uma economia global, caracterizada por maior especialização e pelo crescimento da importância dos recursos intangíveis (informação e conhecimento).

A globalização também alterou profundamente as relações de poder, estimulando a transição do modelo comparativo de desenvolvimento (com os países vizinhos ou diretos competidores) para um modelo de desenvolvimento orientado para a obtenção de vantagem competitiva num mercado global (Nunes, 2010). Desenvolveu-se desta forma uma economia à escala planetária onde o progresso económico e a melhoria dos níveis de vida deixaram de estar exclusivamente sob controlo do Estado, dependendo cada vez menos da sua estrutura interna e cada vez mais da sua capacidade de intervenção e interação com os diversos centros do poder que intervêm no Sistema Político Internacional.

Acentuando esta tendência, o desenvolvimento tecnológico impulsionou a utilização generalizada da internet, aproximando os homens e as sociedades, independentemente da sua nacionalidade, cultura, raça ou credo religioso. O conceito de "aldeia global" surge, em grande parte, deste novo mundo, onde o "poder da identidade" (Castells, 2003) e os fundamentos e formas de interação entre os diversos tipos de atores se transformam.

---

[2] De acordo com a definição e com a caracterização apresentada por Cabral Couto (1988), o Sistema Político Internacional pode ser definido como "um conjunto de centros independentes de decisões políticas que interactuam com uma certa frequência e regularidade" (Couto, 1988: 44).

As infraestruturas tecnológicas, destinadas a garantir o acesso à Sociedade de Informação, também designadas por "novas acessibilidades do ciberespaço", constituem hoje um factor de desenvolvimento e progresso, materializando um aspecto central da política dos Estados. Neste âmbito, a emergência de uma interação em tempo-real, através de uma rede de cobertura mundial, tem contribuído para impor a compressão do "espaço-tempo" e para facilitar o relacionamento entre os diversos atores que compõem o Sistema Político Internacional. O espaço geográfico (físico), enquanto palco das relações sociais, perde desta forma relevância face ao surgimento do ciberespaço, como um novo domínio de interação global.

A realidade com que os Estados se confrontam atualmente, independentemente da sua localização geográfica, passa também pelo surgimento de novas ameaças e novos poderes, desenvolvidos por organizações complexas que abandonaram a tradicional estrutura hierárquica/piramidal. Devido essencialmente às oportunidades que as novas Tecnologias de Informação e Comunicação (TIC) oferecem, estas organizações privilegiam a adoção de um modelo organizacional em rede, onde a coordenação e direção descentralizada favorece uma atuação transnacional. Estas organizações podem ser constituídas por empresas multinacionais, por organizações internacionais, grupos criminosos ou até mesmo por movimentos terroristas. Todas elas, pela sua natureza e formas de atuação, podem constituir-se como "contrapoder" ao Estado Soberano, provocando a erosão das suas estruturas e bases de poder (político, económico, judicial ou mesmo militar), condicionando a condução das suas atividades tanto no domínio social e económico como ao nível do exercício da sua soberania.

Num "ambiente em rede", caracterizado por elevado dinamismo e turbulência, onde os Estados enfrentam permanentes desafios ao nível da sua envolvente externa e interna, tornou-se necessário compreender como estes podem afirmar a sua independência e soberania no domínio da informação.

O ciberespaço pode, neste contexto, ser visto como a face mais visível deste movimento de mudança, promovendo e acentuando o aparecimento de tendências supranacionais, conducentes a unidades políticas mais vastas e complexas, onde o conceito tradicional de fronteira, de base geográfica ou territorial, perde importância. De acordo com esta visão, que pretende evidenciar o incontornável contributo do ciberespaço para a definição dos diversos tipos de forças (tangíveis e intangíveis),

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 fator 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.

Evolução Tecnológica, Inovação e Guerra

Ao longo da história da Humanidade, conforme refere Clausewitz (1976), o fenómeno da guerra sempre constituiu a "*persecução da Política dos Estados por outros meios*". No entanto, procurando caracterizar a natureza dos conflitos e a dinâmica das ameaças, de forma a garantir a segurança das sociedades, o mesmo autor também refere que "t*odas as Eras têm o seu tipo de guerra, as suas próprias condicionantes e as suas preconceções peculiares*".

De facto, esta constatação histórica encontra-se também expressa nas obras de Alvin e Heidi Toffler, "A Terceira Vaga" (1991) e "Guerra e Antiguerra" (1995), onde se defende a ideia de que as guerras ocorridas ao longo das várias épocas históricas são caracterizadas por descobertas tecnológicas revolucionárias que causam "vagas"[3] de transformação social. Na sua essência, estes autores referem-se a uma evolução dos objetivos das guerras, impostas pelas estruturas socioeconômicas predominantes nas diversas épocas. Desde a Antiguidade Clássica, passando pela Época Medieval e até à Era Pré-Industrial, os objectivos das guerras eram geralmente materializados através da conquista e/ou controlo de recursos territoriais. Posteriormente, a guerra da Era Industrial passou a ter por objectivo a redução e limitação dos recursos de produção de um oponente. Assumindo os princípios que estão na

[3] De acordo com estes autores, a primeira vaga (agrária) foi caracterizada pelo cultivo da terra e pela domesticação de animais; a segunda vaga (industrial) foi caracterizada pela mecanização, produção em larga escala e pela divisão do trabalho; a atual terceira vaga (da informação) é caracterizada pela digitalização, computadores e tecnologia de informação.

génese destes conflitos como válidos, as guerras futuras serão travadas para assegurar o controlo de dados, de recursos de informação e do conhecimento.

Esta nova Era, em que a evolução tecnológica desempenha um papel determinante na capacidade de projeção de poder no domínio militar, não pode assim ser descontextualizada desta dinâmica, sendo também caracterizada pela existência concorrente dos três grandes tipos de armamento que se sucederam em importância ao longo dos tempos, dentro do duelo milenar entre ofensiva e defensiva: as armas de obstrução (fossos, rampas, bastiões, couraças e fortificações de todos os gêneros), as armas de destruição (lanças, arcos, peças de fogo, mísseis, etc.) e, por fim, as armas de comunicação (sinais, vetores de informação e de transporte, telegrafia ótica, radiotelefonia, radares e satélites, entre outras). Cada um destes tipos de armas dominou um tipo particular de confrontação: a guerra de cerco para as primeiras, a guerra de movimento para as segundas e a guerra relâmpago para as últimas. A criação da Internet e a sua crescente taxa de utilização à escala global, apresenta hoje um forte impacto na tipologia da moderna conflitualidade que, de forma inovadora, utiliza cada vez mais o ciberespaço.

A utilização do ciberespaço como vetor privilegiado de condução de ações militares, tem vindo a assumir uma importância crescente para as sociedades ocidentais. No entanto, conforme já foi referido, a utilização de uma nova arma ou de uma inovação tecnológica para a criação de uma vulnerabilidade estratégica não poderá ser considerada como algo inesperado ou absolutamente novo. Ao longo do último século, surgiram efetivamente três novos vetores estratégicos de projeção de poder que, devido à sua exploração militar se transformaram também em domínios operacionais: o ar, com o surgimento da aviação militar na 1ª Grande Guerra; o espaço com a "conquista do espaço" e o surgimento do programa "Guerra das Estrelas"; e, mais recentemente, o ciberespaço, com a criação de "Cibercomandos" por parte de vários Países (EUA, China, Rússia, Alemanha, Reino Unido, França, etc.).

Dentro deste contexto, tendo por base os seus efeitos, também as ciberarmas, poderão ser consideradas como armas de "disrupção massiva" (Libicki, 1996; Morris, 1995), apresentando a sua utilização um enquadramento estratégico semelhante ao das Armas de Destruição Maciça (ADM). 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 decor-

rentes do lançamento de ataques cibernéticos por parte de atores hostis, nomeadamente, por parte de indivíduos, grupos criminosos, ativistas, terroristas ou, até, por parte de outros Estados. No atual ambiente de informação, um ciberataque poderá desta forma ser considerado de nível estratégico se o seu impacto for tão importante que afete (ou possa vir a afetar) a capacidade de um Estado assegurar as suas funções vitais (segurança e bem-estar da sua população).

Os fundamentos associados ao lançamento de ciberataques, apresentam assim grandes semelhanças com os princípios do "bombardeamento estratégico"[4], permitindo este paralelismo uma melhor perceção da forma como os ataques às infraestruturas críticas de um Estado afetam a sua sociedade.

Um ator só pode avaliar o seu Poder relativamente a outro ator quando o exerce[5] (Nunes, 2010). 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 ator utilizar o domínio da informação (ciberespaço) para exercer Poder sobre outro ator, 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.

---

[4] Constata-se que já na 1ª Guerra Mundial, alguns pensadores europeus como o General Giulio Douhet e Major-General Hugh Trenchard defendiam ser possível afetar a capacidade inimiga para conduzir a guerra, através do lançamento de ataques aéreos contra as suas infraestruturas 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 elétricas, os centros industriais e os sistemas de transportes que suportavam o esforço de guerra inimigo.

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

Pelas suas diretas implicações na condução da Política e Estratégia nacional, os diversos Países terão de garantir a defesa e a proteção das suas infraestruturas de informação, nomeadamente, daquelas que, pela sua natureza, se assumem como críticas para a afirmação da soberania nacional e para a sua sobrevivência. 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.

Ciberespaço e Gestão do Risco Social

No ciberespaço, os Estados são confrontados com a existência de um ambiente de informação global, assente num conjunto de redes transnacionais, onde não é possível definir de forma clara o que representa a Infraestrutura de Informação Nacional (IIN). Na prática, passamos a dispor, não de diversas redes mas apenas de uma única rede, onde os fluxos de informação gerados impõem a existência de um ambiente de informação global (ciberespaço), que transcende e se sobrepõe às fronteiras físicas dos Estados.

Ao longo das últimas três décadas, o desenvolvimento e o bem-estar das sociedades foi-se cimentando com base na Internet e através do ciberespaço, de forma quase descontrolada. Na maior parte dos casos, este processo decorreu sem que tenham sido devidamente acautelados os riscos derivados das dependências entretanto criadas. De facto, existe hoje um conjunto de infraestruturas críticas e serviços essenciais à nossa sociedade que, fruto de uma cadeia de interações funcionais, dependem da IIN. Esta interdependência assumiu especial importância e tornou-se especialmente evidente na passagem do último milénio, em que um problema informático ("*Bug* do ano 2000") obrigou à realização de testes exaustivos a todos os sistemas informáticos que utilizassem processadores. A perceção dos efeitos negativos resultantes dos cortes prolongados de energia

elétrica, da indisponibilidade dos sistemas eletrónicos bancários, dos sistemas de controlo de tráfego aéreo ou mesmo da rede nacional de emergência (112), constituem certamente um motivo de reflexão. A quebra dos fluxos de informação, necessários ao funcionamento de qualquer um destes sistemas, poderá ter consequências catastróficas.

Uma falha prolongada do abastecimento de energia eléctrica poderá por em causa o funcionamento de todas as infraestruturas nacionais. A IIN, constituída pelas redes de telecomunicações, dependerá também da rede eléctrica. No entanto, no caso das restantes infraestruturas críticas do Estado, existe uma dupla dependência (Nunes, 2016) uma vez que estas só funcionarão se puderem dispor, simultaneamente, de energia eléctrica (dependência estrutural) e das infraestruturas de informação que suportam o seu funcionamento (dependência funcional).Temos assim que enfrentar a existência de uma "pirâmide de infraestruturas críticas", formada por sistemas tecnológicos agregados, difíceis de testar em condições limite, cujo comportamento se revela também difícil de simular e que, pela sua natureza complexa, revela pontos fracos passíveis de ser explorados por atores hostis.

A proteção 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 existentes. Na análise do risco social associado à IIN (Nunes, 2011), 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 infraestrutura de informação e das ameaças que, explorando essas vulnerabilidades, podem afectar os recursos que pretendemos proteger.

A gestão do risco poderá concretizar-se através da sua redução (adoção de contramedidas), manutenção (aceitação do risco) ou transferência para terceiros. A escolha associada a cada uma destas três opções depende normalmente do valor atribuído ao recurso a proteger. Quanto mais crítico for um recurso, maior será a necessidade de assegurarmos a adopção das contramedidas necessárias para reduzir o risco que se lhe encontra associado.

A ameaça de um ciberataque de larga escala (nível estratégico), elimina por completo a distinção entre sistemas militares e civis. A necessidade dos Estados disporem de uma proteção e segurança de foco alargado, no domínio do ciberespaço, torna-se assim evidente. No entanto, subsiste a incómoda questão de sabermos como poderá qualquer Governo proteger a sua IIN, sobre a qual não detém nem a posse nem o controlo integral.

Considera-se que o caminho a seguir, na implementação do Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN), se deverá articular de acordo com uma perspectiva de gestão do risco: Proteção, Deteção e Reação. Dentro deste contexto, a proteção da IIN passará por (Nunes, 2003):

- Identificar os recursos de informação de interesse nacional que podem ser atacados através de componentes da IIN partilhadas;
- Caracterizar os procedimentos e mecanismos necessários para assegurar a sua defesa contra os diversos tipos de ameaças à IIN;
- Implementar um sistema de alerta que permita antecipar, detectar e identificar os ataques conduzidos contra a IIN e/ou contra os utilizadores da informação considerada de interesse nacional;
- Definir os condicionamentos impostos pelo espectro da ameaça e as possíveis respostas a adoptar, criando regras de empenhamento tanto ao nível nacional como internacional;
- Assegurar uma auditoria externa e a execução de testes permanentes à IIN através da constituição de equipas especializadas.
- Garantir a formação de um grupo de especialistas civis e militares, especialmente vocacionado para a segurança das infraestruturas de informação e para a condução de Operações no ciberespaço, uma vez que estas áreas exigem a mobilização de competências específicas.
- Identificar o papel a desempenhar pelo Governo e pelas entidades privadas, na criação, gestão e operação dos sistemas ligados à capacidade de cibersegurança e ciberdefesa nacional.

Tendo por base este enquadramento, uma vez que o ciberespaço materializa uma área de responsabilidade colectiva, é ainda necessário assegurar uma efetiva coordenação das ações a desenvolver por todas as Entidades/Organizações envolvidas na garantia da sua disponibilidade e utilização segura.

Relativamente ao primeiro objetivo, considera-se que a proteção, resiliência e segurança da Informação que circula nas redes de comunicações nacionais constitui um pré-requisito para a livre utilização do ambiente da informação e que esta só pode ser garantida através de um conceito alargado de proteção das infraestruturas de informação, onde a articulação e a exploração de sinergias entre a cibersegurança e a ciberdefesa é decisiva para garantir essa proteção. Reconhecendo-se que se trata de garantir o funcionamento ininterrupto e a recuperação das infraestruturas de informação face à ocorrência de ciberataques de grande impacto disruptivo, importa também perceber que as Forças Armadas só serão capazes de atingir este objetivo se tiverem capacidade para defender o País contra este tipo de ataques, nomeadamente, detendo e neutralizando aqueles que coloquem em risco a Soberania Nacional. A proteção, deteção e reação têm a ver essencialmente com a área da cibersegurança ao passo que o defender e o deter se encontram mais ligados à Ciberdefesa.

A resposta nacional terá de passar também pela criação de legislação específica que, garantindo o difícil equilíbrio entre os direitos individuais e as responsabilidades institucionais, permita clarificar o objectivo, as atribuições e as competências dos diversos órgãos da estrutura do SPIIN. Poderá assim evitar-se a sobreposição de competências e os conflitos de interesses daí decorrentes, estimulando a cooperação, quer no âmbito nacional quer internacional.

Ciberdefesa Nacional: Enquadramento e Edificação de Capacidades

A defesa dos Estados passa cada vez mais por enfrentar as "novas ameaças", num contexto de "guerra híbrida", em que pontuam não só as ações terroristas e a criminalidade transnacional, mas também as atividades desenvolvidas por atores Estado no ciberespaço. Explorando assimetrias e vários vetores de projeção de poder

(ex: diplomático, informação, militar e económico), assistimos hoje, de forma praticamente ininterrupta, a uma conflitualidade de baixa intensidade mas de natureza permanente, transversal e híbrida.

Eliminando ou atenuando as fronteiras estabelecidas entre os diferentes domínios operacionais, neste tipo de conflitos verifica-se o emprego de diferentes capacidades e tácticas, em diferentes combinações, com o objetivo de atingir o maior efeito possível. Esta nova vertente da moderna conflitualidade, tornou-se particularmente evidente nos conflitos mais recentes (ex: Geórgia e Ucrânia), caracterizados não só por uma utilização extensiva do ciberespaço para a condução de ciberataques, mas também como vetor privilegiado para ações de propaganda e recrutamento. A designada "guerra híbrida", apesar de não ser um fenómeno novo, encontrou assim na componente cibernética um instrumento de ação de elevado potencial em função do custo reduzido, rapidez de atuação, sensação de anonimato e leque crescente de possíveis alvos com potencial impacto no domínio cibernético.

O crescimento sustentado da Internet, em rede, coloca Portugal na vanguarda da transformação digital. Neste contexto, a disponibilidade e fiabilidade da IIN, é reconhecidamente indispensável para o exercício pleno de uma cidadania digital e para a construção de uma sociedade em rede. No entanto, as infraestruturas de informação nacionais podem ser alvo de ciberataques que procuram cada vez mais explorar as suas vulnerabilidades e insuficiências estruturais, facto que impõe a necessidade de assegurar a sua proteção e defesa.

Neste âmbito, impõe-se uma análise cuidada do risco social e do impacto dos diversos tipos de ataque cibernético, separando os de motivação criminosa daqueles que, por apresentarem um maior poder disruptivo, possam colocar em risco a Segurança e Defesa do Estado. Enquanto o primeiro tipo se enquadra no âmbito da Cibersegurança, este último tipo de ataques, enquadra-se no domínio da Ciberdefesa, exigindo uma participação ativa das Forças Armadas. Esta, constitui uma área em que o ritmo da implementação de processos e mecanismos de segurança dificilmente acompanha a dinâmica das vulnerabilidades, exigindo um esforço contínuo de capacitação tecnológica e de acompanhamento da evolução do espectro da ameaça, materializando uma área privilegiada de "guerra assimétrica".

Em linha com o recente reconhecimento do Ciberespaço como o 4º domínio operacional pela NATO, a par da terra, mar e ar, Portugal também considera a existência deste novo domínio de condução de Operações Militares. Esta visão doutrinária, que se tem vindo a construir no plano nacional, a partir da formulação de uma "Orientação Política para a Ciberdefesa"[6] em 2013, tem hoje como face mais visível o levantamento do Centro de Ciberdefesa das Forças Armadas, edificado com base num "Plano de Implementação da Capacidade de Ciberdefesa Nacional".

A "Orientação Política para a Ciberdefesa" (2013), estabelece os seguintes objectivos: (1) garantir a proteção, a resiliência e a segurança das redes e dos Sistemas de Informação e Comunicações (SIC) da Defesa Nacional contra ciberataques; (2) assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proactiva do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional; (3) contribuir de forma cooperativa para a cibersegurança nacional.

Neste contexto, nomeadamente, na área da educação, treino e exercícios, presentemente uma das mais prementes para a NATO e para a União Europeia (UE), onde a cooperação internacional se equaciona com maior acuidade, importa registar e salientar a natureza da participação nacional. Nesta área, Portugal assume atualmente um papel de particular destaque, nomeadamente, por assegurar a liderança do projeto de *Smart Defence "Multinational Cyber Defence Education* & *Training"* e por estar prevista a edificação da futura NATO *Communications and Information Academy* em Oeiras, trazendo desta forma uma acrescida visibilidade nacional perante a NATO e a comunidade internacional.

Também no âmbito da Educação e Treino na área da ciberdefesa da UE, Portugal tem vindo a assumir um papel de especial relevo nos esforços cooperativos desta organização internacional. Neste âmbito, o nosso País assumiu em 2015, conjuntamente com a França, a liderança da *Cyber Defence Discipline* do *EU Military Training Group (EUMTG)*, responsável pela definição dos requisitos de treino em ciberdefesa.

---

[6] Despacho N.º 13692/MDN. Orientação Política para a Ciberdefesa. Diário da Republica II Série, 208, 28 de outubro de 2013, 31977-31979.

Ainda neste domínio, na sequência de um processo aquisitivo lançado pela EDA, foi também atribuída a Portugal a gestão da futura *Cyber Defence Training and Exercises Platform (CDTEXP)*. Esta plataforma, que se prevê venha a incluir diferentes domínios de utilização (nacional, EU e multinacional), constitui desde final de 2017, uma efetiva ferramenta de cooperação internacional.

Neste domínio em particular, entendemos que a cooperação e o desenvolvimento de sinergias entre todos os atores envolvidos no ciberespaço, apresenta indiscutíveis vantagens para a indústria e para o meio académico nacional, para o Ensino Superior Militar, para as Forças Armadas, para as Forças de Segurança e, sobretudo, para a Segurança e Defesa Nacional.

Plano de Ação Estratégica para a Ciberdefesa Nacional

Assumindo um papel de crescente importância para o exercício da soberania e para a defesa dos interesses nacionais, o ciberespaço carece de uma visão política clara e coerente, capaz de permitir definir objectivos e traçar os caminhos conducentes à edificação de capacidades nacionais neste domínio. Neste âmbito, apesar de não existir uma Política nacional formalmente definida, foi elaborada, em Junho de 2015, a "Estratégia Nacional para a Segurança do Ciberespaço"[7]. No âmbito da ciberdefesa, também sem carácter formal, salienta-se a elaboração de um despacho orientador por parte de Sua Exa. O Ministro da Defesa Nacional, em 28 de Outubro de 2013[8].

[7] Ver RCM N.º 36/2015, de 12 de junho, disponível em https://dre.pt/application/file/67443061, consultado em 1/11/2016. Esta estratégia, prevendo o levantamento de capacidades nos vários domínios envolvidos (incluindo a ciberdefesa), define também a necessidade de estabelecimento de uma coordenação político-estratégica das diversas áreas envolvidas.

[8] Despacho N.º 13692/MDN. Orientação Política para a Ciberdefesa. Diário da Republica II Série, 208, 28 de outubro de 2013, 31977-31979.

O desenvolvimento de um quadro estratégico consistente, assente numa articulação coerente e sinérgica das três componentes (operacional, orgânica e genética), estruturantes da Estratégia Nacional de Cibersegurança e Ciberdefesa, assume particular importância mas torna-se essencial ir um pouco mais longe, passando da visão à ação. Neste âmbito, a formulação de um conceito de ação estratégica, permitirá fazer face aos desafios suscitados pela edificação de uma capacidade nacional de ciberdefesa, tendo em atenção o nível de ambição definido.

O plano de ação, a edificar, deverá, sequencialmente e por ordem decrescente de importância, assentar num conjunto de cinco eixos prioritários:

- Levantamento da estrutura de governação e gestão integrada da cibersegurança e ciberdefesa nacional;
- Sensibilização, educação e treino para a cibersegurança;
- Informação e conhecimento situacional do ciberespaço;
- Aquisição de equipamentos e criação de infraestruturas adequadas;
- Sinergias nacionais e cooperação internacional.

No caso específico da ciberdefesa, à luz da hierarquia de prioridades agora definida, tendo também em mente os objetivos a atingir, caberá ainda às Forças Armadas a formulação de um conceito de emprego operacional e, subsequentemente, a elaboração de um plano de implementação da capacidade de ciberdefesa.

A existência de um plano de ação, concretizando a visão estratégica formulada ao nível político, permitirá assim realizar a ponte entre o conceito e a ação, contribuindo decisivamente para conferir uma maior solidez à execução da Estratégia Nacional para a Ciberdefesa.

Conclusões

Devido ao ritmo acelerado da evolução tecnológica e à crescente dependência das modernas sociedades em relação à internet, o ciberespaço constitui, atualmente, um novo domínio de acesso aberto e global, caracterizando-se pela ausência das tradicionais fronteiras físicas.

Portugal constitui hoje uma Sociedade da Era da Informação. A sua infraestrutura de informação é reconhecidamente indispensável para a vida da nossa sociedade, constituindo um fator estruturante do desenvolvimento económico e contribuindo para a interação e coesão social. Não sendo as infraestruturas de informação nacionais absolutamente seguras, estas podem ser alvo de ciberataques que procuram explorar as suas vulnerabilidades e insuficiências estruturais, facto que impõe a necessidade de assegurar a sua proteção e defesa. A percepção de que os processos e mecanismos de segurança existentes dificilmente acompanham a dinâmica das vulnerabilidades, levanta a necessidade urgente de uma forte sensibilização nacional para a importância da defesa e proteção das infraestruturas e recursos de informação nacionais, obrigando a uma revisão dos atuais conceitos de Segurança e Defesa.

A emergência de novos modelos de interação global, acompanhada pelos recentes sinais de uma crescente exploração militar da internet por parte de alguns Estados, tem um impacto profundo no ambiente estratégico internacional, produzindo inevitáveis implicações sociais, económicas e militares. A defesa dos Estados passa cada vez mais por enfrentar as "novas ameaças", num contexto de "guerra híbrida", em que pontuam não só as ações terroristas e a criminalidade transnacional, mas também as atividades desenvolvidas por atores Estado no ciberespaço. Trata-se de uma área em que o ritmo da implementação de processos e mecanismos de segurança dificilmente acompanha a dinâmica das vulnerabilidades, materializando uma área privilegiada de "guerra assimétrica".

A natureza dos desafios que se colocam, em matéria da estratégia a adotar pelo país no domínio da cibersegurança e da ciberdefesa, parece assentar em três vertentes integradas e complementares: clareza nas opções estratégicas a operacionalizar, determinação na política de reformas estruturais e realismo na definição das capacidades a levantar no domínio da segurança e defesa das infraestruturas críticas nacionais. Isto significa também que, independentemente de se edificar uma estratégia, assente nos seus 3 pilares (estrutural, operacional e genético) se torna imprescindível a sua concretização através de um plano de ação coerente e exequível.

A evolução das condicionantes estratégicas da última década, tanto no plano nacional como internacional, aconselha pois a uma reflexão profunda sobre as alterações entretanto registadas. É em função delas que Portugal deve dispor de um entendimento claro sobre o papel que quer desempenhar neste novo contexto e

sobre as consequências que resultam tanto do modelo de levantamento de capacidades como das opções especificas de investimento que, em função do mesmo, se venham a assumir.

Bibliografia

Arquillia. J., Ronfeldt, D. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defense Research Institute – RAND.

Campen, A. D., Dearth, D. H. (2000). *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*, AFCEA International Press.

Castells, M. (1999). *A Sociedade em Rede*. São Paulo, Paz e Terra.

Castells, M. (2003). *O Poder da Identidade*, Volume II. Fundação Calouste Gulbenkian, Lisboa.

Couto, C. (1988). *Elementos de Estratégia*, Volume I, IAEM.

Clausewitz, C. V. (1976). *Da Guerra*, Publicações Perspectivas e Realidades, Lisboa.

Erbschloe, M. (2001). *Information Warfare: How to Survive to Cyber Attacks*, McGraw-Hill.

Harris, S. (2014).*@War: The Rise of the Military-Internet Complex*, Boston-New York.

IDN-CESEDEN (2013). *Estratégia da Informação e Segurança no Ciberespaço*. Caderno IDN, 12. Lisboa, Imprensa Nacional Casa da Moeda

Libicki, M. (1995). *What is Information Warfare?*, National Defense University Press, Washington D.C.

Nunes, P. (2003). *A Conflitualidade da Informação: da Guerra de Informação à Estratégia da Informação*, Trabalho de Investigação Individual do Curso de Estado-Maior 2002-04, IAEM.

Nunes, P. (2010). *Mundos Virtuais, Riscos Reais: Fundamentos para a definição da Estratégia da Informação Nacional*, Actas I Congresso Nacional Segurança e Defesa, Editora Diário de Bordo, Dezembro.

Nunes, P. (2012). *A Definição de uma Estratégia Nacional de Cibersegurança*, artigo publicado na Revista "Nação e Defesa", Nº 133, número especial dedicado à "Cibersegurança", Imprensa Nacional – Casa da Moeda.

Nunes, P. (2016). *Sociedade em Rede, Ciberespaço e Guerra de Informação: Contributos para o Enquadramento e Construção de uma Estratégia Nacional da Informação*, Coleção Atena n.º 34 – 2ª Edição, Editora Diário de Bordo, ISBN 978-972-9393-34-1.

OPCD (2013).*Orientação Política para a Ciberdefesa*, Despacho n.º 13692/MDN. Diário da República II Série, 208, 28 de outubro de 2013, 31977-31979.

Rid, T. (2011). *Cyber War Will Not Take Place*, Journal of Strategic Studies.

Singer, J. P. and Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press.

Toffler, A. (1991). *The Third Wave*, Warner Books, New York Bantam Books, New York.

Toffler, A. e Toffler, H. (1995). *War and Anti-War: Survival at the Dawn of the 21st Century*, Warner Books, New York.

Waltz, E. (1998). *Information Warfare: Principles and Operations*, Artech House.

Sites e Páginas da Internet

Morris, C., Morris, J., & Baines, T. (1995). *Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos*, *Airpower Journal*, Primavera. Disponível em: http://www.cdsar.af.mil/air-chronicles.html (18-05-2003 /19h34)

ENSC (2015). *Estratégia Nacional de Segurança do Ciberespaço*. RCM n.º 36/2015, de 12 de junho. Disponível em https://dre.pt/application/file/67443061, consultado em 1/11/2016.