# A Segurança e a Defesa no Ciberespaço

António de Almeida Tomé*

*Resumo*

O aumento constante do número e do tipo das ameaças e das suas manifestações através de infiltrações deliberadas contra o aparelho dos Estados tem obrigado a dispor de ferramentas tecnológicas especializadas que possam detetar e bloquear o crescente número de ciberataques e o identificar da sua natureza disruptiva e transnacional.

Pretende-se com este artigo contribuir para a restauração da inicial utilização livre da *internet*, cuja atividade normal e segurança não poderão continuar comprometidas em nenhum dispositivo ou componente da sua rede global

Perante o emergir de novos riscos e da insegurança crescente, e porque se encontra em causa a defesa da inerente soberania nacional, os Estados têm de continuar a envidar esforços e recursos no sentido de conjugarem as suas abordagens à problemática da prevenção de ciberataques de ordem disruptiva, que colocam em causa e em permanência o normal funcionamento das infraestruturas críticas, as capacidades de Intelligence, as redes de Aviso e os sistemas de Segurança e Defesa Nacionais.

*Palavras-chave*: ciberespaço, ciberguerra, cibersegurança, ciberdefesa, intelligence

* Professor Associado da Universidade Lusófona de Humanidades e Tecnologias

*Abstract*

The steady increase in the number and type of threats and its manifestations through deliberate infiltration against the States structures, have required to create specialized technological tools with the capacity to detect and block the increasing number of cyber attacks and able to identify its disruptive and trans-national nature.

This article is intended to contribute to the restoration of the Internet initial free use, whose normal activity and security must be assured any time in any device of its global network.

Face to the emergence of new risks and growing insecurity, and because this matter afects the national sovereignty defence, all States must continue to make efforts and resources in order to combine their approach to the problem of the prevention of cyberattacks, much of them disruptive; type of atacks that all times may put in danger the normal functioning of critical infrastructure, the Intelligence capabilities and the National Security and Defense systems

*Keywords*: cyberspace, cyberwarfare, cybersecurity, cyber defence, intelligence

O tema centra-se na evidente necessidade de alertar os decisores políticos, militares, policiais e CEOs civis para a urgência da implementação de medidas de Segurança e Defesa no ciberespaço, domínio onde, com frequência alarmante, os Estados se confrontam com as novas *ameaças não tradicionais* de nova geração que nele operam através de novas formas de guerra no interior dos Estados e no sistema mundial, com a consequente desestabilização de um meio de comunicação e de informação supostamente livre que deveria a todos servir, e não o seu contrário.

O termo *Ciberespaço* foi criado em 1982 por William Gibson, um escritor de ficção científica (Thill, 2011). Mais tarde escreve o livro *Neuromancer*, cuja principal personagem é um perturbado *hacker* de computadores e consumidor de alucinogénios. Nesta sua obra, ele descreve *ciberespaço* como um novo espaço de dimensão virtual, que passa a ser aceite pela comunidade universal e a ser utilizado por biliões de operadores.

A criação literária de Gibson revelou-se quase de imediato como uma extraordinária antevisão do que viria a acontecer na internet nos anos seguintes. O ciberespaço tornou-se desde então num domínio integrando meios de computorização, de redes e de *networks*, cabos de fibra ótica, ligações sem fios e de outras infraestruturas como estações terrestres e de satélites, que o creditam como um novo *espaço* utilizado por biliões de pessoas, de Estados e de Organizações localizados por todo o planeta através da *world wide web*, mais conhecida por internet.

Atualmente, os diferentes conceitos de ciberespaço que se refletem nas estratégias e planos de Segurança de muitos países são muito diversificados, dependendo de se tratarem de grandes Potências ou de pequenos Estados e consoante os recursos disponíveis.

Nesta matéria, os Estados Unidos definem ciberespaço como uma nova dimensão de espaço traduzida numa infraestrutura digital de informações e de comunicações de interconexão global, que sustenta de forma crescente todo o espaço real em que assenta a sociedade internacional dos países e dos outros atores não-estaduais. Já para o Reino Unido, o mesmo ciberespaço refere-se a toda a forma de comunicações e de atividades sob a forma de conteúdos e de ações conduzidas no interior das redes digitais (D'Amato, 2002: 69).

Interessará ainda referir que o prefixo *cyber* constitui um elemento composto que vem da palavra *cibernética*, ciência que faz referência

ao estudo das analogias existentes entre os sistemas de controlo e de comunicação dos seres humanos e aqueles que os interconectam com as máquinas; em geral, caracteriza a aplicação dos mecanismos de regulação biológica e tecnológica (Figueiredo, 2013: 9).

No âmbito específico da Segurança e da Defesa, as três dimensões que caracterizam a terra, o mar e o espaço têm constituído os domínios tradicionais de desenvolvimento das operações militares (e das forças de segurança); daí ser nelas que se têm centrado os empenhos relacionados com a obtenção das necessárias capacidades militares e policiais. Mas desde há algum tempo, para além da 4ª e 5ª dimensão materializadas no Tempo e no Espaço (exterior), o ciberespaço tem vindo a ser definido e aceite como o sexto domínio operacional, no qual se levam a efeito operações militares muito específicas do âmbito deste novo domínio.

Contudo e qualquer que seja a diversidade de definições adotadas pelos vários países, as mesmas passarão sempre pela decisão de incluir o conceito de ciberespaço nos problemas de Segurança e respetivas estratégias e operações a descoberta ou encobertas, normais ou maliciosas. Hoje, o ciberespaço é uma realidade nos sistemas de relações sociais ou de afirmação de Poder a ter em consideração, sempre que se empregam os tradicionais instrumentos clássicos de relação entre os Estados e respetivas organizações, entre os atores secundários transnacionais, e ou entre aqueles e estes.

*****

Nesta nova Era da Informação e da ocorrência dos extraordinários avanços tecnológicos e científicos, o ciberespaço tornou-se num domínio virtual de atividade paralela ao existente mundo real, que influencia fortemente a soberania dos Estados em geral e interfere no sistema de Comando e Controlo de qualquer Potência que se queira afirmar como tal. Seja na vida privada, nos setores comercial e económico-financeiro e nos mais diversos tipos de atividade dos indivíduos, das sociedades, e dos Estados, o ciberespaço constitui uma rede de interdependências entrosada profundamente à escala global numa infraestrutura Tecnológica de Comunicação e da Informação – TICs (Figueiredo, 2013: 12-13).

No seu interior, são incontáveis os computadores interconectados e todos os seus meios de apoio, desde os servidores aos cabos de fibra ótica**;** todos integrando uma rede constitutiva de estruturas tecnológicas as quais, no seu mais elevado escalão, constituem o suporte da componente técnica de sistemas operativos integrando avançados meios de alta performance que servem de sustentáculo às denominadas infraestruturas críticas do Estado (Kuehl, 2009).

Devido a isso, haverá então que assegurar em permanência no interior deste domínio que esta área se torne num instrumento poderoso ao serviço do Estado e das comunidades nacionais que o integram, em toda a sua dimensão integrativa real e virtual, prolongando-se para aquelas internacionais que integram a globalização. O que irá sempre implicar um combate permanente contra os agentes predadores e perturbadores da ordem internacional, como sejam aqueles que materializam o terrorismo transnacional, o crime organizado em rede mundial, as organizações transnacionais do narcotráfico, os Estados párias e os Estados falidos onde grupos radicais religiosos fanáticos e amantes da prática da morte se instalaram. Acresce o combate às mentes perversas de indivíduos e grupos sem escrúpulos que praticam e provocam verdadeiros danos reais às diferentes sociedades, aos seus bens e aos Estados, através da exploração insidiosa e maliciosa deste domínio visando objetivos disruptivos ou desintegradores.

Neste contexto torna-se imprescindível que o ciberespaço se torne um espaço de funcionamento, pacífico e integrador, que a todos sirva e beneficie, como que uma *estrada* bem iluminada que não albergue os esconsos da *escuridão* que permite aos *hackers* atacar.

E porque à falta de melhor os Estados ainda constituem a estrutura que mais garantias oferece quanto ao suporte das coletividades e da Ordem internacional possível, haverá que tomar consciência do facto que a Segurança Nacional se encontra profunda e diretamente envolvida na problemática, concretamente no que respeita à sua proteção e no que concerne à compreensão de que este domínio integra algo de essencial para a economia, a geração de riqueza que sirva a todos, e muito principalmente para a Segurança e bem-estar das sociedades que através dele comunicam e se procuram integrar.

Trata-se de uma temática que visa salvaguardar a vida privada das pessoas e de garantir a disponibilidade e a honesta integridade da *informação* e da *comunicação*, mantendo a confiança e a fiabilidade das

tecnologias que o integram; ainda, e no que diz respeito ao prestígio e potencialidades do Estado, permitir através dele adquirir a capacidade de empreender acções e assumir posições de superioridade de informação visando explorar as vantagens daí resultantes que lhe permitam dominar o eterno ciclo da obtenção privilegiada da *informação*, seleccioná-la através da *intelligence* e traduzi-la em *knowledge* superior nos teatros operacionais, materializando-o no final em *conhecimento* antecipado face aos outros atores que buscam a supremacia.

De sublinhar que ameaças reais ou potenciais sobre as comunidades e os Estados sempre existiram e tiveram lugar na História dos povos, por parte de competidores em tempos de conflito, de crise ou de guerra. Sempre constituiu uma realidade das relações sociais e humanas.

Contudo, e nesta transição do século XX para o actual e depois de ter ocorrido a implosão da URSS, mais parecia existir por parte dos utopistas a convicção de que a «paz iria reinar para sempre»… Mas o que tem acontecido, nomeadamente com a exploração das novas tecnologias, é que os cenários de Ameaça, que anteriormente não passavam disso mesmo, têm vindo a mudar de natureza e a transformarem-se em cenários de ataque em tempo de paz, causadores de danos reais levados a cabo por ciberatacantes de difícil ou imprecisa identificação[1].

Estes ataques, quase sempre de ordem desintegradora e conduzidos por agentes e meios maioritariamente anónimos, procuram na maior parte das suas investidas desestabilizar e penetrar no interior dos Estados e das Instituições que os suportam, assim como nas grandes Empreses, Bancos e Complexos industriais, sendo causadores de perdas por vezes difíceis de reparar no espaço e no tempo.

Constituem ataques sobre infra-estruturas e sistemas de computadores considerados críticos e representam uma forma encapotada e alternativa de conduzir a guerra, quando de Estado para Estado. Mas e numa via paralela, também as grandes organizações criminosas e os grupos terroristas, de forma independente ou ao serviço de Estados que contratam os seus serviços, têm vindo a desencadear acções hostis, não apenas contra empresas e organizações não estaduais como principalmente através de ataques selectivos aos serviços de informações de um Estado visando atingir *interesses nacionais*.

1. Tomé, A.A., "A Guerra Fria Continua, mas Agora por Outros Meios", em Conferências na AACDN e em intervenções gravadas como comentador na TVI 24, Nov-Dez 2014, e Jan-Fev 2015.

A confirmação da globalização tem vindo a agravar as situações de Segurança com que os Estados se confrontam. A realidade actual indica que as ameaças que se perfilam no ciberespaço têm vindo a aumentar de forma exponencial, assim como o número e diversidades dos seus agentes e atores, através das práticas de *hacking*, *cracking*, de actos criminosos e de terrorismo e, no seu limite, de verdadeiros atos de guerra causadores de perdas danosas, assumindo por vezes a forma de ataques massivos que poderão no limite bloquear toda a atividade organizativa de um País. Os exemplos mais flagrantes materializaram-se nos ataques às forças armadas da Geórgia aquando da invasão russa em Agosto de 2008, que as paralisou na área de C3I; já anteriormente, em Abril/Maio de 2007 e com a mesma proveniência, uma série de ataques coordenados tinha conseguido paralisar por semanas o próprio aparelho estadual da Estónia e as respetivas Forças Armadas (Guedes, 2010).

Caberá então aqui definir e precisar o termo *ciberguerra*: engloba e privilegia acções ofensivas combinando ataques a redes de computadores e de Sistemas de Comando, Controlo, Comunicações e de Computadores das Forças Armadas (C4IRS), visando negar a utilização e aquisição da Informação das redes nodais do adversário ou mesmo a negação da utilização dos seus respectivos satélites. Poderá sempre ocorrer em simultâneo com outras capacidades de ataque, como ataques eletrónicos, eletro-óticos e ataques físicos reais no *terreno*. Também se verifica que, neste tipo de ataques noutra dimensão paralela à real, são empregues os mesmos tradicionais princípios doutrinários operacionais próprios das Forças Armadas, como o ataque em massa ou a defesa escalonada em profundidade.

Neste desiderato interessará referir que em Portugal, o levantamento das questões relativas às acções no ciberespaço encontra-se previsto no novo Conceito Estratégico de Defesa Nacional com o desenvolvimento da respectiva estratégia (IDN, 2013: 519-520; 532-534). Também estabelece o desenvolvimento de uma Estratégia Nacional de Cibersegurança (Nunes, 2012) e de uma rede nacional de CSIRT (Computer Security Incident Response Teams), tendo em consideração as directivas da NATO (Fernandes, 2012: 26-29) e da UE, Aliança e União onde o País se encontra inserido. Nesta ótica, encontra-se também equacionada a possibilidade de as Forças Armadas poderem vir a assumir a direção na Ciberdefesa Nacional, encontrando-se prevista a

interligação do futuro Centro Coordenador de Ciberdefesa e respectivas funções CERT (Computer Emergency Response Team) à rede de CSIRT nacional, exigindo a adaptação da doutrina vigente e o reforço das capacidades nas estruturas Militares. Nesta ótica, a criação da RRT (Rapid Response Team) tem-se revelado de considerável eficácia (Figueiredo, 2013: 55-58).

Constitui, portanto, um facto que, num mundo globalizado e onde o ciberespaço e as ações que nele se desenvolvem a cada minuto afetam no quotidiano a vida das sociedades nacionais e da internacional, a *sociedade da informação* materializa o seu grande suporte; mas gerando novos desafios no que concerne à segurança do Estado como um todo, seja ao âmbito interno quanto às forças policiais e da eficácia das suas forças armadas, seja no aspeto mais complexo das respetivas políticas externas na arena sempre conflituosa das relações internacionais.

Com efeito, a atividade no interior de uma estrutura de rede aberta e sem delimitação de fronteiras físicas geográficas, as relações de interdependência entretanto criadas e aquelas de dependência energética, económicas ou outras, as vulnerabilidades próprias de infraestruturas críticas, de natureza tecnológica e a sua exposição em cada segundo a qualquer tipo de ataques, têm tornado o ciberespaço sensivelmente mais vulnerável a indesejáveis intrusões, nomeadamente àquelas de natureza massiva e disruptiva como as referidas nos dois casos típicos citados.

Acresce que, o tornar mais seguro o ciberespaço se revela de enorme dificuldade por a arquitetura da internet ter sido desenhada para promover maioritariamente a conectividade e não a sua segurança; até porque os seus fundadores pensaram pouco em segurança contra as ameaças por acreditarem que, o facto de na América todo o network se encontrar então fortemente associado à componente militar norte-americana de onde era proveniente, isso constituiria uma garantia. Mas rapidamente os perigos de intrusão ou de ameaça se tornaram exponenciais, pelo que os iniciais níveis de segurança, baseados em antivírus e em programas de *firewalls*, em breve viriam a revelar-se insuficientes, exigindo sucessivos meios de proteção (Giles, 2014).

Nesta evolução das ameaças e face à velocidade de mutação das intrusões maliciosas ou criminosas, a árdua tarefa de conseguir e manter a cibersegurança nomeadamente contra o cibercrime, o ciberterrorismo, a espionagem industrial online e a ciberguerra, tem vindo a

revelar-se uma missão cada vez mais árdua e difícil de cumprir (Carr, 2011: 2-11).

Também se verifica que os casos de ataques selecionados que têm sido desencadeados no campo da ocorrência de sucessivas sabotagens a sistemas vitais do Estado têm vindo a aumentar. Constitui disso um exemplo o incidente representativo de uma sabotagem de elevado perfil ocorrido em 2012, levado a cabo por um novo vírus denominado *Shamoon* contra o sistema de computadores e respectivas infra-estruturas da Empresa colosso da Arábia Saudita de petróleo e gás natural, a Saudi Aramco; os atacantes conseguiram extrair das placas-mãe e de todas as *drives* em dezenas de milhares de computadores toda a enorme quantidade de informação e bases de dados que continham, tendo deixado no final a figura de uma bandeira americana a arder nos ecrãs dos computadores atacados. Este ataque arrasador e desencadeado de forma inovadora foi considerado pelos especialistas ocidentais como tendo sido levado a cabo pelo Irão, sob a *supervisão* da Coreia do Norte, como represália contra um outro levado a cabo dois anos antes pela América por meio de um poderoso vírus, *o Stuxnet*, contra as centrais nucleares iranianas, proibidas pelo Conselho de Segurança da ONU**,** mas que aquele país teima em manter e incrementar visando o fabrico da arma nuclear. Com efeito, a simples existência de um Irão de governo religioso fortemente radical sob a égide suprema dos ayatollahs, que cultivam o martírio, o combate aos cristãos e incentivam grupos terroristas no Líbano, em Gaza e recentemente no Iraque a desestabilizar toda a região, irá sempre representar um pesadelo nuclear, não apenas para Israel mas para toda a Europa, desde há anos debaixo do alcance dos seus mísseis.

Paradoxalmente, a ameaça à segurança das sociedades, dos Estados e das instituições com relevo para as TIC, alvos que se encontram na mira do cibercrime e da ciberespionagem, tem sido pouco coordenada, alegando-se razões de segurança nacional. Atenta ao peso determinante destas tecnologias quanto ao desenvolvimento socioeconómico e de proteção securitária das comunidades, a Organização das Nações Unidas aprovou cinco resoluções orientadas para a cibersegurança das Potências e das Organizações, considerando que os ataques no ciberespaço passem a constituir atos de guerra contra os Estados pela Lei da Guerra (Figueiredo, 2013: 9).

A ameaça global no ciberespaço é um dado adquirido e tende a aumentar, pois os mais inteligentes e melhor organizados *hackers* multifacetados, que nem sequer têm de seguir as *regras* normais existentes entre os Estados, trocam conhecimentos e prestações de serviços entre si, encontrando-se sempre à frente dos ciberdefensores; até porque, e como criminosos, tendem a ignorar as leis internacionais que regulam as suas relações interestaduais e aquelas próprias dos Estados. E como são aliciados e pagos com quantias invejáveis, o Ocidente democrático terá sempre problemas adicionais quanto ao seu recrutamento face aos seus opositores de regimes totalitários, o que levanta novos problemas de segurança quanto a esses técnicos.

Será pertinente então referir que, no vocabulário inglês, *ciberdefesa* é definida como a aplicação das medidas de segurança visando proteger as infraestruturas TIC de ataques gerais ou direcionados, sob a assunção de que estes ciberataques se caracterizam como uma forma de guerra cibernética que poderá sempre ocorrer em estreita combinação com um ataque físico aeroespacial com a finalidade de causar a disrupção dos sistemas de informação ou de proteção de dados de um adversário (Figueiredo, 2013: 22-23).

No entanto algumas medidas de prevenção e de deteção encontram-se em vigor ou a ser seguidas contra o inimigo comum, com o objetivo último de tornar o ciberespaço um lugar mais seguro.

Uma dessas medidas consiste em assegurar que as Organizações adotem medidas básicas de prevenção ou de anti-intrusão, que deverão complementar com medidas de detecção de ataques e de adaptação das suas defesas ao evoluir da Ameaça. A área das tecnologias, bem como as iniciativas industriais de inovação e de proteção, poderão contribuir largamente para melhorar as defesas através da partilha de *intelligence* sobre a origem e a natureza dos riscos com que as empresas e as organizações têm de confrontar-se, atendendo à sua transmutação.

Outra medida, já em execução em alguns países, reconhece que existe uma necessidade urgente para providenciar incentivos destinados ao aumento da cibersegurança, seja através dos fornecedores de serviços de internet ou por parte das empresas responsáveis pelas ligações via internet, com o intuito de partilhar mais responsabilidades na identificação ou no ajudar à *limpeza* e eliminação dos possíveis *malware*, *software* malicioso, dos computadores infectados (Giles, 2014).

Em suma, tudo passará por encontrar formas de assegurar que os fabricantes e inovadores de software produzam códigos que dificultem ou impeçam as penetrações perniciosas de hackers, ao colmatarem falhas de segurança ainda existentes pelas quais possam penetrar e explorar.

Todas as medidas possíveis de cibersegurança e de ciberdefesa, para além das mencionadas, que possam auxiliar e salvaguardar a Segurança geral do Estado e da Sociedade em geral, nunca serão demais para a manutenção da Lei e da Ordem, pois a aceleração da conjuntura internacional em constante mutação irá prosseguir e transformar o mundo.

Neste pressuposto, coloca-se finalmente mais uma razão adicional para incentivar as Empresas de alta tecnologia a serem mais interventivas e a dirigir mais as suas prioridades para a segurança do ciberespaço, nomeadamente porque o espaço *virtual* do ciberespaço se encontra em vias da ocorrência de outra massiva mudança. A racional desta afirmação baseia-se no reconhecimento de que, nos anos mais próximos, revolucionários dispositivos de alta tecnologia inovadores irão entrar em força nos mercados, desde novas aplicações nos automóveis, passando pela gestão *inteligente* das casas e dos grandes espaços comuns, até ao equipamento médico e à autonomia *inteligente* das nano-cápsulas; tudo passará a ser gerido em muito maior grau por computadores miniaturizados que ligarão estas e outras actividades de intervenção a uma *web* de elevada velocidade e poder de resolução tornando-os infinitamente mais potentes, rentáveis e de maiores capacidades. Como exemplos e entre outras citam-se os já existentes (embora de 1ª geração) controladores de *drones* pela via nano-elétrica da rede cerebral do ser humano; e as novas aplicações de *smartphones* para monitorizar e dar ordens a dispositivos médicos cirúrgicos ou de exploração de *nano cápsulas* atuando local e diretamente na eliminação das células cancerígenas ou de outro tipo que constituem o seu alvo, atuando por via remota ou dirigidas por sofisticados programas de computadores.

Esta entrada nos mercados de novos e mais *futuristas* dispositivos obrigarão a disporem de uma proteção de segurança, visto que darão azo também à criação de áreas mais numerosas que poderão ser atacadas e penetradas, obrigando à constante ampliação das defesas (Shimeall, Williams & Dunlevy, 2001).

## Conclusão

As TIC têm vindo a contribuir poderosamente na condução do sistema mundial para a denominada *sociedade da informação* (Figueiredo, 2013: 76). Neste *salto* tecnológico deu-se a emergência de novos teatros de operações estratégicas, como o Espaço e o ciberespaço, domínios onde**,** a par das outras dimensões**,** terão lugar os mais complexos e futuros conflitos.

Como o funcionamento do ciberespaço pressupõe o acesso livre à Internet, este novo domínio origina novas formas de interação mas também de confrontos, colocando aos países os mais diversificados e inesperados desafios quanto à sua tentativa de acompanharem as dinâmicas próprias da revolução tecnológica que ocorre num mundo ligado em redes cada vez mais alargadas e permeáveis (Adams, 1998: 78-98).

Neste contexto, os Estados têm de criar em tempo instrumentos fundamentais que lhes permita orientar as novas condicionantes às suas políticas de Segurança, de Defesa e da promoção do seu desenvolvimento nacional. O que implica que seja previamente estabelecida a montante a definição de uma atualizada visão estratégica e a implementação de um programa de *segurança digital* que estabeleça um *ciberconceito* de Defesa Nacional e a sua prática neste complexo domínio.

Ainda e no que respeita às áreas vitais da Segurança e da Defesa, o constante aumento do tipo das ameaças e da sua manifestação ou infiltração deliberada contra o aparelho do Estado tem obrigado a dispor de ferramentas tecnológicas que possam detetar e bloquear o crescente número de ciberataques e identificar da natureza cada vez mais disruptiva das ciberameaças, que não conhecem barreiras geográficas e eliminam as diferenças do que é o ambiente nacional e o estrangeiro. Trata-se de uma tentativa para restaurar a utilização livre da *internet*, cuja atividade normal não pode ficar comprometida**,** ou ser colocada em causa a sua segurança em qualquer dispositivo da rede global.

Perante esta nova realidade, de novos riscos e de elevada insegurança, considerada a necessidade de proteger ou mesmo de defender a soberania nacional, os Estados têm envidado esforços no sentido de conjugarem as suas abordagens à problemática da prevenção de ciberataques, nomeadamente os de maior capacidade disruptiva, os quais

constituem ameaças permanentes ao normal funcionamento das infra-estruturas críticas; e aos meios, recursos e capacidades de *informação* e de *intelligence* nacionais que os suportam.

Neste sentido, haverá que promover e fomentar uma cultura de segurança no ciberespaço abrangente a toda a sociedade e aos seus cidadãos**,** tanto nos sectores públicos como nos privados.

Mas como existirá sempre o seu lado mais obscuro, nomeadamente lealdades que sempre poderão ser compradas face às recompensas oferecidas, continuará a haver inopinadas fugas de Informação e de dados ultra-secretos que poderão infligir sérios danos na política interna e principalmente na política externa de qualquer potência, por mais poderosa que seja. O caso mais grave ocorreu com a deserção de Edward Snowden, um funcionário médio da National Security Agency norte-americana, o qual, segundo informações credíveis dos respetivos serviços de segurança, terá sido recrutado pelos adversários mais proeminentes dos Estados Unidos: a China e a *nova* Rússia, que lhe forneceram os meios de fuga (Giles, 2014)[2]. Desta forma, terão conseguido obter informação valiosíssima sobre todo o dispositivo de segurança norte-americano, com as consequentes repercussões. As pretensas razões éticas por si apresentadas apenas serviram para encobrir *um crime de lesa pátria*, pois não existe qualquer ética ou moral quando se atraiçoa e se provocam danos irreparáveis ao próprio país (Martins, 2012).

Devido à sensibilidade dos assuntos de Informação e de catalogação das ameaças e dos seus agentes que são próprios desta nova dimensão, a lealdade à Pátria e aos seus concidadãos exige uma acurada filtragem no recrutamento dos peritos a operar neste domínio de grande sensibilidade, que possa evitar a ocorrência de um dado e esperado ataque num dado e selecionado momento o qual, sendo suposto vir do exterior, acabe por germinar e surgir no próprio interior do Estado. Esta problemática quanto ao recrutamento, sobretudo nas democracias ocidentais, constitui por razões óbvias uma vulnerabilidade quando em confronto com as ditaduras totalitárias, pelo que exige adequado en-

2. De referir que já anteriormente o caso Wikileaks de Julian Assange tinha colocado em causa a segurança dos Estados Unidos e de países europeus, com a divulgação de 250.000 documentos sensíveis e do SIPRNET (Secret Internet Protocol Router Network).

quadramento cadastral, social e psicológico dos elementos que operam os dispositivos constitutivos deste domínio.

*As medidas de segurança* terão de abarcar em permanência os Sistemas no seu todo, as infra-estruturas, os meios de transmissão, as tecnologias e uma segura e apropriada selecção do meio humano que as opera, diretamente ou de forma acessória e periférica.

Na infinidade dos recônditos da *net*, com adequadas e apropriadas normas de segurança no *infinito do ciberespaço*, será então possível acompanhar a adaptação antecipada dos Estados irracionais e grupos criminosos às medidas preventivas e de segurança indispensáveis aos mantenedores da ordem internacional, visando garantir afinal aquilo que a *internet* deverá ser: um bem precioso ao serviço da Humanidade.

## Referências Bibliográficas


Adams, J. (1998). *The Next World War. The Warriors and Weapons of the New Battlefields in Cyberspace*. London: Hutchinson.

Carr, J. (2011). *Inside Cyber Warfare: Mapping the Cyber Underworld*. 2nd ed. Sebastopol: O'Reilly Media.

D'Amato, A. (2002). "International Law, Cibernetics and Cyberspace". *International Law Studies*, vol. 76, pp. 59-71.

Fernandes, J. (2012). "Utopia, Liberdade e Soberania no Ciberespaço". *Nação e Defesa*, nº 133, pp. 11-31.

Figueiredo, L.C. (coord.) (2013). *Estratégia da Informação e Segurança no Ciberespaço*. Lisboa: Instituto da Defesa Nacional.

Giles, M. (2014). *Special Report – Cyber-security: Defending the Digital Frontier*. Online: <http://www.economist.com/category/print-sections/special-report?page=2> (referência de 14-07-2014).

Guedes, A.M. (2010). "The New Geopolitical Coordinates of Cyberspace". *Revista Militar*, nº 2503-2504, pp. 823-847.

IDN [Instituto da Defesa Nacional] (2013). *Conceito Estratégico de Defesa Nacional: Contributos e Debate Público*. Lisboa: Instituto da Defesa Nacional.

Kuehl, D.T. (2009). "From Cyberspace to Cyberpower: Defining the Problem". In: F.D. Kramer, S.H. Starr & L.K. Wentz (eds.), *Cyberpower and National Security*. Washington: Potomac Books, pp. 24-42.

Martins, M. (2012). "Ciberespaço: Uma Nova Realidade para a Segurança Internacional". *Nação & Defesa*, nº 133, pp. 32-49.

Nunes, P.V. (2012). "A Definição de uma Estratégia Nacional de Cibersegurança". *Nação e Defesa*, nº 133, pp. 113-127.

Shimeall, T.; Williams, P. & Dunlevy, C. (2001). "Countering Cyber War". *NATO Review*, vol. 49, pp. 16-18.

Thill, S. (2011). *March 17, 1948: William Gibson, Father of Cyberspace*. Online: <http://www.wired.com/2011/03/0317cyberspace-author-william-gibson-born/> (referência de 02-10-2011).

Tomé, A.A. (2003). "A Transformação em Curso e os Avanços Tecnológicos: Uma Revolução Global Militar". *Revista Militar*, vol. 55, nº 10, pp. 975-982.

Tomé, A.A. (2011). *Relações Internacionais: Geopolítica e Geoestratégia*. Lisboa: Edições Universitárias Lusófonas.