Ciberespaço: uma Nova Realidade para a Segurança Internacional

Marco Martins
Professor da Universidade de Évora. Investigador do NICPRI. Doutor em Relações Internacionais pelo ISCSP. Auditor de Política Externa Nacional.

Resumo

Assiste-se na arena internacional a novas formas emergentes de ameaças que cada vez mais se posicionam na rede cibernética, provocando a deslocação do campo de batalha para o ciberespaço. A internet representa uma realidade incontornável das relações internacionais no quadro político e da segurança internacional.
Não só as novas tecnologias revolucionaram o mundo como também provocaram um sentimento negativo em torno do fator de segurança, nomeadamente em questões de privacidade e garantia dos sistemas de informação do Estado.
Aliás, atualmente não é possível afirmar a existência de um sistema de informação totalmente seguro e invulnerável. Ao contrário, a emergência de novas ameaças localizadas no ciberespaço representa um novo rosto do inimigo que se tornou invisível perante os nossos olhos.

Abstract
Cyberspace: a New Reality for International Security

We are witnessing in the international arena to new emerging forms of threats that are causing the displacement of the traditional battlefield to the cyberspace. Internet represents an inevitable reality in international relations and in the political framework of international security.
Not only the new technologies have revolutionized the world but also have triggered a negative feeling about the safety factor, especially in matters of web navigation and also regarding the security of the state information systems.
Indeed, it is currently not possible to sustain the existence of an information system totally safe and impenetrable. Rather, the emergence of new threats that is located in cyberspace represents a new face of the enemy that is invisible to your eyes.

A Realidade Virtual

O século XXI tem vindo a ser paulatinamente assinalado pela afirmação da incerteza do tempo que, por sua vez, marca a inconstância dos factos na realidade internacional, provocando a gestação de uma mudança não só na natureza do ser humano como também na aceção clássica do papel do Estado enquanto entidade soberana e reguladora quer da ordem interna quer da externa. Procura-se identificar a real imagem do mundo a partir e em torno da capacidade de sobrevivência do Homem. Esta sociedade, agora qualificada de global, perspetiva uma observação da imagem real do mundo inserida numa cosmovisão do lugar do Homem na redefinição geopolítica da hierarquia das potências. A atenção focaliza-se na perspetiva do ser humano envolvido na sociedade civil para compreender a *complexidade crescente* da ordem internacional a que se encontra sujeito, tendo em consideração a multiplicidade de identidades, a proliferação de estruturas e de novos atores no sistema internacional.

Para além da multipolaridade, emerge um outro sistema que segundo Richard Haass (2008), presidente do *Council on Foreign Relations*, se diferencia dos restantes por se caracterizar pela não-polaridade e por surgir num momento de combate à tendência hegemónica ambicionada pelos Estados Unidos. A instabilidade no sistema não-polar pode contribuir para o incremento de ameaças, tais como o terrorismo, as operações no mercado financeiro, o investimento, o comércio, afetando consequentemente a estrutura do Estado, das finanças à política. A não-polaridade institui um ambiente perturbador e perigoso, sendo necessário optar por uma cooperação multilateral no intuito de incrementar o grau de integração global na promoção da estabilidade, dado que na rede económico-financeira a interdependência provoca uma reação institucional no sentido de que nenhum Estado se encontre autoimune à realidade neoliberal que acabou por agravar a pobreza à escala global.

Tornou-se numa evidência de que os dispositivos tecnológicos mudaram radicalmente e substancialmente o mundo e o lugar do Homem. Nesse sentido, o caminho do Homem converge e relaciona-se cada vez mais acentuadamente na necessidade de profetizar o futuro, tendo por base o passado situado na sua memória. A dimensão tecnológica implementada no ciberespaço superou a dimensão humana e social. Perante esta nova realidade, circulam novos valores em nome de uma sociedade mais aberta e democrática que tende a traduzir-se numa verdadeira ideologia técnica a qual tem vindo a revolucionar a forma como o ser humano se insere nesta nova sociedade considerada de virtual. Importa referir que na opinião

de Dominique Wolton (1999) epistemologicamente não é passível de confundir a técnica, a cultura e a sociedade visto estes últimos enquanto modelos culturais e organizacionais evoluem e definem-se a uma velocidade não comparável à do progresso tecnológico.

O Ciberespaço como uma Nova Dimensão Temporal

Para o Estado soberano o processo de decisão torna-se progressivamente de maior complexidade devido à dificuldade de adaptação e de conciliação no sistema internacional. Assim sendo, a projeção do tempo para a rede geograficamente localizada no ciberespaço renuncia às características tradicionais, nas quais o Estado operava e se baseava desde os tempos mais remotos na definição das suas políticas e na defesa do interesse nacional. Essa situação ocorre, por um lado, pela crescente interdependência resultante da globalização e, por outro lado, da própria velocidade comunicacional dos fluxos de informação que cruzam todas as fronteiras terrestres em tempo real e imediato sem sequer outorgar a possibilidade de filtrar ou de analisar todo o volume informativo. Resulta que a impossibilidade de filtrar devidamente a informação que circula no tempo mundial no ciberespaço constitui por si só e para qualquer sistema político um facto perturbador.

Aliás, diga-se de passagem que a velocidade dos fluxos de informação e a inovação tecnológica operada no ciberespaço incita em termos objetivos a uma modificação gradual do comportamento geracional que inevitavelmente terá consequências de cariz cultural e social junto da sociedade no seu todo. De acordo com Eric Delbecque (2007) a batalha para a aquisição de novas tecnologias e/ou inovação é reservada somente a determinados atores económicos e Estados que atempadamente conseguirão antever e decifrar os mais variados acontecimentos que ocorrerão na arena internacional. Perante tal facto, provoca um novo sentimento no Homem que terminará por agir e operar no seio de um ambiente a uma velocidade superior àquela a que no passado se submetia.

Portanto, a navegação em tempo imediato concebe a impossibilidade de distinguir em termos temporais o passado, o presente e o futuro, tendo o Homem neste caso concreto a consciência da necessidade de agir cada vez mais num ambiente a velocidade superior à escala global e não somente ao nível local. Além disso, registamos uma das mudanças no comportamento do ser humano no quadro do desenvolvimento tecnológico aplicado ao ciberespaço que consiste na questão de como o Homem e o respetivo ambiente externo, leia-se aqui no campo das relações internacionais, conseguem gerir a imagem que se projeta sistematicamente da realidade diária para a virtualidade da rede na qual a mesma outorga a possibilidade

de se assumirem novas identidades e consequentemente novos papéis a desempenhar. Note-se que esta questão termina por envolver a análise a um nível distinto na esfera das relações internacionais como sendo o caso da junção ou a amálgama no ciberespaço do espaço virtual e do meio físico (satélites, cabos de fibra ótica, servidores, computadores) dos mais diversos sistemas políticos, económicos, culturais e religiosos capazes de provocar e conceber novos sistemas de valor cuja imagem transmitida pode ou não traduzir efetivamente a realidade diária.

Com efeito, o presente processo introduz nem uma relativização da realidade virtual nem uma anulação da influência física, mas sim a edificação de um imaginário com consequências reais e por vezes nefastas no mundo concreto. Existe de facto uma projeção de uma realidade para outra, contudo em ambos os casos é introduzida uma nova dimensão de maior complexidade na qual as relações internacionais acabam por operar entre a virtualidade, o imaginário e a realidade. Mesmo que não se pretenda integrar o sistema cibernético, o ser humano termina por indiretamente e involuntariamente ver-se introduzido num terreno paralelo localizado espacialmente entre a ficção e a autenticidade. A presente transferência vem modificar as relações entre o ambiente interno e o ambiente externo, agregando o sentimento de liberdade absoluta, de navegabilidade e mobilidade virtual sem precedentes e sem sujeição hierárquica.

A realidade internacional move-se no interior desse tempo mundial, procurando controlar e monitorizar a emergência de novas ameaças que circulam pelas redes do ciberespaço. Todas estas transformações levam a que o Estado desenvolva um papel virtual no ciberespaço na procura constante do aperfeiçoamento tecnológico. Diga-se de passagem que o Estado perde a sua capacidade de controlar o poder derivado dos mecanismos relacionados com a utilização das novas tecnologias que pode de facto incrementar a distância entre a virtualidade e a realidade no terreno, produzindo consequentemente um processo de ineficácia política (Noya, 2010). A principal ideia advinda da utilização da internet reside na propagação da livre circulação do saber à escala planetária. Nesse contexto, a elite política ou os próximos líderes deverão demonstrar uma capacidade superior de interpretação do verdadeiro sentido da magnitude de transmissão de dados a velocidade imediata através da rede virtual. Todavia, a médio prazo, o poder de influência localizar-se-á gradualmente no ciberespaço, onde o destino do mundo se irá concretizar através de quem detiver a capacidade de dominar a rede virtual.

Neste caso concreto, evidenciam-se por um lado as clivagens entre os diversos atores na capacidade de acesso à tecnologia, dependendo de Estado para Estado e, por outro lado, as desigualdades socioculturais que se caracterizariam pela aceção de infoincluídos em contraponto com os infoexcluídos. Por conseguinte, formar-se-iam discrepâncias advindas do próprio conceito de informação/conhecimento com interligação ao grau de liberdade e de democracia na mera utilização dos

meios tecnológicos. De facto, a internet fornece os mais variados serviços ao indivíduo, em nome do conhecimento do Estado, como por exemplo: (1) serviços de compra e venda; (2) lazer, jogos em linha e em simultâneo; (3) serviços públicos no quadro da extensão da administração central do Estado; (4) ligação em rede de instituições, de empresas, de bancos; (5) a oferta de conhecimento enquanto tal, como o acesso a universidades, a centros de estudo, de investigação, a livros em formato digital, a textos, à imprensa internacional; (6) a disponibilização de redes sociais de contacto universal; (7) a possibilidade de ligar as mais diversas unidades móveis operadas independentemente do espaço físico.

Salientamos a capacidade que o ciberespaço possui em possibilitar o acesso a infinitas aplicações que terminam por se integrar no Estado, na vida de cada família à escala global sem diferenciação de pertença social ou de nacionalidade. Contudo, o acesso pleno ao ciberespaço dependerá evidentemente da capacidade do cibernauta quer no domínio da utilização quer nos meios financeiros de que dispõe, para além da sua localização geográfica. Anotemos por exemplo, a título comparativo, os casos de um utilizador num determinado país onde o acesso se encontre limitado por razões de desenvolvimento ou condicionado por motivos de controlo político ou simplesmente inexistente, e de outro que viva num ambiente cuja realidade virtual faça parte integrante da realidade física. Entendemos assim que os infoexcluídos consistem naqueles que não conseguem aceder, neste caso concreto, à realidade cibernética, derivada da própria condição de exclusão da sociedade ou da impossibilidade de navegar no ciberespaço por razões económicas ou políticas. Se porventura se tratar de consequências meramente de ordem económica, referimos o conceito de infopobres, abrangendo aqueles que se deparem em condições extremas de pobreza, por desemprego ou por impossibilidade de inclusão na realidade virtual cuja prioridade consiste não na obtenção de conhecimento e navegação no ciberespaço, mas sim na procura da sua sobrevivência. Assim, se o ciberespaço se encontra acessível em qualquer ponto do globo não significa porém que todos os indivíduos detenham a respetiva entrada ou sequer a possibilidade de utilizar o potencial que lhes é oferecido.

Apesar de ser passível separar cada um dos exemplos acima referenciados, numa perspetiva cibernética, o todo interliga-se numa rede de maior complexidade e interdependente formada numa unidade virtual que se desenvolve em três escalas simultâneas: (1) para além das fronteiras físicas dos Estados; (2) no indivíduo; (3) no âmbito coletivo. Por outras palavras, apesar de numa primeira análise se considerar a internet como um espaço por excelência de liberdade absoluta e sem fronteiras, a realidade porém, leva-nos a observar o ciberespaço como um local não somente virtual e físico mas isento de regulamentação jurídica, onde os mais diversos crimes se podem manifestar, desde a invasão do computador sem sequer o utilizador comum ter a noção exata de que fora alvo da violação da sua

privacidade do seu espaço, à espionagem, à propagação de vírus e inclusive ao roubo de dados sensíveis na esfera governamental.

Consequentemente, o cibernauta ao consciencializar o risco e a possível ameaça emanadas da realidade virtual sente que efetivou a passagem de um sentimento de utopia para o de distopia em que afinal não se encontraria no "melhor dos mundos", recordando a obra *Brave New World* de Aldous Huxley, mas sim integraria um campo onde o desconhecido se revelaria na principal fonte de medo e de insegurança no qual o conceito de crime se transferira para a qualidade de cibercrime, colocando a "ciberliberdade" em causa com consequências nefastas do Estado ao indivíduo. Entendemos que o ideal democrático aplicado ao ciberespaço é afetado pela realidade adversa resultante da impossibilidade aparente de controlar globalmente o conteúdo da internet sem distinguir informação pública de privada, o que vem colocar problemas em matéria de segurança virtual e física visto que os dados obtidos na realidade virtual podem provocar danos irreversíveis quer na imagem de um Estado quer no próprio indivíduo em caso de rapto ou roubo.

Aliás, este problema advém no momento em que o cibernauta inocentemente constrói por exemplo uma página no *Facebook* na qual posteriormente fornecerá informação respeitante à sua vida, quer pessoal quer profissional, a um indeterminado número de supostos amigos mesmo sem os conhecer particularmente. Precisamente, essa transmissão de dados privados tornados públicos podem colocar em causa não só a sua vida mas também os próximos, arriscando-se as consequências a constituir uma primeira etapa da destruição da sua vida por representar uma ameaça à entidade empregadora, caso desempenhe funções de importância acrescida para entidades privadas ou para o Estado em setores sensíveis. Note-se que se regista um número elevado de setores profissionais que antes de contratarem um funcionário consultam a página pessoal das redes sociais para saber se, de facto, representa ou não uma ameaça. Perante esta situação, o ser humano encontra-se num processo de descontinuidade da sua existência real na conjunção com a virtualidade cibernética. O cibernauta tenderá a ver-se confrontado com a aquisição de uma dupla identidade resultante da sua nova condição na rede. No domínio psicológico, a dificuldade surgirá a partir do momento em que ambas as identidades se fundirão numa só o que trará inevitavelmente consequências e riscos quer para o cibernauta quer para o Estado na forma de *e.gov* enquanto entidade soberana visto a sua crescente dependência da web 2.0. na relação intragovernamental e extragovernamental, entenda-se para com o cidadão, as empresas, os serviços disponibilizados, o comércio, os setores vitais como a defesa, a saúde, a gestão de barragens e centrais elétricas ou nucleares, entre outros.

Com efeito, a gestão do saber acompanhada de capacidade criativa funcionará na forma de um agente catalisador de um novo poder situado na internet, esca-

pando por conseguinte ao mecanismo clássico do Estado, o que traduz a incapacidade de outorgar uma nacionalidade ao cibernauta por este navegar no território numérico sem estar sequer acompanhado pela correspondente bandeira nacional. Na opinião de Dennis Ettighoffer (2008) o saber penetrou a esfera do mercado, circulando livremente no ciberespaço, oferecendo uma nova forma de comunicabilidade. Torna-se inquestionável que o Homem se tenha convertido num membro do ciberespaço e atue em plena autonomia, criando empresas e comunidades virtuais cujas informações são transfiguradas pelo espírito humano numa mutação da informação com desideratos precisos, onde o saber requer a obtenção de conhecimento na forma de dados na rede virtual.

O Fator de Insegurança no Ciberespaço

Atualmente, a internet não possui uma bandeira nacional ou uma lei internacional que impeça a livre navegação. Contudo, existem casos pontuais como a Coreia do Norte, por sinal o único país do mundo cuja utilização da internet se encontra proibida à população, e permanece em exclusividade para a elite política; ou a República Popular da China (RPC) que quando se sente ameaçada decide optar pelo bloqueio de determinadas páginas ou motores de procura como o *Google* alegando a defesa do interesse nacional o que constitui para a comunidade internacional uma violação da liberdade. A postura de ambos os países traduz a necessidade de impedir quer o acesso quer a circulação da informação para que a mesma não influencie negativamente as estruturas governativas ou simplesmente para evitar que se tenha conhecimento da realidade para além fronteiras.

No quadro do controlo da internet a *OpenNet Initiative* (ONI) (Deibert, 2009: 323-337) tem por principal objetivo o levantamento exaustivo do comportamento e formas de censura e vigilância na rede. Importa referenciar que, ao contrário da perceção geral por parte dos internautas, a internet não representa uma infraestrutura aberta e descentralizada, pois as ligações efetuam-se via satélite, cabos submarinos e fibra ótica que se ligam localmente a servidores, a *routers* através do *Internet Service Provider* (ISP) e também por meio do *Internet Exchange Points* (IXP), pontos internacionais e companhias de telecomunicações. Se por um lado, a internet representa uma realidade virtual, por outro lado, encontra-se fortemente dependente de estruturas físicas de comunicações que por sua vez se localizam no interior dos Estados. A existência dessa interdependência para com os meios físicos gera a possibilidade de se controlar eficazmente o tráfego, os fluxos de informação pela utilização de filtros e de programas informáticos de vigilância, de *chokepoints* por razões políticas e/ou económicas. A título de exemplo, a RPC converge o seu controlo nas seguintes áreas: (1) direitos humanos; (2) movimentos independentistas;

(3) minorias; (4) grupos pró-democráticos; (5) motores de procura (nomeadamente o *Google*); (6) *e-mails*; (7) serviços de *webhosting*; (8) pornografia.

No âmbito da censura, para além do Irão e da Arábia Saudita, a RPC com 258 milhões de utilizadores, à data de 2008, surge segundo dados da ONI como o país que maior controlo exerce sobre a navegação no ciberespaço. A RPC utiliza um sistema de filtragem a múltiplos níveis que por sua vez envolvem um número considerável de agências e milhares de profissionais (*OpenNet Initiative*). Neste caso, é possível controlar através do bloqueio de acesso a um determinado *Internet Protocol* (IP), por exemplo, no caso de Estados que pretendam restringir ou até proibir o acesso a determinados conteúdos e/ou *sites* é possível com a tecnologia disponível bloquear e filtrar o tráfego utilizando os pontos de acesso internacional. Contudo, se enquadrarmos o conceito de *global commons* aplicado ao ciberespaço, a internet consiste por um lado num lugar onde qualquer individuo detém a possibilidade de aceder livremente e, por outro lado nenhuma entidade quer particular quer coletiva ou estatal pode reivindicar esse espaço como sendo da sua propriedade ou sequer tomar o seu controlo.

Acresce ainda que no quadro das relações internacionais, os seguintes países impedem estrategicamente o acesso a determinados *sites*: (1) a Coreia do Sul bloqueia *sites* relacionados com a Coreia do Norte; (2) a Índia impede o acesso a *sites* de grupos extremistas, concretamente islâmicos e hindus; (3) a Jordânia, a Síria, a Arábia Saudita, os Emirados Árabes Unidos e o Bahrein procedem pontualmente ao bloqueio de domínios israelitas. Diga-se de passagem que as autoridades locais nesses países concentram o controlo e a monitorização em blogs, em chats, no envio de SMS e em mensagens instantâneas e serviços de *Voice Over Internet Protocol* (VOIP). Note-se todavia que o controlo e o bloqueio por parte da RPC, da Índia, da Coreia, do Paquistão, do Uzbequistão, de Mianmar, da Tailândia, do Vietname, da Etiópia, da Líbia, da Tunísia, do Irão, dos Emirados Árabes Unidos, da Síria, e do Bahrein, são precedidos ao nível interno e local do que propriamente numa esfera mais alargada que poderia atingir o global.

É de salientar nesse sentido que o indivíduo transformado em cibernauta pode atuar na qualidade e em nome de um grupo de pressão com possibilidade de mudar ou de alterar o destino das relações internacionais a partir da internet. Revela-se de interesse o facto de a *primavera árabe* possuir como ponto de partida não só o acontecimento trágico de Mohamed Bouazizi, mas também a mensagem que o mesmo escreveu na sua página pessoal do *Facebook*, de pedido de perdão à sua mãe pelo ato que iria cometer e de culpabilização da realidade vigente que o levara à imolação pelo fogo no fatídico dia 17 de dezembro de 2010, na praça de central de Sidi Bouzid, na Tunísia. Note-se ainda o gesto, pouco antes de renunciar e de entregar o poder às forças armadas egípcias no dia 11 de fevereiro de 2011, do ex-Presidente Hosni Mubarak na tentativa de bloquear todo o tipo de acesso à inter-

net para evitar a propagação da revolta para o campo cibernético das redes sociais contra o seu regime. Frank La Rue (2011) refere expressamente no seu relatório *The Promotion and Protection of the Right to Freedom of Opinion and Expression*, apresentado no dia 16 de maio de 2011 perante a Assembleia Geral das Nações Unidas, que são utilizados sistemas de filtragem na China que bloqueiam o acesso a *sites* contendo palavras como "democracia" ou "direitos humanos". Salienta ainda a importância e a força que a internet possui em momentos cruciais e determinantes nas relações internacionais como por exemplo os acontecimentos no Norte de África, no Médio Oriente e concretamente nos casos da Tunísia e do Egito, nos quais a população utilizou a internet como um instrumento por excelência na defesa da liberdade.

Como se pode verificar, uma das consequências inevitáveis da expansão da internet resulta no facto de considerar, retomando o conceito de Adriano Moreira, que todo o facto doméstico sucedido no seio do Estado enquanto entidade soberana pode constituir um facto ou uma ação potencialmente internacionalizável pela sua transposição ou deslocalização do espaço físico para a realidade virtual. Trata-se de um dos riscos que os Estados enfrentam, quer internamente quer externamente, porque presentemente não se torna possível separar o Estado da internet e da respetiva projeção à escala global. Se por um lado, a internet significa conhecimento e traduz claramente a vantagem de beneficiar do acesso a partir de um ponto específico do globo a um número infinito de ligações em rede que conectam o planeta a uma outra realidade, por outro lado, a negatividade pode surgir a partir do roubo da identidade ou da invasão do domicílio virtual sem o consentimento do internauta o que provoca a suspensão temporária do sentimento de ciberdemocracia. A partir desse preciso momento, o internauta regressa à realidade ao tomar consciência da existência de uma nova ameaça em forma de crime no mundo virtual, o que consequentemente cria um sentimento de medo constante no simples teclar e navegar na rede.

Contudo, assiste-se paralelamente a uma transferência do campo convencional de batalha, onde as ameaças se identificariam com certa facilidade, para o ciberespaço, onde existe um novo rosto invisível denominado internauta. Assim, as novas ameaças representam um risco com implicações globais para os Estados e a humanidade. Para o Estado, o inimigo sem rosto e sem identidade provoca um sentimento de temor e de perigo superior ao das guerras ou conflitos ditos tradicionais. A internet incita nessa perspetiva à propagação da militância extremista e à formação de redes criminosas que operam em ambiente virtual.

A insegurança no ciberespaço transformou-se no mundo dos rostos invisíveis, onde aqueles que transgridem o espaço de liberdade do internauta comum e penetram as fronteiras físicas dos Estados terminam conhecidos como *hackers*. Neste caso, importa destacar os "*hackers de chapéu branco*" que se consideram no meio vir-

tual como aqueles que protegem a integridade do sistema sem pretender traduzir as suas ações em crime, ao contrário dos "*hackers de chapéu preto*". As principais vítimas são aquelas que se encontram perante uma posição de vulnerabilidade, caso das crianças quando não devidamente acompanhadas por um adulto e de indivíduos que se sentem isolados e/ou sozinhos. Para além deste tipo de vítima, o Estado, as suas instituições, o setor empresarial ou a banca simbolizam um novo alvo a explorar e a abater por representar um motivo de desafio para quebrar os sistemas de segurança ou uma forma de transmitir a revolta contra as políticas definidas ou um meio para denunciar as violações dos direitos humanos. Os cibercriminosos utilizam os dados recolhidos para posteriormente vender segredos de empresas, códigos de programação ou divulgar segredos de Estado que possam colocar em causa a segurança internacional. Portanto, o *hacker* não representa exclusivamente os adolescentes norte-americanos que a partir de uma garagem conseguiam atravessar qualquer tipo de barreira de segurança dos sistemas de informação na rede.

O caso *Wikileaks* de Julian Assange reproduz para a comunidade internacional um exemplo claro de guerrilha informática global que provocou a possibilidade de colocar em causa a segurança, através da ausência de efetivo controlo do ciberespaço, concretamente no acesso a informação estratégica, vital e sob segredo de Estado. Os mais de 250 mil documentos provenientes do Departamento de Estado Norte-americano e do *Secret Internet Protocol Router Network* (SIPRNET) trazidos a público comprometem a esfera de atuação quer militar quer diplomática e causam danos irreparáveis de elevado impacto nas relações internacionais, nomeadamente na perceção por parte da sociedade civil. Trata-se sobretudo de uma denúncia pública comprometedora de segredos de Estado, tanto militares como diplomáticos. Neste campo, a problemática foca-se sobretudo no acesso a documentação supostamente classificada e restrita a um delimitado número de indivíduos, de decisores governamentais e na generalidade de atores políticos e diplomatas.

Com efeito, o *hacker* opera num mundo paralelo à realidade diária do ser humano no qual a sua motivação expressa um sentimento de revolta em nome de uma causa. Esta mudança que se regista revela uma nova forma de defender os direitos humanos e compreende uma perspetiva do sentimento de ciberdemocracia que consiste no ciberactivismo por envolver a sociedade e projetar o movimento em desobediência civil por vezes com ligações a organizações como a Greenpeace ou a Amnistia Internacional. A esse ciberactivismo torna-se possível acrescentar hacktivismo por subverter ou infetar determinados sítios na internet através da construção de sítios espelhos como sendo os casos do *World Bank*, transformado em *Whirled Bank* com o desígnio de "*our dream is a world full of poverty*" para denunciar justamente a pobreza e o sistema financeiro (McCaughey, 2003).

O Reforço da Cibersegurança

A internet tem vindo a converter-se num novo campo de batalha não convencional cujos rostos invisíveis tendem paulatinamente a dominar o ciberespaço, dotando-se de uma arma que representa uma maior perigosidade e ameaça do que a nuclear num cenário virtual dotado de soldados digitais devidamente preparados para atuar em ambiente de ciberguerra. A arma por excelência no ciberespaço reside na capacidade de enviar códigos que consigam quebrar todo o tipo de protocolos de segurança nas mais diversas redes informáticas. No campo de ação do ciberespaço, a obtenção de informação não representa somente um objetivo concreto, verifica-se assim a constituição de outros, como por exemplo, detetar vulnerabilidades em redes estratégicas para a sobrevivência do Estado.

Neste contexto, a administração norte-americana liderada por Barack Obama decidiu no ano de 2009 proceder à criação do cargo de "ciberczar", referente ao coordenador para a cibersegurança na Casa Branca, ocupado por Howard Schmidt, tendo igualmente indicado em 2010 o General Keith Alexander para representar a nova estrutura cibermilitar do Pentágono, a US Cybercommand (USCYBERCOM ou CYBERCOM), localizada em Fort George Meade que conta com um total de 90 mil profissionais civis para proteger os sistemas informáticos (Macon, 2009; Lawson, 2010). Note-se que desde 2006, a *Doutrina Conjunta de Operações de Informação* do Pentágono estabelece a necessidade de obter a superioridade das forças militares devidamente preparadas para qualquer tipo de intervenção em tempo mundial no ciberespaço. Estas operações defensivas e ofensivas pretendem garantir a integridade do sistema informático norte-americano e dos aliados. Para isso, o objetivo último para vencer uma ciberguerra abrange o controlo da informação e a neutralização dos rostos invisíveis. Aliás, a *Comprehensive National Cybersecurity Initiative* do *Executive Office of the President of the United States*, tem por princípios: estabelecer uma linha de defesa contra ameaças imediatas que possam colocar em causa o governo; defender contra todo o tipo de ameaças através do incremento de operações de contrainformação; reforçar o futuro ambiente de cibersegurança concretamente pelo desenvolvimento de ações de formação, de educação em ambiente ciber e pela definição de estratégias para dissuadir atividades hostis e maliciosas no ciberespaço.

Estipula ainda a necessidade de consolidar uma rede com *Trusted Internet Connections* (TIC); implementar um sistema de deteção de intrusão dotado de sensores passivos como parte integrante da rede governamental; desenvolver um sistema de prevenção de intrusão operado em tempo real denominado de EINSTEIN 3 para identificar e caracterizar o tráfego da internet para reforçar a segurança do ciberespaço; incrementar a segurança e a respetiva classificação da informação sensível para garantir a integridade do sistema e da defesa do interesse nacional; inves-

tir na educação do ciberespaço para que a sociedade civil possua o conhecimento adequado quanto à utilização do espaço virtual e, por último, definir o papel do governo na segurança de infraestruturas críticas e vitais do Estado. Nesse sentido, à data de 15 de abril de 2011, a administração Obama determinou a *National Strategy for Trusted Identities in Cyberspace* para intensificar a segurança e estabelecer os princípios fundamentais no desenvolvimento do comércio eletrónico.

O Pentágono assume o reconhecimento oficial deste novo campo de batalha não convencional do século XXI. Desde 2010 que o *US Cyber Comand* se encontra operacional, tendo o apoio dos *Marine Corps Forces Cyberspace*. Nos dois últimos anos, os Estados Unidos intensificaram operações de simulação de ataques denominados por *cyberstorm* para incrementar a capacidade defensiva em tempo real, tendo em consideração o facto de a ciberguerra partir de um ataque em qualquer ponto do globo não previamente identificado. Sublinhe-se que o *US Cyber Comand* tem o apoio da comunidade de informações dos países aliados. Neste momento, a principal preocupação por parte desta nova força que é constituída por homens e mulheres não dotados de capacidade de resistência para sobreviver em ambientes hostis extremos de um campo de batalha convencional, mas sim detentores de conhecimentos técnicos específicos para combater em situação de ciberguerra cujo propósito, reside na defesa e proteção dos domínios ".gov" e ".com", para além de todo o tipo de infraestruturas governamentais, do setor de educação à defesa (Lynn, 2010).

Na esfera europeia, com o apoio da Europol, pretende-se dotar os Estados-membros de condições tecnológicas suficientes para combater em ambiente de ciberguerra. Contudo, ao contrário da posição norte-americana que apesar de defender e de demonstrar certa preocupação, a União Europeia tem vindo a defender o reforço não só dos efetivos, mas também do desenvolvimento de ferramentas jurídicas e penais para condenar criminalmente em sede própria, o cibernauta que cometa infrações e viole inequivocamente a lei. No tocante ao cibercrime, a União Europeia procede igualmente com o auxílio da *European Cybercrime Task Force* e da *European Union Cybercrime Unit*. Assim sendo, para as autoridades europeias e respetivos governos tornam-se evidentes a introdução de um direito penal específico ao ciberespaço e do reforço do controlo da navegação dos cibernautas o que levaria inevitavelmente à violação do direito à privacidade do internauta, visto a possibilidade de monitorizar a sua navegação em ambiente virtual consistir numa clara violação do espaço de liberdade. Por seu turno, o novo conceito estratégico da NATO considera no seu articulado respeitante ao ambiente de segurança que os ciberataques, dotados de maior organização, têm por um lado vindo a incrementar e, por outro lado, causado danos de elevado custo a determinados setores como o administrativo, as empresas, as infraestruturas vitais. Anotemos ainda que se traduz numa ameaça para a prosperidade, a segurança e a estabilidade dos Estados. Assinala igualmente que os serviços de informações, as forças armadas, a

criminalidade organizada, grupos terroristas e/ou extremistas constituem fontes de possíveis ataques.

Importa destacar que o ciberespaço representa uma ferramenta por excelência para comunicar por canais não detetáveis, por vezes encriptados, que atravessam todo o tipo de barreiras sofisticadas de segurança, o que permite conceber operações de ataque a alvos essenciais como as estruturas vitais do Estado. Note-se ainda que a junção de ciber com terrorismo forma o conceito de ciberterrorismo que, quer para a elite política quer para a sociedade civil, induz o medo pelo sentimento da deslocalização geoespacial do território físico para a rede virtual. O ciberterrorista ao contrário do *hacker* tem por aspiração e missão causar o maior número possível de danos não reparáveis aos sistemas informáticos, do setor estatal ao privado, com a possibilidade de envolver danos físicos e psicológicos em civis.

Portanto, procura-se um equilíbrio entre as forças tradicionais militares para garantir a defesa das fronteiras e intervir em caso de conflitos internacionais e entre a componente civil ao serviço do Estado na defesa do ciberespaço e das múltiplas redes informáticas. O ciberterrorismo opera igualmente na internet para a obtenção de fundos financeiros que lhe permitam levar a cabo as respetivas missões. Essa angariação de fundos compreende por exemplo o roubo de dados financeiros dos internautas registados em contas bancárias ou em números de cartões de crédito. Evidencia-se a utilização e a exploração por parte de grupos terroristas projetados para a esfera da rede virtual de *software* ou de sítios na internet que permitam a edição ou o *upload* de ficheiros sem custos adicionais, evitando assim a identificação através de transações bancárias e mantendo consequentemente o anonimato.

Além disso, o ciberespaço para os grupos qualificados de terroristas serve de base para a troca de comunicação entre os diversos grupos sem qualquer tipo de risco em ser detetado (Lewis, 2002). Recorde-se que Abu Musab al-Zarqawi, o autoproclamado líder da *Al Qaeda* no Iraque, transmitia e divulgava as suas mensagens via *fora* e *video streaming* na internet, o que provocava e fomentava uma nova atração para os seguidores *jihadistas* (Kohlmann, 2006). Um outro exemplo, abrange o caso do *Hezbollah* que reclama a utilização da internet como fonte de informação e de propaganda na luta contra Israel através do sítio <www.hizbollah.org> que por sua vez foi alvo de ataques por parte de *hackers* israelitas. Nesse contexto, em nome de uma *e-jihad*, o *Hezbollah* reconhece a utilidade e a vantagem da internet numa possível ciberguerra árabe-israelita. Sublinhe-se a criação do sítio UNITY <www.ummah.net/unity>, presentemente inativo, para implementar estratégias específicas no sentido de causar o maior impacto e danos ao governo israelita, substancialmente na desativação de sítios pertencentes à rede governamental ou no colapso de sítios ligados a setores financeiros como a banca ou o *Israel's Stock Exchange* (Trendle, 2002).

Importa referir, numa outra perspetiva, o facto de se considerar o conflito do Kosovo como a primeira guerra localizada na internet, na qual se assistira por parte dos diversos atores desse conflito a operações de informação quer na versão de *InfoOps* ou de *PsyOps*, criticando inclusive abertamente os opositores. Acresce a intervenção de *hackers* ao dar voz à escala mundial contra a situação na Jugoslávia e à postura da NATO perante o escalar do conflito, tendo determinados sítios governamentais sido alvo de ataques no sentido de desativar os mesmos. Neste caso, o ciberactivismo praticado consistiu sobretudo na exploração e na denúncia na arena internacional a partir do ciberespaço na divulgação do sentimento de horror de um conflito geograficamente localizado em território europeu. Comparativamente para um grupo terrorista um ataque perpetrado em território não virtual outorga um sentido de superioridade em termos de danos e de impacto dramático junto das entidades políticas e da sociedade civil do que uma ação ocorrida no ciberespaço que terminaria circunscrita naquele espaço. Porém, acompanha-se gradualmente um escalar de tensão e de hostilidade na utilização deste novo poder operado no espaço cibernético. Um ciberataque por parte de um grupo terrorista pode manifestar-se na interrupção de serviços em infraestruturas críticas, do aprovisionamento de água à gestão e manutenção de uma central nuclear. Em ambos os casos as consequências implicam e visam estruturas físicas com impacto junto da população civil.

Entre janeiro e março de 2011, ocorreram dois ataques por parte de *hackers*: o primeiro visava o acesso a informação estratégica de defesa do *Defence Research and Development Canada* e o segundo contra a rede do governo francês para a obtenção de informação vital que eventualmente pudesse representar uma ameaça para as próximas cimeiras do G20. Regista-se que recentemente o Departamento de Justiça norte-americano anunciou o desmantelamento de uma rede criminosa que se servia da internet para roubar dados pessoais através da propagação de um vírus espião denominado de *coreflood* que tinha por incumbência o registo das teclas utilizadas pelo utilizador aquando da sua navegação. O *coreflood* terminou por infetar cerca de 2,3 milhões de computadores.

A título exemplificativo, numa investigação levada a cabo por entidades norte-americanas e canadianas, identificou-se uma rede cibernética localizada e sediada em Chengdu, em Sichuan, na China, denominada de *Shadow* cujo alvo consiste em aceder a computadores, a sistemas informáticos, a contas do *gmail*, a plataformas de redes sociais e a *blogs* não só a nível mundial como também pertencentes a instituições governamentais indianas e a bases militares (Lemon, 2010). Um outro caso, consistiu no *worm Stuxnet*, descoberto em julho de 2010, cujo propósito residiu no ataque ao sistema operacional *Scada*, da Siemens, que controlava nas centrais nucleares as centrifugadoras de enriquecimento de urânio, tendo como alvo o reator da central de Bushehr no Irão (McMillan, 2010). Aliás, segundo o relatório *Did*

Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? do *Institute for Science and International Security* presume-se que o *Stuxnet* tenha destruído cerca de mil centrifugadoras em Natanz derivado da alteração da velocidade dos motores, o que vem afetar substancialmente o programa nuclear iraniano (Albright, Brannan, Walrand, 2010). Nesse sentido, na opinião da empresa russa *Kasperky Labs* considerar-se-á que se trata de um protótipo de uma nova ciberarma dotada de capacidade de provocar uma corrida armamentista no âmbito da possibilidade de uma ciberguerra. Respeitante a custos, o cibercrime coloca em evidência as repercussões da propagação de vírus, de ataques a alvos como as praças financeiras, a degradação dos sistemas de comunicação. Os custos financeiros representam por um lado, perdas na ordem dos mil milhões de dólares respeitantes à propriedade intelectual, a fraudes financeiras, à destruição de dados confidenciais no setor bancário e empresarial, e, por outro lado, denote-se que na fase posterior a um ataque, a dificuldade reside na recuperação da confiança perdida quer internamente quer externamente.

As Implicações: do Ambiente Terrestre ao Virtual

Tendo em consideração a dimensão do ciberespaço, torna-se evidente a impossibilidade de se pretender ou possuir sequer a intenção de o controlar na globalidade por representar o lugar por excelência de liberdade na sua plenitude, apesar de operar num novo espaço geopolítico, na senda de Solveig Godeluck (2002) ao depender de estruturas físicas e de territórios que por sua vez são controlados por Estados, para além de reproduzir e transpor os conflitos reais para uma nova fronteira no ciberespaço. Verificamos, por conseguinte, uma crescente interdependência entre duas realidades ou ambientes distintos, por um lado, o ciberespaço e, por outro lado, o mundo no qual vive o ser humano. O *linkage* comprovado entre ambos os ambientes emerge nas mais diversas formas como os casos da comunicação, da aviação, dos serviços governamentais, das finanças, da banca, das instituições público-privadas, do comércio, da medicina e da segurança, entre outros setores. A conexão de toda esta interdependência origina a possibilidade de colocar em causa e em risco não só informação irrelevante mas, sobretudo, dados estratégicos e vitais do Estado à sociedade civil.

Assumindo que o ciberespaço detém, por um lado, a capacidade de alocar um número infinito de páginas em linha sem custo adicional e, por outro lado, a possibilidade de desenvolver e de acompanhar os fluxos de informação em tempo mundial, pode considerar-se que representa uma ferramenta superior à de uma bomba nuclear dotada de capacidade de destruição global, não para o internauta comum mas para aqueles que pretendam desenvolver ações criminosas. Estas novas ame-

aças emergentes que começam a operar para além do alcance das fronteiras físicas têm vindo a fomentar o incremento da segurança e a gestão de risco do Estado, nomeadamente no tocante ao sistema informático localizado nas estruturas vitais institucionais bem como a constituição de uma nova força não militar representada por civis que saibam operar em caso extremo de ciberguerra.

Assim, presencia-se uma transformação da configuração dos setores da segurança e defesa que se projetam do Estado soberano para a realidade virtual, o que gera uma modificação da definição da política interna numa perspetiva internacional, dado que o ciberespaço não possui uma nacionalidade e/ou um território. Torna-se por conseguinte necessário, no sentido de proteger o Estado e respetivos cidadãos, o desenvolvimento de mecanismos de segurança e o reforço do papel do Estado enquanto entidade soberana e ator das relações internacionais, daí a perspetiva de David Rothkopf (1998) ao referir que a *realpolitik* de hoje não é mais do que a *ciberpolitik* de amanhã, concretamente por derivar do fator de poder, concernente a relevância estratégica e política do papel que o ciberespaço possa vir a desempenhar quer numa perspetiva das relações humanas quer nas relações internacionais. Diga-se de passagem que o poder que outrora seria reservado a determinadas potências com capacidade de projetar a ambição de domínio é na atualidade transferido e facultado no ciberespaço para aqueles que não detinham sequer essa possibilidade à escala global.

Por último, anotemos que garantia de um ambiente de segurança no ciberespaço significa o equilíbrio do sistema internacional na realidade contemporânea das relações internacionais. A emergência de novas ameaças que possam colocar em causa o equilíbrio mundial e provocar uma ciberguerra fora do campo de batalha convencional traduz-se num perigo não só para os Estados, mas para toda a humanidade. Todavia, acresce ainda que no quadro da gestão de risco, que constitua uma ameaça à segurança do território ou da sociedade civil, torna-se imperativo uma política de prevenção e de planeamento para tornar eficaz a ação perante o espectro da conflitualidade a levar a cabo quer numa perspetiva doméstica quer internacional. Daí que as Nações Unidas, através da *United Nations Interregional Crime and Justice Research Institute*, tenham na sua agenda a elaboração de um código de conduta internacional referente à utilização do ciberespaço e da envolvente política e jurídica do Estado em caso de intervenção na internet, concretamente na identificação do criminoso que poderá encontrar-se fisicamente localizado fora do domínio jurisdicional.

Bibliografia

Albright, David, Paul Brannan e Christina Walrond (2010). "Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant?" Disponível em http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf, data de acesso 18/9/2011.

Deibert, Ronald J. (2009). "The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace" em Andrew Chadwick e Philip Howard (eds), *Routledge Handbook of Internet Politics*. London: Routledge, pp. 323-336.

Delbecque, Eric (2007). *L'Intelligence Économique: Une Nouvelle Culture Pour un Nouveau Monde.* Paris: PUF.

Ettighoffer, Denis (2008). *Netbrain, Planète Numérique: Les Batailles des Nations Savantes*. Paris: Dunod.

Godeluck, Solveig (2002). *Géopolitique d'Internet*. Paris: La Découverte.

Gray, Chris Hables (2005). *Peace, War, and Computers*. London: Routledge.

Haass, Richard (2008). "The Age of Nonpolarity: What Will Follow U.S. Dominance". *Foreign Affairs,* vol. 87, n.º 3, pp. 44-56.

Haraway, Donna (1991). *Simians, Cyborgs, and Women: The Reinvention of Nature.* London: Routledge.

Kohlmann, Evan (2006). "The Real Online Terrorist Threat". *Foreign Affairs*, vol. 85, n.º 5, pp. 115-124.

Lawson, Sean (2010). *General Alexander's Confirmation and the Failure of Cyberwar Transparency*. Disponível em http://www.forbes.com/sites/firewall/2010/05/13/general-alexanders-confirmation-and-thefailure-of-cyberwar-transparency/, data de acesso 19/7/2011.

Lemon, Sumner (2011). "Researchers track cyber-espionage ring to China". Disponível em http://www.csoonline.com/article/589717/researchers-track-cyber-espionage-ring-to-china?page=1, data de acesso 11/10/2011.

Lewis, James A. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Disponível em http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf, data de acesso 12/07/2011.

Lynn, William J. (2010). "Defending a New Domain: The Pentagon's Cyberstrategy'". *Foreign Affairs*, vol. 89, n.º 5, pp. 97-108.

Mccaughey, Martha e Michael Ayers (2003). *Cyberactivism: Online Activism in Theory and Practice*. London: Routledge.

Mcmillan, Robert (2010). "Was Stuxnet built to attack Iran's nuclear program?" Disponível em http://www.infoworld.com/d/security-central/was-stuxnet-built-attack-irans-nuclear-program110, data de acesso 15/10/2011.

National Strategy for Trusted Identities in Cyberspace. Disponível em http://www.whitehouse.gov/blog/2011/04/15/president-obama-releases-national-strategy-trusted-identities-cyberspace?utm_source=related, data de acesso 22/8/2011.

Noya, Javier e Beatriz Rodríguez (2010). *Teorias Sociológicas de la Globalización*. Madrid: Tecnos.

OpenNet Initiative. Disponível em http://opennet.net/. Data de acesso 26/9/2011.

Phillips, Macon (2009). *Introducing the New Cybersecurity Coordinator*. Disponível em http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cyber-security-coordinator, data de acesso 19/7/2011.

Rothkopf, David. (1998). "Cyberpolitik: The Changing Nature of Power in the Information Age" em *Journal of International Affairs*, vol. 51, n.º 2, pp. 325-359.

Rue, Frank La (2011). *Report of the Special Rapporteur on the Promotion and Protection of the rRght to Freedom of Opinion and Expression*. Disponível em http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, data de acesso 11/10/2011.

The Comprehensive National Cybersecurity Initiative. Disponível em http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative, data de acesso 23/07/2011.

Trendle, Giles (2002). "Cyberwar". *The World Today*, vol. 58, n.º 4, pp. 7-8.

United Nations Interregional Crime and Justice Research Institute. Disponível em http://www.unicri.it/, data de acesso 17/7/2011.

Whirled Bank. Disponível em http://www.whirledbank.org/, data de acesso 21/9/2011.

Wolton, Dominique (1999). *Internet et Après? Une Théorie des Nouveaux Médias.* Paris: Flammarion.