Terrorismo e Violência Política: Como Combater o Ciberterrorismo e a Radicalização

Paulo Moniz
Diretor de Segurança de Informação e Risco de TI do Grupo EDP

Resumo
O ciberespaço, sendo uma realidade recente na história da humanidade, apresenta-se já como um espaço disruptivo onde se registam grandes alterações nas dinâmicas de poder e nos paradigmas de funcionamento da sociedade. Este artigo tem como objetivo compreender os fenómenos de radicalização, terrorismo e violência política no contexto do ciberespaço, propondo estratégias de atuação para o seu combate. Para atingir esse desiderato parte-se de uma definição do conceito do Ciberespaço e Ciberpoder, analisando-se as características que os distinguem e como as mesmas podem potenciar a atuação eficaz de grupos terroristas e radicais nesta nova conjuntura. São ainda identificadas as atuais formas de uso da internet por parte destes indivíduos ou organizações criminosas, dando-se uma perspetiva da evolução das suas atividades e as ameaças que encerram. Com base na formalização apresentada, são finalmente identificadas estratégias de combate aos fenómenos de ciberterrorismo e radicalização.

Abstract
Terrorism and Political Violence: How to Combat Cyberterrorism and Radicalization

Cyberspace, a recent reality in the history of mankind, presents itself as a disruptive space where great changes are taking place with impact on the power dynamics and in the paradigms that govern the functioning of society. This article aims to understand the phenomena of radicalization, terrorism and political violence in the context of cyberspace, offering strategic actions to combat them. To achieve this goal, we start with a definition for the Cyberspace and Cyberpower concepts, analyzing the characteristics that distinguish them and how they can, in this new context, enhance the effective performance of terrorist and radical groups. The manner Internet is used by these individuals or criminal organizations is also identified, providing information on the evolution of their activities and the threats they contain. Finally, we identify strategies to combat the phenomena of cyberterrorism and radicalization, based on the presented setting.

Introdução

Fenómenos como o terrorismo e a radicalização estão presentes na nossa sociedade e vivem nos nossos subconscientes, nas decisões que tomamos, muito mais do que queiramos admitir. O modo como os destinos das viagens de férias flutuam, consoante a localização dos episódios de violência ou a ocorrência de atentados terroristas recentes, são exemplos dos sintomas destes fenómenos assim como os impactos que têm na sociedade.

A ideia que temos do terrorismo está fortemente ligada às imagens que nos causam horror, que induzem emoções fortes no ser humano, todas elas baseadas no mecanismo básico do medo. O 11 de Setembro de 2001, com os cenários do embate das aeronaves nos edifícios emblemáticos dos EUA, o fogo imenso das torres que desmoronam, assim como os sucessivos saltos suicidas, foram, talvez, as imagens mais perfeitas que o terrorismo alguma vez conseguiu almejar. Na realidade, todas estas imagens aconteceram no plano real, no mundo convencional, por oposição ao que poderemos designar pela dimensão virtual do ciberespaço, materializada principalmente no conceito de internet, que, não deixando de ser uma estrutura física, constitui uma dimensão nova de interação, criada pelo homem, da qual a nossa sociedade depende, cada vez mais.

Parece, portanto, sensato afirmar que, para a biologia atual do ser humano, as imagens do 11 de Setembro de 2001 são muito mais poderosas e eficazes para os intentos dos terroristas, no que concerne ao ativar dos nossos medos, do que, por exemplo, a privação do acesso a certas localizações na internet ou a indisponibilidade do serviço de mensagens de texto, num determinado país, durante várias horas – ainda que estes acontecimentos possam ter um forte impacto económico e mesmo social. Assim sendo, não obstante o campo convencional continuar a reinar na capacidade de gerar imagens de horror, a verdade é que, atualmente, falamos cada vez mais da utilização do ciberespaço, quer como palco das ações terroristas, quer como veículo privilegiado para potenciar as mesmas no mundo convencional – por exemplo pela ciberpropaganda. Dentro deste domínio de utilização do ciberespaço, ainda que a balança penda, atualmente, para o seu uso enquanto meio para potenciar ações de terrorismo e radicalização, mais do que o cenário físico eleito para atentados, não invalida que esta nova dimensão tenha cada vez mais um papel preponderante e crucial na atuação destes indivíduos ou grupos, pelo que urge entendê-la, de modo a conseguir identificar e implementar estratégias para a neutralização deste tipo de ações.

No contexto deste trabalho, com o objetivo de melhor compreender a dinâmica do ciberespaço, no espectro da radicalização e do terrorismo, será conveniente começar por estabelecer e caracterizar alguns conceitos como "ciberespaço", "cibepoder" e "ciberterrorismo", para depois se descrever a utilização atual dos mesmos no contexto dos grupos radicais e, no final, identificar estratégias de combate à radicalização, ao ciberterrorismo e à ciberpropaganda.

Ciberespaço, Informação e Difusão do Poder

O "Ciberespaço", à semelhança dos oceanos ou espaço aéreo exterior, povoado pelos satélites de comunicações civis e militares à escala global, é muitas vezes entendido como um *Global Common*, assumindo-se como um domínio ou espaço partilhado pelos diversos Estados, mas que não pode ser reclamado como propriedade de nenhum Estado em particular (Buck,1998). Nesta linha de raciocínio é legítimo englobar o "Ciberespaço" como o primeiro *Global Common* totalmente criado pelo homem, sendo que nele assenta a internet, uma rede global de troca de informação e conhecimento partilhada e utilizada, quase sem barreiras, por todos.

Através da internet, em particular pela disponibilização de aplicações e conteúdos, estabelecem-se trocas de informação entre indivíduos e organizações de forma praticamente imediata, criando-nos a sensação de que as fronteiras físicas perdem o sentido e as distâncias deixam de ter significado. Não obstante o nível de abstração do plano físico proporcionado pelo uso da internet, a questão assume uma complexidade adicional, se nos lembrarmos que esta rede global de troca de informações assenta numa estrutura física, composta por servidores, equipamentos de rede e *links* de comunicações, instaladas em territórios geográficos de diferentes Estados soberanos, regidos por leis secularmente estabelecidas e gerida, quase na totalidade, por empresas privadas. Este facto, relevante para o entendimento do conceito do "Ciberespaço" e das dinâmicas de poder que nele se estabelecem, leva a que alguns autores rejeitem a sua classificação como *Global Common* (Tsagourias e Buchan, 2015), alegando que o princípio da não exclusão de acesso não é assegurado.

É neste novo contexto do "Ciberespaço" que assistimos a um novo nível de "democratização da sociedade", permitindo que indivíduos com poucos recursos, situados em locais remotos no globo, tenham uma voz ativa e a possibilidade de influenciar os acontecimentos do mundo como nunca antes. Alguns observadores apontam para um "achatamento" da estrutura social, com a eliminação de centros de controlo burocráticos e hierárquicos, passando, inclusivamente, algumas funções dos Estados a ser executas por privados e assentes em tecnologias inovadoras. Neste contexto, veja-se o exemplo da tecnologia *blockchain*[1] e os impactos que a mesma poderá ter em todo o processo da celebração de contratos entre diferentes partes (EU Blockchain Observatory and Forum, 2018). É também no ciberespaço que cir-

1 *Blockchain*, é uma tecnologia que consiste numa base de dados distribuída por vários nós numa rede, que guarda, de forma segura e confiável, registos de transações, que podem ser validados por todos os nós participantes de uma rede de *blockchain*, sem a necessidade de validação por uma entidade central.

cula uma quantidade de informação que era inimaginável apenas há 20 anos atrás[2], emergindo praticamente por todo o lado e circulando a uma velocidade estonteante, levantando a questão de qual será o impacto deste fenómeno para os governos e as dinâmicas de poder no século XXI.

As assimetrias ou os diferentes equilíbrios de "Poder" entre Estados são fenómenos a que estamos habituados e que têm estado sempre presentes ao longo da história das sociedades modernas. O fenómeno relativamente novo a que estamos a assistir diz respeito à difusão do "Poder" potenciada pela internet, em concreto pela geração de fluxos informação e acessos a conteúdos de forma pouco controlada e instantânea por qualquer individuo. Os Estados sempre foram ciosos de controlo da informação, pelo que um dos grandes desafios que se lhes apresenta na atualidade prende-se com a aparente incapacidade do exercício de pleno controlo sobre um novo domínio, em especial no que concerne à disseminação e delimitação da circulação de fluxos de informação à escala global.

Ainda que se possa defender que as implicações da disseminação da informação nas dinâmicas de poder não sejam um fenómeno novo, pois, por exemplo, a invenção de Gutenberg no Sec XV permitiu a distribuição e o acesso à Bíblia em larga escala, o que foi considerado um fator decisivo para a Reforma da Igreja Católica, é factual que o fenómeno a que estamos a assistir tem diferenças fundamentais em relação a qualquer outro ocorrido na história da humanidade, em concreto no que diz respeito à sua velocidade exponencial, à abrangência e escala global, assim como às dificuldades no estabelecimento de mecanismos de controlo.

Ciberpoder

O conceito de "Poder" é, como não poderia deixar de ser, um conceito controverso. Existem inúmeras definições de "Poder", criadas em diferentes contextos e adaptadas às diferentes situações, que foram evoluindo ao longo do tempo, contudo é razoável afirmar que o "Poder" implica a capacidade de exercer "força" ou "influência" de modo a provocar um efeito desejado em determinado domínio. O "Ciberpoder" é o entendimento dessa capacidade no ciberespaço.

O "Ciberpoder" pode, portanto, ser definido como a capacidade de usar o ciberespaço para criar vantagem ou eventos de influência em outros ambientes operacionais através de instrumentos de poder (Nye Jr., 2010). Constata-se, com base nesta definição, que para produzir efeitos do exercício de poder dentro ou fora do próprio ciberespaço, é possível utilizar, com diferentes gradações, instrumentos de poder disponibilizados, quer no ciberespaço, quer no mundo físico convencional.

2 Um estudo muito citado da empresa DOMO apontava que, em 2017, 90% de toda a informação existente na internet tinha sido criada nos dois anos anteriores e que, diariamente, se produziam 2,5 Triliões de Bytes. Ver DOMO (2017).

Com o objetivo de clarificar estas combinações entre meios e efeitos, apresenta-se, na figura 1, exemplos das dimensões do "Ciberpoder" de forma esquematizada.

Figura 1 – Dimensões do Ciberpoder com Exemplos

Dimensão Física e Virtual do Ciberpoder	Efeitos dentro do Ciberespaço	Efeitos fora do Ciberespaço
Instrumentos do Ciberespaço para o exercício de poder	**Intrusivos:** Ataques de negação de serviços na internet. **Ligeiros:** Estabelecimento de normas e standards para requisitos de segurança.	**Intrusivos:** Ataques aos sistemas que controlam infraestruturas físicas. **Ligeiros:** Difusão de mensagens na internet para a mudança de opinião publica.
Instrumentos "Físicos" para o exercício de poder	**Intrusivos:** Controlo dos Governos sobre as empresas e os serviços de internet que disponibilizam. **Ligeiros:** Disponibilização de plataformas e comunicações para suportar causas ligadas à defesa dos direitos humanos.	**Intrusivos:** Destruição física de recursos tecnológicos. **Ligeiros:** Discriminação seletiva de serviços ou mesmo a difamação de certas localizações na internet.

Fonte: adaptação de Nye Jr. (2010).

Na dimensão de utilização de instrumentos de poder disponibilizados no ciberespaço, é possível conseguir alcançar efeitos:

- **Dentro do próprio ciberespaço**, utilizando instrumentos intrusivos que podem passar pelo lançamento de ataques tecnológicos de negação de serviço através do uso de *botnets*[3], direcionados a certas localizações da internet, ou, então, pela utilização de instrumentos mais ligeiros, como o estabelecimento de normas e requisitos que contribuam para um elevado nível de segurança dos recursos tecnológicos das organizações.
- **Fora do ciberespaço**, com a utilização de instrumentos intrusivos, que podem passar por um ataque informático aos sistemas que controlam infraestruturas críticas[4], resultando desse ataque consequências no mundo físico, tais como

3 A utilização de *botnets,* para perpetrar ataques de negação de serviço a localizações na internet, é uma prática comum das organizações criminosas. As *botnets* são redes de computadores infetados, sem o conhecimento dos seus utilizadores, que são controlados remotamente através de um *software* de comando e controlo, estando essa rede de máquinas ao dispor de atores mal-intencionados para participar em ataques a outros recursos tecnológicos da rede.

4 Um dos tipos de sistemas mais conhecidos, que permitem o controlo de infraestruturas físicas, algumas delas críticas, são os sistemas SCADA (Supervisory Control And Data Aquisition), utilizados geralmente pelas *utilities* e empresas industriais para monitorizar as variáveis de controlo dos processos com impactos no mundo físico – exemplo, a distribuição em redes de energia ou água. Um ataque bem sucedido a estes sistemas pode ter consequências catastróficas na segurança da sociedade.

uma falha generalizada do abastecimento de energia. Por via do uso de instrumentos mais ligeiros, constitui-se como um bom exemplo desta atuação, a disseminação de informação pelas redes sociais de modo a influenciar a opinião pública.

Na dimensão de utilização de instrumentos "físicos" de poder, os efeitos são os seguintes:

- **Dentro do ciberespaço**, tendo como exemplo de um instrumento intrusivo o controlo direto dos governos sobre os serviços de internet das empresas privadas ou de outras organizações, ou, na categoria dos instrumentos ligeiros, a disponibilização de plataformas tecnológicas de *hardware* para suportar causas ligadas à defesa de direitos humanos.
- **Fora do ciberespaço**, dentro da esfera dos instrumentos intrusivos, pode-se falar na utilização de ataques convencionais com objetivo de destruição física, de modo a colocar inoperacionais infraestruturas de servidores e comunicações ou, na gradação dos instrumentos ligeiros, pode-se exemplificar com uma ação de discriminação seletiva de serviços ou mesmo na difamação de certas localizações na internet[5].

Ciberespaço e Ciberpoder

A caracterização do ciberespaço passa essencialmente pela identificação e análise dos seus elementos diferenciadores no contexto da sua utilização pelo ciberpoder. Neste âmbito, identificam-se os seguintes quatro fatores essenciais a destacar:

1. **Baixas barreiras de entrada**. Vivemos atualmente numa sociedade interligada através de uma rede global com uma acessibilidade nunca antes experienciada. É fácil, a qualquer individuo, praticamente em qualquer parte do planeta, ligar um recurso computacional a esta rede global e aceder instantaneamente a sistemas num outro lado do mundo. Para além da facilidade de acesso tem-se assistido ultimamente à proliferação de ferramentas fáceis de utilizar pelos ciberatacantes, acessíveis através de plataformas concebidas para a sua comercialização, exigindo-se destes cada vez menos capacidades tecnológicas para perpetuar ações criminosas.
2. **Possibilidade de ocultação**. Este é outro aspeto fundamental para o estudo do exercício do poder no ciberespaço e prende-se com a facilidade que indivíduos mal-intencionados têm para esconder as suas ações sem correrem

5 Para ilustrar melhor esta dimensão que envolve o ciberespaço, mas ao mesmo tempo o exclui, quer como alvo de efeitos diretos, quer na sua utilização como meio para o exercício de poder, temos o exemplo dos protestos de 2006 nas ruas de Washington, contra a divulgação pela Yahoo da lista de ativistas chineses, que conduziu à prisão destes indivíduos pelo governo desse país (Nye Jr., 2010).

grandes riscos de ser identificados ou detetados. Esta facilidade deve-se à simplicidade de entrar na rede através da criação de identidades fictícias ou à possibilidade de realizar ações em geografias remotas. Como ilustrado por Peter Steiner, 24 anos atrás, num famoso *cartoon* do *The New York Times*: "on the Internet, nobody knows you're a dog" (Fleishman, 2000).

3. **Mutabilidade do ciberespaço**. Trata-se de uma outra característica que importa perceber para compreender o exercício de poder no ciberespaço. A internet tem uma forma muito mutável, com a capacidade de criar e desmantelar dinamicamente sítios de internet ou locais de armazenamento de dados. Uma operação num campo convencional tem como base o reconhecimento territorial e a assunção de que o mesmo, embora possa sofrer mutações, manter-se-á, no essencial, na sua forma física conhecida. Já no ciberespaço, essa premissa não pode ser assumida.
4. **Ausência de fronteiras**. Outro aspeto que dificulta muito o controlo do ciberespaço está relacionado com a ausência de fronteiras geográficas, no sentido convencional como as conhecemos. Na prática, a navegação na internet e o acesso aos diversos recursos acontece de forma transversal, sem respeito pelas fronteiras dos Estados, o que dificulta muito a atuação jurídica, dado que um crime, perpetrado sobre um recurso em determinada localização geográfica, pode ter origem numa outra, remota, com enquadramentos legais totalmente diferentes.

Pode-se assim entender o ciberespaço como um ambiente assimétrico no que diz respeito ao exercício de poder, na medida em que potencia ações maliciosas de agentes com poucos recursos. Deve-se, no entanto, deixar claro que a difusão do poder não é o mesmo que a sua equalização, ou seja, não obstante qualquer ator poder ter um papel relevante no exercício do poder no ciberespaço, não implica que o faça da mesma forma e com o mesmo grau de eficácia que um outro agente que disponha de grandes recursos.

Agentes que Exercem Poder no Ciberespaço

Tendo por base o objetivo de compreender o exercício de poder no ciberespaço é agora conveniente proceder a uma breve identificação dos principais agentes que nele atuam, assim como as suas motivações. Para uma identificação mais clara dos agentes do ciberespaço existem alguns modelos muito completos, como aquele que apresenta a ENISA (2016, p. 59), contudo, para o objetivo que aqui se pretende atingir, a aproximação defendida por Nye Jr. (2010) é suficiente para enquadrar as estratégias apresentadas no final deste estudo. Este autor distingue as seguintes categorias de agentes do ciberespaço: Estados; as organizações com redes estruturadas; e indivíduos com redes fracamente estruturadas. Neste contexto, os diversos atores podem ser caracterizados da seguinte forma:

1. **Estados**. Os governos têm um papel determinante no governo do ciberespaço pois, tal como referido anteriormente, o ciberespaço, apesar de se apresentar com um domínio sem fronteiras, depende de infraestruturas físicas instaladas em territórios com quadros legais próprios, que servem o desígnio da soberania das Nações a que pertencem. Neste contexto o espaço geográfico é relevante e os governos podem atuar em diversos planos, desde a educação para a cibersegurança, capacitação de infraestruturas, aplicação de legislação específica ou mesmo exercendo poder de forma coerciva. Para ilustrar este último cenário recorde-se, como exemplo, a ação levada a cabo pelo governo chinês, nas greves de Xinjiang em 2009, deixando indisponíveis serviços de comunicação, resultando em 19 milhões de pessoas sem acesso a mensagens de texto e chamadas internacionais (LaFraniere e Ansfield, 2010). Ainda dentro deste tipo de ações na esfera de atuação dos Estados, existem registos de atos de guerra como, por exemplo, os atos de sabotagem de equipamento eletrónico no Iraque em 2003 ou na Georgia em 2008 (Harris, 2009).
2. **Organizações com redes estruturadas.** Nesta secção, enquadram-se como exemplo, grandes empresas multinacionais, como a Microsoft e a Google, ou até organizações criminosas, que possuem recursos financeiros, humanos e tecnológicos muito avançados com presença transnacional. No que diz respeito às empresas de grande dimensão, algumas delas apresentam um poder maior que alguns Estados, tendo mesmo levado a Dinamarca a criar, na sua estrutura diplomática, um embaixador para estes gigantes tecnológicos (Gramer, 2017). Com o aumento da utilização da computação em nuvem[6], quer para o alojamento de dados e aplicações, quer para uso de ferramentas corporativas como o e-mail, acentua-se cada vez mais o domínio que estas organizações possuem no ciberespaço, assim como a dependência da própria sociedade nos seus serviços e na segurança dos produtos que desenvolvem. Pelo lado mais negro, temos as organizações criminosas que fazem uso do ciberespaço para alimentarem o seu crescimento orgânico e as suas operações. A Al-Qaeda, por exemplo, deixou de ser uma organização fortemente hierárquica e confinada geograficamente para ser uma rede global e horizontal com uma forte dinâmica no recrutamento e na capacitação dos seus operacionais (Nye Jr., 2010, p.12).
3. **Indivíduos sem redes estruturadas.** Esta categoria assume especial importância, devido a um dos fatores distintivos do ciberespaço, que é a baixa barreira de entrada. É com facilidade que indivíduos podem interagir na rede

6 O conceito de computação em nuvem – em inglês, *cloud computing* – refere-se à utilização de memória, capacidade de armazenamento e cálculo, de computadores e servidores, interligados em rede, e acedidos através da internet. Consultar https://pt.wikipedia.org/wiki/Computa%C3%A7%C3%A3o_em_nuvem [Acedido 27 outubro 2018].

global, juntando-se a organizações ou atuando sozinhos. Neste contexto, as ferramentas desenvolvidas e disponibilizadas para a sua atuação tornam menos clara a distinção entre estes agentes e as organizações com redes estruturadas. Pelo lado negativo, o fenómeno a que assistimos mais frequentemente neste plano, está associado ao cibercrime, em que as vitimas são indivíduos e organizações e a principal motivação dos atacantes é o lucro económico. Cenários típicos de cibercrime são os ataques de *randsomware*, em que os atacantes cifram as máquinas das vítimas exigindo um resgate para as desbloquearem ou, então, os ataques de *phishing*, onde se tentam obter credenciais ou outra informação relevante, capaz de aportar valor económico a ser extraído das vítimas. Enquadra-se também nesta categoria os denominados ataques internos, normalmente perpetrados por indivíduos contra as organizações de que fazem parte.

A figura 2 ilustra os diferentes agentes e a sua capacidade de uso das ferramentas de poder descritas anteriormente.

Figura 2 – Utilização das Ferramentas de Poder pelos Diferentes Agentes do Ciberespaço

	Estados	Organizações com redes estruturadas	Indivíduos sem redes estruturadas
Instrumentos do Ciberespaço para o exercício de poder	**Intrusivos:** Podem exercer poder no ciberespaço através de valências como, por exemplo, os centros de ciberdefesa das forças armadas. **Ligeiros:** Podem estabelecer normas e *standards* para requisitos de segurança para operadores de comunicações.	**Intrusivos:** Podem ter ações coordenadas com os Estados e enquadradas nas sociedades de direito (por exemplo os operadores de internet bloquearem a propagação de mensagens ou acesso a domínios de internet). **Ligeiros:** Podem divulgar e promover ideais e convicções organizacionais, como a luta contra o racismo, através dos seus canais no ciberespaço (sites, contactos com clientes, entre outras).	**Intrusivos:** Não está previsto, sendo que, inclusive, algumas atuações na internet, como a procura de vulnerabilidades em serviços, podem ser classificadas de cibercrime pelo quadro legal em vigor. **Ligeiros:** Podem, em blogs ou redes sociais, divulgar e promover os seus ideais e convicções.
Instrumentos "Físicos" para o exercício de poder	**Intrusivos:** Podem exercer controlo sobre serviços de empresas mediante enquadramento legal (ex: para investigação criminal). **Ligeiros:** Podem disponibilizar meio tecnológicos como plataformas e comunicações para generalizar o acesso à internet.	**Intrusivos:** Não está previsto no quadro das organizações legitimas. **Ligeiros:** Podem participar e promover ideais e convicções organizacionais, como a luta contra o racismo, fora do ciberespaço.	**Intrusivos:** Não está previsto. **Ligeiros:** Na sua atuação como cidadão pode difamar certas utilizações da internet (por exemplo, condenando alguns locais da internet, na defesa da propriedade intelectual de musicas e livros).

Fonte: elaboração do autor.

Terrorismo e Ciberpoder: Ciberterrorismo

Antes de adotarmos uma definição para "Ciberterrorismo", será sensato partirmos de uma definição para "Terrorismo". No entendimento do Departamento de Defesa dos EUA, "Terrorismo" corresponde ao uso premeditado, não legitimado na lei, de violência ou ameaça, para criar medo, coagir ou intimidar governos e sociedades,

na persecução de objetivos políticos, religiosos ou ideológicos (DoD, 2018, p.232).
No que diz respeito ao "Ciberterrorismo", apesar de existirem várias definições, optar-se-á por uma que tenha em consideração a definição de "Terrorismo" aqui apresentada, assim como toda a caracterização relativa ao ciberpoder aqui feita. Deste facto resulta, como exemplo, que se exclui à partida definições de "Ciberterrorismo" que não integrem na sua definição os ataques físicos a recursos de informação, pois não seria coerente com a abordagem mais ampla aqui apresentada sobre os instrumentos do ciberpoder. Uma definição particularmente interessante do "Ciberterrosimo", pela sua simplicidade e abrangência, diz-nos que se tratam de ações premeditadas, com motivações políticas, contra informação, sistemas, programas de computadores e dados, que resultem em violência contra entidades não-beligerantes, perpetradas por grupos ou agentes clandestinos (Pollitt, 1997). Na prática, no quadro aqui apresentado, o "Ciberterrorismo" materializa a convergência dos objetivos e ideais terroristas com a realidade do ciberespaço, explorando, nesse domínio, os instrumentos do ciberpoder, com o desiderato de aumentar a eficácia no atingimento dos seus objetivos.
Atualmente, porventura pelo facto referido anteriormente, a saber, que os ataques a recursos no ciberespaço não têm o mesmo atrativo espetacular dos ataques convencionais, pois não proporcionam imagens de terror facilmente captáveis pelos meios de comunicação social, não existem registos evidentes da sua utilização pelo ciberterrorismo. O ciberespaço tem sido sim, usado pelas organizações terroristas, para potenciar e aumentar a eficácia dos ataques convencionais, em concreto nas seguintes dimensões (UNODC, 2012):

1. **Propaganda**. Trata-se basicamente de utilizar o ciberespaço para a disseminação dos ideais dos grupos terroristas, em concreto como um método importante para concretizar o ciclo de recrutamento, radicalização e instigação à ação violenta. A ciberpropaganda pode assumir várias formas, desde apresentações; documentos; revistas; filmes; vídeos ou mesmo jogos. Um dos exemplos é a revista *Dabiq*[7], utilizada para promoção dos objetivos do autoproclamado "Estado Islâmico". A ciberpropaganda acaba por beneficiar da rapidez oferecida pelo ciberespaço, mas também das baixas barreiras de entrada, o que permite aos grupos disseminar informação sem qualquer filtro e em qualquer lugar de forma imediata, ao mesmo tempo que lhes faculta a possibilidade de o fazer de maneira camuflada. Beneficia também da estru-

7 A revista *Dabiq* foi publicada, em várias línguas, pela primeira vez em julho de 2014 pelo autoproclamado "Estado Islâmico". Inicialmente era publicada através da *deep web* – internet não acessível nos motores de busca normais, utilizada, genericamente, para fins menos lícitos – mas facilmente estava disponível em outros sítios na internet acessíveis por qualquer cidadão. Disponível em https://en.wikipedia.org/wiki/Dabiq_(magazine) [acedido 25 outubro 2018].

tura de enquadramento das sociedades democraticamente mais avançadas, onde o direito à liberdade de expressão é uma prerrogativa basilar a preservar, ainda que seja aceite que tal não se aplica quando estão em causa mensagens capazes de ameaçar a segurança nacional. Pode-se, com propriedade, dizer que os locais chave para a radicalização deixaram de ser áreas geográficas, como o Iémen ou Afeganistão, e passaram a ser as comunidades virtuais estabelecidas com base na internet (Roy, 2010).

2. **Financiamento.** Segundo o relatório da United Nations Office on Drugs and Crime (UNODC, 2012) sobre o uso da internet para o cibercrime, existem quatro formas de angariação de fundos que beneficiam das características únicas do ciberespaço: solicitação direta; comércio eletrónico; pagamentos e transferências *online*; e utilização de organizações sem fins lucrativos. O financiamento direto diz respeito às solicitações realizadas através de e-mails diretos, *chats* ou sítios da internet, enquanto o comércio eletrónico está orientando para a venda de material referente às organizações, tais como livros ou vídeos. As transferências *online* são operações realizadas através de aplicações tipo PayPal ou mesmo usando moedas virtuais, sendo que, dentro desta categoria, ainda se enquadram os métodos ilegítimos, tais como roubo de credenciais e cartões de crédito ou fraudes eletrónicas. Existem também formas de financiar grupos terroristas através de organizações sem fins lucrativos, como se verificou com o financiamento de grupos terroristas no Médio Oriente, realizado através de organizações com nomes como Benevolence International Foundation ou Global Relief Foundation, que justificavam a sua atividade com base em fins de caridade (UNODC, 2012, p.7).
3. **Treinos.** Ultimamente as organizações terroristas têm utilizado a internet como plataforma de treino dos seus membros. Diversos sítios na internet providenciam informação e instruções pormenorizadas, sob o formato de manuais, ficheiros de áudio ou vídeo, em várias línguas, sobre as formas de alistamento, como construir explosivos ou planear atentados[8]. Muitas vezes estas plataformas também incluem medidas e métodos de apoio ao desenvolvimento de atividades de contra informação e *hacking*, explicando como aumentar a segurança nas comunicações através da sua encriptação e anonimização. Em síntese, as características particulares do ciberespaço, permitem às organizações terroristas uma capacidade de treino muito mais eficiente e com menor risco, por oposição às deslocações físicas através das fronteiras de diversos estados, para frequentar ações de formação, que se apresentam como demasiado arriscadas.

8 Exemplo deste tipo de atuação é possível encontrar na revista *Inspire*, publicada pela Al-Qaeda, que tem como objetivo facilitar o treino em casa dos muçulmanos para a *jihad*.

4. **Planeamento.** O planeamento das operações é outro exemplo do uso do ciberespaço pelos grupos terroristas de modo a concretizarem com sucesso os seus objetivos. Uma vez mais a facilidade de estabelecimento de comunicações seguras e praticamente anónimas entre diversas partes, assim como a disponibilização de informação em tempo real, transformam a internet numa ferramenta essencial para o planeamento de ataques. No planeamento de ações terroristas, pode-se ainda fazer uso de um manancial de informação pública, muitas vezes desprotegida, como imagens de edifícios de interesse, número de pessoas concentradas num determinado local numa certa hora do dia ou, ainda, informações pessoais de possíveis vítimas, disponibilizadas em redes sociais.
5. **Execução.** Neste plano considera-se a internet como o espaço privilegiado para coordenar e perpetrar ataques físicos, mas também para concretizar outras ações com o objetivo de gerar o medo generalizado. No primeiro caso, podemos recordar o uso intensivo da internet nos atentados do 11 de Setembro de 2001, enquanto no segundo se enquadram os vídeos, recentemente difundidos, de decapitações, apedrejamentos e genocídios perpetrados pelo autointitulado "Estado Islâmico".
6. **Ciberataques.** Apesar de se ter referido antes que os cenários de ataques terroristas no ciberespaço são menos frequentes e apetecíveis para os efeitos de medo que os terroristas pretendem atingir, existem alguns registos desses atos, com consequências, quer no plano virtual quer no plano físico, consubstanciando exercícios de poder no ciberespaço e fora dele. Com consequências no ciberespaço, recorde-se o exemplo do ataque ocorrido à TV5 francesa, inicialmente assumido pelo autoproclamado "Estado Islâmico", mas, mais tarde, atribuído a *hackers* russos[9]. Contudo, não obstante os exercícios de força no ciberespaço começarem a ganhar o seu protagonismo, as maiores consequências, ainda não muito exploradas, serão aquelas que os terroristas consigam almejar através de ações no ciberespaço com impactos no mundo físico. Fala-se, neste plano, das infraestruturas críticas de informação, que são aquelas que controlam em tempo real equipamentos como sistemas de sinalizações de redes de transporte; controlo do espaço aéreo; produção e distribuição de energia – por exemplo em centrais nucleares – ou redes de distribuição de águas, entre outras. A maioria destas infraestruturas estão sobre

9 Este caso foi um exemplo típico de uma APT (*Advanced Persistent Threat*), iniciado e preparado muito antes do dia da concretização do ataque propriamente dito, e que conseguiu colocar os onze canais da TV5 indisponíveis, difundir mensagens de reivindicações islâmicas nos meios de comunicação da empresa na internet, assim como tornar indisponíveis os recursos tecnológicos deste canal.

controlo de empresas privadas, o que implica que estas entidades têm responsabilidades na sua defesa e proteção, no plano do ciberespaço, semelhantes às forças armadas e de segurança no campo convencional. Se as infraestruturas destas empresas não tiverem implementados mecanismos de defesa e reação, a segurança da nossa sociedade, e em última instância a soberania dos países, pode ficar ameaçada[10].

Estratégias de Combate ao Ciberterrorismo e Radicalização

Estamos agora em condições de estabelecer e compreender melhor as estratégias de combate ao ciberterrorismo e radicalização, que deverão ter em consideração todas as características que aqui já foram identificadas sobre o ciberespaço, assim como a dinâmica de poder que se desenrola nesse ambiente. Segundo Lachow (2009) podem-se definir três tipos de estratégias de combate, nomeadamente no plano físico, informacional e cognitivo.

Estratégia de Combate no Plano da Infraestrutura Física

O objetivo desta estratégia é atingir as infraestruturas físicas que suportam a internet de modo a causar indisponibilidade ou disrupção dos seus serviços. Convém aqui lembrar o que até aqui dissemos sobre o ciberespaço, a saber, que, não obstante este se apresentar, numa determinada camada de abstração, como um espaço sem fronteiras, virtual, na verdade ele assenta em recursos físicos e materiais perfeitamente identificáveis, instalados em territórios de Estados soberanos. Podemos estar a falar de ações que destruam nós de comunicações nevrálgicos (infraestruturas de comunicações) ou mesmo centros de dados que albergam servidores utilizados por organizações terroristas.

As ações neste domínio de atuação serão mais eficazes quando mais focalizadas e dirigidas elas poderem ser. Destruir uma infraestrutura poderá ter um efeito imediato e com alguma durabilidade, contudo, também poderá afetar outros serviços legítimos, muitas vezes de Estados aliados, que partilhem as mesmas infraestruturas. Neste contexto, recorde-se que as plataformas internet mais utilizadas para comunicação e disponibilização de informação estão instaladas em Estados europeus ou norte-americanos. Depreende-se com facilidade que a destruição convencional de uma infraestrutura física que afete apenas o alvo desejado só poderá acontecer, com grande sucesso, em situações muito excecionais, como por exemplo equipamentos que suportem grupos terroristas em locais de treino remotos, onde os efeitos colaterais serão residuais.

10 Esta é uma das razões que levou a União Europeia a criar a legislação NIS (Network and Information Security) para toda a comunidade, com o objetivo de nivelar e reforçar as capacidades de defesa destas infraestruturas por todas as geografias do espaço europeu.

Mais eficaz neste domínio será solicitar aos operadores de serviços de internet dos Estados aliados que desliguem ou inativem serviços que estão a ser usados pelos terroristas. Contudo estas ações também têm alguma dificuldade em ser materializadas, se recordarmos o que atrás se referiu, constatando-se que o ciberespaço permite, com alguma facilidade, o desenvolvimento de uma ação camuflada e que o mesmo tem uma geografia muito mutável. Desta forma, não é difícil para os grupos terroristas moverem-se para outros serviços de internet e fazer uso dos mesmos para continuarem a perpetuarem as suas ações.

Finalmente, pode-se considerar que, dentro deste tipo de estratégia de atuação, a vigilância física das infraestruturas, sem disrupção física dos serviços, poderá ser, em muitos casos, a medida mais eficaz, monitorizando as comunicações entre organizações criminosas e utilizando essa informação para atuar no contraterrorismo. A principal e relevante dificuldade desta abordagem prende-se com eventual violação de direitos estabelecidos nas sociedades democráticas, uma vez que uma atitude de vigilância aumenta o grau de desconfiança dos cidadãos nos serviços e governos, podendo, inclusive, vir a ter impactos económicos.

Em resumo, os principais benefícios desta estratégia são obviamente a sua eficácia em termos da destruição e bloqueio do acesso à internet como instrumento de poder, dado que o seu suporte físico fica seriamente afetado no local atingido. Não obstante se conseguir um efeito destrutivo imediato, não poderemos considerar esta estratégia como a mais eficaz a longo prazo, pelas razões de que, não só a maioria dos recursos se encontram instalados em territórios europeus e norte-americano, mas também porque, ao afetar de forma pouco seletiva alguns desses recursos, estar-se-ia a afetar outros serviços, legítimos, de Estados aliados, que também fazem uso dessas infraestruturas. Corre-se assim o risco destas ações serem interpretadas como atos de guerra. É um nível de estratégia de atuação que entra nas competências dos Estados e que apenas fará sentido em ações táticas ou operacionais em determinado cenário de conflito.

Estratégia de Combate no Plano Informacional

As ações neste nível estratégico têm como objetivo intervir nas propriedades de segurança da informação, em concreto na sua confidencialidade, integridade e disponibilidade.

No que diz respeito à confidencialidade, a capacidade de interceção de mensagens difere da descrita na estratégia anterior, no plano da infraestrutura, na medida em que aqui, ao contrário do referido anteriormente, não se prevê a interferência junto dos operadores de serviços de internet, mas sim na utilização de agentes capazes de entrar nos grupos eletrónicos dos terroristas ou na capacidade de decifrar as mensagens trocadas entre indivíduos criminosos. Neste plano, as agências governamentais são os principais agentes, mas também existem outros participantes, como

por exemplo o SITE Institute[11], que foi, durante anos, uma organização sem fins lucrativos que monitorizava os sítios internet utilizados pelos grupos terroristas.
Já no que se prende com a integridade, entendem-se aqui as ações que visem conduzir a decisões erradas por parte dos atacantes, tais como, realizar intrusões nas bases de dados ou em sítios internet, utilizados pelas organizações criminosas, com o objetivo de criar desconfiança entre os atacantes. Existe neste ponto um aspeto muito relevante e que dá conta das especificidades do ciberespaço atrás descritas. Dentro dos registos deste tipo de atuação, à partida atribuído aos Estados, existem casos de cidadãos que se infiltraram em redes terroristas e que trabalham voluntariamente para as agências governamentais.
No que se refere à disponibilidade, já mencionada no plano físico através da condução de ações destrutivas mais convencionais, constata-se agora uma clara ligação a aspetos mais tecnológicos, como a capacidade de realizar ataques DoS (*Denial of Service*)[12] aos serviços internet utilizados pelos terroristas ou então às ações desenvolvidas para provocar a indisponibilidade de recursos através da exploração das suas vulnerabilidades.
Em suma, constata-se que as estratégias desenvolvidas ao nível informacional são mais fáceis de levar a cabo do ponto de vista logístico e têm menos consequências colaterais do que as estratégias desenvolvidas no plano físico. Contudo, também é verdade que estas ações necessitam de muitos recursos técnicos e não é difícil, para os atacantes, contornarem estas ações movendo-se entre localizações na internet ou alterando o esquema de cifrar mensagens que trocam entre si, mantendo-se dessa forma anónimos no ciberespaço. Fundamentalmente, é necessário perceber que estas estratégias, apesar de mais perenes e eficazes que as desenvolvidas no plano físico são também mais demoradas a produzir efeitos, exigindo mais recursos intelectuais e tecnológicos. O aspeto mais curioso e que é fundamental aqui realçar, é que estas podem ser levadas a cabo não só pelos Estados, mas também por outros agentes, como organizações com redes estruturadas ou indivíduos com recursos limitados.

11 O SITE Institute (Search for International Terrorist Entities Institute) foi fundado em 2002 e tinha como objetivo monitorar a atividade *online* de organizações terroristas. O projeto terminou em 2008 e alguns dos elementos que o integravam continuaram as suas atividades numa outra organização denominada SITE Intelligence Group.

12 DoS (*Denial of Service*), é uma interrupção de um serviço de internet causado por acessos legítimos ou ilegítimos, normalmente com intuitos maliciosos. Acessos legítimos podem ser oriundos de uma rede *botnet*, que lançam um número extraordinariamente elevado de pedidos, concentrados temporalmente, a páginas de internet, com o objetivo de esgotar a capacidade de resposta dos servidores e provocar indisponibilidade. Acessos ilegítimos podem ser atacantes que explorem vulnerabilidades de sítios da internet.

Estratégia de Combate no Plano Cognitivo

Finalmente, a um nível mais elevado de sofisticação, temos estratégias ao nível cognitivo, que têm como objetivo a mudança de perceção por parte do público em geral, influenciando desta forma as suas decisões. Neste cenário, inserem-se, por exemplo, as ações de contrapropaganda. A atuação neste plano pode ter como objetivo, entre outros, diminuir a atratividade das organizações terroristas sobre certas franjas da população, sendo fundamental para tal ter em consideração aspetos cruciais como o contexto sociopolítico, a cultura, a língua ou mesmo os valores. Para levar a cabo ações nesta dimensão será também necessário coordenar esforços, quer na vertente diplomática, quer junto dos órgãos de comunicação, balançando o respeito pela liberdade de imprensa e a necessidade de transmitir as mensagens corretas.

As ações levadas a cabo neste plano podem ser comparadas a uma guerra de ideias, onde é mais eficiente ser pró-ativo que reativo. É sabido que é necessário muito mais esforço para conseguir mudar a opinião de uma audiência quando esta já tem uma ideia preconcebida do que estabelecer novos factos e perceções. Neste âmbito, devem ser empreendidos esforços para edificar ideias nas populações mais frágeis e suscetíveis de abraçar as motivações dos terroristas, tendo em atenção o seu contexto cultural e cuidando de todos os aspetos da comunicação, desde a utilização das terminologias corretas – por exemplo, evitar a expressão "Estado Islâmico" sem referenciar a sua auto intitulação, caso contrário fica a ideia de uma legitimação que não é real – até à disponibilização abundante de contrainformação sobre as mensagens dos grupos radicais.

É sabido que a eficácia máxima só será conseguida através da educação, essencialmente na promoção dos valores que devem reger as sociedades de bem e na capacitação dos cidadãos para discernir e questionar a qualidade da informação que lhes é disponibilizada. Os Estados devem investir numa correta educação e preparação dos seus cidadãos para as novas realidades emergentes do ciberespaço. Contudo, a dificuldade destas estratégias surge porque muitos dos problemas são atuais e emergentes, sendo que, as medidas estruturais profundas que esta abordagem exige, demoram muito tempo a surtir efeito. Estas medidas tornam-se mesmo pouco atrativas para as alternâncias políticas que passam pelo poder, omitindo-se estas de empreender quaisquer esforços na criação de políticas concretas e de longo prazo em áreas fundamentais à sociedade.

Estratégia Global da Informação e Estrutura Orgânica

Foram apresentadas estratégias de combate que, como constatámos, podem ser levadas a cabo por diversos agentes e fazer uso de diferentes tipos de instrumentos de poder. Será agora conveniente realizar agora uma breve análise sobre alguns aspetos relevantes para a criação de governo que permita a implementação, com sucesso, dessas estratégias.

As estratégias de combate aqui referidas evidenciam um novo tipo de conflitualidade que se desenvolve no ciberespaço, e que é baseada na informação e nos sistemas que a suportam. Atendendo ao princípio de que cada forma de coação corresponde uma estratégia global, então a utilização conflitual da informação como forma de coação, deve fazer emergir uma Estratégia Global da Informação (Nunes, 2015). A Estratégia Global da Informação influencia outras estratégias globais, até porque a informação revela-se como um recurso necessário para atuação em outros domínios, como o económico ou militar. Neste sentido, os domínios de defesa militar e segurança do ciberespaço, respetivamente ciberdefesa e cibersegurança, deveriam, idealmente, edificar as suas estratégias em consonância com uma Estratégia Global da Informação. Considerando o que foi aqui exposto, mormente as alterações nas dinâmicas de poder proporcionadas pelo ciberespaço, conclui-se também, que as estratégias de combate ao ciberterrorismo e radicalização aqui descritas, não podem ser operacionalizadas de forma desgarrada, e só terão sentido e maior eficácia se estiverem enquadradas numa Estratégia Global da Informação que, consoante o quadro a considerar, poderá ser de âmbito nacional ou europeu.

O ciberespaço é um domínio onde existe uma responsabilidade coletiva, tornando-se necessário clarificar os papéis a desempenhar pelos diversos atores. Determinar as origens, intenções, ou mesmo o impacto dos ciberataques, não se assume como tarefa fácil, levando a que o plano de atuação integre os eixos civil-militar e nacional-internacional. Neste contexto, apesar de ser fundamental deixar clara a distinção entre ciberdefesa e cibersegurança, por terem missões diferentes, é também igualmente fundamental assegurar uma articulação entre estes dois domínios. Por oposição aos cenários convencionais, um ataque a uma infraestrutura crítica, perpetrado por via do ciberespaço, poderá exigir uma atuação coordenada, quer das forças de segurança e defesa, como, em especial, das organizações privadas detentoras dessas infraestruturas, sendo que, com elevada probabilidade, nenhum dos atores mencionados terá capacidades suficientes, em isolado, para combater uma ameaça desse tipo.

A cooperação, quer entre Estados, quer entre entidades do Estado e atores civis, surge como orientação fundamental nas estratégias combate ao ciberterrorismo e radicalização. Da mesma forma deverá existir uma entidade responsável e regulamentação dirigida à coordenação entre os dois domínios da Cibersegurança e Ciberdefesa, de modo a aproveitar sinergias e concertar políticas de proteção e reação, em especial, na edificação de uma capacidade de resposta conjunta em cenários de crise. Estabelecer protocolos de atuação com os operadores de serviços de internet ou com as empresas que controlam infraestruturas críticas, são exemplos, que não esgotam, de forma alguma, o rol das iniciativas possíveis, de contributos para uma maior eficiência das estratégias de combate, assim como de ações capazes de estabelecer um nível de confiança dos cidadãos.

Conclusão

O ciberespaço, sendo uma realidade muito recente na história da humanidade, apresenta o potencial para provocar a maior das disrupções da nossa civilização. Neste espaço virtual, criado pelo homem, já se começaram a produzir alterações estruturais ao funcionamento das sociedades, sendo que algumas delas ameaçam baralhar as dinâmicas de poder nelas estabelecidas, conduzindo, ainda, a uma fragilização do controlo exercido pelos governos dos países. É um domínio que apresenta uma grande facilidade de acesso e ocultação, com circulação de enormes volumes informação de forma praticamente instantânea e sem controlo, oferecendo, desta forma, uma assimetria de exercício do poder (ainda que os atores com mais recursos continuem a ter muito mais probabilidades de êxito nas suas ações).

No contexto do ciberterrorismo e radicalização, constata-se que, atualmente, indivíduos ou organizações terroristas, continuam a privilegiar o mundo físico convencional para os seus golpes, em prejuízo dos ataques em que os alvos são recursos no ciberespaço. Cientes do poder das imagens mediáticas e dos cenários trágicos de terror, que provocam medo na mente das populações, estes agentes mal-intencionados preferem utilizar a internet como meio para aumentar a eficácia dos seus ataques convencionais, sendo poucos, ou inexistentes de forma claramente assumida, os registos de ataques terroristas com efeitos no próprio ciberespaço.

Não obstante esta tendência preferencial, para as ações de terrorismo e radicalização, seria perigoso descurar, não só o atual nível de utilização do ciberespaço pelas organizações terroristas, como as possibilidades ainda não exploradas, por estes indivíduos ou organizações, que constituem verdadeiras ameaças à nossa sociedade, como é o caso de eventuais ataques direcionados às infraestruturas críticas. A evolução tecnológica e do bem-estar social fez com que infraestruturas, como redes de energia ou águas, estejam, atualmente, quase na totalidade, dependentes de sistemas e comunicações instalados no ciberespaço. Um ataque aos sistemas que controlam infraestruturas críticas pode ter consequências dramáticas, no limite catastróficas para as nossas sociedades.

Com o objetivo de combater o ciberterrorismo e a radicalização, há que compreender os agentes com capacidade de intervenção no ciberespaço, as possibilidades das suas ações no âmbito dos instrumentos de poder oferecidos por este ambiente, e as estratégias de combate eficazes a diversos níveis. É importante ainda perceber que a atuação deverá estar assente sobre pilares estratégicos e estruturais muito fortes, nomeadamente numa definição de uma estratégia global da informação e uma coordenação muito clara e eficaz entre os domínios militar e civil.

Estamos na presença de desafios com contornos diferentes daqueles que estávamos habituados no passado, problemas sistémicos e holísticos, que exigem abordagens de colaboração e coordenação, a escalas globais, quer dos Estados e das forças de defesa e segurança, quer das empresas e cidadãos. Resolver os problemas das socie-

dades contemporâneas com metodologias do passado, baseadas em silos e centradas em competências específicas, ignorando a partilha e o diálogo, não produzirá certamente os efeitos que se desejam. Acresce que o tempo de reação aos acontecimentos não permitirá que cheguemos a essa conclusão de forma vagarosa, pelo que urge atuar, reforçando e melhorando todas as iniciativas nacionais e europeias já implementadas, assegurando ainda, ao nível da governação, acordos para estratégias eficazes de longo prazo, de modo a assegurar um melhor bem-estar às próximas gerações.

Finalmente, existe um aspeto fundamental que deverá estar presente em qualquer estratégia de combate ao ciberterrorismo e radicalização, trata-se do respeito que Estados e organizações deverão ter em relação aos direitos humanos e às legislações em vigor, em que a Lei de Proteção de Dados Europeia é um exemplo relevante. É crucial, para confiança nas sociedades democráticas, deixar claro que as medidas de contraterrorismo e o respeito pelos direitos humanos não são objetivos conflituosos. Não é necessário sacrificar os direitos adquiridos das nossas sociedades democráticas em prol de estratégias de combate ao terrorismo. São efetivamente finalidades complementares, em espaços colaborantes, e não conflituosas.

Bibliografia

Buck, S. J., 1998. *The Global Commons: An Introduction*. Washington: Island Press.

Department of Defense (DoD), 2007. *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication 1-02, 12 April 2001 as amended through 17 October 2007. Washington: The Joint Staff. [online] Disponível em: https://marineparents.com/downloads/dod-terms.pdf

DOMO, 2017. Data Never Sleeps 5.0. *DOMO* [online]. Disponível em: https://www.domo.com/learn/data-never-sleeps-5 [acedido 16 outubro 2018].

European Union Agency for Network and Information Security (ENISA), 2016. *ENISA Threat Landscape 2015*, janeiro, ENISA. [online] Disponível em: https://www.enisa.europa.eu/publications/etl2015/at_download/fullReport [acedido em 18 de outubro de 2018]

EU Blockchain Observatory and Forum, 2018. *Blockchain Innovation in Europe*. Workshop report, EU Blockchain Observatory and Forum, European Commission, Rathaus Vienna, 22 de maio. [online] Disponível em: https://www.eublockchainforum.eu/sites/default/files/reports/20180613_workshop_report_blockchain_innovation_europe.pdf

Fleishman, G., 2000. Cartoon Captures Spirit of the Internet. *The New York Times* [online], 14 de dezembro. Disponível em: https://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html [acedido em 18 de outubro de 2018].

Gramer, R., 2017. Denmark Creates the World's First Ever Digital Ambassador. *Foreign Policy* [online], 27 de janeiro, 2:37 PM. Disponível em: https://foreignpolicy.com/2017/01/27/

denmark-creates-the-worlds-first-ever-digital-ambassador-technology-europe-diplomacy [acedido em 18 de outubro de 2018].

Harris, S., 2009. The Cyberwar Plan. *National Journal*, 13 November, Washington.

Lachow, I., 2009. Cyber Terrorism: Menace or Myth? Em Franklin Kramer, Stuart Starr e Larry Wentz, eds., *Cyberpower and National Security*. Washington: Center for Technology and National Security Policy, National Defense University Press, pp. 437-464.

LaFraniere, S. e Ansfield, J., 2010. Cyberspying Fears Help Fuel China's Drive to Curb Internet. *The New York Times*. [acedido em 18 de outubro de 2018].

Nunes, P. V., 2015. *Sociedade em Rede, Ciberespaço e Guerra de Informação: Contributos para o Enquadramento e Construção de uma Estratégia Nacional da Informação.* Lisboa: Instituto da Defesa Nacional.

Nye Jr., J., 2010. *Cyber Power*, maio. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School. [online] Disponível em: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf [acedido em 18 de outubro de 2018].

Pollitt, M., 1997. Cyberterrorism: Fact or Fancy? Conference Paper, *20th National Information Systems Security Conference*, October 7-10, Baltimore, Maryland. Disponível em National Institute of Standards and Technology (NIST): https://csrc.nist.gov/publications/detail/conference-paper/1997/10/10/proceedings-of-the-20th-nissc-1997

Roy, O., 2010. Recruiting Terrorists. *International Herald Tribune*, 11 de janeiro.

Tsagourias, N. e Buchan, R., eds., 2015. *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing.

United Nations Office on Drugs and Crime (UNODC), 2012. *The use of the Internet for terrorist purposes.* Nova Iorque: United Nations Publication. Disponível em: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf