Do 11 de Setembro de 2001 à Guerra ao Terror

reflexões sobre o terrorismo no século XXI

Organizadores
André de Mello e Souza
Reginaldo Mattar Nasser
Rodrigo Fracalossi de Moraes

ipea
Por um Brasil desenvolvido

Governo Federal

Secretaria de Assuntos Estratégicos da Presidência da República
Ministro interino Marcelo Côrtes Neri

ipea **Instituto de Pesquisa Econômica Aplicada**

Fundação pública vinculada à Secretaria de Assuntos Estratégicos da Presidência da República, o Ipea fornece suporte técnico e institucional às ações governamentais – possibilitando a formulação de inúmeras políticas públicas e programas de desenvolvimento brasileiro – e disponibiliza, para a sociedade, pesquisas e estudos realizados por seus técnicos.

Presidente
Marcelo Côrtes Neri

Diretor de Desenvolvimento Institucional
Luiz Cezar Loureiro de Azeredo

Diretor de Estudos e Relações Econômicas e Políticas Internacionais
Renato Coelho Baumann das Neves

Diretor de Estudos e Políticas do Estado, das Instituições e da Democracia
Daniel Ricardo de Castro Cerqueira

Diretor de Estudos e Políticas Macroeconômicas
Cláudio Hamilton Matos dos Santos

Diretor de Estudos e Políticas Regionais, Urbanas e Ambientais
Rogério Boueri Miranda

Diretora de Estudos e Políticas Setoriais de Inovação, Regulação e Infraestrutura
Fernanda De Negri

Diretor de Estudos e Políticas Sociais
Rafael Guerreiro Osorio

Chefe de Gabinete
Sergei Suarez Dillon Soares

Assessor-chefe de Imprensa e Comunicação
João Cláudio Garcia Rodrigues Lima

Ouvidoria: http://www.ipea.gov.br/ouvidoria
URL: http://www.ipea.gov.br

Do 11 de setembro de 2001 à guerra ao terror : reflexões sobre o terrorismo no século XXI / organizadores: André de Mello e Souza, Reginaldo Mattar Nasser, Rodrigo Fracalossi de Moraes. – Brasília : Ipea, 2014.
186 p. : grafs.
Inclui Bibliografia.

ISBN 978-85-7811-195-3

1. Terrorismo. 2. Política Internacional. 3. Relações Econômicas Internacionais. 4. Segurança. 5. Religião. 6. Internet. 7. Crimes de Informática. I. Souza, André de Mello e. II. Nasser, Reginaldo Mattar. III. Moraes, Rodrigo Fracalossi de. IV. Instituto de Pesquisa Econômica Aplicada.

CDD 303.625

SUMÁRIO

APRESENTAÇÃO **7**

INTRODUÇÃO **9**

CAPÍTULO 1
A RELEVÂNCIA DO TERRORISMO NA POLÍTICA INTERNACIONAL CONTEMPORÂNEA E SUAS IMPLICAÇÕES PARA O BRASIL 13
André de Mello e Souza
Rodrigo Fracalossi de Moraes

CAPÍTULO 2
PANORAMA DA POLÍTICA DE SEGURANÇA DOS ESTADOS UNIDOS APÓS O 11 DE SETEMBRO: O ESPECTRO NEOCONSERVADOR E A REESTRUTURAÇÃO ORGANIZACIONAL DO ESTADO 45
Marcos Alan S. V. Ferreira

CAPÍTULO 3
AS FALÁCIAS DO CONCEITO DE "TERRORISMO RELIGIOSO" 65
Reginaldo Mattar Nasser

CAPÍTULO 4
O IMPACTO ECONÔMICO DO 11 DE SETEMBRO 89
Renato Baumann

CAPÍTULO 5
"NINE/ELEVEN": REPERCUSSÕES NO PENSAMENTO EUROPEU 107
Luís Moita

CAPÍTULO 6
O PAQUISTÃO E O COMBATE AO TERRORISMO NA ÁSIA MERIDIONAL: ENTRE O INTERVENCIONISMO ESTADUNIDENSE E A REGIONALIZAÇÃO DA SEGURANÇA 129
Edson José Neves Júnior

CAPÍTULO 7
A SECURITIZAÇÃO DO CIBERESPAÇO E O TERRORISMO: UMA ABORDAGEM CRÍTICA 161
Marco Cepik
Diego Rafael Canabarro
Thiago Borne

CAPÍTULO 7

A SECURITIZAÇÃO DO CIBERESPAÇO E O TERRORISMO: UMA ABORDAGEM CRÍTICA

Marco Cepik*
Diego Rafael Canabarro**
Thiago Borne***

1 INTRODUÇÃO

O crescimento do ciberespaço e o aumento do número de usuários da Internet, a partir da comercialização do acesso à rede em 1995, fizeram com que ela alcançasse o *status* de serviço público global (Blumenthal e Clark, 2009, p. 207) e passasse a ser considerada a "espinha dorsal" do mundo globalizado (Kurbalija e Gelbstein, 2005, p. 7; Zukang, 2007, p. 6). Contudo, à medida que cresce a dependência da sociedade em relação a sistemas informáticos e computacionais, bem como se diversificam as possibilidades de aplicação destas tecnologias para fins lícitos e ilícitos, intensifica-se o debate em torno dos desafios que a era digital apresenta à segurança nacional e internacional.

A exploração do ciberespaço para fins político-estratégicos, seja por atores estatais seja por atores não estatais, integra há tempos a agenda de pesquisa dos estudos de segurança (Arquilla e Ronfeldt, 1997; 2001). Entretanto, foi a partir do desencadeamento da guerra global ao terrorismo com os atentados de 11 de setembro de 2001 – diante do comprovado emprego da Internet e de outras tecnologias da informação e da comunicação pela al-Qaeda (Weimann, 2006) – que um rol bastante variado de atividades levadas a cabo por redes computacionais passou a ser indiscriminadamente tratado como assunto de segurança (Starr, 2009; Clarke e Knake, 2010).

* Professor dos programas de Pós-Graduação em Ciência Política e Estudos Estratégicos Internacionais da Universidade Federal do Rio Grande do Sul (UFRGS). Diretor do Centro de Estudos Internacionais sobre Governo (CEGOV) da UFRGS.
** Doutorando em ciência política pela UFRGS. Assistente de pesquisa do GT Governança Digital do CEGOV/UFRGS.
*** Doutorando em estudos estratégicos internacionais pela UFRGS. Assistente de pesquisa do GT Defesa, Inteligência e Segurança do CEGOV/UFRGS.

Diante disso, este capítulo propõe-se a delimitar as principais razões, bem como avaliar criticamente as consequências da securitização[1] da Internet a fim de clarificar algumas das confusões conceituais que vêm se proliferando a partir da adição do prefixo "ciber" à guerra e ao terrorismo. Para tanto, o texto divide-se em quatro seções, além desta introdução. Para abordar a interação entre a Internet e o terrorismo, a seção 2 delimita em termos técnicos e sociais o escopo do ciberespaço e da Internet. Parte-se do pressuposto de que o estudo da interação entre tecnologia e sociedade carece, no âmbito das ciências sociais, de atenção para os aspectos técnico-estruturais de determinada tecnologia estudada (Winner, 1986), bem como para os aspectos institucionais e organizacionais que moldam a aplicação desta tecnologia em um determinado contexto social (Fountain, 2001). Em seguida, na seção 3, apresentam-se alguns dos principais eventos que incorporaram a Internet às agendas acadêmica e política de segurança nacional e internacional. A seção procura sinalizar as principais consequências decorrentes da securitização da Internet, ressaltando questões teóricas e práticas que deverão ser aprofundadas pelos estudos de segurança com o avanço da digitalização. Na seção 4, aborda-se especificamente uma destas questões: a relação entre Internet e terrorismo, em especial no contexto dos dez anos que se seguiram ao 11 de Setembro. Ao fim, na seção 5, avalia-se criticamente o tratamento securitizado do ciberespaço e da Internet na atualidade, e demonstra-se a impossibilidade de se desvincular o estudo da segurança de aspectos técnicos fundamentais e de questões políticas inerentes às tecnologias da informação e da comunicação.

2 CIBERESPAÇO E INTERNET

Ciberespaço e Internet não são exatamente a mesma coisa. O primeiro precede o desenvolvimento do segundo em décadas. O ciberespaço é um domínio operacional marcado pelo uso da eletroeletrônica e do espectro eletromagnético com a finalidade de criação, armazenamento, modificação e/ou troca de informações pelas redes interconectadas e interdependentes (Kuehl, 2009, p. 29). Neste sentido, as redes de telégrafo, radioamador, telefonia fixa e/ou móvel e televisão via satélite configuravam o ciberespaço muito antes do advento da Internet.

1. Securitização é um conceito desenvolvido por Buzan, Wæver e Wilde (1998), da Escola de Copenhague. Para os autores, que procuram sintetizar correntes realistas e construtivistas da Teoria das Relações Internacionais, o estudo da segurança e/ou da insegurança deve englobar tanto aspectos materiais – armas, distribuição de poder, questões demográficas etc. – quanto imateriais próprios das fontes de insegurança. Os aspectos imateriais se referem a processos sociocognitivos de interpretação de ameaças inerentes à forma com a qual determinado assunto – não necessariamente relacionado ao emprego da força, como, por exemplo, o caso das migrações ou a degradação do meio ambiente – é enquadrado como ameaça existencial a um objeto de referência – a população do país que recebe migrantes, ou a humanidade, respectivamente, no caso dos exemplos citados anteriormente. Segundo a teoria, quando determinado assunto é legitimamente percebido como ameaça existencial, justifica-se a adoção de medidas extraordinárias que extrapolam a ordem regular do processo de decisão política daquele país, diante da urgência de medidas que garantam a segurança do objeto ameaçado. Inicialmente, a Escola de Copenhague identificou processos de securitização nos setores militar, econômico, ambiental, político e social das relações internacionais. Um panorama a respeito da Escola de Copenhague pode ser encontrado em Duque (2009). Mais recentemente, Hansen e Nissenbaum (2009) se propuseram a ampliar o ferramental teórico dos estudos de segurança da Escola de Copenhague, a partir da avaliação de eventos de securitização relacionados ao ciberespaço e à Internet, agregando assim o setor cibernético à análise.

Contudo, com a revolução científico-tecnológica da década de 1970 e a invenção dos circuitos eletrônicos integrados – os populares *microchips* –, tais redes passaram a se apoiar em tecnologias da informação e comunicação (TIC) centradas na computação. Aos poucos, e notadamente a partir dos anos 2000, a Internet tornou-se não apenas a principal rede que compõe o ciberespaço, mas a plataforma para a qual têm convergido as demais tecnologias (Serra, 2006).

O crescimento da Internet coincidiu com o fim da Guerra Fria e a decisão do governo norte-americano de explorar comercialmente aquilo que, até então, era a ARPANET, uma rede de comunicação piloto montada pelo Departamento de Defesa dos Estados Unidos (DoD), interligando instituições de ensino e pesquisa que desenvolviam projetos financiados pelo DoD (Kleinwächter, 2007; Bygrave e Bing, 2009). Contribuiu para a popularização da rede a proliferação do número de protocolos de comunicação para as diferentes aplicações especializadas da Internet (*e-mail*: *simple mail transfer protocol* – SMTP; troca de arquivos: *file transfer protocol* – FTP; acesso a sítios virtuais graficamente constituídos: *hypertext transfer protocol* – HTTP; entre outros). Provavelmente, o mais influente destes protocolos foi o HTTP, que permitiu a criação da *world wide web* (www), ou simplesmente *web*, uma aplicação que funciona como uma espécie de janela de entrada a partir da qual outros endereços da Internet são acessados mediante o clique sobre um signo – palavra, imagem, animação etc.[2] A *web* aumentou em muito a usabilidade da Internet para o usuário não especializado e, segundo estatísticas de junho de 2012, a rede é acessada por mais de 2,2 bilhões de pessoas no mundo, tendo crescido 528% entre 2000 e 2012 (World Internet Users and Population Stats, 2012).[3]

Inicialmente, a avaliação do impacto dessa trajetória de popularização da Internet assumiu forma extremamente otimista e antiestatista (Van Dijk, 2005).[4] Mas o escrutínio apurado da engenharia da Internet revela um cenário

2. O princípio de funcionamento dessa aplicação é simples: as informações armazenadas em servidores e computadores distintos podem ser ligadas por meio de uma linguagem de formatação de documentos (*hypertext mark-up language* – HTML) que permite a criação de *links* entre bancos de dados distintos. Este sistema, quando traduzido para uma linguagem compreendida por seres humanos, deixa *mark-ups* (marcas) no conteúdo publicado que levam o leitor a outros sítios virtuais (Berners-Lee, 1989). O documento originalmente desenvolvido por Berners-Lee pode ser acessado no sítio virtual da World Wide Web Consortium: <http://www.w3.org/History/1989/proposal.html>.

3. Primeiro, a *web* assumiu uma versão chamada de 1.0, em que os sítios virtuais funcionavam como vitrines divulgadoras de conteúdo em uma via unidirecional. A tecnologia continuou a se desenvolver até chegar ao cenário atual, marcado pelas redes sociais, *Web* 2.0 (ou multidirecional) e Governo 2.0. O último termo, em especial, refere-se ao emprego de TIC pelos governos não apenas de maneira unidirecional, como no fornecimento de informações ou na coleta de tributos a partir de sistemas informatizados, mas também de maneira multidimensional, como na colheita de *inputs* de participação no ciclo de políticas públicas e nos processos de consulta democrática.

4. O otimismo inerente à popularização da Internet pode ser sintetizado pelo texto seminal de John Perry Barlow, um dos mais reconhecidos entusiastas e pioneiros da vida virtual. Em sua declaração de "ciberindependência", publicada em 1996, o autor proclama uma verdadeira transformação da ordem westfaliana centrada na soberania estatal: "medidas crescentemente hostis e coloniais nos põem na mesma posição de alguns antepassados amantes da liberdade e da autodeterminação que tiveram de rejeitar as autoridades de potências distantes e desinformadas. Devemos declarar nossa existência virtual imune a sua soberania, mesmo que continuemos consentindo às suas jurisdições sobre nossos corpos. Nos espalha virtualmente através do planeta de maneira que ninguém poderá prender os pensamentos" (Barlow, 1996, tradução nossa).

mais complexo, longe da percepção inicial de completa desvinculação entre o usuário ou conteúdo *on-line* e determinado espaço físico submetido à jurisdição soberana de algum Estado (Goldsmith e Wu, 2006). Nesse sentido, a Internet está estruturada em, no mínimo, três camadas distintas.

A *camada inferior* tem relação com os elementos físicos que dão suporte às conexões e ao fluxo de dados que por meio delas circulam. São, por exemplo, as linhas telefônicas, os cabos de conexão, as antenas de transmissão, os satélites etc. A *camada superior* compõe-se das informações partilhadas e acessíveis pelos usuários, que são codificadas e decodificadas de padrões compreensíveis por seres humanos para padrões computacionais por aquilo que se encontra na *camada intermediária*, os padrões técnicos e lógicos responsáveis por esta tradução. O uso e a partilha destas informações por diferentes usuários geram ainda uma *quarta camada*, um espaço vastíssimo de interações sociais (Eisenberg e Cepik, 2002) que se desenvolve de maneira transnacional e impõe múltiplos desafios aos processos de governança política nos planos nacional e internacional (Mueller, 2002; Malcolm, 2008; Drake, 2008).

A geografia do ciberespaço é delimitada, de um lado, por constrangimentos técnico-tecnológicos que definem as condições de uso da Internet em cada uma das camadas apresentadas anteriormente. Um exemplo disto é o modelo atual de endereços IP (IPv4), que, limitado a 4 bilhões de combinações matemáticas possíveis, tende à insuficiência, dada a crescente necessidade de novos identificadores para a conexão de dispositivos à Internet.

De outro lado, existem limites socioeconômicos e políticos que restringem para mais ou para menos a possibilidade de uso e a capacidade de organização dos usuários da Internet. São exemplos: a exclusão digital; os diferentes custos de conexão ao *backbone* da Internet; a preponderância do alfabeto latino nos nomes de domínio que identificam sítios na *web*; a legislação dos diferentes Estados etc.

Essas questões, entre muitas outras que integram a agenda abrangente de governança da Internet, transcendem em muito o campo técnico-tecnológico referente ao ciberespaço e à Internet: o que antes era uma matéria restrita aos círculos especializados em computação, passou a ter implicações para inúmeras áreas da vida em sociedade e a pautar a agenda mais ampla da política global na era digital (Canabarro, 2012). A seção seguinte aborda uma destas questões, a saber, a segurança cibernética e a securitização do ciberespaço.

3 A SECURITIZAÇÃO DO CIBERESPAÇO

O crescimento atual da Internet é marcado por duas tendências: *ubiquidade* e *convergência digital*. A *ubiquidade* diz respeito à qualidade de onipresença da rede, com dispositivos de todo o tipo sendo desenvolvidos para conectarem-se uns aos

outros, utilizando os protocolos de comunicação da Internet. A *convergência digital* é um fenômeno social complexo de integração de mídias distintas em um único canal de transmissão, a qual vem revolucionando as instituições e o modo de produção midiática do século XX. Um moderno telefone celular, por exemplo, é, ao mesmo tempo, uma televisão, um rádio, um telefone, um *modem*, uma máquina fotográfica, uma plataforma de acesso à *web* etc. Atualmente, a telefonia móvel é a TIC que mais cresce no mundo e tem o maior potencial de diminuir o custo e aumentar as possibilidades de acesso à Internet (World..., 2012). Se, por um lado, estas integrações de mídias podem ser vistas como oportunidades comerciais para a ampliação de mercados consumidores de serviços relacionados à Internet, por outro, podem significar uma possibilidade de democratização do acesso, que, em diversos países, ainda tem preços impeditivos para a maioria da população.

Contudo, os avanços observáveis até o momento e a ampliação do tamanho da Internet trouxeram, além de benefícios econômicos e administrativos para governos, empresas e cidadãos, uma série de implicações políticas relacionadas à maior disponibilidade de canais de interação e comunicação entre as populações do planeta. Na década de 1990, por exemplo, as transmissões de televisão via satélite permitiram que públicos distantes vissem, em tempo real, imagens de guerras ocorrendo em locais antes remotos. A influência deste formato de transmissão sobre a opinião pública e sobre o ciclo de políticas públicas recebeu o nome de *efeito CNN* (Strobel, 1996; Livingstone, 1997). Na primeira década de 2000, como decorrência do crescimento da Internet, o efeito CNN foi potencializado por aplicações que permitem interação bidirecional entre fornecedores e consumidores de informação. Nestas aplicações – *blogs*, redes sociais etc. –, o mesmo canal midiático que transmite determinada informação, permite, em geral, a réplica, a contestação e a mobilização daqueles que a recebem (Richardson, 2009).

Além disso, no processo de desenvolvimento da Internet, as preocupações com a segurança dos usuários individuais e da sociedade ficaram em segundo plano em relação a questões técnicas como disponibilidade, funcionalidade, interoperabilidade de diferentes sistemas, facilidade de uso e velocidade de conexão. Um dos criadores da Internet, Vincent Cerf (Krill, 2009), explica que, apesar de todo o projeto da rede ter sido desenvolvido sob comando do DoD e em plena Guerra Fria, o pessoal civil da área de TI nas universidades e empresas envolvidas no projeto de construção da ARPANET mantinha relativa autonomia. A Internet era antes um projeto piloto, tendo alcançado a abrangência que tem hoje justamente por causa da colaboração entre pares que se formou em torno da comunidade de usuários, técnicos e empresas de TI. Só recentemente ela passou a atrair a atenção mais focada dos Estados, tanto por suas aplicações positivas quanto pelas possibilidades de empregá-la de maneira nociva. É a partir deste cenário que se pode pensar as questões relativas às vulnerabilidades e ameaças inerentes à era digital.

3.1 Ameaças cibernéticas contemporâneas

Nos últimos anos, ações deliberadas de indivíduos e/ou de organizações de caráter variado inundaram os noticiários, ganharam espaço na literatura e passaram a movimentar o debate relativo à segurança nacional e internacional. Notadamente, o relatório intitulado *Strategic trends 2012: key developments in global affairs*, do Centro para Estudos de Segurança do Instituto Federal de Tecnologia da Suíça, dedicou um capítulo inteiro ao tema da securitização do ciberespaço (Möckli, 2012). O capítulo apresenta um histórico dos principais incidentes cibernéticos – não necessariamente relativos à Internet – registrados desde 1986 (Cavelty, 2012, p. 108-109). Entre estes, estão: os vírus *Morris Worm* (1986), *Michelangelo* (1992), *I Love You* (2000), *Nimda* (2001) e *Stuxnet* (2010); o acesso não autorizado a contas do Citibank (1994), que gerou ao banco um prejuízo, à época, de US$ 10 milhões; o escândalo do *Cablegate* (2010), em que um conjunto de comunicações classificadas de chancelarias ao redor do mundo foi trazido a público pela organização *Wikileaks*; e uma série de eventos vinculados a operações militares a partir da década de 1990, especialmente pelo emprego de TIC como ferramentas a serviço da guerra informacional – Kossovo, em 1999, e Iraque, em 1991 e 2003 –, de retirada do ar de sítios virtuais – Estônia, em 2007 –, e de inviabilização de linhas de comunicação inimigas – Geórgia e Rússia, em 2008.

BOX 1
O *bug* do milênio

Provavelmente, o primeiro episódio de comoção global em relação aos perigos da computação relacionou-se com o evento que ficou conhecido como o *bug* do milênio.

No início do desenvolvimento da programação computacional, cada *byte* (ou caractere) de memória era muito caro. O custo de produção de um *megabyte* (106 *bytes)* pela IBM, em 1956, estava estimado, em valores atuais, em US$ 10 mil. Em 2010, com apenas um centavo de dólar, a empresa Western Digital era capaz de produzir 122 *megabytes* (122 x 106 *bytes*). Para economizar memória, portanto, em vez de grafarem as datas com quatro algarismos – 1983, por exemplo –, as empresas de TI gravavam-nas com apenas dois – 83. Esta técnica revelou-se perigosa com a aproximação do ano 2000, tendo em vista a potencial inadequação daquele sistema para interpretar a nova data – 00.

Um exemplo do que poderia acontecer em termos de catástrofe se relaciona com os juros de aplicações financeiras. Considere-se o acumulado na poupança de um indivíduo em 1999 – ou, para os computadores, 99. Como o *software* que calcula a correção monetária e os juros em um banco interpretaria o ano 2000 (ou 00)? Intuitivamente, ponderou-se que o 00 poderia ser interpretado como 1900 e, por isso, ou seriam calculados juros negativos, ou os programas de computador colapsariam diante do evento inesperado. Ambos os resultados trariam efeitos devastadores para o sistema financeiro global. O mesmo poderia acontecer com o planejamento logístico de empresas, uma vez que, ao invés de andar para frente, os calendários dos sistemas computacionais poderiam ser reiniciados para o início do século XX, o que poderia levar à paralisação dos processos produtivos. Estima-se que mais de US$ 300 bilhões[1] tenham sido investidos para corrigir os inconvenientes das técnicas de programação dos anos anteriores, especialmente no âmbito do sistema financeiro (Stuxnet..., 2000).

A partir daí, refletiu-se de forma crescente sobre os perigos da dependência e das vulnerabilidades intrínsecas a sistemas informatizados e de tecnologia computacional.

Elaboração dos autores.
Nota: [1] Aproximadamente US$ 400 bilhões em valores de 2012 – correção pelo Consumer Price Index – All Urban Consumers, dos Estados Unidos.

O ex-oficial da Agência Central de Inteligência (em inglês, Central Intelligence Agency – CIA), Thomas Reed (2004), conta em seu livro de memórias que os Estados Unidos cometeram uma ação de sabotagem contra a União Soviética em 1982, gerando a maior explosão não nuclear registrada durante a Guerra Fria. Segundo o autor, a CIA infiltrou-se em uma empresa canadense de produção de *softwares*, a qual havia sido contratada pela União Soviética para desenvolver uma ferramenta denominada *Supervisory Control and Data Acquisition* (SCADA) para a automação das atividades do gasoduto transiberiano que ligava as cidades russas de Urengoy, Surgut e Chelyabinsk. O trabalho dos americanos foi o de incorporar, aos códigos lógicos de funcionamento da ferramenta, códigos maliciosos programados para criar um descompasso funcional entre as partes mecânica (*hardware*) e digital (*software*) do sistema. Informações desencontradas e contraditórias entre estas duas pontas levaram à sobrecarga do gasoduto, gerando uma explosão da ordem de três quilotons de dinamite.

Outro evento semelhante é narrado por Richard Clarke – ex-coordenador de segurança, proteção de infraestrutura e contraterrorismo da Casa Branca. Clarke e Knake (2010) detalham o bombardeio, por Israel, de um local na Síria onde seria construída uma instalação nuclear. Em linhas gerais, o trabalho de Israel foi o de sabotar ("*hackear*") o sistema de radares da Síria, tornando os caças israelenses invisíveis aos olhos da força aérea inimiga. Como meios possíveis de terem sabotado o equipamento sírio, Clarke aponta a infiltração de pessoal, a interceptação física de cabos de redes de fibra óptica e, ainda, o envio de vírus de computador por sinais eletrônicos a partir de veículos aéreos.

Em 2007, registrou-se na Estônia uma série de ataques a servidores do governo, da imprensa e de bancos, que acabaram por desconectar o país da *web* (Davis, 2007). Da mesma forma, tanto antes quanto durante a guerra entre Rússia e Geórgia, em 2008, grande parte do acesso à *web* na Geórgia foi bloqueada. Nestes casos, suspeita-se do envolvimento de atores estatais e não estatais russos para: retaliar o governo estoniano por uma decisão adotada em desconsideração à história da União Soviética; e como forma de cortar os canais de comunicação da Geórgia com o mundo, de maneira a assegurar à Rússia vantagem estratégica no conflito (Klymburg, 2011).

Nenhum desses eventos, entretanto, foi tão contundente quanto o espalhamento do vírus Stuxnet, em 2010, em sistemas digitais de controle e automação fabricados pela empresa alemã Siemens para o controle de centrífugas nucleares em uma usina na cidade de Natanz, no Irã. O vírus desativou aproximadamente 20% das centrífugas de purificação de urânio iranianas, o que pode ter atrapalhado significativamente a capacidade do país de gerar energia nuclear (Stuxnet..., 2010). O Stuxnet foi desenvolvido com a finalidade de sabotar

sistemas de controle industriais, reprogramando sua parte lógica e fazendo com que atuassem de maneira diferente da especificada originalmente, sem que os técnicos responsáveis por sua operação percebessem quaisquer modificações em seu funcionamento.

Apesar de se assemelhar à ação da CIA no caso do gasoduto da Sibéria, são a amplitude e a complexidade da tarefa de desenvolvimento, suas características funcionais, seu espalhamento a partir da Internet e sua capacidade de infecção seletiva que fazem do Stuxnet um vírus sem precedentes na história da computação (Symantec, 2011). Ele congrega inúmeras técnicas de programação maliciosa, de identificação e violação de alvos específicos, bem como um conjunto robusto de informações de inteligência destinadas a alimentar e retroalimentar o vírus (Sommer e Brown, 2011).

Desde a descoberta do Stuxnet, outros códigos maliciosos tão ou mais complexos vieram a público, como o Flame (CrySyS Lab, 2012) e o Gauss (Kaspersky, 2012). Grande parte das infecções registradas para o vírus Flame se deu no Oriente Médio e no norte da África – em ordem decrescente de severidade: Irã, Israel e Palestina, Sudão, Síria, Líbano, Arábia Saudita e Egito (Zetter, 2012). O vírus Gauss, por sua vez, infectou sistemas financeiros do Oriente Médio, especialmente de bancos operando no Líbano, com a finalidade de espionar contas bancárias específicas (Kaspersky, 2012).

A complexidade desses códigos computacionais levantou a suspeita de ação estatal por trás de sua criação. Em junho de 2012, o jornal *The New York Times* revelou que o Stuxnet é um dos frutos de um programa do governo norte-americano inaugurado ainda na gestão Bush, em 2006, que objetiva dotar o país de "armas cibernéticas" (Sanger, 2012). Muitas das ações que ocorrem sob esta rubrica relacionam-se com o monitoramento individual de potenciais terroristas e a derrubada de sítios eletrônicos identificados com atividades criminosas. Mesmo que o país jamais tenha oficialmente admitido tê-las empregado, a reportagem revela uma aproximação entre os serviços de inteligência dos Estados Unidos e de Israel na tarefa de desenvolver, testar, espalhar e fazer funcionar o Stuxnet.

Diante desse cenário, tentativas de classificação de incidentes cibernéticos ganharam fôlego. Ações deliberadamente danosas têm sido classificadas empírica e hipoteticamente em um espectro que varia do ativismo à guerra, passando por atos criminosos, espionagem, sabotagem e, logicamente, terrorismo (Cavelty, 2012).

Uma forma de categorizar tais incidentes é a que se encontra no quadro 1, construído a partir da tipologia de conflitos cibernéticos desenvolvida por Möckly (2012, p. 116) com base nos motivos e nos alvos das ações.

QUADRO 1
Tipologia de conflitos cibernéticos segundo Möckly (2012)

Tipo de conflito	Caracterização
Hacktivismo	Mistura de ações *hacker* com ativismo político. Geralmente tem como objetivo a inviabilização de sítios eletrônicos e servidores.
Crime cibernético	Desenvolvimento de ações ilícitas com o emprego de computadores e da Internet.
Espionagem cibernética	Acesso não autorizado a computadores e servidores com a finalidade de se testar a configuração e os sistemas de defesa de um determinado computador, ou ganhar acesso a informações sigilosas.
Sabotagem cibernética	Criação de empecilhos ao desenvolvimento de processos e rotinas de trabalho nos setores público e privado a partir de meios eletrônicos.
Terrorismo cibernético	Ataques ilícitos *contra* computadores – e a informação neles armazenada – e redes computacionais com o objetivo de intimidar ou coagir governos e/ou suas populações para o alcance de objetivos políticos. Dos ataques, *deve* decorrer a violência contra bens e pessoas, tanto quanto for necessária para se gerar o nível de medo adequado ao rótulo de 'terrorismo cibernético' (grifos nossos). Nas palavras de Möckly (2012, p. 116, tradução nossa): "O termo é também usado de forma imprecisa e vaga para incidentes cibernéticos de natureza política variada".
Guerra cibernética	Emprego de meios eletrônicos para atrapalhar as atividades de um inimigo, bem como atacar sistemas de comunicação. Nas palavras de Möckly (2012, p. 116, tradução nossa): "[o] termo é também usado de forma imprecisa e vaga para incidentes cibernéticos de natureza política variada".

Fonte: Möckly (2012, p. 116).
Elaboração dos autores.

Pode-se complementar a tipologia apresentada no quadro 1 a partir de sua conjugação com níveis de complexidade para incidentes cibernéticos. O quadro 2, elaborada por Lachow (2009, p. 439), sintetiza esta ideia.

QUADRO 2
Níveis de complexidade de incidentes cibernéticos segundo Lachow (2009)

	Simples	Avançado	Complexo
Escala do alvo	Sistema ou rede singular	Múltiplos sistemas ou redes	Múltiplas redes
Análise do alvo	Não há	Básica	Detalhada
Controle dos efeitos	Desfocado	Focado	Escalável
Recursos necessários	Pessoa(s) com conhecimento básico	Programador(es) com conhecimento avançado. Plataforma de testes.	Equipe de programação, análise e planejamento. Plataforma de testes.
Estrutura requerida	Não há	Não há	Time sincronizado
Uso potencial	Assédio	Ataques táticos	Ataques estratégicos

Fonte: Lachow (2009, p. 439).

Quando se leva em conta esta tipologia conjugada, pode-se afirmar que a maioria das ocorrências registradas na atualidade dificilmente pode ser enquadrada no nível avançado. Isto ocorre, especialmente, por conta da necessidade de conhecimento técnico e de recursos disponíveis para operar e empregar as ferramentas e *softwares* no ciberespaço como se fossem verdadeiras armas, testáveis de antemão, cujos efeitos são controláveis e que, nos casos mais extremos, podem ser articuladas a ações cinéticas de toda ordem.

O surgimento de novas ameaças e a interpolação de casos, contudo, resultaram em tipologias por vezes confusas e desencontradas. A tipologia apresentada revela que eventos cibernéticos variam em relação à forma, à complexidade e ao alvo. Percebe-se, também, que métodos semelhantes podem ser atribuídos de maneira indistinta a ações contra indivíduos, empresas e governos. Como definir, por exemplo, incidentes como o Stuxnet? A tarefa é dificílima, uma vez que – neste caso e em muitos outros – a ausência de evidências e o sigilo que naturalmente permeiam este tipo de operação impossibilitam a responsabilização do culpado pelo ato.

O que muda em cada ocorrência, em geral, é o impacto que as ações instrumentalizadas pelas TIC podem ter na vida cotidiana, no âmbito doméstico dos Estados e nas relações internacionais, bem como as respostas dadas a estes eventos, o que se passa a estudar a seguir.

3.2 A escalada em direção à militarização do ciberespaço e as questões conceituais decorrentes

Antes mesmo dos ataques ao Pentágono e ao World Trade Center, em 2001, o governo norte-americano considerava a possibilidade de que organizações terroristas fizessem uso da Internet para infligir algum tipo de dano às instituições e à infraestrutura do país (Weimann, 2004b). O 11 de Setembro revelou que, antes de ser um alvo preferencial da ação de grupos terroristas, a rede pode ser considerada uma ferramenta polivalente de suporte a suas atividades.

Após os atentados, a ameaça terrorista ganhou proporções descomunais na agenda de segurança dos Estados Unidos. Ao mesmo tempo, o crescimento da importância do ciberespaço para as atividades humanas implicou sua inclusão nos debates sobre segurança nacional. Em uma década marcada pela "guerra global ao terror" e, ao mesmo tempo, pelo crescimento do número de incidentes cibernéticos, a sobreposição entre os temas da cibersegurança e do terrorismo foi uma ocorrência natural. Diante do caos decorrente das ações da al-Qaeda, fatores não apenas psicológicos, mas também políticos e econômicos – como o aumento da relevância dos produtos e serviços de TI voltados para a segurança – combinaram-se para promover o tema do ciberterrorismo (Weimann, 2004a, p. 3). Em pouco tempo, o termo ciberterrorismo passou a aparecer com frequência nas páginas dos principais jornais e revistas do país, ganhando penetração cada vez maior na sociedade norte-americana e na comunidade internacional.

Acontece que a vinculação entre terrorismo e ciberespaço ocorreu em meio à própria popularização da militarização e do uso do ciberespaço por forças militares regulares, com destaque ao tratamento do assunto por países como China (Hsiao, 2010), Estados Unidos (Kramer, Starr e Wentz, 2009), Rússia (Giles, 2011) e,

mais recentemente, Brasil.[5] No caso dos Estados Unidos e do Brasil, ao contrário dos casos de Rússia e China, a institucionalização da defesa cibernética vem sendo amplamente divulgada.

A *Estratégia de segurança nacional* dos Estados Unidos, por exemplo, apresenta o ciberespaço como um quinto domínio operacional para as forças armadas do país, ao lado da terra, da água, do ar e do espaço sideral (United States, 2010a). No Brasil, a *Estratégia nacional de defesa* (END) de 2008 tratou o ciberespaço como um setor estratégico, ao lado dos setores espacial e nuclear (Brasil, 2008).

Nos dois casos, as Forças Armadas criaram comandos cibernéticos: em 2009, os Estados Unidos criaram o Comando Cibernético dos Estados Unidos (USCYBERCOM),[6] que passou a operar em 2010 com a missão de:

> [a] planejar, coordenar, integrar, sincronizar e conduzir atividades para direcionar as operações e a defesa de redes de informação do Departamento de Defesa; e [b] preparar-se para, quando ordenado, conduzir operações militares de amplo espectro no ciberespaço com a finalidade de habilitar ações em todos os domínios, garantir a liberdade de ação dos Estados Unidos e de seus aliados no ciberespaço, bem como negar essa capacidade a seus adversários (United States, 2010b, tradução nossa).

A exemplo dos Estados Unidos, o Comando do Exército Brasileiro iniciou, em agosto de 2010, a implementação do Centro de Defesa Cibernética do Exército (CD Ciber), com a missão de gerenciar e supervisionar o setor cibernético do Exército Brasileiro (Brasil, 2010a; 2010b).[7]

---

5. Apesar de a Internet ser relativamente nova, cabe ressaltar que a discussão a respeito das possibilidades, das limitações e dos riscos do emprego do ciberespaço no âmbito militar vem de décadas. Durante os anos 1980, especialmente no contexto do desenvolvimento de estratégias para o emprego de força aérea, o conceito de guerra informacional passou a ganhar contornos mais precisos como forma de: incrementar a capacidade de acumular e assegurar informação e comunicação entre os integrantes de um mesmo esquadrão; e incrementar a capacidade de georreferenciamento e, ao mesmo tempo, de gerar confusão nas linhas de comunicação do inimigo, de forma a minar sua capacidade de conhecer, se comunicar e se posicionar (Dunnigan, 2003). Do ponto de vista estratégico, no contexto da Revolução dos Assuntos Militares (RMA), termos como guerra digital, guerra virtual, guerra eletrônica e guerra cibernética – mesmo sem fronteiras conceituais bem esclarecidas – passaram a ser empregados para identificar opções estratégicas, operacionais e táticas que habilitam a guerra à distância, minimizando o número de baixas, aumentando a precisão dos diversos tipos de ataque e a economia de recursos a partir de uma melhor sincronização no campo de batalha (Arquilla e Ronfeldt, 1997).

6. O USCYBERCOM é uma subunidade de comando subordinada ao Comando Estratégico das Forças Armadas do país. Integram o contingente do USCYBERCOM membros do Comando Cibernético do Exército, o 24º Batalhão da Aeronáutica, o Comando Cibernético da Marinha e um Comando Cibernético dos Fuzileiros Navais (United States, 2010b).

7. O "Setor Cibernético do Exército Brasileiro" diz respeito aos ambientes interno e externo da força. Este setor é apresentado em detalhes por Carvalho (2011, p. 9-16). As Portarias nºs 666 e 667, de 2010, ambas do comandante do Exército, apenas puseram em funcionamento um "Núcleo de Defesa Cibernética no âmbito do Exército", submetido ao Departamento de Ciência e Tecnologia. Cabe lembrar que a END, adotada pelo Brasil em 2008, atribuiu ao Exército o papel de integrar e coordenar as Forças Armadas do país no que diz respeito às atividades de defesa relativas ao setor cibernético. Por conta disso, em 2011 e 2012, o Exército tomou medidas para aprofundar a institucionalização – inclusive pela via da adoção de um Decreto Presidencial – do Centro de Defesa Cibernética, previsto para funcionar plenamente em 2015. A "prova de fogo" do núcleo ocorreu na Rio+20. Mais informações a respeito estão na entrevista concedida à Folha de São Paulo pelo general José Carlos dos Santos, comandante do CD Ciber (Sá, 2012). A segurança cibernética, no Brasil, entendida como uma atividade mais abrangente que a defesa, e mais voltada para o estabelecimento de diretrizes e políticas de segurança a serem observadas na digitalização do Estado brasileiro, fica a cargo do Gabinete de Segurança Institucional da Presidência da República. Mais informações em: <http://dsic.planalto.gov.br>.

Nos últimos anos, percebe-se, portanto, uma maior disposição e organização de esforços por parte dos Estados para preparar-se para a guerra cibernética e enfrentar ameaças que variam de acordo com as tipologias apresentadas anteriormente. A consciência desta necessidade implica, por sua vez, o desenvolvimento de capacidades de ataque, defesa e dissuasão no ciberespaço – e por meio do ciberespaço.

Além disso, dada a natureza descentralizada e distribuída dos recursos de infraestrutura do ciberespaço,[8] bem como as diferentes teias sociais que se estabelecem a partir de seu emprego, muitos países vêm adotando estratégias coletivas de defesa cibernética. A Organização do Tratado do Atlântico Norte (OTAN), por exemplo, criou, em 2008, um Centro Cooperativo de Excelência em Defesa Cibernética com a finalidade de "aumentar a capacidade, a cooperação e a partilha de informações na Organização, entre seus membros e parceiros, na área da defesa cibernética, a partir de educação, pesquisa e desenvolvimento, lições compartilhadas e consultas".[9]

Diante da crescente dependência e essencialidade das TIC para inúmeras esferas da ação humana, a compreensão das implicações mútuas entre defesa e digitalização vem sendo, portanto, relacionada à própria viabilidade existencial das sociedades (Klymburg, 2011, p. 42). Acontece, porém, que isto vem sendo feito de maneira confusa e imprecisa, carente de rigor conceitual e de capacidade analítica. A pergunta fundamental daí resultante diz respeito justamente aos limites que distinguem os diversos tipos de incidentes cibernéticos. A precisão desta resposta é condição necessária para que se possam avaliar as respostas dadas pelos diferentes países às diferentes ameaças cibernéticas.

Na tentativa de contribuir com parte dessas respostas, a seção a seguir se propõe a analisar algumas questões teóricas e práticas relativas à imbricação entre terrorismo e ciberespaço.

4 O TERRORISMO E O CIBERESPAÇO

O conceito de terrorismo ainda carece de definição consensualmente aceita. Além de envolver caracteres com campos semânticos bastante imprecisos, aplicá-lo – ou não – na caracterização de determinado evento é, por si só, uma questão política. Para auxiliar na compreensão do que pode configurar o ciberterrorismo, é fundamental destacar as definições de terrorismo propostas por Wardlaw (1982) e por Diniz (2002). Para o primeiro, terrorismo é:

8. O trabalho seminal de Baran (1964) foi o responsável por esclarecer as diferenças entre redes centralizadas, descentralizadas e distribuídas. Apesar de datar da década de 1960, o trabalho continua sendo um dos principais textos introdutórios ao estudo de redes computacionais. Para um aprofundamento a respeito de arquiteturas de redes computacionais, ver Kurose (2010).

9. O centro está sediado em Tallinn, na Estônia. Mais informações em: <http://www.ccdcoe.org>. Da mesma forma, a União Europeia realizou exercícios com simulação de ataques cibernéticos em 2010. A iniciativa intitulada *Cyber Europe* é coordenada pela Agência Europeia de Segurança de Redes e Informação (Enisa). Vale ressaltar que a ênfase da *Cyber Europe* não é, prioritariamente, militar. Mais informações em: <http://www.enisa.europa.eu>.

> o uso, ou a ameaça do uso de violência por um indivíduo ou um grupo, atuando a favor ou contra uma autoridade estabelecida, quando essa ação é delineada para criar ansiedade extrema ou efeitos que induzem medo em um alvo mais amplo que as vítimas imediatas com o propósito de coagir aquele grupo a atender uma demanda política dos perpetradores (Wardlaw, 1982, p. 6, tradução nossa).

Diniz vai mais longe. Para ele, o terrorismo é

> uma forma específica de luta política, um estratagema voltado para alterar rapidamente a correlação de forças. Tem como fim uma meta política; emprega como meio de ação uma forma específica de emprego da força – o terror; mas emprega-a não de forma a produzir imediatamente aquela meta política, isto é, não visa a dissuadir nem a compelir, mas sim a induzir no alvo um comportamento que permita derrotá-lo. (Diniz, 2002, p. 18).

Ou seja, terrorismo: *i)* representa o emprego de uma espécie de violência e/ou força ou ameaça do uso desta espécie de violência e/ou força (o terror); *ii)* age em prol ou contrariamente a uma autoridade estabelecida (ação política, tanto por agentes estatais, quanto não estatais); *iii)* objetiva, mirando parcelas representativas (vítimas diretas) de um grupo maior (vítima indireta), induzir coercivamente este a adotar determinado comportamento; e *iv)* milita em virtude de efeito psicológico (ansiedade, medo, etc.) imputado nele a partir da ação. Em conjunto, estes pontos permitem ressaltar, como faz Diniz (2002), que o terror se diferencia de outras espécies do uso da força pelos efeitos psicológicos que gera no alvo da ação política. Estes efeitos psicológicos da ação são o que Wardlaw (1982) chama de ansiedade extrema ou medo. E o alvo da ação política é mais amplo que o rol de pessoas afetadas pela ação imediata.

Se a própria definição de terrorismo é escorregadia e invariavelmente política em termos práticos, em torno da qual é difícil se alcançar consenso na comunidade internacional (Deen, 2005), há de se fazer menção especial ao hermetismo das áreas técnicas em TIC como um complicador adicional para se avaliar de forma satisfatória as verdadeiras ameaças e vulnerabilidades inerentes à – e decorrentes da – era digital. E isto não se aplica apenas aos tomadores de decisão em políticas públicas, mas também à população em geral, que é afetada em seus direitos e deveres por tais decisões e é parte fundamental no processo de *accountability* política.

Apesar do destaque atual que o tema vem recebendo nas agendas acadêmica e política, as imbricações entre ciberespaço e terrorismo não estão claramente definidas. Para alguns analistas, o termo ciberterrorismo seria inapropriado, uma vez que ataques cibernéticos jamais causariam o mesmo impacto e terror que ataques cinéticos. Para outros, ataques cibernéticos poderiam, sim, afetar significativamente a vida em sociedade, gerando caos comparável àquele oriundo de ações perpetradas em meio físico (Theohary e Rollins, 2011).

Diferentes definições são adotadas, ademais, pelo Federal Bureau of Investigation (FBI), dos Estados Unidos, e por Zuccaro (2011, p. 61), no documento intitulado *Desafios estratégicos para a segurança e defesa cibernética*, lançado recentemente pela Secretaria de Assuntos Estratégicos da Presidência da República (SAE/PR) do Brasil. No primeiro caso, ações de terrorismo cibernético são definidas como: *i*) ataques premeditados contra sistemas informáticos, que resultem em *ii*) violência ou danos contra alvos não combatentes, *iii*) por grupos subnacionais ou agentes clandestinos. A definição brasileira, por sua vez, é formulada a partir de três componentes: *i)* alvos identificados direta ou indiretamente com Estados ou grupos de Estados; *ii)* agência não estatal como força motriz; e *iii)* motivação política para a ação. A primeira definição é: específica no que diz respeito ao alvo – sistemas informáticos – e aos agentes – atores subnacionais ou agentes clandestinos; genérica no que diz respeito aos efeitos – violência ou dano; e silente no que diz respeito à motivação. A segunda, por sua vez, é: genérica no que diz respeito aos alvos; específica no que diz respeito à motivação – política – e aos agentes – agência não estatal; e silente no que diz respeito aos efeitos da ação.

Diante disso, evidenciam-se as insuficiências e os riscos inerentes à série de definições de ciberterrorismo que vem se proliferando nos últimos anos (Grauman, 2012). Em geral, estas definições não determinam de forma convincente o tipo de instrumento de terror – cinéticos, cibernéticos e/ou a combinação de ambos. Há uma tendência de se restringir sua autoria a grupos não estatais. E, o mais grave: não delimitam de forma precisa o traço que separa os efeitos do terror de outros tipos de emprego da violência politicamente motivada. Tais incertezas são agravadas pelo fato de que não há, até o presente momento, registros do emprego de terror contra, por, ou por meio de dispositivos computacionais e redes de computador.

Isso deve, entretanto, ser visto com a seguinte ressalva: algumas organizações, de 2009 em diante, passaram a chamar a atenção do mundo pela audácia de suas ações e pela ambição de sua agenda de demandas políticas. Grupos hacktivistas, como o Anonymous e o Lulsec,[10] vêm lançando mão de ataques de negação de serviço – tornar determinada máquina, determinado servidor, inacessível por sobrecarga de tráfego – e desfiguração de sítios virtuais – invasão de servidores com alteração das informações e arquivos divulgados *on-line* – de governos, empresas e indivíduos apontados como inimigos. Outros grupos, como a Wikileaks e a Openleaks, desenvolveram plataformas de divulgação de informações governamentais e não governamentais sigilosas, adquiridas tanto por ações cibernéticas, quanto por contato direto com pessoas dispostas a revelar tais informações, a quem se garante o anonimato e o sigilo da fonte. Diante da severidade destas ações, especialmente diante do escândalo intitulado *Cablegate*, ganham espaço iniciativas de se catalogar como terroristas atores dedicados ao ativismo cibernético.[11]

10. Para mais informações, ver: <http://anonnews.org> e <http://lulzsec.co.uk>.
11. Nesse sentido, ver Mccullagh (2010).

Conforme um estudo publicado recentemente pelo grupo de pesquisa coordenado pelo professor Gabriel Weimann, da Universidade de Haifa, em Israel, no início dos anos 2000, todas as organizações terroristas, assim caracterizadas pelo *Antiterrorism and effective death penalty act* dos Estados Unidos, possuíam sítios na *web*. Além dos sítios oficiais, outras centenas de páginas eletrônicas revelavam apoio às causas destas organizações (Weimann, 2006).

Passados mais de dez anos, desde o início das pesquisas, não há indicativo de que a tendência de presença terrorista extensiva na rede tenha se modificado. O terrorismo na Internet não é apenas um fenômeno dinâmico, no sentido de que sítios aparecem e desaparecem da rede, modificando seus formatos e endereços periodicamente. A própria natureza e suas características estruturais fazem da Internet um espaço de interação para grupos terroristas distintos.

Em geral, a despeito de estarem crescendo as tentativas de controle estatal do acesso e do conteúdo *on-line*[12] e da grande exclusão digital ainda hoje registrada, a Internet oferece a estas organizações um ambiente de alcance mundial, bastante fragmentado em termos de regulamentação e de ação coordenada de contraterrorismo e combate ao crime organizado. Além disso, a manutenção de sítios é uma atividade de baixo custo e possibilita que células terroristas atinjam audiências potencialmente amplas e descentralizadas, por meio de mídias variadas. Soma-se a isto a velocidade com que os fluxos de informação ocorrem na rede, bem como a possibilidade de anonimato, a partir do emprego de ferramentas técnicas apropriadas, para grande parte das operações realizadas *on-line*.

O potencial anonimato da rede permite que células terroristas circulem em diferentes esferas, realizando uma gama variada de operações – tanto lícitas, quanto ilícitas[13] – e com mais flexibilidade que em meios físicos convencionais. Este mesmo anonimato permite que estes grupos desenvolvam laços com organizações criminosas. Sabe-se, por exemplo, de criminosos que: alugam seus serviços de *hacking*; vendem números de cartões de crédito para a realização de fraudes;

12. Exemplos disso são iniciativas como o *Anti-Counterfeiting Trade Agreement* (ACTA) e projetos de lei dos Estados Unidos: Pipa (Bill S.968), Sopa (H.R. 3261) e Cispa (H.R. 3523). Estes foram formulados com a finalidade de auxiliar no combate à pirataria e à violação a direitos de propriedade intelectual a partir do controle da rede e do monitoramento dos usuários. O Cispa emprega estes mesmos mecanismos com o objetivo de monitorar ameaças à segurança nacional dos Estados Unidos. Iniciativas semelhantes são encontradas em inúmeros outros países e podem ser conhecidas a partir do sítio virtual OpenNet, disponível em: <http://opennet.net/country-profiles>. Para acessar o tratado e as legislações citadas, ver, respectivamente: <http://register.consilium.europa.eu/pdf/es/11/st12/st12196.es11.pdf> e <http://www.govtrack.us>.

13. Não se pode, *a priori*, dizer que é ilícito todo e qualquer uso da Internet por um indivíduo considerado terrorista pela legislação de determinado país. Como afirmar ilícito o uso que um indivíduo considerado terrorista faz da *web* para ler jornais e revistas? Quais são os limites que distinguem entre a licitude e a ilicitude das postagens de um *blogueiro* que se dedica a escrever sobre a cultura islâmica? Até que ponto suas manifestações, mesmo aquelas ofensivas ao Ocidente, devem ser protegidas sob o manto da liberdade de expressão, e a partir de que momento elas são atos passíveis de punição civil e/ou criminal? Tome-se o seguinte exemplo: sítios de leilões de objetos que fazem alusão ao nazismo são proibidos na Europa. São, portanto, ilícitos. Nos Estados Unidos, porém, estes sítios estão protegidos pela Primeira Emenda à Constituição, que garante a liberdade de expressão (Goldsmith e Wu, 2006). Isto significa que, dependendo do ordenamento jurídico em questão, a licitude ou a ilicitude do uso da Internet pode variar.

ou simplesmente usam a Internet para negociar drogas, armas e materiais embargados (Wilson, 2008).[14] Este tipo de associação ilícita oferece a grupos terroristas mercados alternativos de produtos e serviços, ao mesmo tempo em que expande a sua área de influência.

O anonimato traz ainda a possibilidade de vinculação de organizações criminosas – terroristas ou não – a Estados. Tal tipo de associação incrementaria a escala das ações cibernéticas, uma vez que Estados, em geral, possuem mais capacidade para a orquestração de ações complexas e podem despender uma quantidade maior de recursos para sua realização que grupos não estatais, ainda que estes sejam mais capacitados para operar no ciberespaço. Esta espécie de guerra por *proxies* vem sendo apontada por Clarke e Knake (2010) e Krekel, Adams e Bakos (2012), entre outros, como uma das principais atividades cibernéticas do Irã, da China e da Rússia para manterem um nível alto de hostilidade contra os Estados Unidos sem serem diretamente implicados em ações de contra-ataque.

Estas três possibilidades – o estabelecimento de laços com outros tipos de organizações criminosas, o potencial anonimato na rede, e o uso de *proxies* –, porém, são de difícil constatação empírica e apresentam alguns desafios intrínsecos para se efetivarem. No primeiro caso, porque a forma de se identificar o liame entre terrorismo e crime organizado é a partir do sucesso da ação repressiva de agências estatais. Além disso, há um *trade-off* que precisa ser considerado: o que é mais vantajoso para uma organização terrorista? Constituir capacidade interna para operar no ciberespaço – o que demanda tempo e recursos que poderiam ser direcionados a ações mais contundentes no plano físico – ou terceirizar estas atividades a outros atores – correndo mais riscos de monitoramento e interceptação? No segundo caso, porque são raros os registros de agressões e contra-ataques publicamente assumidos e cabalmente atribuíveis a qualquer ator, seja ele estatal ou não – como o caso do Stuxnet apresentado neste capítulo.

É importante perceber, porém, que o mesmo véu de anonimato que pode favorecer a ação de organizações terroristas pode fazer com que seus objetivos sejam frustrados. O motivo é simples: em geral, grupos terroristas querem atenção (Conway, 2011). O espetáculo – nefasto, naturalmente – oferecido pela explosão de dois aviões contra as torres gêmeas de Nova Iorque dificilmente seria superado por ações lançadas a partir da *web*. Em outras palavras, o 11 de Setembro tornou-se uma meta a ser superada por estas organizações. Basta pensar no impacto causado pelos atentados em Madri e Londres, em 2004 e 2005, respectivamente. Soma-se

14. É difícil estimar a parcela dos fluxos de dados da Internet dedicada a atividades ilícitas. Um complicador adicional a esta mensuração é a *deep web*, ou a *web* profunda. Ela diz respeito a parcelas da rede hospedadas em computadores e bases de dados específicas que empregam mecanismos técnicos para se tornar invisíveis a olhos leigos e a grande parte dos motores de busca – *google.com*, *yahoo.com* – que simplificam o processo de pesquisa de conteúdo. Mais informações sobre o tema podem ser encontradas em Bergman (2001).

a isto o fato de que muitos ataques cibernéticos poderiam passar despercebidos pela mídia, ou, pior, serem atribuídos a outras causas ou atores. Disto resulta que os custos de se levar a cabo um ataque cibernético poderiam superar os benefícios de fazê-lo com sucesso.

Pelas razões mencionadas, o uso que grupos terroristas fazem da Internet é, por ora, bastante semelhante ao do usuário comum. Em uma série de pesquisas, a equipe de Weimann (2004a; 2004b; 2005; 2006) registrou que o emprego terrorista da Internet ocorre, em geral, nas seguintes formas:

a) meio de acesso a, divulgação e troca de informações;

b) mecanismo de *networking*;

c) mecanismo para trocas comerciais e financeiras, inclusive para captação de recursos;

d) ferramenta para recrutamento e mobilização de novos membros;

e) meio auxiliar para o planejamento e a coordenação de ações; e

f) meio de guerra psicológica.

Além disso, há a possibilidade de que grupos terroristas estejam realizando campanhas de "cibermedo", exagerando suas capacidades reais, a fim de aterrorizar a população – sem necessariamente empregar a força – sobre os danos que possíveis ataques a sistemas computadorizados acarretariam. A ideia não é de todo implausível. Cabe, contudo, ponderar em que medida este tipo de discurso não passa de retórica para impressionar e coagir os Estados a adotarem posturas que favoreçam os interesses terroristas. Até o momento, porém, de acordo com os critérios antes apontados, seria incorreto rotular tais ações como atos terroristas por excelência de acordo com as definições de Wardlaw e Diniz – ainda que, nos Estados Unidos, por exemplo, o *Patriot Act* de 2002 (Public Law Pub. L. 107-56) tenha equiparado tais usos da *web* a verdadeiros atos terroristas.

O que se observa, portanto, passados mais de dez anos do início da guerra global ao terror, é o emprego da Internet como um meio valioso para a articulação interna e externa de ações de grupos criminosos diversos, inclusive terroristas. O uso que estes grupos fazem da rede não difere substancialmente daquele feito por Estados, empresas e organizações não governamentais (ONGs).

A essa altura, pode-se fazer duas ressalvas. Primeiramente, à capacidade de grupos terroristas afetarem o funcionamento da Internet, seja por ataques virtuais, seja por ataques cinéticos. E, em segundo, ao uso que as mesmas organizações fazem da própria rede.

No primeiro caso, pode-se assegurar que a maior parte dos grupos terroristas – se não todos – não seria capaz de infligir danos consideráveis à estrutura robusta – uma complexa teia de infraestrutura física e lógica distribuída por todo o

planeta – que a Internet alcançou na atualidade (Zetter, 2012). No segundo caso, diante do potencial comunicacional que a Internet tem para a operacionalização de células terroristas na atualidade, pensá-la como um alvo chega a ser contraintuitivo.

O ciberespaço é instrumental a inúmeros tipos de organizações: Estados, sociedade civil organizada em geral, grupos criminosos e células terroristas. Se, neste caso, dar à Internet o *status* de alvo parece descabido, não se pode prescindir de segurança e proteção de sistemas informatizados que dão sustentação a atividades setoriais das mais distintas na atualidade – economia e finanças, saúde, infraestrutura crítica etc. –, em virtude das diferentes categorias de ameaças e riscos apontados anteriormente. Entretanto, a capacidade de gerar medo, terror e pânico generalizado e indiscriminado pelo ciberespaço é, por ora, apenas um exercício hipotético, cuja viabilidade está sujeita a escrutínio futuro.

5 CONSIDERAÇÕES FINAIS

Este capítulo buscou revelar a impossibilidade de se tratar dos impactos da Internet – e, com isto, do ciberespaço – nos domínios da segurança nacional e internacional de maneira desvinculada de seus aspectos técnicos fundamentais e de uma conjunção política mais ampla. Se, entre outras coisas, o estudo da guerra e do terrorismo, em conjunto e isoladamente, representa um desafio extraordinário e multidimensional para as áreas dos estudos de segurança e para os estudos estratégicos, a adição do prefixo *ciber* – em um contexto de ubiquidade e pervasividade das TIC, bem como de convergência midiática, na vida contemporânea – a cada um destes termos amplia ainda mais a complexidade da tarefa.

Conforme se observou, os diferentes tipos de incidentes cibernéticos carecem de uma clara delimitação conceitual. A confusão semântica que se estabeleceu em torno desses conceitos não apenas prejudica a pesquisa, mas impõe desafios à adoção de políticas públicas relativas ao ciberespaço e à Internet. Afinal, quais incidentes cibernéticos devem ser alvo de políticas de segurança e defesa? Eventos ocorridos no ciberespaço? Através do ciberespaço? Contra o ciberespaço? Que garantias e direitos fundamentais devem ser observados neste processo? Quais os limites da ação do Estado no enfrentamento de ameaças cibernéticas?

Os casos apresentados ao longo do texto demonstram que, por ora, tanto a guerra quanto o terrorismo – os eventos mais severos no rol de ações violentas politicamente motivadas – têm utilizado o ciberespaço como mera plataforma de apoio a operações no mundo físico. Mas não é de hoje que militares e terroristas utilizam a *web* na tentativa de maximizar seus ganhos de inteligência, recrutamento ou divulgação. Se o espectro eletromagnético, neste caso a Internet, é instrumental a atores estatais e não estatais, suas diversas aplicações – *web*, governo digital, redes sociais – tornam-se alvos potenciais e merecem ser protegidos. Quanto maior a

dependência de tais aplicações por parte da sociedade, maior a relevância estratégica de ações ofensivas contra – e defensivas de – tais alvos.

A Internet é um conjunto de padrões tecnológicos que permite a interconexão de uma série de redes de *hardwares* distintos que, em conjunto com *softwares* variados, habilita a interconexão de um sem-número de outros tipos de redes – sociais, econômicas, políticas – espalhadas pelos quatro cantos do planeta. Por isso, a Internet é muito capilarizada, robusta e resiliente, e parece tarefa hercúlea inviabilizar toda esta infraestrutura de uma vez só, bem como bloquear todos os caminhos alternativos pelos quais os fluxos de dados e informações circulam de maneira geograficamente distribuída através de distintas linhas de comunicação.

Grande parte do alarme observável ultimamente, nesse sentido, se refere à *web*: uma única aplicação entre tantas outras, mas que continua sendo a principal porta de acesso à Internet. A *web* depende de um nodo centralizado – treze servidores raízes, replicados em todos os continentes – para o endereçamento alfanumérico de máquinas, uma espécie de agenda telefônica dos sítios eletrônicos existentes (Mueller, 2002). A despeito da relevância do modelo *web* para a Internet, a última não depende do primeiro para funcionar. Por isso é seguro afirmar que a Internet continuará existindo ainda que o modelo *web* venha a desaparecer. O conhecimento consciente das diferenças entre cada um destes conceitos é fundamental quando se pretende nortear investigações científicas e políticas públicas na era digital.

Isso se liga diretamente à outra questão oriunda da imprecisão conceitual em torno da securitização do ciberespaço: é útil se tratar o ciberespaço como um quinto domínio operacional, autônomo em relação aos demais, como vem acontecendo a partir da doutrina militar norte-americana? A criação de comandos cibernéticos em países como os Estados Unidos e o Brasil denota, por um lado, o reconhecimento da Internet como possível origem de ameaças à segurança daqueles países e, por outro, um elemento crítico à viabilidade socioeconômica e política de sociedades inteiras. Esta percepção parece correta, mas a existência destes comandos especializados revela um paradoxo que se relaciona com a natureza ubíqua e pervasiva da computação na atualidade. Como se sabe, dispositivos computacionais vêm sendo embarcados aos mais variados objetos. Soma-se a isto o fato de que os padrões tecnológicos que organizam o funcionamento da Internet habilitam a interoperabilidade e a convergência de inúmeras tecnologias digitais – televisão, telefonia, rádio etc. Com isto, é possível que a Internet venha a estar presente em praticamente todos os lugares e possa ser acessada por diferentes aparelhos interconectados, para diferentes finalidades. A reflexão sobre o ciberespaço, entretanto, sempre foi uma necessidade inerente à prática militar. É impossível pensar a guerra sem pensar, por exemplo, o papel das linhas de comunicação – por meio de diferentes tecnologias – pelas quais a informação é transmitida no – e ao – teatro de operações.

Por isso, uma vez que todas as armas – Aeronáutica, Exército e Marinha e, em alguns casos, o Comando do Espaço Sideral – fazem uso de diferentes parcelas do espectro eletromagnético que compõem o ciberespaço, por que tratá-lo como um quinto domínio operacional como preconiza a doutrina militar dos Estados Unidos – e que vem sendo seguida substancialmente pelo Brasil? Esta questão ganha consistência quando se considera que a própria doutrina norte-americana prevê a capacitação de suas forças para operações de amplo espectro no ciberespaço em conjunto com ações em outros domínios. Ou seja: pela ótica de um Estado, em um contexto de guerra, não faria sentido optar exclusivamente pelo emprego de armas cinéticas ou digitais.

Finalmente, parece razoável supor que qualquer ato de violência levado a cabo no, através do, ou contra o ciberespaço, para ser considerado um ato de guerra ou de terrorismo, terá de possuir implicações físicas diretas e/ou indiretas. Isto porque, por mais que a Internet tenha estendido seus tentáculos a praticamente todos os aspectos da vida em sociedade, a desvinculação completa do mundo terreno, ao contrário do que profetizou John Perry Barlow ao propor, em 1996, a desvinculação dos *netizens* da jurisdição soberana dos Estados, continua a ser ficção científica. Até o momento, não se viu uma ação perpetrada no – ou através do – ciberespaço que tenha gerado impacto comparável ao de outros atentados terroristas registrados até aqui, especialmente o de 11 de Setembro.

O que é inegável, contudo, é que vem crescendo o emprego de TIC como instrumento de ação política. Se – como afirmou Clausewitz – a guerra é a política por outros meios, espera-se que o emprego de TIC seja também instrumental nos pontos mais extremos do espectro de ações políticas, tanto de maneira unívoca, quanto em conjunto com os demais instrumentos à disposição da violência política. É justamente a gradação valorativa dos diferentes pontos deste espectro – como ativismo, terrorismo ou ato de guerra, por exemplo – que exige cautela e mais conhecimento a respeito do ciberespaço e de seu funcionamento.

No plano normativo, a guerra continua tendo as suas possibilidades e limitações de engajamento restringidas pelo direito internacional vigente. O emprego de TIC, especialmente da Internet, dificulta precisar, em geral, a origem do ataque e, portanto, o alcance que a retaliação legítima pode ter. Discute-se, neste caso, se ações ofensivas ou defensivas têm mais peso em estratagemas militares. Não se sabe, ainda, além disso, se estratégias de dissuasão funcionam no ciberespaço da mesma forma que em caso de guerra nuclear. Apesar disso, os Estados inegavelmente têm – por sua maior capacidade de mobilização de recursos – posição de vantagem na preparação e na realização de atividades complexas que podem ser categorizadas como verdadeiras guerras cibernéticas, com o maior nível de complexidade e escopo possível.

Grande parte dos problemas analíticos e práticos do ciberterrorismo, pela ótica da ciência política e das relações internacionais, relaciona-se justamente ao tratamento a ser dado às ações de atores não estatais. Nesse ponto, repetem-se e replicam-se as controvérsias políticas e jurídicas relativas ao tratamento de combatentes ilegais, à guerra por *proxies* e, especialmente, aos tipos de prerrogativas que o Estado tem em termos de vigilância e monitoramento da população em um contexto securitizado. Como um reflexo próprio após mais de dez anos dos ataques terroristas aos Estados Unidos, o tratamento de ameaças não militares a partir de uma lógica militar – securitizada – reacende o *trade-off* normativo entre a segurança e o respeito a liberdades e direitos fundamentais. Em um cenário em que a Internet se espalha cada vez mais e se consolida como uma plataforma central para a vida em sociedade, soluções homogeneizantes para aquela equação são inaceitáveis. Especialmente pela ótica do mundo em desenvolvimento que, diante da inclusão digital mais avançada do mundo desenvolvido, tende a ser o principal espaço de crescimento do ciberespaço no próximo século.

REFERÊNCIAS

ARQUILLA, J.; RONFELDT, D. **In Athena's camp**: preparing for conflict in the Information Age. Santa Monica: Rand Publishing, 1997.

_____. **Networks and netwars**: the future of terror, crime and militancy. Santa Monica: Rand Publishing, 2001.

BARAN, P. **On distributed communications**: I. introduction to distributed communications networks. Santa Monica: Rand Corporation, 1964.

BARLOW, J. P. **A declaration of the Independence of Cyberspace**. Davos, 1996. Disponível em: <http://goo.gl/HFDh >.

BERNES-LEE, T. **Information management**: a proposal. Mar. 1989. Disponível em: <http:// http://goo.gl/w92v>.

BERGMAN, M. K. The deep web: surfacing hidden value. **The journal of electronic publishing**, v. 7, n. 1, Michigan, Aug. 2001. Disponível em: <http://goo.gl/cytSeG>.

BLUMENTHAL, M.; CLARK, D. The future of the Internet and cyberpower. *In*: KRAMER, F.; STARR, S.; WENTZ, L. **Cyberpower and National Security**. Washington, D.C.: National Defense University Press, 2009.

BRASIL. **Estratégia Nacional de Defesa**. Brasília, 2008. Disponível em: <http://goo.gl/3Ttvtn>.

_____. **Portaria nº 666, de 4 de agosto de 2010**. 2010a. Disponível em: <http://tinyurl.com/aebz5yw>.

_____. **Portaria nº 667, de 4 de agosto de 2010**. 2010b. Disponível em: <http://tinyurl.com/aebz5yw>.

BUZAN, B.; WÆVER, O.; WILDE, J. **Security**: a new framework for analysis. Boulder: Lynne Rienner Publishers, 1998.

BYGRAVE, L. A.; BING, J. **Internet Governance**: infrastructure and institutions. New York: Oxford University Press, 2009.

CANABARRO, D. A governança da Internet: atores, aspectos institucionais e questões políticas em confronto. *In*: ENCONTRO DA ASSOCIAÇÃO BRASILEIRA DE CIÊNCIA POLÍTICA, 8., 2012, Gramado, Rio Grande do Sul. **Anais**... Gramado: ABCP, 2012. Disponível em: <http://goo.gl/VDif3>.

CARVALHO, P. S. M. **A defesa cibernética e as infraestruturas críticas nacionais**. Rio de Janeiro, 24 maio 2011. Disponível em: <http://goo.gl/1qjMf8>.

CAVELTY, M. The militarisation of cyber security as a source of global tension. *In*: MÖCKLI, D. **Strategic trends 2012**: key developments in global affairs. Zurich: Center for Security Studies (CSS), 2012. Disponível em: <http://goo.gl/tBmeiu>.

CLARKE, R.; KNAKE, R. **Cyber war**: the next threat to national security and what to do about it. New York: Ecco, 2010.

CONWAY, M. Against cyberterrorism: why cyber-based terrorist attacks are unlikely to occur. **Communications of the ACM**, v. 54, n. 2, p. 26-28, Feb. 2011.

CRYSYS LAB. **sKyWIper (a.k.a. Flame a.k.a. Flamer)**: a complex malware for targeted attacks. Budapest: Budapest University of Technology and Economics, 2012. Disponível em: <http://goo.gl/NS9W1>.

DAVIS, J. Hackers take down the most wired country in Europe. **Wired magazine**. 2007. Disponível em: <http://goo.gl/RqGJu>.

DEEN, T. U.N. member states struggle to define terrorism. **IPS News Agency**, July 2005. Disponível em: <http://goo.gl/XH2GFr>.

DINIZ, E. Compreendendo o fenômeno do terrorismo. *In*: ENCONTRO DA ASSOCIAÇÃO BRASILEIRA DE CIÊNCIA POLÍTICA, 3., 2002, Niterói, Rio de Janeiro. **Anais...** Niterói: ABCP, 2002. Disponível em: <http://goo.gl/ndG74Z>.

DRAKE, W. J. Introduction: the distributed architecture of network global governance. *In*: DRAKE, W. J.; WILSON III, E. J. (Ed.). **Governing Global Electronic Networks**: international perspective on policy and power. London: MIT Press.

DUNNIGAN, J. F. **How to make war**: a comprehensive guide to modern warfare in the twenty-first century. London: Harper Paperbacks, 2003.

DUQUE, M. G. O papel de síntese da Escola de Copenhague nos estudos de segurança internacional. **Contexto Internacional**, v. 31, n. 3, dez. 2009. Disponível em: <http://tinyurl.com/cbtvvps>.

EISENBERG, J.; CEPIK, M. **Internet e política**: teoria e prática da democracia eletrônica. Belo Horizonte: Editora da UFMG, 2002.

FOUNTAIN, J. E. **Building the Virtual State**: information technology and institutional change. Washington: Brookings Institution Press, 2001.

GILES, K. Information Troops: a Russian cyber command? *In*: INTERNATIONAL CONFERENCE ON CYBER CONFLICT, 3., 2011, Tallin. **Anais...** Tallinn: CYCON 2011. Disponível em: <http://goo.gl/ZFJLyR>.

GOLDSMITH, J.; WU, T. **Who controls the Internet?** Illusions of a borderless world. New York: Oxford University Press, 2006.

GRAUMAN, B. **Cyber-security**: the vexed question of global rules. Brussels: SDA, 2012. Disponível em: <http://goo.gl/0fVTw1>.

HANSEN, L.; NISSENBAUM, H. Digital disaster, cyber security, and the Copenhagen School. **International studies quarterly**, v. 53, n. 4, p. 1.155-1.175, 2009.

HEADRICK, D. **Technology**: a world history. Oxford: University Press, 2009.

HSIAO, L. C. R. China's cyber command? **China Brief**, v. 15, n. 10, p. 1-2, 2010. Disponível em: <http://goo.gl/ZFJLyR>.

KASPERSKY. **Kaspersky Lab discovers 'Gauss'**: a new complex cyber-threat designed to monitor online banking accounts. 2012. Disponível em: <http://goo.gl/GZBlg>.

KLEINWÄCHTER, W. The history of Internet governance. *In*: OSCE. **Governing the Internet**: freedom and regulation in the OSCE region. Vienna: OSCE, 2007. Disponível em: <http://www.osce.org/fom/26169>.

KLYMBURG, A. Mobylising Cyber Power. **Survival**, v. 53, n. 1, p. 41-60, 2011.

KRAMER, F. D.; STARR, S. H.; WENTZ, L. (Ed.). **Cyberpower and National Security**. Washington: National Defense University Press, 2008.

KREKEL, B.; ADAMS, P.; BAKOS, G. **Occupying the information ground**: Chinese capabilities for computer network operations and cyber espionage. Northrope Grumman, March 2012. Disponível em: <http://goo.gl/XM7y0Q>.

KRILL, P. Cerf: turning off pieces of the Internet 'not sensible' as security strategy. **InfoWorld**. Sept. 2009. Disponível em: <http://goo.gl/h0xOeQ>.

KUEHL, D. From cyberspace to cyberpower: defining the problem. *In*: KRAMER, F. D.; STARR, S. H.; WENTZ, L. **Cyberpower and National Security**. Washington: National Defense University Press, 2009.

KURBALIJA, J.; GELBSTEIN, E. **Gobernanza de Internet**: asuntos, actores y brechas. Geneva: Diplo Foundation, 2005.

KUROSE, J. **Redes de computador e a Internet**: uma abordagem *top-down*. São Paulo: Addison Wesley, 2010.

LACHOW, I. Cyberterrorism: menace or myth. *In*: KRAMER, F.; STARR, S.; WENTZ, L. **Cyberpower and National Security**. Washington: National Defense University Press, 2009.

LIVINGSTONE, S. **Clarifying the CNN Effect**: an examination of media effects according to type of military intervention. Cambridge: The Joan Shorenstein Center, June 1997. (Research Paper R-18) Disponível em: <http://goo.gl/WVBvkn>.

MALCOLM, J. **Multi-stakeholder Governance and the Internet Governance Forum**. Wembley, Australia: Terminus Press, 2008.

McCULLAGH, D. Congressman wants WikiLeaks listed as terrorist group. **CNET**. 28 Nov. 2010. Disponível em: <http://goo.gl/62KII>.

MÖCKLY, D. **Strategic trends 2012**: key developments in global affairs. Zurich: Center for Security Studies (CSS), 2012. Disponível em: <http://www.css.ethz.ch/publications/pdfs/Strategic-Trends-2012.pdf>.

MUELLER, M. **Ruling the root**: Internet governance and the taming of cyberspace. Cambridge, USA: MIT Press, 2002.

REED, T. **At the Abyss**: an insider's history of the Cold War. New York: Presidio Press, 2004.

RICHARDSON, W. **Blogs, wikis, podcasts, and other powerful webtools for classrooms**. Londres: SAGE, 2009.

SÁ, N. General detalha implantação do Centro de Defesa Cibernética, novo órgão brasileiro. **Folha de São Paulo**, São Paulo, 7 maio 2012. Disponível em: <http://goo.gl/blt8Y>.

SANGER, D. Obama order sped up wave of cyberattacks against Iran. **The New York Times**. June 2012. Disponível em: <http://goo.gl/4SfG5>.

SERRA, A. P. G. Convergência tecnológica em sistemas de informação. **Integração**, v. 12, n. 47, p. 333-338, 2006.

SOMMER, P.; BROWN, I. **Reducing systemic cybersecurity risk**. Jan. 2011. Disponível em: <http://goo.gl/B0azWg>.

STARR, S. Toward a preliminary theory of cyberpower. *In*: KRAMER, F.; STARR, S; WENTZ, L. **Cyberpower and National Security**. Washington: National Defense University Press, 2009.

STUXNET 'hit' Iran nuclear plans. **BBC News**, Nov. 2010. Disponível em: <http://goo.gl/mX9XB>.

STROBEL, W. P. The CNN effect. **American Journalism Review**. May 1996. Disponível em: <http://goo.gl/KRqIj>.

SYMANTEC. **W32. Duqu**: the precursor to the next stuxnet. Symantec, Nov. 2011. Disponível em: <http://goo.gl/4ikDz>.

UNITED STATES. **National Security Strategy**. May 2010a. Disponível em: <http://goo.gl/pBBP>.

_____. **U.S. Cyber Command Fact Sheet**. May 2010b. Disponível em: <http://goo.gl/yi6Db>.

VAN DIJK, J. **The Deepening Divide**: inequality in the information society. Thousand Oaks: Sage Publications, 2005.

WARDLAW, G. **Political Terrorism:** theory, tactics and counter-measures. Cambridge: Cambridge University Press, 1982.

WEIMANN, G. www.terror.net: how modern terrorism uses the Internet. **United States Institute of Peace**, Washington, n. 116, Mar. 2004a. Disponível em: <http://goo.gl/0OMV1>.

_____. Cyberterrorism: how real is the threat? **United States Institute of Peace**, Washington, n. 119, Dec. 2004b. Disponível em: <http://goo.gl/KMsUo>.

_____. Cyberterrorism: the sum of all fears? **Studies in conflicts and terrorism**, v. 28, n. 2, p. 219-149, 2005.

_____. Virtual Disputes: the use of the Internet for terrorist debates. **Studies in conflicts and terrorism**, v. 29, n. 7, p. 623-639, 2006.

WILSON, C. **Botnets, cybercrime, and cyberterrorism**: vulnerabilities and policy issues for congress. Jan. 2008. Disponível em: <http://goo.gl/5L9H8W>.

WINNER, L. **The Whale and the Reactor**: a search for limits in an age of high technology. Chicago: The University of Chicago Press, 1986.

WORLD INTERNET USERS AND POPULATIONS. **Internet usage statistics**: the Internet big picture. 2012. Disponível em: <http://goo.gl/L8hG>.

ZETTER. **Meet 'flame', the Massive Spy Malware Infiltrating Iranian Computers**. May 2012. Disponível em: <http://goo.gl/R6UDb>.

ZUCCARO, P. M. Tendência global em segurança e defesa cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço. *In*: BARROS, O.; GOMES, U. **Desafios estratégicos para a segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

ZUKANG, S. Message by Sha Zukang, under-secretary-general, United Nations Department of Economic and Social Affairs (UNDESA). *In*: KLEINWÄCHTER, W. **Internet Governance Forum**: the first two years. 2007. Disponível em: <http://goo.gl/bRffKU>.

BIBILIOGRAFIA COMPLEMENTAR

FALLIERE, N.; MURCHU, L. O.; CHIEN, E. **W32. Stuxnet Dossier**. Symantec, Feb. 2011. Disponível em: <http://goo.gl/qL71>.

GUSTIN, J. F. **Cyber Terrorism**: a guide for managers. Lilburn: Fairmont Press, 2004.

NELSON, B. *et al*. **Cyberterror**: prospects and implications. Monterey: Center for the Study of Terrorism and Irregular Warfare, 1999.

PARISER, E. **The Filter Bubble**: what the Internet is hiding from you. New York: The Penguin Press, 2011.

THEOHARY, C.; ROLLINS, J. Terrorist use of the Internet: information operations in cyberspace. *In*: CONGRESSIONAL RESEARCH SERVICE, 2011, Washington. **Anais…** Washington: CRS, 2011. Disponível em: <http://goo.gl/Ii4Mhq>.