DECORRÊNCIAS DA UTILIZAÇÃO DA INTERNET POR ORGANIZAÇÕES TERRORISTAS: o recurso da comunicação tecnológica como proposta de mudança não-democrática de poder[1]

Romulo Rodrigues Dantas

"Estamos em uma batalha e mais da metade dessa batalha é travada na mídia, à distância. Essa batalha tem por alvo os corações e as mentes do nosso povo".[2]

Ayman al-Zawahiri

Resumo

Gerar publicidade e propaganda é axioma fundamental do terrorismo, que, historicamente, vale-se de recursos também à disposição da sociedade contemporânea. A internet é um desses. Com a união do efeito de demonstração do fanatismo do século XII com o alcance da comunicação do século XXI, as palavras 'terrorismo' e 'cibernética' fundem-se e geram nova expressão – terrorismo cibernético ou ciberterrorismo – e capitalizam efeitos psicológicos decorrentes do temor do desconhecido e da imprevisibilidade do ato, embasados na dependência das sociedades nas redes de informação. A Convenção de Budapeste estabelece o que constitui crime cibernético, mas é pouco provável que o Brasil vincule-se automaticamente ela. O momento histórico, os referenciais internacionais e a disposição do Brasil em aprimorar sua legislação sobre crimes cibernéticos ensejam prever tipificar a utilização da internet por organizações terroristas e dotar a atividade de Inteligência de Estado brasileira com os recursos jurídicos necessários para o acompanhamento analítico, estratégico e sistemático dessas organizações.

Apresentação

Em 7 de outubro de 2001, algumas horas após o inicio da reação militar dos Estados Unidos da América (EUA) contra instalações do regime Talibã e da al Qaeda no Afeganistão, um vídeo foi divulgado por meio da internet e, depois, pela televisão. Nele, um homem magro, de barba longa e desarrumada, vestindo jaqueta militar camuflada, com turbante na cabeça, um fuzil AK-47 a seu lado e

[1] Texto originalmente apresentado no Seminário Internacional: Crimes Cibernéticos e Investigações Digitais, organizado pela Câmara dos Deputados, em 28 de maio de 2008.

[2] Carta de 2005 de Ayman al-Zawahiri, vice-chefe da al Qaeda, para Abu Mussab al-Zarqawi, então comandante militar da organização no Iraque.

tendo montanhas ao fundo, falava de modo pousado, mas firme, olhando diretamente para a câmara. De modo desafiador, Osama bin Laden declarou, naquele momento, o começo da segunda etapa da guerra que iniciara em 11 de setembro do mesmo ano.

A mensagem de bin Laden evidenciou que a internet também estava à disposição da al Qaeda, com qualidade, segurança, alcance global e oportunidade, e que as armas à disposição da organização não mais se resumiam a fuzis e bombas, mas agora incluíam computadores, seus acessórios e periféricos.

A propaganda é técnica essencial de que se valem organizações extremistas, especialmente com a finalidade de atrair seguidores.

Um dos axiomas mais duradouros do terrorismo o considera fundamentalmente destinado a gerar publicidade e atrair a atenção para os terroristas, as causas que defendem e a mensagem que objetivam divulgar.

Poucas palavras têm carga política ou emotiva semelhante a 'terrorismo'. Estudo do final da década de 90 constatou mais de cem definições do fenômeno, com 22 elementos conceituais diferentes. O ponto de convergência entre estes é que terrorismo é uma forma de ação não-tradicional, que considera o uso da violência ou a ameaça de seu uso.

Ao se analisar a história do terrorismo, constata-se que é fenômeno em evolução, que se vale de recursos também à disposição da sociedade contemporânea. A internet é um desses.

As decorrências de tal constatação impõem a governos e sociedades a necessidade de dispor e se valer de dispositivos legais e de segurança capazes de confrontar a ameaça, porém sem restringir o acesso à informação. Essa dicotomia traz desafios crescentes ao modelo tradicional de monopólio da comunicação por entidades estatais e comerciais, na medida em que organizações não-governamentais e de natureza não-democrática também se valem desses recursos para lograr fins políticos violentos.

A propaganda é técnica essencial de que se valem organizações extremistas, especialmente com a finalidade de atrair seguidores. Por décadas, material impresso, vídeos com operações e treinamentos, discursos, história e realizações têm estado à disposição de interessados, em redes de distribuição difusas, clandestinas e de acesso limitado. Entretanto, no século XXI, pessoa interessada em conhecer, apoiar ou aderir a esse tipo de organização pode individualmente e de maneira aberta se valer da internet e obter a informação desejada, tanto por meio de páginas estáticas quanto interativas, como salas e fóruns de discussão.

Ao unir o efeito de demonstração do fanatismo do século XII com o alcance global da comunicação do século XXI, as palavras 'terrorismo' e 'cibernética' fundem-se e geram nova expressão, dimensão e conceito – terrorismo cibernético ou ciberterrorismo –, que capitaliza efeitos psicológicos decorrentes do temor do desconhecido e da imprevisibilidade do ato, embasados na dependência das sociedades nas redes de informação.

Igualmente, por se caracterizar como fenômeno recente, o terrorismo cibernético ou ciberterrorismo também carece de definição consolidada e universalmente aceita.

Isso decorre, provavelmente, do entendimento tradicional de que as expressões **terrorismo** e **internet** aparentemente não coexistem nem se complementam. Mas o certo é que essa combinação ainda é pouco estudada pela ciência política.

Com essa percepção, objetiva-se discorrer sobre a relação entre essas expressões. Apesar de serem apresentadas definições operacionais[3] para se estabelecer bases de entendimento, não se terá por objetivo a busca de definição ideal ou satisfatória para elas, mas, apenas, ater-se a entendimentos que se fundamentam no senso comum da variedade de definições acadêmicas e governamentais sobre o tema.

Trata-se, assim, de percepção acadêmica e não se deve atribuir a ela valor institucional.

Estratégia Global das Nações Unidas de Contraterrorismo

A Estratégia Global das Nações Unidas de Contraterrorismo foi adotada pela Assembléia-Geral em 8 de setembro de 2006. Esta estratégia estabelece ações concretas que devem ser implementadas, individual ou coletivamente, pelos Estados-membros em matéria de terrorismo. Atividades de coordenação e cooperação da estratégia incluem tarefas relacionadas a: facilitar sua implementação; fazer frente a ações radicais e extremistas que possam resultar em atos terroristas; impedir o uso da internet com finalidades terroristas; proteger os direitos humanos, mesmo ao se combater o terrorismo; proteger e fortalecer alvos vulneráveis; apoiar e destacar as vítimas do terrorismo; e combater o financiamento do terrorismo.

No que se refere à utilização da internet com finalidades terroristas, os Estados-membros acordaram que a estratégia teria por objetivo identificar e proporcionar o debate com atores públicos e privados sobre o assunto e identificar maneiras possíveis de combater essa ação, nos níveis global, regional e sub-regional.

Ainda que se tenha incluído tópico sobre a prevenção ao uso criminal, é escasso o conhecimento sobre a ameaça representada pela utilização da internet por terroristas, que a têm utilizado para recrutar adeptos, arrecadar fundos e estabelecer ações de propaganda, em escala global.

Utilização da internet por Organizações Terroristas

O estudo da conexão entre terrorismo e internet – ou, conforme proposto neste ensaio, – tem sido objeto de interesse de acadêmicos e especialistas, dos setores privado e público, a partir da segunda metade da década de 90 e, especialmen-

[3] Conforme estabelecido por Portaria de 2004 do Conselho Consultivo do Sistema Brasileiro de Inteligência (Sisbin), para a Agência Brasileira de Inteligência (Abin) e os demais órgãos deste Sistema, **terrorismo** é *a ameaça ou emprego da violência física ou psicológica, de forma premeditada, por indivíduos ou grupos adversos, apoiados ou não por Estados, motivado por razões políticas, ideológicas, econômicas, ambientais, religiosas ou psicossociais, e objetiva coagir ou intimidar autoridades ou parte da população*, *para subjugar pessoas ou alcançar determinado fim ou propósito* (SISTEMA...,2004, grifo nosso). **Terrorismo cibernético** ou **ciberterrorismo**, academicamente, é definido pela Escola de Inteligência, como o *uso premeditado de ações de interrupção ou ameaça de interrupção de serviços com base em computadores ou redes de informação, com motivação criminal ou ideológica e visando a provocar danos ou intimidação*.

te, após os ataques de 2001. Walter Laqueur (2000) foi um desses visionários.

No âmbito acadêmico, artigos têm sido produzidos, vislumbrando supostos esforços de organizações terroristas – sobretudo a al Qaeda – para a aquisição de meios técnicos, destinados à realização de ataques com super-alta tecnologia contra infraestruturas críticas ocidentais, particularmente dos EUA, por meio de redes de computadores.

Especialistas em áreas de Inteligência de Estado, inclusive no Brasil[4], avaliam que, atualmente, é pouco provável que a al Qaeda ou qualquer outra organização terrorista conhecida tenha capacidade de realizar ações que demandem emprego de recursos de alta tecnologia. Entretanto, há concordância de que fatores críticos para a continuidade da al Qaeda incluem planejamento operacional aprimorado; ênfase no sigilo das informações; uso planejado de técnicas de comunicação e propaganda; exploração de lacunas legais, além de criatividade e inovação na utilização de táticas convencionais de ataque.

Organizações criminosas, movimentos radicais e a tendência deles à violência não representam novidade no cenário dos países. Governos têm continuadamente buscado formas de aprimorar sua capacidade de confrontar a ameaça. Para tanto, é fundamental dotar organismos de segurança e de Inteligência de Estado com treinamento e recursos legais e materiais compatíveis com demandas que se apresentam, respeitados competências específicas e limites estabelecidos.

Vive-se em uma Era em que a tecnologia da informação é parte integrante dos variados aspectos que compõem a sociedade contemporânea. A internet é a 'face' mais conhecida do processo de globalização. As vantagens que computadores, redes computacionais e tecnologia associada oferecem à sociedade e ao comércio também auxiliam organizações criminosas a realizar suas atividades, o que é facilitado pela ainda incipiente capacidade de resposta dos Estados, como parte de estratégia universal concertada. O Brasil não é exceção.

Tipicamente, as páginas-*web* terroristas apresentam história e feitos da organização; biografia de líderes, fundadores e heróis; informações sobre objetivos almejados; e críticas aos opositores. De modo geral, o uso considera a internet para arrecadar fundos, recrutar adeptos, obter informações e coordenar ações.

Muitas das condutas cometidas com o uso de computadores e redes computacionais surgiram em função desses objetivos, como invasão de sistemas e interceptação de comunicações eletrônicas sem autorização judicial. Naturalmente, a internet se constitui ambiente ideal para organizações terroristas, em decorrência: do fácil acesso; da carência de legislação universalmente aceita; do pouco controle ou de crítica governamental ou de órgãos de autorregulamentação; do alcan-

[4] Nos termos do art. 3º da Lei nº 9.883, de 7 de dezembro de 1999, cabe exclusivamente à Abin, órgão de assessoramento direto ao Presidente da República, que, na posição de órgão central do Sistema Brasileiro de Inteligência, tem, exclusivamente a seu cargo, planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, obedecidas a política e as diretrizes estabelecidas em lei.
O acompanhamento de manifestações do terrorismo de bases científica ou tecnológica integra a relação de assuntos acompanhados sob ótica analítica e estratégica pela Abin – especificamente, por meio do Departamento de Contraterrorismo –, com a finalidade de prevenir o terrorismo e seu financiamento, no Brasil ou contra interesses brasileiros no exterior.

ce global a públicos-alvo imediato e potencial; da instantaneidade da comunicação; dos razoáveis anonimato e segurança; do baixo custo de operação e manutenção; do ambiente multimídia; da simplicidade, entre outros fatores.

A internet é espécie de biblioteca digital, onde informações são obtidas a custo baixo e podem dizer respeito a serviços de transporte, imagens de infraestruturas críticas, horários e regras de acesso a edifícios públicos, aeroportos e portos; rotinas e procedimentos de segurança, inclusive contra ações terroristas.

Em 2003, Dan Verton descreveu entrevistas de organizações terroristas, sobretudo a al Qaeda, que operam com o auxilio de bases de dados com detalhes de objetivos potenciais ao redor do mundo e se valem da internet para obter Inteligência sobre tais objetivos. Com programas computacionais comerciais ou especificamente concebidos, identificam debilidades, projetam resultados desejados, avaliam impactos econômicos decorrentes e resultados nos direitos civis.

Desafio Legal

Sob a ótica da Inteligência de Estado, as tarefas de responder a condutas criminosas envolvendo recursos computacionais não são triviais nem teóricas e impõem desafios: **Técnicos** – relativos à capacidade de se identificar fatos e situações de interesse; **Legais** – capazes de prover o embasamento jurídico de resposta ao delito; e **Operacionais** – para assegurar capacidade a profissionais de organizações especializadas de analisar de forma célere e com abordagem estratégica a vinculação entre terrorismo e internet, até mesmo no exterior.

O acompanhamento de atividades terroristas pela internet requer que agências de Inteligência de Estado disponham dos instrumentos legais imprescindíveis para a obtenção, em bases racionais, de dados e conteúdo relacionados à interceptação, análise e avaliação de tendências de atividades terroristas e conexas a ela, com fiscalização e limites estabelecidos, proativamente. Entretanto, não deve competir a essas agências executar tarefas de natureza processual, forense ou de polícia judiciária.

O primeiro acordo multilateral sobre crime cibernético foi firmado entre países europeus em 23 de novembro de 2001, em Budapeste, Hungria, sem a participação do Brasil. O acordo é conhecido como Convenção do Conselho Europeu sobre o Cibercrime, ou Convenção de Budapeste. Essencialmente, esse instrumento objetiva proteger a sociedade contra crimes na internet, por meio da adoção de legislação adequada e do avanço da cooperação internacional, decorrentes da conscientização acerca das mudanças do processo de comunicação digital.

O acordo entrou em vigor em 1º de julho de 2004, depois que cinco países o ratificaram, sendo três integrantes do Conselho Europeu. Quarenta e sete países já ratificaram o tratado. Os EUA são o único país de fora do Conselho Europeu que o ratificou, em 29 de setembro de 2006. O Japão e o Canadá o assinaram.

A uniformização da lei internacional centrada na convenção ainda é limitada e precisa ter a participação de maior número de países, além de sofrer adição de outras modalidades de delitos cibernéticos. Entretanto, para ser eficaz, necessita ter adesão universal, no âmbito

das Nações Unidas, para poder potencializar suas chances de sucesso.

A convenção estabelece o que constitui crime cibernético e permite que as polícias de cada país cooperem nas investigações desses delitos, podendo até prender suspeitos de crimes cometidos fora de seu território. Críticos do documento questionam os poderes atribuídos à polícia, que, segundo eles, poderiam comprometer a preservação da liberdade na internet. Muitos países já dispõem de legislações que permitem que organismos de segurança monitorem a internet, mas especialistas temem que esses poderes sejam ampliados nos países que adotarem o tratado.

Não há, entretanto, provisão com o objetivo de proporcionar o debate com atores públicos e privados sobre o uso da internet com finalidade terrorista e identificar maneiras possíveis de combater essa ação, nos níveis global, regional e sub-regional.

Discute-se no Brasil a agregação de novos paradigmas relativos ao delito eletrônico, de forma a adequar o ordenamento jurídico brasileiro para responder a essa nova modalidade de crime e a possibilitar ao País se inserir em um modelo de cooperação internacional – provavelmente, a Convenção de Budapeste –, para prevenir e combater crimes cibernéticos. A análise e o monitoramento do uso da internet com finalidades terroristas deveria ser uma dessas adequações.

O Legislativo brasileiro tem buscado aprimorar o debate sobre o tema e incorporar contribuições ao substitutivo que o senador Eduardo Azeredo (PSDB-MG) apresentou ao Projeto de Lei nº 76/2000, em tramitação no Senado. O substitutivo define e tipifica os delitos da área de informática e aglutinou três projetos de lei que já tramitavam no Senado, enfocando crimes e condutas realizados mediante uso de sistema eletrônico, digital ou similares, de redes de computadores, ou que sejam praticadas contra redes de computadores, dispositivos de comunicação ou sistemas informatizados e similares.

Nesse sentido, em 10 de junho de 2008, a Comissão de Assuntos Econômicos (CAE) do Senado aprovou a proposta do senador Eduardo Azeredo para tipificar e punir os crimes cometidos com o uso das tecnologias da informação.

Com base nessa proposta, os novos tipos penais são: 1) acesso não-autorizado a dispositivo de informação ou sistema informatizado; 2) obtenção, transferência ou fornecimento não-autorizado de dado ou informação; 3) divulgação ou utilização indevida de informações e dados pessoais; 4) destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheiro; 5) inserção ou difusão de vírus; 6) agravamento de pena para inserção ou difusão de vírus seguido de dano; 7) estelionato eletrônico; 8) atentado contra segurança de serviço ou utilidade pública; 9) interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado; 10) falsificação de dados eletrônicos públicos; e 11) falsificação de dados eletrônicos particulares.

Não há, entretanto, provisão com o objetivo de proporcionar o debate com atores públicos e privados sobre o uso da internet com finalidade terrorista e identificar maneiras possíveis de combater essa ação, nos níveis global, regional e sub-regional, contrariando o que dispõe a Estratégia Global das Nações Unidas de Contraterrorismo.

Também na Europa, já foram adicionados à Convenção de Budapeste, pelo Conselho Europeu, três novos delitos cibernéticos: propaganda, recrutamento e treinamento terroristas, com a intenção de, posteriormente, harmonizar o combate ao ciberterrorismo no continente. O Comitê de Especialistas em Terrorismo (Codexter, em espanhol) estuda o tema e pesquisa nos países as modificações necessárias no conjunto normativo existente, para combater essa forma emergente de crime.

Considerações Finais

O continuado interesse no aprimoramento da legislação brasileira sobre o tema dos delitos digitais e a busca por incorporações de atores públicos e privados sobre a matéria ensejam legitimidade, eficácia e identificação de ameaças para a ação do Estado brasileiro. Adicionalmente, criam oportunidades para considerar novas contribuições, que potencializam a capacidade de se adequar às novas modalidades criminais que se apresentam nos níveis global, regional e sub-regional, entre elas, a utilização da internet por organizações terroristas.

Internacionalmente, o referencial proporcionado pela Convenção de Budapeste é reconhecido como marco da tentativa de harmonização da legislação de combate às manifestações de crime cibernético. Apesar de esse fato representar passo significativo na matéria, considera-se que sua eficácia é diretamente proporcional à adesão que obtiver.

Como principio e tradição da diplomacia do País, os sucessivos governos brasileiros aderem aos tratados cujo processo de elaboração considera interesses e percepções nacionais, posteriormente acordados no âmbito das Nações Unidas.

Assim, ao se cotejar princípios que norteiam a ação governamental brasileira com a gênesis do referencial jurídico disponível, refuta-se como pouco provável que o Brasil vincule-se jurídica e automaticamente à Convenção de Budapeste, sem que o País seja convidado pelo Comitê de Ministros do Conselho Europeu ou que a Convenção seja discutida universalmente para ser legitimada. A segunda hipótese representaria reforço ao princípio do multilateralismo no combate ao crime cibernético, numa evidência de compromisso e disposição dos 192 Estados-membros das Nações Unidas para enfrentar o problema.

A utilização da Internet por grupos terroristas transcende o mero uso da tecnologia e alcança dimensões organizacional e de transformação estratégica, além de constituir método e meio capazes de disseminar informação original desses grupos, sem interpretações ou censura, de modo instantâneo e com alcance global.

Essa nova modalidade de crime terrorista depende da revolução da informação e da tecnologia associada e tem foco na relevância do debate livre para o funcionamento das instituições democráticas.

O momento histórico, os referenciais internacionais e a disposição do Brasil em

aprimorar sua legislação sobre crimes cibernéticos ensejam prever tipificar a utilização da internet por organizações terroristas e dotar a atividade de Inteligência de Estado com os recursos jurídicos necessários para o acompanhamento analítico, estratégico e sistemático dessas organizações.

Proativamente, essa ação previne a capacidade que têm as organizações terroristas de potencializar, por meio da internet, não mais apenas o consumo de ideologias não-democráticas, bem como de produzi-las e de usar os recursos de comunicação tecnológica como proposta de mudança de poder.

Referências

BRASIL. Congresso. Senado Federal. Projeto de Lei do Senado nº 76/2000, de 27 de março de 2000. Define e tipifica os delitos informáticos, e dá outras providências. Disponível em: <http://www.senado.gov.br/sf/atividade/Materia/detalhes.asp? p_cod_ mate=43555>. Acesso em: 12 fev 2008.

BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L9883.htm>. Acesso em: 12 fev. 2008.

CONVENÇÃO DE BUDAPESTE (2001). Convenção do Conselho da Europa sobre o Cibercrime. Budapeste, 23 de novembro de 2001. Disponível em: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>

LAQUEUR, Walter. *The new terrorism: Fanaticism and Arms of Mass Destruction*. New York: Oxford University Press, 2000.

SISTEMA BRASILEIRO DE INTELIGÊNCIA. Conselho Consultivo. *Manual de Inteligência:* Doutrina Nacional de Inteligência; bases comuns. Brasília: Abin, 2004. 44p. (Manual aprovado pela Portaria nº 5/GSI/PR, de 31 de março de 2005).

VERTON, Dan. Black Ice: *The invisible threat of cyberterrorism*. Osborne, McGraw-Hill Osborne Media, 2003.