Terrorismo no ciberespaço: o poder cibernético como ferramenta de atuação de organizações terroristas

Terrorism in cyberspace: the cyberpower as acting tool of terrorists organizations

Mayara Gabrielli Gardini*

Resumo

O ciberespaço é um novo domínio de poder nas relações internacionais onde atuam diversos atores, entre eles as organizações terroristas. Estas organizações encontraram no espaço cibernético um novo campo para expandir suas ideias e alcançar seus objetivos. Dessa forma, o tema do terrorismo no ciberespaço é uma questão relevante no contexto internacional. Posto isto, o objetivo da pesquisa foi demonstrar a forma que estes grupos operam neste novo domínio de poder, sendo necessário a apresentação de conceitos como ciberespaço, poder cibernético, terrorismo e terrorismo cibernético, além da aplicação das formas de atuação das organizações terroristas neste espaço em situações reais. O problema da pesquisa foi demonstrar de que maneira estas organizações utilizam-se do espaço cibernético como ferramenta de atuação. Para isso, o método de pesquisa utilizado foi o bibliográfico e o levantamento de informações foi realizado a partir de livros, artigos e publicações na internet. Com a pesquisa finalizada, foi possível conluir que os grupos terroristas utilizam-se do poder no ciberespaço para divulgar propaganda, levantar fundos, transmitir informações para treinamento, planejar atos terroristas, auxiliar na execução desses atos e efetuar ataques cibernéticos.

Palavras-chave: Relações Internacionais. Ciberespaço. Poder cibernético. Organizações terroristas. terrorismo cibernético.

Abstract

Cyberspace is a new power domain in international relations where operate several actors, including terrorists organizations. These organizations found in cyberspace a new field to expand their ideas and to achieve their goals. In this way, the subject of terrorism in cyberspace is a relevant issue in the international context. That said, the objective of the research was to demonstrate how these groups operate in this new power domain, requiring the presentation of concepts such as cyberspace, cyberpower, terrorism and cyberterrorism, besides the application of forms of action of terrorist organizations in this space in real situations. The problem of research was to study how these organizations use the cyberspace as acting tool. For this, the research method used was bibliographic and information gathering was conducted from books, articles and publications on the internet. With the research completed, it was concluded that terrorists groups use power in cyberspace to divulge propaganda, to raise funds, to transmit information for training, to plan terrorists acts, to assist in the execution of these acts and to carry out cyber attacks.

Keywords: International Relations. Cyberspace. Cyberpower. terrorist organizations, cyberterrorism.

* Graduanda em Relações Internacionais na Universidade do Vale do Itajaí. Contato: mayara_gardini_@hotmail.com

Introdução

A questão do terrorismo no ciberespaço é bastante recorrente nas notícias pelo mundo. As organizações terroristas, grupos politicamente motivados que utilizam-se da violência para alcançar seus objetivos, estão cada vez mais presentes no espaço cibernético e vêm adquirindo poder dentro deste domínio. Por este motivo, o tema do terrorismo no ciberespaço é relevante para o estudo das relações internacionais.

Do ponto de vista acadêmico, o estudo do poder cibernético e a sua relação com a forma em que os Estados e outros atores se organizam no mundo atual é fundamental. A figura estatal ainda é importante, mas a diversidade de atores presentes e suas capacidades de influência sobre assuntos que antes só eram discutidos por Estados devem ser analisadas por estudiosos da área com atenção. Neste sentido, especial relevância deve ser dada ao crescimento do poder cibernético ao longo dos últimos anos e à maneira como ele possibilita a atuação de uma gama cada vez mais diferenciada de atores, principalmente diante das incertezas trazidas pela atuação de grupos terroristas. Estas incertezas demonstram a necessidade de um maior entendimento sobre as questões de segurança que estão relacionadas ao ciberespaço.

No contexto internacional, a segurança no mundo virtual (ou a falta dela), tornou-se tema de destaque na agenda. Este é um problema que afeta tanto assuntos internos quanto externos dos países, pois, no ciberespaço, há uma difusão de poder, na qual a força física e a soberania deixam de ser critérios norteadores e os custos de atuação relativamente baixos, favorecem a atuação de outros atores além dos Estados. Ademais, diante de tais facilitadores e da ausência de um confronto físico, um ente pode facilmente manter-se anônimo. É por isto que é difícil estabelecer regras que contribuam para um ambiente mais seguro. Alguns atores se aproveitam desta fraqueza para disseminar ideias que contestem a conjuntura internacional atual, de forma a gerar medo e desconfiança entre os usuários da rede e, ainda, deixar Estados em alerta, com medo da atuação das organizações terroristas.

A possibilidade de ações que esses grupos podem realizar no ambiente virtual é preocupante, pois ao contrário do espaço físico, onde os terroristas não possuem o poder militar e econômico dos Estados, as barreiras são menores e os danos de um ataque podem

causar problemas sérios, como a de uma investida na dimensão física. Essas ações e a forma como são realizadas, por meio de um espaço onde praticamente todos têm acesso, é um ponto de interesse mundial, pois qualquer ator, do Estado ao indivíduo, pode ser afetado de alguma maneira por essas organizações.

Sendo o ciberespaço e o terrorismo temas complexos, foi preciso delimitar de forma precisa a questão estudada. Desta forma, a delimitação do tema foi centrada nas formas de atuação das organizações terroristas no ciberespaço.

A cada dia, existem novas informações sobre organizações terroristas que chamam a atenção para as forma como estas usam o espaço cibernético para a sua atuação; seja como forma de disseminar suas ideias, recrutar novos membros em redes sociais, ameaçar e executar ataques aos seus inimigos ou expor em vídeos as execuções feitas em nome de sua causa. Assim, para demonstrar estas ações de modo mais preciso, o problema da pesquisa indaga sobre as formas de atuação que as organizações terroristas utilizam no ciberespaço para alcançar seus objetivos.

Apresentado o problema, o objetivo da investigação é demonstrar a forma que os grupos terroristas operam neste novo domínio de poder. Para atingir este objetivo, é necessário apresentar o ciberespaço e o poder cibernético, assim como o terrorismo e o terrorismo cibernético, de forma a fornecer uma melhor compreensão da resposta do problema da pesquisa.

No desenvolvimento da pesquisa, o método utilizado é a pesquisa bibliográfica e o levantamento de informações foi realizado com base em livros, artigos e notícias disponíveis na internet. Para alcançar o objetivo do trabalho e responder o problema da pesquisa, a primeira seção aborda a definição de ciberespaço e poder cibernético, como os atores do contexto internacional atuam neste diferente domínio e a questão da segurança no espaço cibernético. Posteriormente, na segunda seção, são fornecidas definições de terrorismo e terrorismo cibernético e, ainda, as formas que as organizações terroristas atuam no ciberespaço, de acordo com o relatório "*The Use of the Internet for Terrorists Purposes*", do Escritório das Nações Unidas sobre Drogas e Crimes. Finalmente, na terceira seção, são dados exemplos da atuação do "Estado Islâmico", a organização terrorista mais ativa no ciberespaço no momento, e outras organizações terroristas.

Ciberespaço e poder cibernético[1]

Ciberespaço[2] e poder cibernético são fenômenos recentes que vêm se tornando cada vez mais presentes em diversas áreas, entre elas as Relações Internacionais. O motivo desse interesse pelo assunto, tanto de pesquisadores quanto a população em geral, é a dificuldade de mensurar, com precisão, a sua real capacidade e extensão. A mesma rapidez e facilidade de acesso a informações e comunicação que é benefício para uns, pode ser um problema para outros.

Na presente seção, será apresentada a definição de ciberespaço e poder cibernético, como os atores internacionais atuam neste diferente domínio e a questão da segurança no espaço cibernético.

Definição de ciberespaço e poder cibernético

No âmbito acadêmico, existem várias definições de ciberespaço, com diferentes perspectivas e elementos, uma dessas definições é trazida por Kuehl, que explica o ciberespaço enquanto:

> Um domínio operacional dentro do ambiente de informação cuja distinta e única característica é enquadrada pelo uso de eletrônicos e espectros eletromagnéticos para criar, armazenar, modificar, trocar e explorar informações via redes interdependentes e interconectadas usando tecnologias de informação/comunicação.[3] (KUEHL, 2009, não paginado, tradução nossa)

Em outras palavras, o espaço cibernético é um ambiente virtual de comunicação, transmissão e armazenagem de dados que pode ser acessado nos mais diferentes dispositivos eletrônicos conectados por redes eletromagnéticas. Com o passar dos anos, este domínio tornou-se cada vez mais difundido e presente, seja através de sinais de rádio e televisão, computadores, satélites, telefonia ou sistemas em geral que estão, de alguma forma, interligados ao espaço cibernético. (NYE JÚNIOR, 2012, p. 163)

Devido ao desenvolvimento da tecnologia e a redução de custos, as barreiras de entrada no ciberespaço estão cada vez me-

1. Dada a complexidade do fenômeno, as questões relativas ao ciberespaço serão expostas de forma a apresentar apenas os pontos necessários para compreender o objetivo do trabalho, ou seja, a parte técnica do espaço cibernético não será abordada.

2. Neste trabalho, o ciberespaço e espaço cibernético serão apresentados com o mesmo significado.

3. "Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."

nores, pela possibilidade de facilitar o acesso à informação por diferentes tipos de pessoas, organizações e Estados. Uma outra face do ciberespaço é a velocidade de mudanças, pois por ser um ambiente virtual, estas ocorrem de forma mais rápida do que no mundo físico, isto porque a geografia do espaço cibernético tem uma maior mutabilidade que em outros ambientes. (NYE JÚNIOR, 2012, p. 164) As definições de Kuehl e Nye Júnior se complementam, sendo a do primeiro mais generalizada, enquanto a do segundo possui aspectos importantes para o desenvolvimento do presente artigo.

Há diferentes formas de usar o ciberespaço, a mais conhecida é por meio da internet, uma rede global que conecta milhões de computadores e outros dispositivos eletrônicos, que pode ser definida como "um sistema em camadas que possibilita processar, manipular e usar informação, e facilita a expansão da comunicação humana assim como a interação de humanos e informação."[4] (CHOUCRI, 2012, p. 268, tradução nossa.)

O ciberespaço pode ser entendido como um regime único de propriedades físicas e virtuais. (NYE JÚNIOR, 2012, p. 162.) As relações via espaço cibernético não se dão apenas no mundo virtual, elas têm raízes no mundo físico (cabos e aparelhos com conexão à rede, por exemplo) que são regidas pelas leis de cada Estado. Ataques podem ocorrer, tanto de dentro para fora do ciberespaço, quanto de fora para dentro. Sabendo disso, uma das definições para poder cibernético pode ser "a capacidade para obter resultados preferidos mediante o uso dos recursos de informação eletronicamente conectados do domínio cibernético." (NYE JÚNIOR, 2012, p. 163.)

Outra definição de poder cibernético é apresentada por Starr (2009, tradução nossa), onde "poder cibernético é definido como a habilidade de usar o ciberespaço para criar vantangens e influenciar eventos em outros ambientes operacionais e através de instrumentos de poder."[5] Por essa definição, o ciberespaço é utilizado pelo poder cibernético como meio de atuação para atingir seus objetivos. As definições apresentadas de Starr e Nye sobre o poder

4. "[...] a layered system that enables processing, manipulation and use of information, and facilitates the expansion of human communication as well as interaction of humans and information."

5. "[...] the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power."

cibernético, além da definição básica, adicionam informações para um melhor entendimento do termo, complementando-se.

No que se refere à prática do poder cibernético, Nye Júnior (2012, p. 165) diferencia tal atividade entre 'poder intraespaço cibernético'[6] e 'poder extraespaço cibernético'[7], e fornece exemplos de como podem ser colocados em prática, indicando quais são poder duro e quais são poder brando.[8]

Em ações intracibernéticas, o poder brando pode ser aplicado por meio de definição de agenda, atração e persuasão. Atacar a rede de computadores de uma empresa com milhares de vírus é um exemplo de poder duro dentro do ciberespaço, um agravante dessa situação é o fato de ser muito difícil rastrear os atacantes. Nos casos de ações extracibernéticas, um exemplo de poder brando é atrair cidadãos em outros países, como uma campanha diplomática para mudar a opinião dessas pessoas. Como exemplo de poder duro, a invasão e o desligamento do sistema de energia de uma cidade do norte no meio do inverno, como Montreal, causaria sérios danos à população. (NYE JÚNIOR, 2012, p. 166-167.)

Exemplos de instrumentos físicos que poderiam afetar o espaço cibernético são: a criação de servidores especiais e softwares para ajudar ativistas de direitos humanos a propagar sua mensagem, apesar de esforços do governo para bloquear (poder brando), a criação de leis pelo governo para conter as ações de companhias dentro do ciberespaço (poder duro). (NYE JÚNIOR, 2012, p. 166-169.)

Existe, ainda, intrumentos de fora do ciberespaço que interferem em sua estrutura física, como um ataque militar a essa estrutura, onde servidores podem ser explodidos e cabos podem ser cortados (poder duro), e uma manifestação para envergonhar empresas da internet por abusar de seu uso, como entregar nomes que deveriam ser protegidos para um governo (poder brando). (NYE JÚNIOR, 2012, p. 168-169.)

6. Refere-se a projeção do poder cibernético dentro do mundo virtual, também será mencionado como ações intracibernéticas.

7. Refere-se ao poder cibernético no mundo físico, será mencionado também como ações extracibernéticas.

8. No livro O futuro do poder (2012), Joseph Nye diz que, nos anos 90, distinguiu poder duro e poder brando indo de um espectro de poder de comando (habilidade de mudar o que os outros fazem) para o poder cooptativo (habilidade de moldar o que os outros querem), o comportamento de poder duro se apoia na coerção e pagamento e o comportamento de poder brando se apoia na definição de agendas, atração e persuasão.

O ciberespaço no jogo de poder internacional

Com o crescimento do uso do ciberespaço no mundo atual, há uma nova arena para conduzir a política internacional. Sendo um novo domínio com facilidade de acesso, baixo custo, capaz de mudanças rápidas e a oportunidade de anonimato, o ciberespaço se torna interessante para Estados, organizações, instituições e até indivíduos, especialmente no que diz respeito ao poder no contexto internacional. Há uma difusão de poder dentro deste espaço, viabilizando outros atores a possuir uma maior participação em assuntos que antes só tinham um peso real quando discutidos por Estados.

Para Nye Júnior (2012, p. 152.), os Estados continuarão sendo os principais atores no palco mundial, porém, passarão por mais adversidades, pois ele estará muito mais povoado e difícil de controlar. Todavia, apesar da diferença de poder no espaço cibernético não ser tanta quanto no que diz respeito ao poder militar, por exemplo, ela ainda existe. Os Estados ainda possuem outros poderes a seu favor, o que ajuda no ambiente cibernético, e o coloca em um nível mais elevado em relação aos Estados menores, ONGs, multinacionais e organizações terroristas. Ainda assim, tal difusão que ocorre no ciberespaço não teria a condição de extinguir o Estado, mas sim, de confrontar seu poder e influência com o de outros atores.

A atuação dos atores no espaço cibernético (quadro resumo a seguir) é apontada por Nye Júnior (2012, p. 174) em três categorias: governos, organizações com redes altamente estruturadas e indivíduos com redes fracamente estruturadas.

Quadro 1 - Recursos de poder relativos dos atores no domínio cibernético

Governos
1. Desenvolvimento e apoio de infraestrutura, educação e propriedade intelectual.
2. Coerção legal e física de indivíduos e intermediários localizados dentro das fronteiras.
3. Tamanho do mercado e controle de acesso- por exemplo, União Européia, China, Estados Unidos.
4. Recursos para ataque e defesa cibernéticos: burocracia, orçamentos, agências de inteligência.
5. Provisão de bens públicos, como as regulações necessárias para o comércio.

6. Reputação para a legitimidade, benignidade e competência que produzem poder brando.
Principais vulnerabilidades: alta dependência de sistemas complexos facilmente danificáveis, instabilidade política, possível perda de reputação.
Organizações com redes altamente estruturadas
1. Grandes orçamentos e recursos humanos, economias de escala.
2. Flexibilidade transnacional.
3. Controle de desenvolvimento de código e produto, geração de aplicativos.
4. Marcas e reputação.
Principais vulnerabilidades: perseguição legal, roubo de propriedade intelectual, danos a sistemas, possível perda de reputação (denúncias).
Indivíduos com redes fracamente estruturadas
1. Baixo custo de investimento para a entrada.
2. Virtual anonimato e facilidade de saída.
3. Vulnerabilidade assimétrica em comparação aos governos e às grandes organizações.
Principais vulnerabilidades: coerção legal e ilegal por parte dos governos e organizações, caso sejam apanhados.

Fonte: Nye Júnior (2012, p. 174)

Os principais governos contam com mais recursos que as outras categorias, pois possuem controle sobre leis, territórios, agências do governo e toda uma estrutura exclusiva do Estado, assim, consequentemente, abre vantagem em relação aos outros atores. Este domínio "permite focar na soberania e territorialidade como princípios finais no qual justificam suas escolhas de movimento no ciberespaço."[9] (CHOUCRI, 2012, p. 269, tradução nossa) Porém, na mesma medida que é vantajoso também apresenta seus problemas, como apresentados no quadro resumo.

No segundo tópico do quadro resumo, são apresentadas organizações com redes altamente estruturadas, como empresas transnacionais e organizações criminosas, as quais possuem grandes orçamentos, um número considerável de funcionários, facilidade em explorar diferentes mercados e acesso à alta tecnologia. No entanto, grande parte dessas organizações estão sujeitas às leis de um Estado, podendo sofrer perseguição legal, e além disso, podem perder a reputação perante a sociedade, em caso de denúncias, e/ou ter

9. "[...] allows a focus on sovereignty and territoriality as the ultimate principles on which to justify moves of choice in cyberspace."

seu sistema invadido.

Os indivíduos com redes fracamente estruturadas, em comparação com as outras categorias, como apontado no quadro resumo, não possuem muita desvantagem, em virtude da facilidade de anonimato e baixo custo de entrada. Logo, não dispõem do mesmo poder que um governo ou uma grande empresa, mas podem causar estragos consideráveis, como invasão de sistemas e divulgação de dados sigilosos.

Ainda há 3 tipos de conflitos dentro do espaço cibernético:

> Primeiro são as restrições sobre a administração do ciberespaço e as características operacionais da internet. Segundo são os usos das vias cibernéticas para vantagem estratégica e alavancar o controle político para regular o acesso cibernético ou negar acesso a conteúdos considerados indesejáveis. E terceiro é a militarização do ciberespaço, incluindo a condução da guerra cibernética, ameaças cibernéticas a estruturas críticas, e vários tipos de crimes cibernéticos e espionagem, entre outros.[10] (CHOUCRI, 2012, p. 270, tradução nossa)

Alguns desses já estão ocorrendo, como as discussões sobre a regulamentação da internet, e outros ainda podem acontecer, como uma guerra cibernética.

Todas essas questões, os diferentes tipos de atores, suas capacidades dentro do ciberespaço e as possibilidades de possíveis acontecimentos com motivações terroristas, mostram a necessidade de estudos nessa área. As características do espaço cibernético o tornam atraente para aqueles que desejam atacar, mas não tanto para os que precisam se defender – motivo pelo qual trata-se de tema complexo e de alta relevância para as relações internacionais atuais.

A segurança no ciberespaço[11]

A fácil acessibilidade ao mundo virtual pode ser um problema no que diz respeito à segurança e é capaz de afetar a todos, incluindo os atores internacionais. Diante disso, constata-se que não

10. "First are contentions over the management of cyberspace and the operational features of the Internet. Second are the uses of cyber venues for strategic advantage and leveraging political control to regulate cyber access or deny access to content deemed undesirable. And third is the militarization of cyberspace, including the conduct of cyber warfare, cyber threats to critical infrastructures, and various types of cyber crimes and espionage, among others."

11. A questão da segurança no ciberespaço envolve discussões que não serão aprofundadas no presente artigo, sabendo disso, serão expostos apenas os pontos necessários para compreender o objetivo do trabalho.

existe nenhum mecanismo de segurança totalmente eficaz quando se refere ao ciberespaço. Os países conseguem ter certo controle sob o espaço cibernético, devido a leis e normas, mas isso não é o suficiente. Com a possibilidade de anonimato, a facilidade de desconectar-se da rede e outras capacidades, como o baixo custo e a rapidez de transformação, é difícil aplicar as leis do mundo real nesse espaço virtual. Existem organizações que tentam estabelecer certas normas, padrões e protocolos no uso da internet, porém, essas regras não são sempre respeitadas. (NYE JÚNIOR, 2012, p. 185.)

A verdade é que o ciberespaço vem crescendo de forma explosiva, tornando-se cada vez mais complicado impedir a atuação de agentes maliciosos. Os computadores conectados à internet geralmente usam processadores de propósitos gerais[12] e sistemas de operação que podem executar qualquer programa apresentado na máquina, fazendo deles flexíveis e expandíveis. Porém, essa flexibilidade resulta na possibilidade de infecção por uma grande variedade de códigos maliciosos. Significantes vulnerabilidades são descobertas todos os dias em estações de trabalho, servidores, equipamentos de rede, e, ainda, um grande número de exemplares de códigos maliciosos são introduzidos na rede todos os dias. Desta forma, o estado da segurança na internet é motivo de preocupação no mundo. (SKOUDIS, 2009)

A questão da segurança no ciberespaço deve ser tratada de forma global, pois em virtude de ser um sistema interligado pela internet, o que não pode ser feito em um país, pode ser feito no outro. Nesse sentido, "a União Européia organizou, e aproximadamente 30 nações aderiram a uma Convenção sobre o Crime Cibernético[13]. No entanto, grande parte do mundo não é coberto por esforços concentrados, o que cria um refúgio a partir do qual os criminosos podem operar."[14] (KRAMER, 2009, tradução nossa)

Leis para controlar o ciberespaço afetariam desde indivíduos até governos e não existem formas de controlar todas as ações que acontecem no mundo virtual, em virtude de que o número de parti-

12. "É um sistema "universal", ou seja, um sistema computacional capaz de resolver uma ampla gama de tarefas." (ATTUX, 2015, p. 2)

13. A Convenção sobre o Crime Cibernético, também chamada de Convenção de Budapeste, foi o primeiro instrumento internacional a tratar do assunto, foi aberto para assinaturas em 23 de novembro de 2001 e entrou em vigor em 1 de julho de 2004.

14. "The European Union has organized, and nearly 30 nations have joined, a Convention on Cybercrime. However, much of the world is not covered by focused efforts, which creates a haven from which criminals can operate."

cipantes é extremamente alto. Logo, ainda se faz necessário muitas discussões para se chegar a um acordo que norteie o que pode e não pode ser feito na internet, limites e liberdade de expressão, por exemplo, mesmo sabendo que isso é quase impossível de ser feito.

Em virtude da falta de um mecanismo de defesa 100% efetivo para evitar ações criminosas de todos os tipos no espaço cibernético, os atores envolvidos com atividades ilegais ganham espaço para ampliar seus negócios e adeptos, como, por exemplo, as organizações terroristas, que vêm ganhando destaque na mídia internacional pela sua ação no ciberespaço.

O uso do poder cibernético por organizações terroristas

Com o uso cada vez mais frequente do espaço cibernético nas mais diferentes áreas, a utilização para fins terroristas também vêm ganhando destaque. Na segunda seção, serão apresentadas definições de terrorismo e terrorismo cibernético e, ainda, as formas que as organizações terroristas atuam no ciberespaço, de acordo com o relatório do Escritório das Nações Unidas sobre Drogas e Crimes, de 2012.

Do terrorismo ao "terrorismo cibernético"

Terrorismo é um termo bastante utilizado na atualidade, porém, não há uma definição precisa e universalmente aceita sobre esta questão. Os Estados Unidos definem terrorismo como "violência premeditada, politicamente motivada perpetrada contra alvos não combatentes por grupos subnacionais ou agentes clandestinos, geralmente intencionados em influenciar uma audiência."[15] (UNITED STATES CODE, Title 22, Section 2656f(d))

Richardson (apud CANTER, 2009, p. 3), apresenta sete características necessárias para a definição de terrorismo. Desta forma, para ser conceituado como terrorismo, deve: ser politicamente inspirado, envolver violência ou uma ameaça de violência, transmitir uma mensagem, o ato e o alvo serem simbolicamente significativos, ser realizado por grupos subnacionais, a vítima e o público não são os mesmos, e o ataque deliberado de civis.

Porém, essas definições, apesar de serem aceitas, não concei-

15. "[...] premeditated, politically motivated violence perpetrated against noncombatant1 targets by subnational groups or clandestine agents, usually intended to influence an audience."

tuam todas as faces do terrorismo, nem são tratadas como unanimidade sobre o assunto. O terrorismo aparece de muitas formas em diversas partes do mundo em busca de diferentes objetivos, assim, o que todos os grupos terroristas partilham é a fragilidade em relação aos seus inimigos e o preparo para matar propositalmente civis em prol de seus objetivos. (RICHARDSON, 2006, p. 2)

Sobre o chamado terrorismo cibernético[16], a definição é ainda mais controversa. Baseando-se na pesquisa de outros autores, Parker (2009, p. 245-246, tradução nossa) conceitualiza ciberterrorismo como:

> [...] um ato ou ações criminais premeditadas, de natureza política, social ou religiosa, contra informação, sistemas de computadores, programas de computadores e/ou dados que resultem em violência ou danos severos contra civis, por grupos sub nacionais ou agentes clandestinos.[17]

No mesmo sentido, Denning (2002 apud LACHOW, 2009, p. 1, tradução nossa) traz uma explicação mais completa, na qual define ciberterrorismo da seguinte maneira:

> [...] um ataque ou ameaça de ataque baseado em um computador com intenção de intimidar ou coagir governos ou sociedades em busca de objetivos políticos, religiosos ou ideológicos. O ataque deve ser suficientemente destrutivo ou perturbador para gerar medo comparável à de atos físicos de terrorismo. Ataques que levam à morte ou lesão corporal, falta de energia prolongada, acidentes de avião, contaminação da água, ou grandes perdas econômicas seriam exemplos... *Ataques que perturbam serviços não essenciais ou que são principalmente um incômodo dispendioso não [seriam ciberterrorismo]*.[18]

A segunda definição abordada é mais detalhada, no entanto, ambas definem ciberterrorismo como ações de objetivos políticos ou religiosos que são realizadas por meio do espaço cibernético para causar graves danos contra a sociedade civil ou governos.

16. Também citado como ciberterrorismo.

17. "[...]' a premeditated criminal act or actions; political, social or religious in nature, against information, computer systems, computer programs, and/or data which results in violence against or severe harm caused to civilians, by sub - national groups or clandestine agents'."

18. "[...] a computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples. . . . Attacks that disrupt nonessential services or that are mainly a costly nuisance would not [be cyber terrorism]."

Logo, após a exposição destas definições nota-se que nem toda ação terrorista que envolve o ciberespaço pode ser considerada terrorismo cibernético. Para Lachow (2009, p. 2, tradução nossa), "ciberterrorismo se refere aos meios utilizados para realizar os ataques, não à natureza dos alvos de um ataque terrorista 'clássico'", como no caso de um ataque físico a um sistema de tecnologia da informação.[19] Sendo assim, grupos terroristas que utilizam o espaço cibernético não podem ter suas ações necessariamente classificadas como terrorismo cibernético, sendo o termo muitas vezes utilizado de forma equivocada, já que esses grupos ainda não chegaram ao nível de espalhar o terror utilizando somente o ciberespaço.

Dessa forma, o termo terrorismo cibernético não será aplicado no presente trabalho, devido ao fato de que, até o momento, não houve um ataque suficientemente destrutivo ou pertubador por meio do ciberespaço que causasse o mesmo sentimento de medo motivado por ataques físicos, como, por exemplo, um evento como o 11 de setembro, onde 19 terroristas sequestraram quatro aviões de passageiros, sendo dois deles jogados contra as torres do World Trade Center em Nova Iorque, o que resultou na morte de quase 3 mil pessoas. (O ATENTADO..., 2011)

Formas de atuação das organizações terroristas no espaço cibernético

Um ataque dentro das definições anteriormente citadas como terrorismo cibernético não aconteceu de fato, mas isso não significa que não exista atuação de grupos terroristas no ciberespaço. O domínio virtual permite aos terroristas:

> [...] operar como redes de franquias descentralizadas, criar uma imagem da marca, recrutar partidários, levantar fundos, proporcionar manuais de treinamento e controlar operações. [...] Graças às ferramentas cibernéticas, a al-Qaeda[20] conseguiu passar de uma organização hierárquica, restrita a células geograficamente organizadas, para uma rede global horizontal, [...] (NYE JÚNIOR, 2012, p. 180.)

O espaço cibernético facilitou o trabalho dos grupos terroristas. Neste sentido, é muito mais fácil alcançar seus objetivos com a ajuda de um espaço que permite o anonimato, mudanças rápidas,

19. "Cyber terrorism refers to the means used to carry out the attacks, not to the nature of the targets of a "classical" terrorist attack."

20. Organização fundamentalista islâmica internacional.

apresenta um baixo custo de entrada e é de fácil acesso, do que ter que alcançá-los em espaços que contenham leis, fronteiras e exércitos no caminho. O ciberespaço potencializa a ação e proporciona mais poder a esses grupos.

O uso do poder do espaço cibernético por organizações terroristas já vêm ocorrendo há algum tempo. Um dos primeiros casos documentados de um ataque contra um sistema de computadores de um Estado por um grupo terrorista foi no Sri Lanka, em 1998, pelo grupo *Tamil Tigers*, onde embaixadas do país pelo mundo foram bombardeadas por semanas com 800 *e-mails* ao dia, trazendo a mensagem "Nós somos os Tigres Negros da internet, e nós vamos romper seus sistemas de comunicação". (SIBONI; COHEN; ROTBART, 2013, p. 20.)

De acordo com o documento *"The use of internet for terrorists purposes"*[21], do Escritório das Nações Unidas sobre Drogas e Crimes[22] (2012), existem seis meios pelos quais terroristas podem utilizar o ciberespaço: propaganda, financiamento, treinamento, planejamento, execução e ataques cibernéticos.

A propaganda é a forma que esses grupos disseminam seus ideais, recrutam novos membros e incitam ações terroristas, sendo o espaço cibernético o meio ideal para isso. A velocidade de informação e facilidade de se manter no anonimato ajudam na propagação de ideias, "isso pode incluir mensagens virtuais, apresentações, revistas, tratados, arquivos de aúdio e vídeo e jogos desenvolvidos por organizações terroristas ou simpatizantes."[23] (UNODC, 2012, p. 3, tradução nossa). Atualmente, a propaganda é utilizada por muitos grupos terroristas, principalmente para ensinar sua doutrina e conquistar novos membros. Um exemplo é o aplicativo *The Dawn of Glad Tidings*[24], que oferece aos usuários informações sobre o grupo "Estado Islâmico". (TROWBRIDGE, 2014.)

Como forma de financiamento, pode-se dividir as formas de captar recursos em quatro categorias gerais: solicitação direta (pode ser realizada por meio de fóruns, chats e páginas da internet diretamente pelos terroristas aos seus apoiadores), comércio

21. O uso da internet para fins terroristas.

22. Também citado pela sigla em inglês UNODC (United Nations Office on Drugs and Crimes).

23. "These may include virtual messages, presentations, magazines, treatises, audio and video files and video games developed by terrorist organizations or sympathizers."

24. O Alvorecer de Boas Notícias.

virtual (venda de produtos relacionados com a organização, como livros, aúdios e vídeos), através de ferramentas de pagamento online (PayPal e Skype) ou por meios ilegais (fraudes eletrônicas e roubos de cartão de crédito) e de organizações de caridade. (UNITED NATIONS OFFICE ON DRUGS AND CRIMES, 2012, p. 7). Um relatório da GAFI[25] mostra diversas formas de financiamento de grupos terroristas na África Ocidental, um deles "ilustra a utilização fraudulenta de Organizações Sem Fins Lucrativos (OSFL) para financiar os movimentos rebeldes no norte do Mali através de processos complexos para transferências internacionais de dinheiro." (GRUPO DE AÇÃO FINANCEIRA, 2013, p. 24.)

O treinamento pode ser realizado por meio de fóruns, vídeos e livros, sendo muito mais prático do que no domínio físico devido à facilidade de comunicação e, novamente, de anonimato. Um exemplo é a revista online *Inspire*, publicada pela al-Qaeda na Península Arábica, que tem como objetivo possibilitar o treinamento de muçulmanos para a *jihad* em casa. (UNITED NATIONS OFFICE ON DRUGS AND CRIMES, 2012, p. 8)

O ciberespaço pode também ser utilizado para o planejamento de atos terroristas, em virtude de que a comunicação e pesquisa são realizadas de forma rápida e privada. Há também a possibilidade de plantar informações que auxiliam nos planos de terroristas em páginas da internet e redes sociais. (UNITED NATIONS OFFICE ON DRUGS AND CRIMES, 2012, p. 10.) Em 2010, a al-Qaeda publicou na internet detalhes do planejamento de um ataque frustrado aos EUA, mostrando tempo de preparação, número de pessoas envolvidas, custos de itens usados na operação, como celulares, tranporte e correio, entre outras informações sobre o ataque. (AL-QAEDA..., 2010).

Informações em páginas da internet e redes sociais podem ser utilizados para a execução de atos terroristas. Ameaças em forma de textos, aúdios ou vídeos podem ser veiculadas, causando um sentimento de medo no público desejado. O ciberespaço também pode ser utilizado para coordenar a execução de ataques físicos. (UNITED NATIONS OFFICE ON DRUGS AND CRIMES, 2012, p. 11.) A divulgação de relatos e vídeos na internet de decapitações, crucificações, apedrejamentos, genocídios e sepultamento de vítimas vivas nas regiões que são dominadas pelo "Estado Islâmico" no

25. Grupo de Ação Financeira.

Iraque e na Síria são exemplos de execução. As ações são realizadas no mundo físico, mas não teriam o mesmo impacto se não fossem disseminadas no ciberespaço. (GERGES, 2014)

De acordo com o relatório da UNODC, os ataques cibernéticos são basicamente ações realizadas através de computadores que visam causar danos, geralmente a uma rede de computadores, servidores ou outro tipo de estrutura relacionada ao ciberespaço, por meio de vírus e ataques de negação de serviço, por exemplo. A UNODC (UNITED NATIONS OFFICE ON DRUGS AND CRIMES, 2012, p. 12) usa como exemplo um caso que ocorreu em Israel em janeiro de 2012, onde páginas virtuais como a Bolsa de Câmbios de Tel Aviv e da linha aérea nacional foram atacadas e detalhes de cartões de crédito e contas de milhares de israelenses foram revelados sem autorização.

As ações dentro do ciberespaço ainda podem ser terceirizadas, o que torna mais difícil ligá-las às organizações terroristas. No entanto, é importante deixar claro que as formas de atuação anteriormente citadas não são consideradas terrorismo cibernético, em virtude de que um terrorista que invade uma conta bancária para roubar informações de cartão de crédito não é chamado de ciberterrorista, mesmo que sua intenção seja utilizar o dinheiro para apoiar uma organização terrorista. O terrorismo cibernético apresenta como objetivo a destruição em um nível mais elevado e fatal. (PARKER, 2009, p. 248.)

Essas formas de atuação são as já utilizadas pelas organizações terroristas, elas são as formas que estão dentro de suas capacidades e que possuem o resultado esperado. Porém, "à medida que os grupos desenvolverem sua capacidade para infligir grandes danos contra a infraestrutura nos próximos anos, a tentação aumentará." (NYE JÚNIOR, 2012, p. 191). Caso não seja criado um mecanismo de segurança capaz de defender sistemas importantes de forma mais eficaz, o aumento da capacidade de ação dos grupos terroristas pode levar à possibilidade de terrorismo cibernético, o que poderia causar tantos ou mais danos que os ataques que já acontecem no mundo físico.

Essas formas de atuação de grupos terroristas no espaço cibernético devem ser monitoradas com atenção pelos demais atores internacionais. O domínio virtual proporciona mais poder a esses grupos, como uma nova oportunidade de atingir seus objetivos, uma oportunidade mais rápida e barata e, com o conhecimento e

vontade necessários, o uso desse meio pode causar tantos danos quanto as armas de fogo.

Não há consenso sobre a existência de organizações terroristas plenamente cibernéticas, visto que a própria definição de terrorismo cibernético é controversa, especialmente alguma com destaque no ambiente internacional, porém, ações terroristas cibernéticas vêm sendo utilizadas em benefício desses grupos e causam medo e insegurança pelo mundo.

Terrorismo no ciberespaço

Com as formas de atuação das organizações terroristas no ciberespaço apresentadas anteriormente, é possível observar alguns exemplos na prática. Organizações como "Estado Islâmico" e Boko Haram já utilizam o espaço cibernético como instrumento de poder. Na terceira seção, serão indicados exemplos da atuação do "Estado Islâmico" e outras organizações terroristas.

O uso do ciberespaço pelo "Estado Islâmico"

O autodenominado "Estado Islâmico" (EI), antes chamado de Estado Islâmico no Iraque e na Síria (ou pela sigla em inglês ISIS), visa estabeler (AL-QAEDA..., 2014). O grupo recorre ao ciberespaço como meio de propaganda, recrutamento, financiamento, treinamento e outras formas de atuação, de uma maneira nunca antes utilizada por outras organizações terroristas.

O "Estado Islâmico" não é a primeira organização terrorista no mundo a usar a internet como instrumento de atuação, mas é a que mais se destaca pela forma que se utiliza do poder cibernético. A presença do EI na internet começou em abril de 2014, pouco depois se declarou o "Estado Islâmico" (antes era conhecido como al-Qaeda no Iraque) e em agosto começaram os vídeos da execução de prisioneiros. (DALE, 2015.)

Considerando os meios apresentados pelo UNODC, o mais fácil de identificar é a propaganda. A revista *Dabiq*[26], o aplicativo *The Dawn of Glad Tidings*[27] e os vídeos da execução de prisioneiros divulgados nas mídias sociais, em alta qualidade e muito bem editados, são exemplos da propaganda do EI, que é potencializada nas notícias publicadas na mídia internacional em geral.

26. Cidade síria que dá nome a revista.

27. O Alvorecer de Boas Notícias.

Como outra forma de propaganda, existem os vídeos de recrutamento. Alguns deles são disponibilizados em 14 idiomas diferentes e mostram ocidentais que foram recrutados pelo EI. A mensagem que querem passar é a de que os membros do "Estado Islâmico" são pessoas comuns, como as que estão assistindo os vídeos. Outros vídeos do grupo mostram crianças e famílias, rezando e fazendo compras, com a intenção de passar a imagem que a vida segue normalmente lá. Com as ferramentas sociais, o EI parece ter milhões de pessoas, mas, na verdade, possui cerca de 50.000 membros. (DALE, 2015.)

As mídias sociais são as principais formas de propagar suas ideias e estilo de vida. Os membros do EI usam o Twitter, Instagram, Facebook, Tumblr[28] para compartilhar o que fazem no dia a dia, ações comuns que também são parte da rotina de bilhões de outras pessoas. A intenção é mostrar uma comunidade que segue apenas a Sharia[29], ilustrar uma história para os que procuram um propósito e ainda demonstra que a vida diária no "Estado Islâmico" não é tão diferente da vida em outros países. (COHEN; LEVIN, 2015). A propaganda realizada para recrutar novos membros resultou em 6.500 novos agentes terroristas somente em julho de 2014. (COHEN, 2014).

De acordo com a FATF,[30] o *Al Hayat* é o centro de mídia do "Estado Islâmico", com foco no ocidente, e é responsável por distribuir a propaganda do grupo pelas plataformas de mídias sociais e controla várias contas dessas mídias relacionadas ao EI. No *Twitter*, o grupo tem grande visibilidade e consegue estar entre os assuntos mais comentados, com a promoção de *hashtags*, como #ISIS e #Islamicfront. Essa presença relevante nas redes sociais permite gerar e converter o apoio dos seus seguidores em algo mais concreto. (FINANCIAL ACTION TASK FORCE, 2015, p. 24.)

O "Estado Islâmico" manipula as redes sociais, encorajando doações e conduzindo campanhas de marketing. Seus métodos podem ser comparados com os das empresas de *crowdfunding*[31], em que utilizam análises estatísticas para encontrar possíveis doadores, que

28. Redes sociais online.

29. Um código ético-moral e um conjunto de leis no Islã, baseado no Alcorão, livro sagrado para os muçulmanos.

30. Financial Action Task Force.

31. Método de extrair doações de um grande número de pessoas, utilizando uma combinação de tecnologia e marketing.

se conectem com a causa, aumentando e incentivando contribuições maiores. Um exemplo de desenvolver uma conexão com o EI foi publicado por um membro do grupo via Twitter, onde ele promete que se 50 dinares[32] forem doados, o responsável pela doação receberá um título de "doador com status de prata", se 100 dinares forem doados, quem contribuiu ganhará o título de "doador com status de ouro". (FINANCIAL ACTION TASK FORCE, 2015, p. 26).

O financimento via ciberespaço é apenas uma das formas encontradas para obter recursos financeiros para o grupo. De acordo com as formas de atuação apresentadas no capítulo anterior e o que se sabe sobre o "Estado Islâmico", o financiamento na internet se dá por meio de solicitação direta e ferramentas de pagamento *online*, porém, o financiamento por meios ilegais e via organizações de caridade não podem ser descartados.

As atividades online vão além da propaganda e do financiamento. A presença do "Estado Islâmico" na internet também "possibilita que seus apoiadores obtenham informações operacionais, incluindo treinamento na preparação de explosivos e carros-bomba, [...]"[33]. (KOREN; SIBONI, 2014, p. 2, tradução nossa)

Nas formas de planejamento e execução citadas pelo documento da UNODC, é mais difícil achar exemplos concretos da sua utilização, porém é quase certo seu uso pelas organizações terroristas. Como forma de planejamento, seria realizada como meio de comunicação entre os membros e para pesquisar sobre lugares e pessoas, por exemplo, de forma rápida e privada. Já para a forma de execução, a publicação de ameaças e a coordenação para realizar ataques físicos seriam exemplos dessa categoria. Conforme já citado no capítulo anterior, a divulgação de relatos e vídeos na internet de decapitações, crucificações, apedrejamentos, genocídios e sepultamento de vítimas vivas nas regiões dominadas pelo "Estado Islâmico" no Iraque e na Síria são exemplos de execução. As ações são realizadas no mundo físico, mas não teriam o mesmo impacto se não fossem disseminadas no ciberespaço. (GERGES, 2014)

Os ataques cibernéticos são realizados por meio do ciberespaço com o intuito de causar danos a computadores, servidores e outros dispositivos conectados à rede. Com relação ao "Estado Islâmico", não há ataques cibernéticos concretos vinculados à or-

32. Moeda nacional de vários países, sendo a maioria deles árabes.

33. "[...] enables its supporters to obtain operational information, including training in preparing explosives and car bombs, [...]"

ganização, somente ataques realizados por terceiros, que são simpatizantes, apoiadores e talvez até membros do grupo, mas nada confirmado pelo EI. Em janeiro de 2015, o grupo "CyberCaliphate", suspostamente vinculado ao EI, invadiu a conta do Twitter do Comando Central do Pentágono, órgão que é encarregado das operações no Iraque e na Síria. A foto do perfil da conta foi alterada, mensagens ameaçadoras foram publicadas, informações pessoais de soldados do Comando Central e militares aposentados foram divulgadas. Uma das mensagens publicadas pelos invasores foi: "O EI está aqui, em seus computadores, em cada base militar. [...] Não vamos parar. Sabemos tudo sobre vocês, suas esposas e crianças". (EI INVADE..., 2015)

O mesmo grupo realizou um ataque contra a rede de televisão francesa TV5Monde em abril. Os atacantes tomaram o controle dos sites e da página do Facebook da rede de televisão, causando danos severos aos seus sistemas e supostamente divulgando informações das famílias de soldados franceses que estão envolvidos nas operações contra o EI. (INTERNATIONAL BUSINES TIME, 2015)

De acordo com Koren e Siboni (2014, p. 2), alguns indicadores sugerem que o "Estado Islâmico" possui habilidades avançadas com relação ao ciberespaço. Em primeiro lugar, o EI conta com líderes radicais jovens, com experiência adquirida junto a al-Qaeda (antigo afiliado) e detém mais entendimento sobre tecnologia. Além disso, há suspeitas de vazamento de informações sobre tecnologia avançada do Irã e Coréia do Norte para organizações terroristas. Outro indicador mostra que o "Estado Islâmico" dispõe de recursos suficientes para financiar o terrorismo cibernético enquanto se liga com organizações terroristas internacionais.

A forma como o grupo utiliza o ciberespaço, especialmente para propaganda, é profissional e eficaz. O EI não é o primeiro grupo que se beneficia do poder no espaço cibernético para agir, mas está reinventando a maneira como as organizações terroristas atuam nele, pela forma ativa que se beneficia do poder cibernético, e estimula outros grupos a seguir esse caminho.

Outras organizações terroristas no espaço cibernético

Além do "Estado Islâmico", existem outras organizações terroristas atuando no ciberespaço, como, por exemplo, o Boko Haram.

Fundado em 2002, o Boko Haram[34] manifestava como foco inicial a oposição à educação ocidental. Em 2009, iniciou operações militares para criar um Estado islâmico e, em 2014, declarou um califado nas áreas sob controle. (CHOTHIA, 2015)

Em março de 2015, o Boko Haram declarou fidelidade ao "Estado Islâmico" por meio de um aúdio postado *online*. Sendo assim, esse movimento ajudaria no recrutamento, financiamento e logística, além de receber auxílio do EI com propaganda e mídia. (ELBAGIR; CRUICKSHANK; TAWFEEQ, 2015).

Da mesma maneira que o "Estado Islâmico", o Boko Haram também divulga vídeos no ciberespaço como forma de propaganda, e após afiliação com o EI, seus vídeos passaram a ser mais sofisticados.

O Boko Haram também atua por meio de ataques cibernéticos. Em agosto de 2012, foi executada uma invasão em nome do grupo na base de dados do serviço secreto nigeriano, onde foram revelados dados pessoais do quadro de funcionários e de seus familiares. (MANTZIKOS, 2013)

A organização vem ganhando destaque na mídia, juntamente com o "Estado Islâmico", e, após a declaração de afinidade, podem se tornar cada vez mais parecidos, inclusive nas formas de atuação no espaço cibernético.

Outra organização que se beneficia do ciberespaço é a al-Qaeda (a Base), um grupo terrorista baseado no Paquistão que se transformou em um movimento transnacional com bases em pelo menos 16 países. (MCCORMICK, 2014)

A revista *Inspire*, utilizada como propaganda, e a divulgação de detalhes do planejamento de um ataque frustrado aos EUA já foram exemplificados nesse artigo como forma de uso do ciberespaço pela al-Qaeda.

Também como propaganda, a al-Qaeda divulga vídeos, porém em menor escala que o EI e o Boko Haram. Em janeiro de 2015, foi divulgado um vídeo onde a al-Qaeda na Península Arábica assume a autoria do ataque terrorista que aconteceu em uma revista de humor em Paris no mesmo mês, matando 12 pessoas. (AL-QAEDA..., 2015)

Desde os ataques de 11 de setembro de 2001 realizados pela própria al-Qaeda, a organização divulga nas suas páginas na inter-

34. O nome oficial em árabe é Jama'atu Ahlis Sunna Lidda'awati wal-Jihad, que significa Pessoas Comprometidas com a Propagação dos Ensinamentos do Profeta e a Jihad.

net anúncios de um ataque massivo a alvos norte-americanos. Esses avisos recebem uma grande cobertura da mídia, levando medo e insegurança pelo mundo, especialmente nos Estados Unidos. (WEIMANN, 2004, p. 5)

A organização também utiliza o ciberespaço como forma de planejamento, onde "[...] operam com a assistência de uma grande base de dados contendo detalhes de potenciais alvos nos EUA."[35] (VERTON apud WEIMANN, 2004, p. 6). Além disso, foram encontradas em um computador capturado da al-Qaeda informações estruturais e de engenharia de barragens, que foram conseguidas na internet e que poderiam capacitar o grupo a simular situações de desastres. Em outro computador, foram encontradas pesquisas a respeito de páginas da internet que oferecem instruções de programação para interruptores digitais que executam redes de água, energia, transporte e comunicação. (WEIMANN, 2004, p. 7)

Uma ação terrorista bastante conhecida também foi planejada e executada com muita ajuda do ciberespaço: os ataques de 11 de setembro de 2001. Milhares de mensagens encriptadas foram encontradas no computador de Abu Zubaydah, terrorista da al-Qaeda arquiteto dos ataques, de maio de 2001 até dois dias antes de sua execução. (WEIMANN, 2004, p. 10)

Weimann (2004, p. 7) diz que a al-Qaeda depende de doações, organizações de caridade, ONGs, entre outras instituições financeiras que fazem as contribuições através de salas de bate-papo e fóruns. Possivelmente, hoje em dia são utilizadas ferramentas mais modernas de pagamento, como PayPal e Skype.

Como forma de treinamento, a organização preparou um manual apelidado de "A Enciclopédia da Jihad", que fornece intruções detalhadas sobre como estabelecer uma organização secreta e executar ataques. (WEIMANN, p. 9)

A al-Qaeda pode não estar tão presente na mídia quanto seu antigo afiliado "Estado Islâmico", mas isso não significa que suas ações são menos preocupantes. Com o crescente aumento das atividades terroristas no ciberespaço (e com a falta de sistemas de defesa completamentes seguros), as organizações podem se tornar mais presentes neste domínio, adquirindo mais poder e investindo em tecnologias para realizar ações cada vez maiores.

35. "[...] operate with the assistance of large databases containing details of potential targets in the U.S"

Considerações finais

A presença das organizações terroristas no ciberespaço e o problema que elas trazem para a segurança dos atores internacionais necessitam de atenção. Suas ações se realizam de diferentes formas, algumas facilmente identificáveis, e mobilizam discussões e curiosidade na sociedade.

A pesquisa se inicia de forma a apresentar o ciberespaço, poder cibernético e a internet, conceitos básicos para entender como as organizações terroristas atuam nesse meio, quais são suas capacidades e a importância delas no contexto internacional atual. Assim, é possível perceber que o ciberespaço é um domínio cada vez mais presente na sociedade e, consequentemente, os atores internacionais utilizam-se do espaço cibernético como mais uma forma de exercer poder. Ao mesmo tempo em que é um novo campo de atuação para as questões internacionais, possui um alto número de usuários, baixos custos de entrada, capacidade de mudanças rápidas e condiciona a difusão de poder, o que acaba resultando na dificuldade de manter esse espaço totalmente seguro.

Essa mesma difusão de poder que possibilita atores menores exercerem um papel maior no contexto internacional de forma positiva e com mais visibilidade, também possibilita a atuação de atores com intenções criminosas, os quais beneficiam-se das falhas nos sistemas de segurança.

No caso das organizações terroristas, elas encontram no ciberespaço a possibilidade de divulgar e propagar seus ideais em uma escala mundial. O aperfeiçoamento dos grupos nas questões cibernéticas resultam na utilização do poder no ciberespaço de uma forma mais eficaz para seus objetivos, o que torna ainda mais importante a discussão desta questão para as relações internacionais, devido à ameaça que elas trazem para o cenário mundial.

Assim, sendo a presença das organizações terroristas um fenômeno crescente no ciberespaço, o problema da pesquisa era indagar de que maneira estas organizações utilizam-se do espaço cibernético como ferramenta de atuação. Como resposta, foi identificada a atuação por meio de propaganda, financiamento, treinamento, planejamento, execução e ataques cibernéticos.

A propaganda é a forma de atuação mais conhecida e facilmente identificada, utilizada para recrutar novos membros, disseminar ideias e incitar ações terroristas. O financiamento se torna mais

fácil pelas ferramentas disponíveis no ciberespaço, assim como o treinamento, proporcionado pela troca rápida de informações e a disponibilidade de manuais e vídeos para a transmissão de conhecimento, sem precisar atravessar fronteiras para isso. O planejamento e a execução, assim como as outras formas de atuação, tomam uma nova proporção, pois é possível ter acesso a uma grande quantidade de informação e pessoas, o que concede aos grupos terroristas mais poder para atingir seus objetivos. Já os ataques cibernéticos são uma forma de poder só praticável neste domínio, que ainda não representa uma grande ameaça se comparado aos atos terroristas fora do mundo virtual.

Com os objetivos delimitados alcançados, é possível perceber que as maneiras que os grupos terroristas se utilizam do poder no ciberespaço intensificou-se nos últimos anos e, se seguir nesta direção, a situação pode se agravar. É difícil controlar o que acontece no espaço cibernético, ainda mais no caso das organizações terroristas. No caso de uma página na internet de um desses grupos, se a mesma for derrubada, a possibilidade de aparecerem mais cinco para o mesmo propósito é grande; e quando não querem ser encontrados, o problema fica ainda mais complexo de resolver (mesmo não sendo impossível), pois existem inúmeras formas de camuflar-se nesse meio e não chamar a atenção.

Outro ponto compreendido foi o terrorismo cibernético, o qual, de acordo com a definição citada, ainda não é praticado. Existem muitas variáveis que precisam ser analisadas para a existência deste fenômeno e mais informações são necessárias para tal afirmação, porém, se não existir um sistema de segurança mais eficaz, é possível que com o aumento das capacidades técnicas e de recursos financeiros dessas organizações, o terrorismo cibernético seja praticável.

Existem muitas questões relacionadas com o espaço cibernético, um ambiente complexo e com inúmeras possibilidades de atuação, onde os grupos terroristas são apenas uma pequena parte do problema, que necessitam de mais atenção por parte da academia, em especial na área das Relações Internacionais. Quanto mais conhecimento sobre o assunto, maior a capacidade de lidar com as ameaças futuras neste meio.

Referências

AL-QAEDA divulga vídeo com ameaça de novos ataques aos franceses. **Correio Braziliense**, 9 jan. 2015. Disponível em: <http://www.correiobraziliense.com.br/

app/noticia/mundo/2015/01/09/interna_mundo,465592/al-qaeda-no-iemen-coordenou-ataque-a-revista-diz-agencia.shtml>. Acesso em: 16 maio 2015.

AL-QAEDA publica online estratégia de ataque frustrado aos EUA. Brasília: BBC News, 22 nov. 2010. Disponível em: < http://www.bbc.co.uk/portuguese/noticias/2010/11/101122_alquedaonline_pai >. Acesso em: 19 nov. 2014.

ATTUX, Romis. **Capítulo 3:** processadores de propósito geral: software. Campinas: UNICAMP, 2015. 66 slides: color. Disponível em: <http://www.dca.fee.unicamp.br/~attux/cap3_09_05.pdf>. Acesso em: 2 jul. 2015.

CANTER, David. The multi-faceted nature of terrorism: an introduction. **Chapter**, p. 1-19, Dec. 2009. Disponível em: <http://migre.me/q9Psj>. Acesso em: 05 jun. 2015.

CHOTHIA, Farouk. **Who are Nigeria's Boko Haram Islamists**?. África: BBC News, 4 maio 2015. Disponível em: <http://www.bbc.com/news/world-africa-13809501>. Acesso em: 09 maio 2015.

CHOUCRI, Nazli. Cyberpolitics. In: KRIEGER, Joel. **The Oxford Companion to comparative politics**. Nova Iorque: Oxford University Press, 2012. Disponível em: <http://ecir.mit.edu/index.php/publications/publications-index/272-cyberpolitics>. Acesso em: 20 mar. 2015.

CLOUGH, Jonathan. **The Budapest Convention on cybercrime**: is harmonisation achievable in a digital world?. Monash University, 2º International Serious and Organised Crime Conference, Brisbane, July. de 2013. Disponível em: <http://www.aic.gov.au/media_library/conferences/2013-isoc/presentations/clough.pdf>. Acesso em: 22 maio 2015.

COHEN, Daniel; LEVIN, Danielle. ISIS: They're Just Like Us. **Ozy**, 23 mar. 2015. Disponível em: < http://www.inss.org.il/index.aspx?id=4300&researcherid=4916>. Acesso em: 23 abr. 2015.

COHEN, Daniel. Fighting Islamic State in cyberspace. [S. l.]: Haaretz, 5 set. 2014. Disponível em: < http://www.haaretz.com/opinion/.premium-1.614320>. Acesso em: 23 abr. 2015.

DALE, Helle. Cyberspace and Terrorism: a global challenge. **The Daily Signal**, 10 Feb. 2015. Disponível em: <http://dailysignal.com/2015/02/10/cyber-space-terrorism-global-challenge/>. Acesso em: 23 abr. 2015.

ELBAGIR, Nima; CRUICKSHANK, Paul; TAWFEEQ, Mohammed. **Boko Haram purportedly pledges allegiance to ISIS**. [S. l.]: CNN News, 9 March 2015. Disponível em: < http://edition.cnn.com/2015/03/07/africa/nigeria-boko-haram-isis/>. Acesso em: 9 maio 2015.

EI INVADE conta do Pentágono no Twitter e divulga documentos. **Exame**, 12 jan. 2015. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/estado-islamico-invade-conta-do-pentagono-no-twitter>. Acesso em: 29 abr. 2015.

ESTADOS UNIDOS. **United States Code**, Title 22, Chapter 1, Section 2656f(d). Disponível em: <http://www.state.gov/documents/organization/65464.pdf>. Acesso em: 11 abr. 2015.

FINANCIAL ACTION TASK FORCE. **Financing of the terrorist organisation**

Islamic State in Iraq and the Levant (ISIL). [S. l.]: FATF, fev. 2015. Disponível em: <http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the--terrorist-organisation-ISIL.pdf>. Acesso em: 23 abr. 2015.

GRUPO DE AÇÃO FINANCEIRA; GRUPO INTERGOVERNAMENTAL DE AÇÃO CONTRA O BRANQUEAMENTO DE CAPITAIS NA ÁFRICA OCIDENTAL. **Financiamento do Terrorismo na África Ocidental**. [S. l.]: GAFI, 2013. Disponível em: <http://www.fatf-gafi.org/media/fatf/documents/reports/FT-na-africa-ocidental.pdf>. Acesso em: 17 nov. 2014.

GERGES, Fawaz A. **Por que o Estado Islâmico utiliza técnicas tão brutais?** [S. l.]: BBC News, 14 set. 2014. Disponível em: < http://www.bbc.co.uk/portuguese/noticias/2014/09/140914_eibrutal_ebc>. Acesso em: 19 nov. 2014.

INTERNATIONAL BUSINES TIME. **Isis-linked hackers launch major cyberattack on French television network TV5Monde**. [S. l.]: IBT, 9 abr. 2015. Disponível em: <http://www.ibtimes.co.uk/isis-linked-hackers-launch-major-cyberattack--french-television-network-tv5monde-1495498>. Acesso em: 29 abr. 2015.

KOREN, Tal; SIBONI, Gabi. Cyberspace in Service of ISIS. **INSS Insight**, nº 601, 4 Sep. 2014. Disponível em: < http://migre.me/q4PEa >. Acesso em: 29 abr. 2015.

KUEHL, Daniel. From Cyberspace to Cyberpower: Defining the Problem. In: KRAMER, Franklin; STARR, Stuart; WENTZ, Larry (Ed.). **Cyberpower and national security**. Center for Technology and National Security Policy, National Defense University, Washington, 2009. Disponível em: < http://ctnsp.dodlive.mil/2009/04/01/cyberpower-and-national-security/>. Acesso em: 27 out. 2014.

LACHOW, Irving. Cyber Terrorism: Menace or Myth. In: KRAMER, Franklin; STARR, Stuart; WENTZ, Larry (Ed.). **Cyberpower and national security**. Center for Technology and National Security Policy, National Defense University, Washington, 2009. Disponível em: < http://ctnsp.dodlive.mil/2009/04/01/cyberpower-and-national-security/>. Acesso em: 11abr. 2015.

MANTZIKOS, Ioannis. Boko Haram anatomy of a crisis. E-International Relations, Bristol, out. 2013. Disponível em: < http://www.terrorism.com/wp-content/uploads/2013/10/Boko-Haram-e-IR.pdf>. Acesso em: 9 maio 2015.

MCCORMICK, Ty. Al Qaeda Core: A Short History. [S. l.]: Foreign Policy, 17 March. 2014. Disponível em: <http://foreignpolicy.com/2014/03/17/al-qaeda-core-a--short-history/>. Acesso em: 16 maio 2015.

NYE JÚNIOR, Joseph S.. **O futuro do poder**. São Paulo: Benvirá, 2012.

O ATENTADO que mudou os EUA e abalou o mundo. **Isto é Independente,** 23 set. 2011. Disponível em: <http://www.istoe.com.br/reportagens/161925_O+ATENTADO+QUE+MUDOU+OS+EUA+E+ABALOU+O+MUNDO>. Acesso em: 11 abr. 2015.

PARKER, Amanda M. Sharp. Cyberterrorism: the emergent Worlwide Threat. In: CANTER, David. **The faces of terrorism:** multidisciplinary perspectives. Chichester: Ed. Wiley-Blackwell, 2009, p. 245-255.

RICHARDSON, Louise. **The roots of terrorism: an overview. In: RICHARDSON, Louise. The roots of terrorism. Nova Iorque: Routledge, 2006, p. 2.**

Disponível em: <http://freescienceengineering.library.elibgen.org/view.php?id=321623>. Acesso em: 5 jun. 2015.

SIBONI, Gabi; COHEN, Daniel; ROTBART, Aviv. The Threat of Terrorist Organizations in Cyberspace. Military and Strategic Affairs, v. 5, n. 3, Dec. 2013. Disponível em: <http://www.inss.org.il/index.aspx?id=4300&researcherid=4916>. Acesso em: 19 abr. 2015.

SKOUDIS, Edward. Information security issues in cyberspace. In: KRAMER, Franklin; STARR, Stuart; WENTZ, Larry (Ed.). **Cyberpower and National Security**. Center for Technology and National Security Policy, National Defense University, Washington, 2009. Disponível em: < http://ctnsp.dodlive.mil/2009/04/01/cyberpower-and-national-security/>. Acesso em: 17 mar. 2015.

STARR, Stuart H. Toward a preliminary theory of cyberpower In: KRAMER, Franklin; STARR, Stuart; WENTZ, Larry (Ed.). **Cyberpower and National Security**. Center for Technology and National Security Policy, National Defense University, Washington, 2009. Disponível em: < http://ctnsp.dodlive.mil/2009/04/01/cyberpower-and-national-security/>. Acesso em: 8 mar. 2015.

TROWBRIDGE, Alexander. **Jihadists on the move in Iraq with weapons, hashtags**. [S. l.]: CBS News, 16 jun. 2014. Disponível em: <http://www.cbsnews.com/news/isis-jihadists-on-move-in-iraq-using-weapons-and-twitter-hashtags/>. Acesso em: 19 nov. 2014.

UNITED NATIONS OFFICE ON DRUGS AND CRIMES. **The use of the internet for terrorists purposes**. Viena: United Nations, 2012. Disponível em: <http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf >. Acesso em: 21out. 2014.

WEIMANN, G. **www.terror.net:** how modern terrorism uses the internet. United States **Institute of Peace**, Washington, n. 116, March, 2004. Disponível em: <http://www.usip.org/sites/default/files/resources/sr116.pdf>. Acesso em: 16 maio 2015.

WHAT is Islamic State?. [S. l.]: BBC News, 26 set. 2014. Disponível em: <http://www.bbc.com/news/world-middle-east-29052144>. Acesso em: 29 abr. 2015.

Recebido em: 16/08/2015
Aceito em: 09/09/2016