CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

CIBERTERRORISMO

ANDRESSA OLIVETTI COSTA

Presidente Prudente – SP

2019

CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO
DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

CIBERTERRORISMO

ANDRESSA OLIVETTI COSTA

Monografia, apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito, sob orientação da Prof. Carla R. F. Destro.

Presidente Prudente – SP

2019

CIBERTERRORISMO

Trabalho de Conclusão de Curso aprovado como requisito parcial para obtenção do Grau de Bacharel em Direito.

BANCA EXAMINADORA

_____

Prof. Carla R. F. Destro

_____

Prof. Luís Fernando Nogueira

_____

Prof. Mário Coimbra

Presidente Prudente, 26 novembro 2019

AGRADECIMENTOS

À Prof. Carla R. F. Destro, meus sinceros agradecimentos pela orientação, pela atenção dada a mim e por garantir a realização deste trabalho, pela paciência e incentivo nos momentos de desespero pois sempre buscou cessar as dúvidas internas.

À minha mãe, Regina Ap. S. Olivetti pelo incentivo, aconselhamentos para elaboração da presente monografia e nunca desistiu de mim.

Aos meus amigos que acompanharam essa jornada e compartilharam os momentos acadêmicos ao meu lado, seja de apoio e consideração por mim. E por tornar a faculdade mais especial. Com ênfase, minhas amigas Carolina, Giovana, Lorrayne e Luiza que me deram apoio e suporte para finalização desta monografia.

Agradeço, por fim a Deus, por sempre se mostrar presente em cada detalhe em minha vida. Demonstrando que não há possibilidade de desistir quando se existe um futuro a enfrentar.

“É muito melhor lançar-se em busca de conquistas grandiosas, mesmo expondo-se ao fracasso, do que alinhar-se com os pobres de espírito, que nem gozam muito nem sofrem muito, porque vivem numa penumbra cinzenta, onde não conhecem nem a vitória, nem derrota”.
(Theodore Roosevelt)

Dedico este trabalho à minha mãe Regina pelo amor incondicional em minha caminhada, bem como a minha avó Marlene e avô Wadir (in memoriam) que sempre apoiaram minhas decisões e esperam meu sucesso. Ao meus amigos que se fizeram presentes nos momentos de dificuldade e por fim, não menos importante ao Bruno que me manteve firme e forte para conclusão deste trabalho.

RESUMO

O presente trabalho detém como objetivo principal discorrer sobre o momento histórico em que fora desencadeado o terrorismo e o ciberterrorismo no âmbito digital, seu conceito e como este se desenvolveu no Brasil. Tendo em vista que o terrorismo é um fenômeno global e tem sua atuação de maneira complexa, mesmo no terrorismo convencional com utilização de armamentos até chegar no ciberterrorismo, onde se tem a invasão por ciberterroristas dentro vida pessoal de algum sujeito ou até sistemas de segurança, bancos, unidades governamentais e etc. Este trabalho também aborda ideias para se ter segurança no âmbito virtual, já que a Internet é uma das principais prioridades de comunicação e de troca de informações no mundo todo. Trata da importância de ter a criação de uma segurança específica para combater o cibercrime, já que primeiramente deve este ser descoberto para conseguir puni-lo, já que são casos complexos e não podem deixar de ser analisados para que haja combate ao terrorismo. A metodologia utilizada neste artigo foi consulta de bibliografias, sendo livros e internet, que auxiliaram a desenvolver a presente pesquisa, analisar métodos para solucionar problemas a lei Antiterrorismo (13.260/16) e quais os pontos fracos e fortes do ciberterrorismo para a segurança da sociedade brasileira.

Palavras-chave: Antiterrorismo. Ciberterrorismo. Globalização. Internet. Legislação Antiterrorismo 13.260/16. Segurança Nacional. Tecnologia. Terrorismo.

ABSTRACT

The presented work has as main objective talk about the historic moment when terrorism and cyberterrorism started at digital environment, its concept and how it was desenvolved in Brazil. It is known of terrorism being a global phenomenon and having your act in a complex way, even at conventional terrorism where using armament until ciberterrorism whith invasion by ciberterroristis inside someone's personal life or even security sistems, banks, government unities and others. This work also approaches ideas to have digital environment security since internet is one of the most priority at comunication and information exchange. It deals about the significance of creating a specific security to fight cibercrime, but first of all it has to be discouvered to punish it since it is a complex case and must be analysed to fight against terrorism. The used methodology at this article was a bibliograph reference of books and internet wich helped to develop the presented research, analyze methods to solve problems about anti-terrorism law (13.260/16) and have knowleged about week and strong points of ciberterrorism for brazilian's society security.

Keywords: Anti-terrorism. Cyberterrorism. Globalization. Internet. Anti-terrorism legislation 13.260/16. National Security. Tecnology. Terrorism.

SUMÁRIO

1 INTRODUÇÃO

A presente pesquisa foi realizada com o fim de esclarecer a complexidade do terrorismo, quais foram os primeiros resquícios do surgimento do terrorismo e a evolução do terrorismo em sua nova modalidade, que é o ciberterrorismo. São analisados quais os efeitos e quais as consequências, com a vinda da globalização, que se tem com a prática do ciberterrorismo. Tendo em vista que conforme a globalização cresce, a população também evolui e o mundo acaba por ficar cada vez mais perigoso, podendo ser alvo de ataques já que no “mundo atual” não há limitação de fronteiras.

Terrorismo emprega de maneira desumana a violência, que além de afetar diretamente a sociedade, afeta, primordialmente, o cunho político. Assim sendo, é possível compreender que o mundo todo pode ser atingido pelo terrorismo, pois este não é totalmente protegido de qualquer atentado ou ameaça de terroristas.

O presente trabalho abordou a globalização, mensurando qual a qualidade de segurança que os países têm ao ter informações invadidas, como lidar com os vazamentos de informações, como conseguir que essas informações não possuam conteúdo sigiloso. Trouxe a definição de terrorismo e ciberterrorismo, como atuam e suas principais diferenças. A internet fez com que tudo se tornasse possível e o ciberterrorismo é o uso do recurso da Internet e de outros meios eletrônicos para obter o terrorismo ou conseguir realizar ataque terrorista a infraestruturas que também estão ligadas à Internet.

Neste contexto, além dos inúmeros benefícios que houve para a humanidade com a evolução do desenvolvimento científico, tecnológico e da comunicação, as barreiras a serem superadas, havendo a possibilidade de contato e interação com toda parte do mundo, há o surgimento de novos impasses.

Insta salientar a evolução do Direito Penal, junto com a evolução da sociedade como um todo, acerca dos meios de comunicação, a facilidade de obter recursos, informações na internet e além disso, a evolução do homem médio de desenvolver maneiras de cometer crimes que não havia previsão anteriormente do avanço da sociedade e da tecnologia.

Conclui que todo indivíduo que possui um computador, independente de se vincular a uma empresa ou não, está sujeito a sofrer um ataque ciberterrorista, observando que o sistema é falho, não há segurança e muito menos, há como

adivinhar quem é aquele que atua por de trás da tela, sendo uma vasta complicação para defender aquele que foi afetado e culpar aquele que conseguiu ter acesso aos dados do particular ou de uma empresa.

Embora aparente que tratar sobre o terrorismo seja algo que não aconteça no Brasil, houve a necessidade de criar normas para que haja um mínimo de prevenção caso houvesse devido acontecimento.

Buscou-se a exploração de como era o terrorismo na antiguidade, seus momentos históricos e as legislações brasileiras que punem esse tipo de atividade.

No presente trabalho houve uma devida preocupação com esse novo tipo de terrorismo, o ciberterrorismo, pelo método utilizado. Utiliza-se de um meio silencioso e muitas vezes imperceptível, mas, que é capaz de causar enormes danos a sociedade e também ao governo do nosso país. Já que por meio delas, grupos terroristas conseguem obter ajuda, recrutar novos aliados e propagar sua ideologia ao redor do mundo. Entretanto, a utilização da internet por terroristas não esgota apenas nisso, há de ser observado que é evidente a utilização da internet para realizar ataques a rede de computadores e sequestrar informações da vida particular de alguém ou de agentes governamentais.

Pela difusão da internet ao redor do mundo, tornou-se, com maior facilidade com que grupos terroristas atuem em distintas partes do mundo sem ao menos serem identificados e com isso, a punição se torna mais complexa, tendo em vista que a inexistência de barreiras no ciberespaço atrapalha a fiscalização das ações desses grupos.

As atividades realizadas pelos terroristas dentro da internet são conceituadas como crimes em inúmeros países, assim como no Brasil, ao se apoderar do meio cibernético para invadir computadores, roubar dados e quebrar privacidade dos usuários.

Por fim, para conclusão da presente monografia, referiu-se ao ciberterrorismo que se encontra dentro da Lei nº 13.260/2016 sobre Terrorismo no Brasil dando um foco mais centrado nas atividades reconhecidas como cibercrimes.

A metodologia do presente trabalho foi utilizada os materiais históricos, dedutivos, específicos, comparativos, doutrinas dos temas tratados, regras, valores científicos, reportagens, documentos que envolvem sobre o terrorismo ao redor do mundo e o bibliográfico para referenciar e que deu base para o surgimento do tema presente da monografia, dando enfoque para uma solução da problematização do

ciberterrorismo para que haja a melhoria na segurança das informações pessoais e até de grandes instituições.

2 TERRORISMO: CONCEITO E SOCIEDADE ATUAL

Antes de adentrar na análise sobre o Ciberterrorismo, há a necessidade de entender o que é o terrorismo. Com isso, trataremos desta conduta, seu conceito, sua origem, *modus operandi*, os modelos de terrorismo e, por fim, a sociedade atual. Destaca-se que o terrorismo no início do século foi um fenômeno de maior impacto na segurança internacional.

Sabe-se que o terrorismo é algo muito antigo e utiliza-se como meio de terror a ameaça, violência física e psicológica como forma de poder, mas também com finalidade de enfraquecer e aterrorizar autoridades. Já que se apoderava de assassinatos, incêndios, explosões com intento de coagir governos.

O terrorismo, é uma das principais ameaças a paz mundial, visto que, além do sentimento de insegurança, realizam atentados e destruições exercidos por determinado grupo de pessoas, que tem por objetivo a violência, seja para fins políticos, religiosos ou de outra natureza.

2.1 Evolução

Como sabemos, o terrorismo não é moderno, ou seja, vem desde a antiguidade.

Há quem entenda que o terrorismo adveio com a Revolução Francesa da (1789/1799), onde a revolução francesa findou com o regime antiquado da época. A revolução francesa foi conhecida como o “terror” da época pois, ocorriam perseguições e sentenças de morte (RICARDO; SUTTI, 2003).

O regime era organizado pelo clero, monarquia absolutista, nobres e a burguesia. Nesta época, era concretizado a igualdade, liberdade e fraternidade e houve brusca disputa entre os políticos revolucionários, de um lado girondinos que representavam a burguesia e de outro, jacobinos membros radicais da Assembleia, do Tribunal Revolucionário e do movimento popular. Devido Tribunal foi reconhecido como o poder estatal e tinha por objetivo espalhar o medo entre a população para que não houvesse oposição ao seu regime (RICARDO; SUTTI, 2003).

O indivíduo que fosse considerado como traidor à época, era levado a guilhotina. Ademais, os inimigos da Revolução Francesa eram mortos a tiros ou de alguma maneira cruel, como afogamento (RICARDO; SUTTI, 2003). Outrossim, a execução de pessoas gerou a nova fase da Revolução, mais conhecido como anteriormente falado como Terror. Desta maneira, o “terror” tratado neste período, possuía um significado diferente, em razão que o terror era desempenhado para estabelecer ordem.

Em contrapartida, há quem diga que “Mão Negra” no século XX em 1914, foi a primeira organização terrorista no mundo. Essa organização planejou o assassinato do herdeiro do trono do Império Austro-Húngaro, Francisco Ferdinando da Áustria e sua esposa. Entretanto, na realidade, quem realmente foi autor do atentado foram os membros da milícia Mlada Bosn, realizado por Gavrilo Princip (ZORZETTI, 2015).

O grupo conhecido como “Mão Negra” era separado em outros grupos menores e após o atentado, passaram a receber treinamentos especializados. Após a morte de Francisco Ferdinand, foi encadeada a Primeira Guerra Mundial, que alcançou quatro anos de guerra (ZORZETTI, 2015).

Já em 1934, com a morte do rei Alexandre I da Iugoslávia, que realizava visita em Marselha na França para consolidar a aliança entre os países, foi assassinado por um pistoleiro chamado Vlado Chernozemski de origem Búlgara. Que aparentava ser realizado o assassinato por outro tipo de grupo terrorista (ALTMAN, 2012).

Vlado Chernozemski, era membro de uma Organização Revolucionária Interna da Macedônia (ORIM). Tal organização, que foi revolucionária e política, defendia seu povo macedônio. Com isso, participavam de guerras e combatiam exércitos da Sérvia, Bulgária e Grécia. Antes mesmo do devido ataque ao rei Alexandre I, já realizavam ataques terroristas no ano de 1903, onde executavam ataques com bombas para atrair atenção das grandes potências (DUFFY, 2009).

Posteriormente, houve inúmeros ataques terroristas. Em especial, o ataque em Munique na Alemanha que ocorreu nos jogos Olímpicos de 1972 onde onze integrantes olímpicos foram reféns de um grupo de terrorista de origem palestina, que se denominava Setembro Negro. Além dos onze reféns, assassinaram dois membros da equipe de Israel (MAGNO, 2013).

A motivação do grupo pelo atentado terrorista era libertar os árabes presos em Israel. Mas a situação terrorista não acabou somente na morte de duas pessoas, ao longo do dia houve tiroteios, explosões com granadas e por fim, houve a morte de dezenove pessoas dentro do atentado terrorista.

Ademais, em Abadan que se situa no território iraniano no ano de 1978, uma organização religiosa militante colocara fogo dentro de uma sala de cinema que, pela grandiosidade do fogo se espalhou contaminando diversas salas e ocorreu um pânico generalizado às pessoas que ali se encontravam. Pela demora da vinda do Corpo de Bombeiro, colaborou pela morte de mais de quatrocentos e setenta e sete pessoas (BREVES ESCRITOS INTERNACIONAIS, 2008).

Com devido massacre ocorrido dentro da sala de cinema, foi demonstrando que havia um interesse religioso, já que encontravam em um sistema de regime monárquico. Com isso, promoveram suas reivindicações para que fosse implementada uma sociedade islâmica que liderasse. Atingindo uma oposição religiosa radical, para que se subordinassem ao movimento revolucionário. O atentado deu origem à Revolução Iraniana (BREVES ESCRITOS INTERNACIONAIS, 2008).

Adiante, em 1983 houve um atentado terrorista contra os quartéis de Marines americanos em Beirute no Líbano. Caminhões-bombas atingiram edifícios que alojavam os militares dos Estados Unidos e da França. Com o choque contra o edifício, houve a morte de duzentos e noventa e nove americanos e franceses. Este ataque também foi atribuído ao grupo xiita Hezbollah, que possui apoio do Irã (AFP, 2017).

Tratou-se do pior ataque sofrido pelos estadunidenses após a Segunda Guerra Mundial. O grupo terrorista Jihad Islâmica, assumiu o atentado terrorista.

O grupo Hezbollah, seu significado é “Partido de Deus”, é uma potência islâmica xiita que possui uma enorme estrutura comparado até mesmo com o Exército. Foi criado em 1982 durante a guerra civil que acontecia no Líbano. Para os Estados Unidos, Israel, Canadá, os países baixos e Reino Unido, veem como um grupo terrorista. Mas, na cultura árabe e mulçumana, possui um grande valor, já que possuem uma enorme força de defesa (SANTANA, 2010).

Por outro lado, o grupo Jihad Islâmica, se opõe a governos árabes alinhados com o Ocidente. É um grupo, que acreditam, não possuir um verdadeiro papel social ou político. Entretanto, possui objetivo de conquistar um Estado palestino islâmico e destruir Israel por meio de uma guerra santa. O grupo foi criado na década dos anos 70, com início na Faixa de Gaza. Conhecidos por ser autores de inúmeros atentados realizados por explosões de bombas (BBC, 2012).

Há o entendimento que o grupo terrorista Hezbollah, se subdivide em inúmeros outros grupos terroristas, que estão espalhados pelo mundo. Uma de suas subdivisões é o grupo Jihad Islâmica.

Ao adentrar no século XXI, houve inúmeros atentados terroristas e o mais conhecido e grandioso foi o ataque as torres gêmeas nos Estados Unidos. O atentado aconteceu pelo choque de dois aviões passageiros às torres gêmeas do *World Trade Center* na cidade de Nova York. Foi praticado por dezenove terroristas árabes que eram participantes do grupo extremista Al Qaeda. Osama Bin Laden que assumiu a autoria do ataque terrorista de 2001 (SOUZA; NASSER; MORAES, 2014).

Além do ataque terrorista em Nova York, no mesmo dia e o mesmo grupo, também se utilizaram de um terceiro avião sequestrado pelos terroristas, caiu sobre o Pentágono na Virgínia e sobre um quarto avião sobre a Pensilvânia. Referidos ataques terroristas pela rede extremista Al Qaeda mataram quase três mil pessoas (SOUZA; NASSER; MORAES, 2014).

A Al-Qaeda, foi uma organização do ano 1989, criada pelo seu líder Osama Bin Laden, que tinha função de conseguir recursos financeiros para lutar contra os russos e possuía como seu principal propósito conter a invasão Soviética no Afeganistão (BUNDE, s.p.).

Um dos primeiros ataques terroristas promovido pelo Osama Bin Laden, foi em 1998 quando atacou duas embaixadas americanas (Estados Unidos da América) que ficavam localizadas na África Ocidental, que foi um grande choque pois houve óbito de 224 pessoas (BUNDE, s.p).

Assim, os Estados Unidos começaram a deter um entendimento e uma política que tinha como objetivo a opressão dos estados muçulmanos. Com isso, aconteceu o atentado às torres gêmeas localizadas no centro financeiro (World

Trade Center) e ao centro militar (Pentágono) na cidade de Nova Iorque e Washington. Com resultado de declaração de guerra aos afegãos pelo EUA.

O grupo Al-Qaeda teve uma grande expansão, pois possuía muitos grupos espalhados pelo mundo e que agiam sem expor o seu líder.

Com isso, fica fácil e nítido enxergar que o ataque terrorista do 11 de Setembro de 2001, foi um marco histórico, pois além de obter a destruição em escala dos edifícios, da morte de inúmeros inocentes foi necessário a criação de novas leis internacionais e nacionais para que houvesse uma proteção específica a esse tipo de acontecimento. Haja vista que não havia, no entanto, tantas medidas necessárias para a segurança da coletividade, mas após esse advento que o atentado trouxe para o cenário internacional com a ameaça à paz e a segurança, influenciou a criação de novos estudos sobre esse método de terror.

Os atentados ao World Trade Center e ao Pentágono, marcaram de maneira preocupante os Estados, já que a força não se encontrava mais a eles, mas sim, a um grupo de terroristas não-estatais que empregavam o uso de armamentos, mísseis, bombas e aeronaves.

Vale relembrar, que o terrorismo é aquele meio em que tem como objetivo impor o medo na população. É um fenômeno antigo e resulta desde o primórdio a utilização do terror e armas.

Ademais, o terrorismo não é somente atacar um determinado local e assassinar pessoas. Tem por meio, impor o pânico no resto da sociedade como um todo. Ou seja, mata-se um pequeno número de pessoas, para atingir uma vasta população assustada. Impondo o medo, violação da vida privada, descumprimento das poucas leis que existiam e a hesitação de se frequentar locais públicos. Desordenar a ordem pública e afrontar a segurança que o Estado garante.

Por essa razão e pela diversidade de meios empregados pelos grupos terroristas houve a necessidade de uma segurança ampliada para que fosse combatido e cesse o terror.

2.2 Pensando em um Conceito de Terrorismo

O terrorismo, em um entendimento mais amplo, poderia ser denominado como a disseminação do medo, realizado por um grupo de

indivíduos, sem determinado número de integrantes que empregam a violência para atingir um objetivo fim. Esse objetivo fim pode ter como finalidade atingir ideologias políticas, religiosas ou estratégicas.

O conceito de terrorismo possui vários significados e definições (LAQUEUR, 2004, p. 5). Todavia, podemos extrair uma das definições de terrorismo como dispõe o site:

> O terrorismo é a dominação pelo terror. Essa dominação verifica-se em atos violentos cujo fim é semear terror. O terrorismo, por conseguinte, procura coagir e pressionar os governos ou a sociedade em geral para impor os seus apelos e as suas proclamações [...] (CONCEITO DE, s.d, s.p).

O termo que mais se faz presente para conceituar o terrorismo, é que independente da motivação, o alvo do terrorista é seu objetivo fim que é aterrorizar a população e autoridades.

Nesse sentido, pela complexidade de obter um conceito de terrorismo, Schmid (2011, p.40) aduz:

> “Terrorismo” pode muito bem ser o termo mais politizado do vocabulário político nos dias de hoje. Usado como um rotulo para certa forma de violência política, que reflete, se ele “gruda”, negativamente sobre um adversário político, demonizando-o e deslegitimando sua conduta. Em sua dimensão pejorativa, o destino do termo “terrorista” é comparável ao uso e abuso de outros termos no vocabulário político – termos como “racista”, “fascista” ou “imperialista”.

Como tratado anteriormente, o terrorismo visa atingir questões políticas, sobre crenças, valores e ideologias daquele que emprega o terror. Quanto a isso, é incompleto dizer que terrorismo há somente um significado e conforme o National Research Council (2001, p.15) trata:

> [...] são entendidos de forma diferente por indivíduos e grupos que trazem diferentes origens, crenças e convicções políticas para argumentar sobre eles. Além disso, os significados de tais palavras mudam em ênfase ao longo do tempo [...].

Portanto, há de se entender que o terrorista é aquele que possui negatividade à determinado fato ocorrido ou opinião pública. Entretanto, há quem entenda que o conceito para terrorismo seria apenas a natureza do ato praticado para caracterizar um grupo como terrorista. Brenda Lutz e James Lutz (2010),

definem como terrorismo o uso de violência ou ameaça, grupo que se organiza para alcançar objetivos políticos. A violência empregada é muitas vezes, é estendida para os civis inocentes.

Para Noberto Bobbio (1998, p. 1243) entende que o terrorismo é uma estratégia de grupos para conseguir a dominação, vejamos:

> O terrorismo é a estratégia a que recorrem grupos de intelectuais, separados das massas, nas quais, na realidade, não confiam e às quais estão organicamente ligados, de modo que a sua ação por caracterizar-se no sentido de uma desconfiança em relação à insurreição, quando faltam condições necessárias para desencadeá-la.

O terrorismo tem como seu ponto crucial a provocação de um sentimento de pavor, pânico, medo, temor dentre outros sentimentos, na população em que o agente vai cometer o terrorismo. A sensação de terror decorre do simples fato do terrorismo não ser previsível e gerar um grande pânico na sociedade que ele é cometido.

> O terrorismo cria a incerteza por sem imprevisível. A hora, o local e a identidade do criminoso são uma surpresa. Esse tipo de ação geralmente tem como alvos civis que estão simplesmente realizando suas atividades cotidianas. Eles não podem saber quem – entre seus companheiros de viagem no metrô, em um ônibus ou em um avião, ou mesmo no meio de uma multidão ou sentado junto deles em um restaurante – vai atacá-los. Os atos de terrorismo em si, mesmo que relativamente menores, são lembretes constantes da vulnerabilidade dos indivíduos (CRENSHAW, 2010 p 39.)

Existe uma ausência para uma única definição para o termo do terrorismo, assim para Heleno Cláudio Fragoso (1981, p. 12):

> Não existe uma específica figura de delito denominada terrorista. Essa designação se aplica a diversas espécies de crimes, que se caracterizam (a) por causa do dano considerável a pessoas e coisas; (b) pela criação real ou potencial de terror ou intimidação generalizada e, (c) pela finalidade político-social.

Pensando além de um único conceito para o terrorismo, há necessidade de observar a junção de atentado e a autoria deste, uma vez que a morte das pessoas é utilizada como instrumento para a obtenção do que se almeja – ou seja, o objeto à ser conquistado. Quando não utilizado o meio que se resulta a morte, então opta-se por outro meio, o qual as vítimas temem pela própria morte. Ademais, pode ocorrer o terrorismo suicida, onde o indivíduo põe fim a sua própria vida para atingir um bem maior, buscando visibilidade, lugares que haja espaço com

aglomeração de pessoas e surpreender com o atentado, sendo a lógica base do terrorismo, onde as ações são pensadas minuciosamente.

Analisando o terrorismo é possível entender que há a necessidade de envolver a barbárie e a violência, existindo a necessidade de demonstração de um poder maior que o poder dominante de segurança governamental. Portanto, é isso que difere o terrorismo de outros crimes previstos em leis, pois o atentado terrorista muitas vezes tem por objetivo coagir o governo e afetar a sociedade em um todo, além do seu meio empregado que age com violência alastrante.

Como dito anteriormente, não necessariamente o terrorismo tem a ver com a política, possui como ênfase o método do medo em que se opera, entretanto, sabemos que existem outras razões diferentes de apenas o medo e sim, o meio religioso e cultural para a justificação de se cometer o terrorismo. Nas palavras de Michael Walzer (2000, p. 69-70):

> As vítimas de um ataque terrorista são terceiros, observadores inocentes: não existe qualquer razão para atacar; qualquer pessoa, dentro de uma vasta classe de pessoas (sem qualquer relação entre elas) servirá. O terrorismo é aleatório, degradante e assustador. É esta a sua marca distintiva e é por isso que não pode ser defendido [...].

E conclui dizendo que, para saber enfrentá-los tem que reconhecer seus agentes de maneira funcional: “O objetivo é destruir o moral de uma nação ou de uma classe, minar a sua solidariedade, o seu método é o assassinato arbitrário de vítimas inocentes. O ataque cego é a característica essencial da atividade terrorista” (WALZER, 2000, p. 197).

De outro lado a Inteligência Brasileira entende que ações dos grupos terroristas se divide em:

> Em caráter geral, o objetivo dos atos e ações são a de criar um clima de insegurança e temor generalizado para demonstrar inconformismo contra um sistema seja político, econômico, social, étnico ou religioso e facilitar o desenvolvimento de um processo de mudanças pretendidas. Em caráter específico seus objetivos são diversos, entre estes:
> - Derrubada e ou substituição de um governo ou de um modelo político-ideológico e religioso;
> - Obtenção de autonomia política para um grupo subnacional;
> - Alteração da política externa de um governo;
> - Defesa do meio-ambiente e dos direitos dos animais;
> - Purificação da humanidade e confirmação de previsões apocalípticas;
> - Inconformismo com o processo de globalização, a exclusão social e consequente desumanização da sociedade;

- Como instrumento de poder entre grupos em conflito;
- Como recurso acessório contra países hostis; e
- Propaganda e marketing (WOLOSZYN, 2006, p. 128-129).

Contudo, conclui-se que o terrorismo é um fenômeno antigo e que existe desde o primórdio da sociedade. De maneira mais ampla, deduz-se que é o uso da violência, de maneira imprevisível e sistemático. A intimidação na busca de atingir seus objetivos alvejando pessoas inocentes. Age com a mínima percepção, pois o age de maneira espontânea, sem deixar rastros.

Para fim de conseguir um efeito psicológico de medo e transmitindo essa mensagem de perigo nos alvos imediatos e mediatos. Logo, sendo uma tática para atingir o governo indiretamente para conseguir que este satisfaça os desejos do grupo terrorista. Deve ser identificado e saber distinguir quais são as causas desse fenômeno para ser descoberto seus agentes e assim saber como enfrentar esse inimigo de maneira elaborada e eficaz, já que com a globalização e a facilidade de comunicação tem tendência dos ataques terroristas se alastrarem mais rapidamente.

3 SOCIEDADE PÓS MODERNA

Como tratado no tópico anterior, o terrorismo não é algo novo no âmbito do crime e que sempre está se modificando para cada vez mais conseguir atingir seus objetivos e se ajustar a modernidade.

É sabido que o terrorismo não é uma exclusividade do ordenamento jurídico brasileiro, a aparição desta figura se dá em diversas legislações ao redor do mundo.

Com isso devemos nos atentar que com a globalização (que veio com sua evolução entre os anos 1960 e 1980, onde ocorreu a fácil integração entre os países e as pessoas do mundo todo, países se comunicam, pessoas, governo, há realização de transações financeiras e etc. Sendo uma facilitação entre as relações, pois criaram uma maneira mais rápida e eficiente para ter contato e relacionar entre si), cada vez mais aumentando o espaço cibernético e assim, consequentemente, aumentando o espaço de usuário com contas na internet e comunicação em tempo real entre várias partes diferentes do mundo (BARBOSA. 2001, s.p).

André de Mello e Souza (2014, p. 160) pondera:

> 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 globalização veio com mudanças e novas características, quais foram (Ianni 1995, p.58) a vinda da energia nuclear como uma nova técnica de guerra que pertence às nações mais poderosas. A revolução da informática que trouxe o poder da informação, formação e indução. O Sistema Financeiro Internacional trazendo as relações econômicas mundiais. O comércio internacional, investimento na bolsa de valores e de bancos, sendo possível realizar transações por meio de computadores, Tablets e Smartphone. Ainda sobre o mercado, mudaram os meios de produção, força de produção, divisão de trabalho e do mercado, se tornando mais amplo e atendendo empresas mundiais, podendo ser controlada a qualquer lugar do mundo.

A vinda do inglês como língua universal facilitando a comunicação a qualquer pessoa em qualquer lugar do mundo e o poder político do neoliberalismo

que defende a absoluta liberdade do mercado e restringe a intervenção estatal sobre a economia, pois assim há o crescimento econômico e o desenvolvimento social de um país. Já que emprega políticas para aumento da produtividade e melhorar a econômica local e global (DICIO, 2019).

A comunicação tornou-se uma comunicação em massa, já que as pessoas podem se comunicar instantaneamente com qualquer pessoa do mundo em apenas um *click*.

Portanto, a globalização não é somente a expansão da economia. Mas sim, a quebra de barreiras entre as nações, economia, política, cultura e meios sociais. Há a integração, internacional e uniformização de valores, ideias e atitudes.

Um dos principais resultados da globalização é a internet e os seus meios de navegação. Hoje, a para criar uma conta no *Facebook, Instagram, Telegram, Twitter, WhatsApp, YouTube* e etc, para poder utilizá-los, há a necessidade de fornecer dados pessoais. Portanto, com os desenvolvimentos de novas redes sociais e de maneira que vão ficando mais conhecidas, simplesmente é normal da época em que estamos querer realizar cadastro para ficar dentro da moda. Mas isso vai além do que é apenas visto aos olhos humanos.

A sociedade carece de entendimento sobre o risco de fornecimento de dados simplórios ou dados pessoais pelo simples fato de querer conquistar seu espaço no meio cibernético. O fluxo de informações e compartilhamento de dados é desmensurado haja vista que é a grande população do mundo em conexão com o individuo que vive no outro lado do mundo. Mas acerca da responsabilidade de captação sobre a guarda dos dados pessoais, muitas vezes são deixados de lado, o que não deveria ser, considerando que os dados pessoais de alguém engloba sua dignidade e privacidade.

Apesar da enorme conquista que foi a evolução da globalização, facilitação de comunicação, estratégias, capital, transformações e etc, há o outro lado da história tendo em vista, que com essa evolução há o crescimento da desigualdade social, já que para consumir as novas ideias, valores e tecnologias a classe alta possui condições de acesso a essas modernidades com muito mais facilidade. Possui a facilidade de viajar ao outro lado do mundo, consumir computadores, celulares e outros meios de comunicação. O mundo age de maneira rápida e pela diferença de classes há aumento da violência.

Mais adiante, apesar das novas tecnologias essas se tornaram tão amplas que a fiscalização não é capaz de controlar o que acontece na internet e sobre o que a população executa.

O perigo do século, não é mais algo desconhecido, haja vista que estamos sempre capazes de sofrer um ataque ou ameaça surpresa, podendo ser cometida pelo terrorismo ou uma “simples” violência no dia a dia.

A difusão de ideias, expansão de comunicação, novas tecnologias abrem portas para a problematização, já que muitos querem a vida que avança junto com a globalização, o obstáculo é que apenas alguns conseguem. A revolta com esse aumento de tecnológica, que alcança somente alguns povos, gera o sentimento de insuficiência e impotência criando ações contrárias a que se aplicam, causando desordem e indignação. Nasce a impossibilidade de alcançar o que o individuo da classe privilegiada consegue e assim, dá margem a indivíduos marginalizados na sociedade empregando o medo e violência dado que é um espaço que vai além do controle estatal, não existindo possibilidade do governo bloquear ou frear o uso, pois é essencial.

Conforme Barros (2015, p.83) aduz sobre a cibernética: “[...] pode lhes ajudar na atuação, no âmbito das relações internacionais, pela busca da dominação da informação, no espaço cibernético e, também, em outros domínios, que se encontram fora do mundo cibernético”. Entende-se que a cibernética, possui um amplo lugar que existe poder já que é possível atingir qualquer indivíduo em qualquer lugar do mundo para estabelecer relações, seja dentro da sua nacionalidade ou de maneira internacional.

Desta maneira, conclui-se que a facilidade de criar uma nova guerra sem deixar vestígios se torna muito mais fácil dado que é um domínio de fácil acesso, não possui custo e é possível agir como um usuário anônimo (GARDINI, 2014, p.13). Não há severa civilização, abrindo portas para a violência de dados e violência de direitos assim, abrindo portas para o terrorismo e capaz de tornar um caos.

4 SURGIMENTO DO CIBERTERRORISMO

Neste capítulo abordaremos a respeito dos grupos terroristas que estão atuando no ciberespaço. O uso da internet para propagar o terror, o medo e a violência que vem crescendo e evoluindo cada vez mais, já que se trata de uma maneira viável de ataque terrorista.

Trataremos sobre a diferença do conceito do terrorismo convencional e o terrorismo cibernético e os meios em que são aplicados.

4.1 Terrorismo Convencional x Ciberterrorismo

Como tratado anteriormente o terrorismo convencional tem como seu *modus operandi* de maneira grandiosa, agindo com surpresa e com um alvo certeiro e por trás um objetivo que é muitas vezes impor o medo e o terror.

Atingir uma maior quantidade de vítimas é o preferível e além das vítimas que foram atingidas em tempo real, atingir aquela população que também não estavam presentes, mas que pela grandiosidade do ataque se sintam intimidadas e com pavor. Os terroristas possuem um caráter onipotente, podem estar em qualquer lugar a qualquer momento, podendo ter um grupo de terroristas prontos para entrar em ação a qualquer tempo e tornar seus atos um espetáculo de terror.

Cada ataque que é promovido foi escolhido de maneira minuciosa, pensado em cada detalhe, em cada alvo e objetivo. E mais que isso, sempre manter o silêncio, agir de maneira que ninguém descubra os meios de preparo para que não sejam interrompidos ou que o ataque venha a falhar.

Conforme Chagas (2012, p.18) trata acerca do terrorismo:

> [...] terrorismo é uma maneira de fazer política através da ameaça ou do uso da violência, procurando através desta, atingir um resultado no nível psicológico do indivíduo, e que algumas vezes utiliza-se de atos genocidas para conseguir tal resultado.

O terrorismo é impelido para criar poder onde não existe ou se existe, se tornar estável ao impor o medo e atingindo seu alvo, que pode ser um grupo

cultural, religioso, o próprio país, um partido político, entidades estatais ou até mesmo o governo tanto nacional ou de nível internacional.

Com a vinda da globalização, como já aludido, a comunicação com indivíduos do mundo todo se tornou mais rápido e com mais facilidade. Por mais que haja inúmeros benefícios com a evolução da internet e da comunicação, existe o outro lado da história. O lado nocivo dessa comunicação em massa e sem restrições permitiu que um novo modelo de terrorismo fosse implantado no nosso sistema, conhecido como ciberterrorismo.

A possibilidade de existir terroristas e formularem ataques destrutivos mesmo a distância não é algo mais remoto, mas, capaz de ganharam força para acontecer, dado que a inserção do mundo físico dentro do mundo virtual se tornou possível. É possível atingir as infraestruturas de um Estado sem muito esforço físico, pois ao invadir um sistema bancário, por exemplo, é possível realizar transações financeiras prejudicando outrem ou o sistema da bolsa de valores prejudicando a compra e venda de ações de uma empresa, já que esta controla o mercado de ações; a invasão de um sistema de controle de tráfego aéreo, falhando o software e causar erro gerando enorme caos aéreo.

No contexto de novas tecnologias, ao abrir acesso de novos ataques pelo meio cibernético, é acreditável causar severos danos com apenas um computador de que utilizar uma bomba para causar temor.

Contudo, antes de adentrar no assunto do terrorismo no ciberespaço, devemos fazer uma breve distinção entre ciberespaço e internet feito por Omar Kaminski:

> A internet pode ser entendida como uma vasta rede internacional composta de cerca de 150,000 redes de computadores individuais e milhões de usuários individuais por todo o mundo. [...] Unida através de uma linguagem comum ou protocolo, a internet permite aos usuários individuais que interajam, a seu modo, como qualquer outra rede ou usuário individual que seja também parte do sistema. Ou seja, a Internet é uma rede de computadores que fala a mesma língua, o protocolo IP. [...] Muitos usuários poderão acessar suas contas de Internet virtualmente de qualquer lugar no mundo através de satélites, dispositivos sem fio. Uma vez que na Net eles podem enviar e receber e-mails, navegar e conduzir negócios. [...] A Internet é um sistema global, e não nacional, estruturada de forma inerente, de modo a ampliar a jurisdição política e jurídica, tornando a regulamentação por apenas uma jurisdição inviável. Não é uma rede de computadores, mas sim a Rede das Redes. (KAMINSKI, 2000, s.p)

Já o entendimento que se tem por Ciberespaço, vem com uma ideia diferente, que é:

> Uma nova realidade, um novo ambiente, diferente de tudo que já se viu, se desacortina; o ciberespaço, termo este que, no contexto da obra, será utilizado para abranger desde a comunicação de massa até a interação interpessoal. Um local de tribos sem índios, de comunicação rápida e de informações tão surpreendentes quanto acessíveis. [...] A Unesco define ciberespaço sendo um novo ambiente humano e tecnológico de expressão, informação e transações econômicas. Consiste em pessoas de todos os países, de todas as culturas e linguagens, de todas as idades e profissões fornecendo e requisitando informações; uma rede mundial de computadores interconectada pela infraestrutura de telecomunicações que permite à informação em transito ser processada e transmitida digitalmente. Tais itens de informação não possuem uma forma material estável no tempo e espaço e circulam principalmente de modo anônimo e desregulado, ignorando, muitas vezes, fronteiras e escapando da legislação e da jurisdição nacionais. (KAMINSKI, 2000, s.p)

Podemos entender que, o ciberespaço e internet são coisas distintas. O ciberespaço por sua vez, veio antes da própria Internet.

O crescimento da Internet e da globalização, se deu com o advento de cada vez mais se ter a ampliação do ciberespaço, obtendo muitas informações e facilidade na comunicação, com uma vasta interconexão pelo mundo todo e assim, a própria sociedade transfere sua vida real para a virtual. há a possibilidade de armazenar dados e assim se tornando de fácil acesso por qualquer dispositivo que contenha rede, se tornando um local que não há fronteiras.

A possibilidade de transferir sua vida real para virtual facilita a comunicação com pessoas do mundo inteiro, que estão separadas geograficamente por longas distâncias e que em apenas questão de segundos, conseguem enfrentar a barreira do espaço e do tempo.

Entretanto, ao mesmo tempo que as novas tecnologias trouxeram inúmeros benefícios, tanto para as pessoas, quanto para empresas e a economia, apresentaram também uma nova onda de ações maléficas. Muitas pessoas, aproveitando-se do ambiente virtual teoricamente anônimo, procuram tirar vantagem dos usuários das redes, abusando da falta de segurança neste ambiente.

Com o aumento da dependência da sociedade dos sistemas eletrônicos e do meio virtual, os terroristas viram uma oportunidade de explorar novos meios de ataque. Assim, consequentemente, se dando a possibilidade de

realização de ataques ciberterroristas, já que a segurança no ciberespaço ainda é muito restrita.

Os ataques realizados no âmbito do ciberespaço, realizados pelos terroristas, tem o nome de ciberterrorismo. Segundo Shimeall (2002 apud LIMA, 2006), entende-se por ciberterrorismo:

> Entende-se por terrorismo informático qualquer ato que se enquadre numa das seguintes situações: destruição (ou a tentativa de...) de infraestrutura de rede a ponto de perda parcial ou total do controle das funções vitais; acesso não autorizado à informação classificada em formato eletrônico; distorção internacional de informação eletrônica com o objetivo de descredito público da instituição.

Essa falta de segurança vem desde o início da globalização, por meio de *hackers* (que são aquelas pessoas que possuem um amplo conhecimento no âmbito da informática e são capazes de modificar algo no sistema informático), que conseguem ferir a segurança de determinado sistema, pois este é fraco e vulnerável e assim, cometer algum tipo de ataque, roubo de informações ou simplesmente por *hobby* e também pelos *crackers* (aqueles que quebram o sistema de segurança de maneira ilegal e cometem atos de vandalismo), já que com o crescimento maciço da internet, a segurança dos indivíduos que as usam ficou em segundo plano, se tornando mais vulnerável e podendo sofrer ameaças.

Esses indivíduos procuram sempre um sistema operacional falho para que possam invadir, de maneira ilegal, para comprometer determinados computadores e roubar informações. Mas também, para invadir determinados computadores para conseguir comprometer outro e assim por diante.

As ações cibernéticas podem ser realizadas por um ataque a computadores de empresas multinacionais, implantando vírus por exemplo. Ou algo mais amplo, invadir a rede de conexão de internet e energia de alguma cidade para causar danos a população.

Para melhor entendimento dos atos de *hackers* e *crakers*, temos o evento da *WikiLeaks*, que foi:

> O WikiLeaks é uma organização que existe desde o final de 2006 e que desde o começo tinha como pretexto ser o grande “dedo duro” do mundo. Divulgando documentos secretos de empresas e governos, a organização pretendia “democratizar” a informação. [...] seu site é basicamente um diretório de arquivos de diversos tipos e para vários fins. Seu nome e

> logotipo fazem referência a um conjunto de informações vazadas, dai vem o “leaks”, que vem do inglês “vazar”.
> Fundada por diversas pessoas que não revelam quem são, tem o diretor e principal porta-voz da organização sendo o australiano Julian Assange, jornalista e ciberativista (ALTERMANN, 2010, s.p).

O *WikiLeaks* foi criado pelo ex-*hacker* australiano Julian Assange, que por meio desse site, conseguiu com que as pessoas consigam ter acesso a documentos que eram secretos e publicou com anonimato.

> Os WikiLeaks, o que ele faz é estimular pessoas que tenham acesso a documentos secretos a divulga-los de forma anônima. Não sendo diferente do que os jornais sempre fizeram. A diferença é que Assange revelou coisas grandes [...] Como o vídeo Assassinato Colateral. A gravação feita em um helicóptero dos EUA em 2007 durante a guerra no Iraque, mostra um ataque que mata dezenas de civis iraquianos e dois jornalistas Reuters. Em julho e outubro, o WikiLeaks divulgou documentos confidenciais das guerras do Afeganistão e do Iraque. Logo em seguida, no final de novembro, os 250 mil telegramas confidenciais da diplomacia dos EUA, vindos de escritórios e embaixadas do mundo todo, começam a ser revelados [...] (QUEROBINO; VERSIGNASSI, 2011).

Esse meio de comunicação acabou por publicar documentos confidenciais do governo dos Estados Unidos, também informações sobre os governos de Portugal e Moçambique, obtendo uma vasta repercussão mundial.

É possível ter fácil acesso ao *WikiLeaks*, tendo em vista que basta somente possuir um computador ou notebook que tenha acesso a Internet, digitar na barra do site “www.wikileaks.org” e pronto, permite o acesso a todos documentos “misteriosos” de primeira mão.

Outro evento de amplo choque, no âmbito brasileiro, foi o grupo de *hacker LulzSec* (grupo de hacker que fazem ataques em perfis e que acabam vazando dados de inúmeras contas) que acabou por invadir o site da Presidência da República e do Governo brasileiro. O grupo ao derrubar os sites, divulgaram em sua própria conta na rede Twitter e logo em seguida as páginas saíram do ar. Entretanto, o Serviço de Processamento de Dados (Sepro) conseguiram detectar o ataque antes mesmo do grupo de hacker atacarem e conseguiram bloquear a ação destes, assim, os sites citados ficarem fora do ar para que fossem preservados (TAGIAROLI, 2011).

O grupo *LulzSec* junto com o grupo *Anonymous* (comunidade online descentralizada, que atua de maneira anônima) juntos anunciam confronto ao governo, instituições bancárias e grandes corporações (TAGIAROLI, 2011).

Entretanto, ciberterrorismo se difere de ciberatuação, é aquela pessoa que se utiliza da tecnologia ou que fazem invasões de *hackers* sem propósitos terroristas. Tendo em vista que o ciberterrorista usa uma rede de computadores para sobrecarregar e destruir um sistema utilizado pelo Governo, por exemplo. Difere-se do terrorista que se utiliza da tecnologia para saber como constrói uma arma química ou uma bomba. Ou seja, a Internet é um meio onde se obtém recursos muito facilmente, sendo possível uma única pessoa com capacidade de invadir um site com alta importância, conseguir intimidar ou coagir governos ou sociedades. Tendo em vista que é um meio acessível e que causam um dano alastrante, o que nos leva a remeter ao Ciberterrorismo.

O ciberterrorismo, possui a finalidade o ataque terrorista realizado Internet, que ter por objetivo atingir sistemas e causar severos danos. É a ameaça baseado em um ataque que é realizado por meio de um computador, com a intenção (no mesmo sentido que o terrorismo convencional) de atingir a sociedade, cultura, religião e intimidar o governo.

O primeiro relato de ciberterrorismo foi em 2007 na Estônia, em que ciberterroristas invadiram, por meio de *hackers*, os sites do governo e deixaram fora do ar. Entende-se que a Estônia fora o primeiro alvo do crime de ciberterrorismo, por ser um país em que todos os seus serviços são diretamente ligados a internet.

No ano de 2011, a empresa *Nokia* teve seu sistema invadido e teve por consequência o comprometimento dos dados pessoais de seus usuários acessados por meio de um ataque de SQL (*Structured Query Language*). Esse SQL nada mais é que uma linguagem utilizada para manipular os bancos de dados. Esse banco de dados é manipulado para inserir e alterar registros, gerenciar o usuário que o utiliza, possibilidade de consultar informações, controlar transações por meio do SGBD (Sistema de Gerenciamento de Banco de Dados Relacionais) (ALVES, 2013).

Em 2017, foi espalhado um vírus através do sistema do Windows que foi identificado pela Agência de Nacional de Segurança dos Estados Unidos. Os agentes causadores desse ataque foram hackers que aproveitaram da vulnerabilidade do sistema e se beneficiaram para captar arquivos privados e que somente seriam liberados através da realização de um pagamento por *bitcoin*. Ataque realizado por um grupo denominado *WannaCry.* Esse vírus foi disseminado via e-mail spam e websites, utilizados como armadilhas, entretanto não havia a necessidade de clicar para conseguir se infectar com o vírus (BBC, 2017).

Nos Estados Unidos ainda, a distribuição de jornais foi invadida e gerou um atraso na distribuição dos jornais *Los Angeles Times*, *Chicago Tribune*, *Wall Street Journal* e *New York Times* em 2018. Foram alvos de ataques cibernéticos que implementaram vírus que afetou o sistema que é utilizado para produzir os jornais (ÉPOCA NEGÓCIOS, 2018).

Além de ameaças e ataques cibernéticos como tratado acima, o grupo Al Qaeda usa a internet para propagar a sua ideologia. Na mensagem enviada para Abu Omar, que tratava acerca do *Jihad* (Guerra Santa) se referia: “Nós somos a energia por trás do caminho da *Jihad*” e Abu Omar expôs: “Assim como os jihad atingiram seu objetivo em 11 de Setembro, nós alcançaremos o nosso através da internet” (NEW YORK TIMES, 2006).

Abu Omar é um dos colaboradores e líderes de um dos grupos existentes que ajudam a Al Qaeda a conquistar outros muçulmanos. Assim, simpatizante da Al Qaeda e defensor dos ataques por eles promovidos, espalha a filosofia de Osama Bin Laden para a Jihad. Com isso, busca conquistar outras pessoas que se inspirem e seguirem a causa. A propagação da mensagem por Abu Omar é realizada via e-mail para grupos que apreciam o grupo por meio de um software especial, de maneira que não seja descoberta as atividades por ele realizadas (NEW YORK TIMES, 2006).

> [...] Graças às ferramentas cibernéticas, a Al Qaeda conseguiu passar de uma organização hierárquica, restrita a células geograficamente organizadas, para uma rede global horizontal [...] (NYE JÚNIOR, 2012, p. 180).

O ataque acontece mesmo se não existe o resultado fim, ou seja, a partir do momento em que o ciberterrorista consegue adentrar ao sistema, já existe uma parcela do êxito do seu ataque, tendo em vista que conseguiu quebrar a “barreira” e conseguiu provar que o sistema de segurança é fraco e falho.

Entretanto, nos dias atuais é vigente a segurança da informação pelas as empresas para proteger e manter os seus arquivos em sigilo, já que ao divulgar qualquer dado pode abalar a confiança de seus consumidores e prejudicar tanto a empresa quanto sua própria marca, sem contar a vida privada que poderá ser invadida causando malefícios à vítima.

4.2 Por que Ciberterrorismo? Como atua na modernidade?

O ciberterrorismo vem sendo utilizado pois tem como vantagem ser um meio imperceptível, uma vez que não se sabe quem é o usuário que está atrás do computador realizando o ciberterrorismo. Desta forma, a segurança e defesa contra aquele que está sendo atacado é totalmente limitada.

Ademais, outro ponto que se tem de vantagem é no tocante à ausência de vítima “morta” para que seja realizado esse meio de terrorismo. Assim, não há a necessidade de “homens bomba” (que é aquele terrorismo no qual um terrorista se envolve com explosivos em volta ao seu corpo e que acaba por finalidade matar todos aqueles que estão ao seu redor), por exemplo. Destarte, sendo uma opção mais atraente e ampla para os ciberterroristas, pois além de atingir seu fim, sem ser reconhecido de imediato, pois o anonimato é “certeiro”, consegue-se atingir o impacto que necessita, causando um vasto dano, além, do impacto psicológico e na segurança daquele que está sendo atingido.

Obter esse poder na mão de ciberterroristas permite à eles “[...] operar como redes de franquias descentralizadas, criar uma imagem da marca, recrutar partidários, levantar fundos, proporcionar manuais de treinamento e controlar operações” (NYE JÚNIOR, 2012, p. 180).

A internet facilita muito na comunicação dos terroristas, que conseguem combinar os ataques, financiar atividades, levantar dinheiro, recrutar e encorajar pessoas a executar ataques terroristas. No âmbito da comunicação, os terroristas, desde antes do ataque de 11 de Setembro, se comunicavam pelo e-mail e atualmente, há a ferramenta do *Whatsapp, Telegram*, *Twitter* e até *Instragram* que são muito utilizados, pois além de se tornar viral em poucos segundos, possuem a ferramenta de mensagens criptografadas ou que passem por sistemas que impedem rastreamento, como a *Deep Web*.

Outro meio utilizado para ser realizado um ataque cibernético é por meio de *ransomware*. Utilizado com um código para captar informações de um computador ou SmartPhone e além disso, gera-se um bloqueio do aparelho ou até mesmo criptografar a senha de arquivos e informações importantes. Entretanto para que o causador não pegue as informações privadas exige um pagamento em troca por meio intimidador (INLEARN, 2019).

A criptografia, por outro lado, é muito utilizada pelos aplicativos dessa nova geração, por conseguirem destruir mensagens de maneira segura. Sendo assim, existe uma proteção dos conteúdos que são enviados por esses aplicativos, que a tornam ininteligível para quem não tem acesso e as informações que são postas no ciberespaço.

Já a *Deep Web* ou também conhecido como “dark web”, são sites que para conseguir entrar nesses sistemas, havia a necessidade de conseguir uma ferramenta especial, mas ao passar do tempo e com muitas atualizações com a globalização, essas ferramentas especiais se tornaram explicitas e o conteúdo nela, que era especial e de difícil acesso, acabou sendo disponibilizada, de modo que qualquer um que possui Internet consegue ter acesso a ela. Uma parte do conteúdo que existia nesses sites, acabaram por ser disponibilizadas até no Google.

Esses sites, que possuem esse tipo de conteúdo, muitas vezes possuem pirataria, troca de conteúdos ilícitos, venda de drogas lícitas e ilícitas, armas, conteúdo de pornografia.

Possuem um objetivo de ter a garantia de anonimato dos usuários que as usam. Mas por mais que possua muitas informações, somente utilizar-se das redes, não se configura ciberterrorismo. Porém, as informações que neles são obtidas podem sim, ser utilizadas para realizar o ciberterrorismo, pois, como já tratado no presente artigo, as redes sociais também são meios eficientes para que se propague as mensagens de terroristas, pois milhões de pessoas possuem contas em redes sociais e assim, tendo fácil acesso à informação.

O Governo internacional e nacional, contam com recursos para controlar esses tipos de sites e conteúdos disseminados pela internet utilizando-se das leis, sistemas militares sensíveis, sistemas de computadores como da CIA e do FBI (que são quase extremamente protegidos).

Uma boa alternativa para que que fosse possível entender como os ciberterroristas atuam, para fácil prevenção, seria aliar-se a algum hacker ou conseguir estudar e entender como eles atuam e qual a capacidade técnica que utilizam. Entretanto, se sabe que hacker e ciberterroristas não são as mesmas pessoas que não atuam igualmente e assim, para conseguir desenvolver o que um hacker consegue fazer, há a necessidade de muita condição tecnológica e teria que ser algo possivelmente rápido.

Como Weimann (2004, s.p) diz “o terrorista de amanhã pode ser capaz de causar mais danos com um teclado do que com uma bomba”.

Weimann aduz que os terroristas vão, cada vez mais, tentar utilizar-se do meio virtual para planejar e conseguir fazer ataques.

> Mas, embora o medo do ciberterrorismo possa ser manipulado e exagerado, não podemos negar nem ignorá-lo. Paradoxalmente, o sucesso na “guerra ao terror” provavelmente fará com que os terroristas se voltem cada vez mais para armas não convencionais, como o ciberterrorismo. E à medida que uma nova geração de terroristas mais experiente em computadores atinge a maioridade, o perigo parece aumentar (WEIMANN, 2004, sp.).

Lima (2006, s.p.) traz que com os ataques terroristas as consequências que são mais prováveis de acontecer são os danos econômicos e psicológicos, mas que não ficam somente a essas duas. Esses terroristas conseguem se infiltrar onde quiser, ou seja, podendo se infiltrar no controle de metrôs, de navios, no sistema de torres de controle aéreo, causando caos. O ciberterrorismo só é possível ser realizado por meios tecnológicos, seja pela parte da vítima e pela parte do terrorista e por conta disso, os alvos serão sempre aquelas empresas multinacionais que se conectam nas redes através de computadores e as estruturas dos estados, se tornando possível uma tragédia em grande escala.

Com isso, ressalta-se que: “Atualmente, os ciberterroristas mundiais elegeram os EUA e as empresas multinacionais como alvos preferenciais [...] tendo a sua incidência aumentado consideravelmente a partir dos atentados de 11 de setembro de 2001” (BATISTA; RIBEIRO; AMARAL, 2004, p.39).

Com o ataque do atentado do 11 de setembro, se verificou a vulnerabilidade da rede virtual e dos computadores. Assim, aqueles que possuem interesses com a segurança, política, empresarial etc, acabaram por se preocupar mais ainda com o assunto, sempre buscando a máxima proteção de dados para que não haja invasão e, se houver, que os dados fornecidos não sejam captados pelos ciberterroristas.

Ademais, a utilização do meio cibernético por terroristas não significa dizer que é um ataque cibernético, podendo ser um termo utilizado de maneira errônea já que muito dos ataques, por mais que sejam praticados por terroristas do outro lado da tela de computador, podem ser encaixados em outro tipo de ataque. Todavia, não podemos deixar de duvidar que é capaz de se tornar o ataque da nova

geração. Uma vez que, a utilização da rede permite com que os terroristas disseminem suas ideologias, levantem fundos, tratarem sobre os meios de controle de ação terrorista e além disso, possível recrutar pessoas para participarem destes grupos. Se tornando mais simples e ágil alcançar o objetivo por meio do anonimato, baixa renda e pouco custo de ação.

Silva (2006. s.p.) aponta a ausência de possibilidade de identificar os autores dos crimes e a dificuldade de encontrar quem pratica o ato:

> A mesma ação pode ter efeito em vários países, de forma simultânea, podendo atingir até milhões de pessoas, como é o caso da disseminação de programas maliciosos. Além disso, os vestígios que poderiam permitir a identificação e a localização dos autores desses crimes podem se perder definitivamente em pouco tempo. O criminoso pode estar em qualquer parte do planeta e, mesmo assim, pode conseguir atingir alvos em quaisquer localidades (SILVA, 2006).

Muitas vezes o ataque cibernético é marcado pela dificuldade de serem rastreados e pela facilidade de ameaça, seja por textos, vídeos, imagem ou áudios causando uma extrema instabilidade no seu público fim. Além da propagação do medo, a internet pode ser utilizada para realizar o planejamento dos atos terroristas pela privacidade e de maneira eficiente no plano físico. Por exemplo, divulgações de vídeos de homens bombas, decapitações, genocídio de vítima vivas etc, quando espalhados e viralizados na internet gera impacto no ciberespaço.

O ciberterrorismo tem por objetivo, uma devastação que vai além do mundo físico onde atuavam, mas atingir um nível de fatalidade gigantesco. Como trata Nye Júnior (2012, p.191) “a medida que os grupos desenvolverem sua capacidade para infligir grandes danos contra a infraestrutura nos próximos anos, a tentação aumentará”. Por conseguinte, a criação de um método de segurança capaz de proteger sistemas operacionais de maneira eficaz se faz necessário, pois de contrapartida o aumento de ocasião para ataques de ciberterrorista se torna mais possível e assim, gerará mais impacto do que um terrorismo no plano físico.

Conforme tratado no tópico anterior, a Al Qaeda utiliza o meio cibernético para recrutar, financiar, treinar, realizar propagandas e demonstrar sua maneira de atuação. Uma maneira de apoderar-se da vulnerabilidade da internet para disseminar ideologias.

Como no caso em que o Estado Islâmico usou um aplicativo conhecido como *TikTok* para espalhar a propaganda do grupo terrorista. O vídeo traz vídeos de

cadáveres nas ruas do EI (Estado Islâmico) armados e participantes que se denominam “jihadistas e orgulhosos”. Utilizaram este meio, já que é muito adotado por jovens atualmente, além do *Facebook*, *Messenger* e *Whatsapp*, assim conseguem demonstrar sua força e que podem ser encontrados em quaisquer meios de comunicação para propagar sua ideologia. No vídeo utilizavam músicas, bandeiras e referências ao grupo extremista (WELLS, 2019).

Além dos aplicativos acima citados, a rede Twitter é um alvo de terroristas que se apossam de contas de usuários já existentes de contas desativadas e utilizam, também, para propagandas terroristas. Neste caso, os membros do Estado Islâmico utilizam de hacker para tomar posse de uma conta desativada e assim compartilhar mensagens e vídeos que pregam atos terroristas, como carro bombas, atentados, mortes e atentar contra pessoas que não sigam Alá (WHITTAKER, 2019).

Assim, mais uma vez evidente que é possível adentrar esses meios utilizados pela falha de proteção a esse tipo de conteúdo malicioso e a dificuldade de estabelecer políticas que freiam esse tipo de conteúdo postado e de acesso livre mundialmente (WHITTAKER, 2019).

Diante de todo o exposto, é possível perceber que a atuação de terroristas no ciberespaço cresce e se especializa cada vez mais em utilizar a Internet como meio de sua atuação, já que seu comportamento e da maneira como age é silencioso e não deixa rastros. Atualmente as ameaças são grandiosas perto da segurança que existe. Assim, deve ser elaborada um controle diretamente direcionada a cibersegurança, para fazer com que exista estabilidade nas redes, obter uma administração sobre informações do governo, prevenir, detectar e por fim, estabelecer um acesso seguro e de confiança a toda população que utiliza da Internet. Não privando arbitrariamente quem a usa, mas sim, proteger a informação e tornar seguro todo o sistema contra eventuais danos e acesso a informações privadas.

5 TERRORISMO E CIBERTERRORISMO NO BRASIL: LEGISLAÇÕES NACIONAIS

Neste tópico trataremos sobre a lei do antiterrorismo e ciberterrorismo na legislação atual que o Brasil adotou e realmente é suficiente para proteger os indivíduos que podem sofrer ataques de ciberterrorismo. Posto que, a cibersegurança é uma preocupação não somente no mundo empresarial, mas por parte de usuários e sua vida particular também, já que se houver uma ciberguerra os usuários que realizarem o ataque possuem um dispositivo mais sofisticado do que um software de proteção.

5.1 Lei do Terrorismo

A Lei de Terrorismo nº 13.260 de 16 de março de 2016, foi criada por pedidos de organismos internacionais que refletiram sobre nosso país e entenderam que por mais que não aconteça, por ora, terrorismo no Brasil, há a necessidade de uma lei específica para o terrorismo. Já que inúmeros países procuram se proteger destes ataques terroristas por meio de uma legislação específica ao tema.

Entretanto, antes de chegar a Lei Antiterrorismo a legislação brasileira passou por várias etapas ao tratar acerca do terrorismo e seu modo de puni-lo.

Uma das primeiras aparições a respeito de terror, se deu na Lei Constitucional nº 1 de 1938, 13) h), que dizia: “atentar contra a segurança do Estado praticando devastação, saque, incêndio, depredação ou quaisquer atos destinados a suscitar terror e que emendou o art. 122 da Constituição de 1937 (BRASIL, 1937).

Outrossim, para criminalizar o terrorismo, veio no Decreto-Lei nº 314, de 13 de março de 1967 que em seu art 25 dizia:

> Art. 25. Praticar massacre, devastação, saque, roubo, sequestro, incêndio ou depredação, atentado pessoal, ato de sabotagem ou terrorismo; impedi ou dificultar o funcionamento de serviços essenciais administrados pelo Estado ou mediante concessão ou autorização (BRASIL, 1967).

Deixando o conceito de “terrorismo” amplo cabendo vários tipos de interpretações. Assim, a Lei de Segurança Nacional elaborada em dezembro de 1983, também tentou definir terrorismo:

> Art. 20. Devastar, saquear, extorquir, roubar, seqüestrar, manter em cárcere privado, incendiar, depredar, provocar explosão, praticar atentado pessoal ou atos de terrorismo, por inconformismo político ou para obtenção de fundos destinados à manutenção de organizações políticas clandestinas ou subversivas (BRASIL, 1983).

Mas não obteve sucesso, já que atos de terrorismo é um sentido muito amplo e vago já que inúmeros delitos poderiam ser encaixados como atos de terrorismo.

A Constituição Federal, em 1988 foi promulgada e em seu art. 5º, XLIII tratou o crime de terrorismo como crime inafiançável e insuscetível de graça ou anistia e que por este responderia os mandantes, executores e os que podendo evitar, se omitirem. Foi equiparado como um crime hediondo (crimes que recebem uma enorme reprovação do Estado brasileiro e que promovem revolta e aversão à sociedade).

Com a vinda da lei de Crimes Hediondos (lei 8.072/90), também tratou o terrorismo de maneira mais severa em seu art. 2º:

> Os crimes hediondos, a prática da tortura, o trafico ilícito de entorpecentes e drogas afins e o terrorismo são insuscetíveis de:
> I- anistia, graça e indulto;
> II- fiança;
> § 1º A pena por crime previsto neste artigo será cumprida inicialmente em regime fechado. [...] (BRASIL, 1990).

Como tratado anteriormente, o terrorismo pode ser identificado por suas condutas premeditadas, pelos ataques de motivação política, cultural, religiosa ou governamental, realizar ataque contra pessoas indefesas e realizadas (não necessariamente) grupos organizados. Novamente, dentro da lei de crimes hediondos o terrorismo veio como um instituto vago e indeterminado, sem um significado certeiro e uma conduta típica punível.

Anos se passaram e fora criada a Lei 13.260/16, a chamada Lei Antiterrorismo e que gerou grande repercussão e polêmicas. Por um lado, críticas já que o Brasil nunca foi alvo de terrorismo e, seja por religião, etnia ou nacionalidade, nosso país nunca sofreu devera intolerância. Por outro lado, os defensores da nova lei concordam e argumentam pela necessidade de prevenir um futuro ataque terrorista e que por realizar eventos internacionais como já realizada, por exemplo a Copa do Mundo de 2014 e os Jogos Olímpicos de 2016, pela repercussão que possuem se torna necessária a devida proteção a um possível ataque.

Dentro da lei a definição de terrorismo em seu art. 2º, consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou incolumidade pública.

Portanto, para que haja punição pelo ato de terrorismo imposto será necessário incorrer em um terror social ou generalizado por um dos crimes supracitados, se encaixa no medo empregado por estes, que fere o patrimônio tutelado pela lei de terrorismo. O patrimônio tutelado se encaixa em (conforme art. 2º da lei) a pessoa, patrimônio, paz pública e incolumidade pública. Ademais, a própria ameaça ao bem jurídico lesado é o bastante para que seja punido quem o comete, pois trata-se de um crime abstrato não havendo a necessária lesão do bem jurídico ou colocado este a risco real, senso insignificante o objetivo final.

A punição de atos preparatórios está prevista no art. 5º da lei, onde os atos preparatórios de terrorismo com propósito de conseguir seu objetivo final e consuma-lo, haverá punição seja pela preparação de um objeto explosivo ou por troca de e-mails, mensagens telefônicas visando a prática do delito.

Além disso, haverá punição a aquele indivíduo que recruta outros para realizar o ataque, aquele que organiza, transporta ou municia o grupo terrorista. Outrossim, aquele que fornece ou recebe treinamento com proposito de praticar atos de terrorismo, conforme art. 5º, §1º incisos I e II da lei.

> Art. 5º:
> § lº Incorre nas mesmas penas o agente que, com o propósito de praticar atos de terrorismo:
> I - recrutar, organizar, transportar ou municiar indivíduos que viajem para país distinto daquele de sua residência ou nacionalidade; ou
> II - fornecer ou receber treinamento em país distinto daquele de sua residência ou nacionalidade. (BRASIL, 2016)

Esse art. 5º da lei, tornou-se o mais polêmico pois trata de uma proteção do “ato preparatório”, ou seja, punir subjetivamente o plano e a intenção do executor que teve por base o reflexo do Direito Penal do Inimigo, que visa punir atos preparatórios e que foi adotado no referido artigo. É uma maneira de prevenção de ataque terrorista, visto que não há sequer um lugar que esteja imune a esse ataque, seja pela complexidade ou de identificação.

5.2 Ciberterrorismo

Como visto anteriormente, o *modus operandi* do ciberterrorismo se distingue do terrorismo convencional, já que atua no ciberespaço. Sua agilidade de ação, não existe um território especifico para atuação e o mundo interconectado em tempo real dificulta muito mais a investigação e a conclusão para capturar o criminoso.

Ao expandir o terrorismo convencional para o ciberespaço, pode ser atacado tanto seus alvos de início, tanto como inúmeras vítimas eventuais.

Por mais que no Brasil não exista indícios de atividades terroristas, com a globalização os fatores contribuem para que essa ideia saia do papel e se torne concreta. A espionagem e o vazamento de estratégias e informações diplomáticas podem causar situações de risco, já que ciberterroristas sempre aprimoram suas obtenções de dados, meios de comunicações e equipamentos.

O vínculo da internet com o executor do ciberterrorismo reforça a possibilidade de existir a mídia, um dos fatores, mas não necessariamente, para incorrer o terrorismo comum, amplificando a divulgação de informações complexas, garantindo o anonimato e dando oportunidade de comunicação, como tratado anteriormente, um âmbito de recrutar membros para participarem da mesma ideologia.

Planejamento de atentados, redução de custos e a divulgação internacional, permitiram aos terroristas uma maior visibilidade em uma nova plataforma de ataque. Terroristas sempre buscam a amplificação de seus ataques para que não se tornem alvos de fácil localização, mas sempre estará intencionalmente presente figura violenta.

O conteúdo do ciberterrorismo é complexo, a existência de criação de sofisticadas ferramentas para atingir seus alvos e controlando o que terceiros desenvolvem em seu computador é estratégia dos ciberterroristas.

O Brasil ao sediar grandes eventos, como a Copa do Mundo de 2014 e Jogos Olímpicos 2016, gerando grande fluxo de pessoas, provocando multidões foi necessário mobilização das forças armadas e entidades da policia federal e militar, tendo em vista que pela conferencia há planejamento da operação por meio eletrônico (BULCÃO, 2012).

A segurança das conexões durante a conferência foi fundamental para que as autoridades não se tornassem vulneráveis, visto que se um indivíduo conseguisse adentrar o sistema, poderia alterar mecanismos aéreos tanto como deslocamentos terrestres. Pelo deslocamento de executivos se transportarem por aeronaves, houve a necessidade de inspeção para realização de protocolos internacionais e segurança (BULCÃO, 2012).

A discussão de estado em alerta pelos grandiosos eventos, foi necessária a mudança de todos os recursos, seja tecnológico ou de órgãos responsáveis pela cibernética do país. Entretanto, mostrou-se necessária a estipulação de novas seguranças e estipular que profissionais brasileiros atuassem no território.

Foi necessário que criasse investimentos em leis internas para proteção. Entretanto, o projeto de lei antiterrorismo, foi em 2015, para que se houvesse algum incidente nas Olimpíadas, o Brasil estaria de modo, protegido e sendo possível tipificar os executores do ciberterrorismo. Assim, evitando o que ocorreu nos Jogos Olímpicos de Munique de 1972, em que foi sequestrado atletas israelenses (MAGNO, 2013).

Pela aprovação da lei 13.260/16, tratou sobre o terrorismo convencional, como tratado no tópico supracitado. Tratando disposições do tipo penal de terrorismo e adentrando sobre disposições investigatórias, processuais e de julgar tais crimes.

No art. 2º § 1º inciso IV, onde:

> Art. 2º. [...]
> § 1º. [...]
> IV- sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento (BRASIL, 2016).

Júnior (2016, p.9) entende que existe o enquadramento do ciberterrorismo neste art. 2º da lei, trazendo as condutas:

> “Sabotar” (prejudicar; impedir funcionamento) ou “apoderar-se” (tomar posse; apoderar-se), na primeira parte usando-se da violência ou da grave ameaça à pessoa e na segunda utilizando de mecanismos cibernéticos (mecanismos de controle e comunicação de máquinas), o controle estruturas fundamentais para a sociedade, como comunicação, transporte, hospitais, instituições de controle e armazenamento de água e energia. (JÚNIOR, 2016, p.9).

Traz um conceito próximo ao ciberterrorismo, já que a intimidação ou coagir a sociedade, bem como governo por intenção de atingir objetivos políticos, religiosos ou ideológicos.

Há de se entender que cometer ciberterrorismo, aquele que sabota ou apodera-se de determinados serviços públicos e recairá como crime de terrorismo.

Nesse sentido, o terrorismo é uma conduta que ter por característica um crime de perigo, merecendo uma atenção especificada e assim, sendo necessária que seus atos sejam evitados e por analogia, também o ciberterrorismo sendo necessária a punição de atos preparatórios já que ocorrer um fato destes, possuem inúmeras gravidades e sendo possível a prevenção.

No art. 19 da lei, aplica-se medidas investigativas, que se misturam com o art. 3º da Lei de Organizações Criminosas, dispondo sobre investigação criminal e os meios de obtenção de provas, aplicando ao ciberterrorismo.

A lei de antiterrorismo teve sua aplicabilidade em um caso concreto, na chamada Operação *Hashtag.* Oito réus presos preventivamente (ação penal nº 5046863-67.2016.4.04.7000/PR) pelo art. 3º da lei, “Promover, constituir, integrar ou prestar auxílio, pessoalmente ou interposta pessoa, a organização terrorista” (BRASIL, 2016) antes dos Jogos Olímpicos do Rio de Janeiro de 2016 (PARANÁ, 2017).

Estes recrutavam pessoas para o Estado Islâmico, uma organização terrorista existente ao redor do mundo. Estes indivíduos se aproveitaram do *Facebook, Twitter, Instagram* e *e-mails* para debater sobre a religião islâmica [...] também tratavam sobre destruição em massa de indivíduos, raça ou propriedade e discriminar aquelas pessoas que tenha visão distinta sobre etnia, estética ou sexual. (MARTINES, 2017)

Os indivíduos da organização tratavam sobre alvos de ataques que eles poderiam realizar no Brasil (estrangeiros durante os Jogos Olímpicos, homossexuais, muçulmanos xiitas e judeus), como orientação sobre a fabricação de

bombar caseiras, a utilização de armas brancas e aquisição de arma de fogo para conseguir esse objetivo (PARANÁ, 2017).

O líder da organização terrorista foi punido pelo art. 5º §1º, inciso I: “recrutar, organizar, transportar ou municiar indivíduos que viajem para país distinto daquele de sua residência ou nacionalidade” (BRASIL, 2016), já que tinha como finalidade de consumar tal delito.

Ainda que o referido artigo traga no corpo da lei a definição do que se trata o terrorismo, o Brasil enfrenta o desafio de trazer do que se trata o terrorismo com exatidão e como se daria este ato, carecendo o sistema jurídico brasileiro de tipificação legal específica no que tange a atos terroristas, com ênfase em ataques ciberterroristas, uma vez que a legislação interna necessita acompanhar a evolução telemática e a migração de crimes para a esfera virtual.

5.3 Estratégias Nacionais de Segurança Cibernética

Tendo em vista a complexidade em punir um ciberterrorista, já que é um meio vasto e passível de ocorrer de inúmeras maneiras, há a necessidade de existir um tipo de punição que vá além do nosso sistema penal brasileiro, que pune apenas condutas, e trabalhe com prevenção de ações futuras.

Sabe-se que para punir ações premeditadas, resta necessária uma forte investigação para proteger a ordem pública.

Outrossim, a vinda da Lei Antiterrorismo gerou muitas discussões e claramente o crime de ciberterrorismo demonstrou a necessidade que seja tratada de maneira adequada, por mais que abordada dentro do referido diploma legal. Observando que a globalização se expande a cada dia e os riscos de situações catastróficas que podem acontecer pelo meio cibernético são cada vez mais impossíveis de ser definidas, pela tamanha complexidade e a evolução da tecnologia, sendo capaz de expandir suas formas, seus canais de intervenção e o seu emprego.

Com a dificuldade de um legislador de acompanhar o crescimento de exploração do ciberespaço, hoje, a necessidade de garantir a soberania e a segurança do país é relevante e fortalecer a infraestrutura de informação é imediato, visto que a internet se encontra em constância evolução e modificação tornando os instrumentos clássicos de legislar escasso para se por em prática.

As ameaças podem ser materializadas por apenas um indivíduo ou por grupos organizados de terroristas que se apropriam da internet para realizar ataques ilícitos. Completa-se por um computador, estrutura necessária de técnica e adentrar no sistema vulnerável para conseguir um fluxo de informações vitais para que órgãos sejam comprometidos pelos executores do ataque.

Com isto, houve a necessidade de um Direito Penal de Emergência como forma de estratégia nacional de segurança cibernética, envolvendo um tema onde o Estado ao se sentir ameaçado por devido fato, poderia editar novas normas penais mediante o fato ocorrido. Sua característica não é somente punição, mas prevenção, ou seja, se prevenir de ações e antecipá-las para poder deter, para que assim seja reduzida a vulnerabilidade de ataques futuros. Por esse motivo, ao ser adotado o direito penal de emergência, se torna capaz de frear o terrorismo, já que é mais eficaz prevenir um ataque do que aguardar eventual ataque que pode gerar inúmeros acidentes.

Esse modelo de emergência se pauta nos momentos de vulnerabilidade e de instabilidade pela quebra dos direitos fundamentais, dado fato que o ciberterrorismo tem por meio o medo e o pânico não em seu alvo apenas, mas em toda a população, em razões governamentais, políticas, religiosas ou ideológicas.

Se torna considerar que o Estado crie um órgão de defesa, uma estratégia nacional de cibersegurança para combater o cibercrime e que existam serviços que atuem no âmbito da ciberespionagem e no ciberterrorismo, existindo previsão de um serviço de informação e de forças de segurança para uma ciberdefesa.

Com a criação de uma defesa cibernética, potencializa a utilização do ciberespaço para garantir uma utilização segura, gerando uma infraestrutura para combater futuros ataques. Levantar mecanismos de ciberdefesa, sistemas que garantem a informação e disponibilidade, tornando-os confidenciais. Explorar o ciberespaço de maneira que salvaguarde a defesa de interesses nacionais.

Além disso, reconhecer a ameaça e se proteger, interligam a uma área de segurança, já detê-la se conecta com a defesa. Revestir de segurança redes de computadores para que detectem pontos fracos e as vulnerabilidades e dominá-las é essencial para se ter êxito.

Dessa forma, investir em proteção nas redes governamentais e da administração pública que tenha mecanismos de resposta a incidentes de invasão, criando maneiras de recuperar o sistema e em atividades específicas, desenvolvendo maneiras de uma segurança certificada, como códigos ou políticas mais severas de segurança e de informação. Verificar quais “pontos fracos” existe no ciberespaço, para que desenvolva um sistema eficaz para combater a cibercriminalidade, reforçando a lei 13.260/16 em investigação criminal no combate a cibercriminalidade, ciberterrorismo, espionagem e em atos preparatórios sem ferir princípios constitucionais. Com isso facilitando o combate ao ciberterrorismo, obtendo uma harmonização global interligada a convenções internacionais que adotem essa estrutura de controle cibernético.

Dado o exposto, a criação de um Conselho Nacional de Cibersegurança, garantindo segurança no ciberespaço nacional, gerando especialistas que dominem a área e desenvolva recursos confiáveis para proteger a rede, construindo uma proteção integral a conexão e a guarda de arquivos. A dimensão do ciberespaço e a amplitude de inúmeras maneiras de promover um ciberataque e se manter encoberto e abusarem do sistema vulnerável, se torna o ambiente um instrumento para realizar o ataque.

Com isso, estabelecer acordos internacionais de cibersegurança e ciberdefesa, influenciando outros fatores de segurança, não focando apenas na segurança de informação da interação global, mas garantindo um ambiente moldado que favoreça os interesses internacionais e forneça um meio de qualidade de confiança ao usuário.

Aplicação de combinações de medidas politicas internas e externas adequadas para verificar esse “espaço cinzento”, torna necessário não apenas órgãos criminais, mas a necessidade de uma inteligência criminal desenvolvendo um sistema pós ataque que determine aspectos do pré ataque, o meio de aplicação do ciberterrorismo, recolher informações para estabelecer padrões e antecipar e precaver-se de ataques futuros. Partilhando entre os organismos que descubram padrões do ataque ciberterrorista e impedindo novos ataques terroristas.

Há necessidade que seja criado um sistema apenas para o ciberterrorismo, para o combate e implementação de estratégias para o combate deste, visivelmente necessário, pois o Estado agiria no plano dos ciberterroristas, por conta de sua complexidade, gerando maior efetivação de prevenção de ataques

cibernéticos contra as infraestruturas afetadas, sendo possível um programa de conscientização, de treinamento para própria segurança na Internet e por fim, a criação de um sistema inteligente que seja de cooperação internacional entre os países que aderirem o programa. Já que o questionamento não se trata apenas se haverá o ciberterrorismo, mas sim, quando e se estaremos preparados para as consequências e os danos.

6 CONCLUSÃO

Ademais, se conclui que o fenômeno terrorismo não é um fato atual, ele vem de longa data, mas desencadeou com o evento do dia 11 de Setembro. Onde o terrorismo tem por realizar danos na sociedade que fora atacada, trazendo pânico à população, governo ou Estado.

Sabe-se que nas gerações anteriores não se utilizavam de “nenhum” recurso virtual para cometer algum tipo de ataque, tendo em vista que havia muito mais complexidade para obter recursos que facilitavam a comunicação entre pessoas do mundo todo e para combinar métodos, como agiriam, onde iriam, como iriam fazer.

Logo, ao desfrutar da Internet, ao longo de muitos anos e com a vinda da globalização, os criminosos optaram por usufruir dela para cometer seus crimes assim, se tornando cada vez mais perigosos e mais difícil de ser punido.

Deve, nos momentos atuais, investir em métodos mais sofisticados para se ter mais segurança, melhoria na qualidade de vida e também proteção a economia do país. Fazendo com o os países invistam mais na segurança dentro do ciberespaço e fazer com que o governo invista cada vez mais na tecnologia segura assim, sendo necessário enfrentar as ameaças que podem surgir.

Assim como o terrorismo, tratar acerca do ciberterrorismo se torna complexo pela ausência de um conceito e existindo a dificuldade de tipificar essa conduta, visto que a modalidade que existe para esse crime se torna insuficiente.

A falta de segurança que temos no meio cibernético, já que o desastre que pode ser efetivado vai além da capacidade que conhecemos. Os dados que muitas vezes são vazados ou contraídos por um usuário com outras intenções são fornecidos, muitas vezes, por nós mesmos. A falta de vigilância e de uma atenção a mais a segurança cibernética e prevenir a propagação de violência ou até mesmo de ataques por ciberterroristas é alastrante e preocupante. Países devem investir mais na segurança dentro do ciberespaço e fazer com que o governo invista cada vez mais na tecnologia segura, assim, sendo necessário enfrentar as ameaças que podem surgir.

A necessidade de saber de qual o ponto fraco ou forte de segurança é indispensável e de a implantação de um profissional que entenda como age e o *modus operandi* de um ciberterrorista para que tente ou chegue perto de constituir

um meio de solucionar a fragilidade do sistema operacional. Levantar pesquisas e informações para prevenir e obter o combate necessário para enfrentar esse risco iminente. Fazendo com que seja possível algum recurso de maneira gratuita ou até mesmo com preço baixo para investir em software que seja capaz de detectar possíveis ameaças a computadores e a informação, tentativas de adentrar em sistema fazendo que tenha alguma possibilidade de localizar aquele que tentou invadir, sendo assim, localizando de onde vem os ataques.

Indivíduos que agem por meio do ciberterrorismo possuem vasto conhecimento de informática e possuem a capacidade de desenvolver vírus, malware e outros dispositivos para prejudicar cidadãos e o governo. Tem por meio invadir meios de comunicação que prevalecem na mídia que geram uma intenção de causar o maior dano que conseguem, seja por suas questões fazendo com que as vitimas atendam à vontade do executor.

A necessidade de existir uma incriminação para essas condutar de ciberterrorismo, a existência de um rol exemplificativo caracterizando quais as condutas de um ciberterrorista é necessário atribuir especificamente a tipificação da conduta, abordar meios de investigação de casos cibernéticos, a desterritorialização e a facilidade de agir pelo desenvolvimento de tecnologias.

Por mais que o ordenamento brasileiro com a lei Antiterrorismo 13.260/16 regulamente um direito penal de emergência, que até mesmo abordou, de maneira simplificada o ciberterrorismo, temos uma evolução que a lei apresenta, mas que ainda se torna escasso perante a alastrante dificuldade de conceituação de terrorismo.

Assim, deve se dar a real importância de se estudar referido tema e de se encontrar algum tipo de mecanismo para enfrentar essa nova criminalidade. Tendo em vista, que a cada dia que passa a dependência do ser humano com a internet cada vez mais cresce, assim como a ameaça que enfrentamos. Conhecer o inimigo, se torna capaz de lidar com suas ameaças futuras e adentrar no meio.

REFERÊNCIAS

AFP. **Atentado de 1983 contra EUA iniciou "guerra ao terror"**. Publicado em 23 out. 2017. Disponível em: https://www.nsctotal.com.br/noticias/atentado-de-1983-contra-eua-iniciou-guerra-ao-terror-diz-pence. Acesso em: 10. out. 2019

ANSA, Agência. Ataque hacker interrompe distribuição de jornais nos EUA. O episódio gerou atraso na distribuição do Los Angeles Times, Chicago Tribune, Wall Street Journal e New York Times. **Época Negócios.** Publicado em: 30 dez 2018. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2018/12/ataque-hacker-interrompe-distribuicao-de-jornais-nos-eua.html. Acesso em: 21 out. 2019.

ALTERMANN, Dennis. **O que é o Wikileaks e por que ele incomoda tanta gente?** Publicado em: 21 dez 2010. Disponível em: https://www.midiatismo.com.br/o-que-e-o-wikileaks-e-por-que-ele-incomoda-tanta-gente. Acesso em: 30 out 2018.

ALTMAN, Max. **Hoje na História: 1934 – Rei da Iugoslávia é morto na França e eleva tensão na Europa**. Publicado em 09. Out. 2012. Disponível em: https://operamundi.uol.com.br/historia/24770/hoje-na-historia-1934-rei-da-iugoslavia-e-morto-na-franca-e-eleva-tensao-na-europa. Acesso em: 12 set. 2019.

ALVES, Gustavo Furtado de Oliveira. **Dicas de Programação. Você precisa saber o que é SQL!**. Publicado em: 26 abril 2013. Disponível em: https://dicasdeprogramacao.com.br/o-que-e-sql/. Acesso em: 21 set. 2019.

BATISTA, Gonçalo; RIBEIRO, Carlos; AMARAL, Feliciano. **Ciberterrorismo: a nova forma de crime do séc. XXI como combatê-la?**. Proelium – revista da academia militar, 2004

BARBOSA, Alexandre de Freitas. **O mundo globalizado – política, sociedade e economia**. Publicado em 2001. Disponível em: https://www.suapesquisa.com/globalizacao/. Acesso em: 03 out. 2018.

BBC Brasil. **Saiba o que é a Jihad Islâmica.** Publicado em 2002. Disponível em: https://www.bbc.com/portuguese/noticias/2002/021109_jihadmp.shtml. Acesso em: 08 out. 2019.

BBC Brasil. **Por que é tão difícil identificar os autores do ciberataques global – e onde podem estar as pistas**. Publicado em 15 de maio de 2017. Disponível em: https://www.bbc.com/portuguese/internacional-39930249. Acesso em: 5 out. 2019

BOBBIO, Noberto. Matteucci, Nicola e Pasquino ,Gianfranco. **Dicionário de política: V I**.; trad. Carmem C, Varriale. Tradução. João Ferreira; ver. geral João Ferreira e Luis Guerreiro Pinto Cacais. 1.ed. - Brasília: Editora Universidade de Brasília, 1998;

BRASIL. [Constituição (1937)]. **Constituição dos Estados Unidos do Brasil**, Rio de Janeiro, RJ: Getúlio Vargas. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao37.htm. Acesso em: 01 out. 2019.

BRASIL. **LEI n.º 8.072, de 25 de julho de 1990**. Dispõe sobre os Crimes Hediondos, nos termos do art. 5º, inciso XLIII, da Constituição Federal, e determina outras providências. Brasília, DF: Fernando Collor. DOU de 26.7.1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8072.htm. Acesso em: 02.out. 2019.

BRASIL. **LEI nº 13.260, de 16 de março de 2016**. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Dilma Rousseff. DOU de 17.3.2016 - Edição extra e retificada em 18.3.2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13260.htm. Acesso em: 29 out. 2019.

BRASIL. **LEI 7.170, de 14 de dezembro de 1983**. Define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências. Brasília, DF: João Figueiredo. DOU de 15.12.1983. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7170.htm. Acesso em: 02. Out. 2019.

BRASÍLIA. **Decreto n.º 314/1967, de 13 de março de 1967**. Define os crimes contra a Segurança Nacional, a ordem política e social e de outras providências. Revogado pelo DEL 898 – 29/09/1969. Lex – Brasília. Revogado pelo Decreto-Lei n.º 898, de 1969. Brasília, DF:H. Castello Branco. DOU de 13.3.1967. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/1965-1988/Del0314impressao.htm. Acesso em: 30 set. 2019.

BREVES ESCRITOS INTERNACIONAIS. **A Revolução Islâmica – O Incêndio de Abadan**. Publicado em: 17 abril 2008. Disponível em: http://brevesescritosinternacionais.blogspot.com/2008/04/revoluo-islmica-o-incndio-de-abadan.html. Acesso em: 30 out. 2018.

BUNDE, Mateus. Al Qaeda. Disponível em: https://www.todoestudo.com.br/historia/al-qaeda Acesso em: 15 out 2018.

BULCÃO, Luís. **A segurança da Rio+ 20: o inimigo agora é outro**. VEJA.com; Net, Rio de Janeiro,RJ. 25 mar 2012. Disponível em: http://memoriadasolimpiadas.rb.gov.br/jspui/bitstream/123456789/187/1/SG070%20-%20VEJA_%202012-03-25%20A%20seguranca%20da%20Rio20%20-%20o%20inimigo%20agora%20e%20outro.pdf. Acesso em: 31 out 2019.

CHAGAS, Morgana Santos das. **Ciberterrorismo: as possibilidades da expansão do terror nas relações internacionais**. 2012. 52f. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Universidade Estadual da Paraíba, João Pessoa, 2012.

CRENSHAW, M. **O terrorismo visto como um problema de segurança internacional**. In: HERZ, M.; AMARAL, A. B. (Org.). Terrorismo e relações internacionais. Rio de Janeiro: PUC-Rio; Loyola, 2006.

DUFFY, Michael. **Who's Who – King Alexander I**. Publicado em 22 ago. 2009. Disponível em: https://www.firstworldwar.com/bio/alexander_serbia.htm. Acesso em 01 out. 2019.

FRAGOSO, Heleno Claudio. **Terrorismo e criminalidade política**. Rio de Janeiro: Editora Forense, 1981;

FRAGOSO, Heleno Cláudio**, Lições de direito penal: parte geral**. 11. ed. rev. Fernando Grasoso. – Rio de Janeiro: Forense, 1987;

INLEARN. **Conheça os ataques cibernéticos que mais crescem no momento**. Publicado em: 23 jan. 2019. Disponível em: https://www.inlearn.com.br/seguranca-da-informacao-ataques-ciberneticos/. Acesso em: 01 out. 2019.

JÚNIOR, Vladimir Vitti. **Análise da lei antiterrorismo (13.260/2016).** Revista Direito e Sociedade. v.4, nº 1. São Paulo: Universidade Zumbi dos Palmares, 2016

KAMINSKI, Omar. A Internet e o ciberespaço. **Revista Jus Navigandi**. Teresina, ano 5, n. 46, 1 out. 2000. Disponível em: https://jus.com.br/artigos/1770. Acesso em: 22 out. 2018.

LEMOS, André. **Ciberurbe:** A Cidade Na Sociedade da Informação. E-Papers Serviços Editoriais Ltda.; Edição 1. 2005 p. 251-267.

LUTZ, Luciano Stumpf. **Terrorismo, direito penal do inimigo e complexidade: sobre os limites e as possibilidades do direito e da ciência jurídica na definição do terrorismo**. 2014, 142 f. (Mestrado em Direito). Universidade Vale do Rio dos Sinos. São Leopoldo, 2014;

LIMA, Jonas. **O Impacto do Terrorismo nas Cadeias Globais de Abastecimento**. Ed. Universidade do Porto, 2006.

MAGNO, Italo. **Massacre de Munique: o atentado que marcou os Jogos Olímpicos**. Publicado em 05 dez. 2013. Disponível em: http://www.museudeimagens.com.br/massacre-de-munique/. Acesso em: 04 out. 2019.

MARTINES, Fernando. **Presos na operação hashtag são condenados com base na Lei de Terrorismo**. Publicado em 04 mai. 2017. Disponível em: https://www.conjur.com.br/2017-mai-04/presos-operacao-hashtag-sao-condenados-lei-terrorismo. Acesso em: 31 out 2019.

NATIONAL RESEARCH COUNCIL. **Terrorism**: **Perspectives from the Behavior and Social Sciences**. Washington: The National Academies Press, 2001.

NEOLIBERALISMO. In: **DICIO**, Dicionário Online de Português. Porto: 7 Graus, 2019. Disponível em: https://www.dicio.com.br/neoliberalismo/. Acesso em: 04 nov 2019.

NEW YORK TIMES. Al Qaeda Usa A Internet para Propagar sua Ideologia. **G1 Mundo**. 03/10/2006. Disponível em: http://g1.globo.com/Noticias/Mundo/0,,AA1296373-5602,00-AL+QAEDA+USA+A+INTERNET+PARA+PROPAGAR+SUA+IDEOLOGIA.html. Acesso em: 29 out. 2019.

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

Os atentados em Nova York e os interesses internacionais do Brasil/ Centro de Integração Empresa-Escola. – São Paulo: CIEE, 2002.

PARANÁ. 14ª Vara Federal de Curitiba. AÇÃO PENAL Nº 5046863-67.2016.4.04.7000/PR. Disponível em: https://www.conjur.com.br/dl/presos-operacao-hashtag-sao-condenados.pdf. Acesso em: 02 nov. 2019.

REDAÇÃO SUPER. O WikiLeaks é só o começo. Da Redação. Vinícius Querobino e Alexandre Versignassi. (27 jan. 2011) Disponível em: https://super.abril.com.br/cultura/o-wikileaks-e-so-o-comeco/. Acesso em: 24 out. 2018.

RELATIVAMENTE INTERESSANTE. **10 Organizações Terroristas Das Quais Pode Não Ter Ouvido Falar**. 8 de julho de 2015. Disponível em: http://www.relativamenteinteressante.com/2015/07/10-organizacoes-terroristas-das-quais.html. Acesso em: 05 nov. 2018.

R7. **Al Qaeda recruta homens-bomba pela internet**.. Disponível em: http://noticias.r7.com/internacional/noticias/al-qaeda-recruta-homens-bomba-pela-internet-20120606.html. Acesso em: 20 out 2018.

SANTANA, Ana Lucia. Hezbollah. Disponível em: https://www.infoescola.com/historia/hezbollah/. Acesso em: 17. out. 2019

SCHMID, Alex P. **The Routledge Handbook Of Terrorism Research**. 1. ed. Estados Unidos: Routledge Taylor & Francis Group, 2011.

SILVA, Paulo Quintiliano da. Crimes cibernéticos e seus efeitos internacionais. In: **Proceedings of the International Conference of Forensic Computer Science**. p. 10-14.

SHIMEALL, Tim. Cyber Terrorism. CERT Centers, Software Engineering Institute. Pittsburg, PA, 2002. In LIMA, Jonas. **O Impacto do Terrorismo nas Cadeias Globais de Abastecimento**. Ed Universidade do Porto, 2006. Disponível em: http://dspace.bc.uepb.edu.br/jspui/bitstream/123456789/11089/1/PDF%20-%20Morgana%20Santos%20das%20Chagas.pdf>. Acesso em: 25 out. 2018.

SOUZA, André de Mello e; NASSER, Reginaldo Mattar; MORAES, Rodrigo Fracalossi de (Orgs.). **Do 11 de setembro de 2001 à guerra ao terror:**reflexões sobre o terrorismo no século XXI. Brasília, DF: IPEA, 2014. 186p. ISBN 978-85-7811-195-3.

SUTTI, Paulo; RICARDO, Sílvia. **As diversas faces do terrorismo**. São Paulo: Editora HARBRA, 2003.

TAGIAROLI, Guilherme. **Grupo Hacker LulzSec derruba site da Presidencia e do Governo do Brasil**. Publicado em 22 jun. 2011. São Paulo, SP. Disponível em: https://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/06/22/grupo-hacker-lulzsec-derruba-site-da-presidencia-e-do-governo-do-brasil.jhtm. Acesso em: 12. Ago. 2018.

TERRORISMO *In:* Conceito de. Disponível em: https://conceito.de/terrorismo. Acesso em: 10 out. 2018.

WALZER, Michael (2000). **Just and Unjust Wars: A Moral Argument with Historical Illustrations**. New York: Basic Books.

WEIMANN, Gabriel (2004) **Ciberterrorismo: A soma de todos os medos ?, Estudos em Conflito e Terrorismo**, 28: 2, 129-149, DOI: 10.1080 / 10576100590905110. Disponível em: https://www.usip.org/publications/2004/05/cyberterrorism-how-real-threat. Acesso em: 30 out 2018.

WELLS, Giorgia. **Estado Islâmico usa app TikTok para espalhar propaganda do grupo terrorista**. Folha de São Paulo. São Paulo, 22. Out. 2019. Disponível em: https://www1.folha.uol.com.br/mundo/2019/10/estado-islamico-usa-app-tiktok-para-espalhar-propaganda-do-grupo-terrorista.shtml?utm_source=twitter&utm_medium=social&utm_campaign=twfolha. Acesso em: 28 out. 2019.

WOLOSZYN, André Luís. **Aspectos gerais e criminais do terrorismo e a situação do Brasil.** Disponível em: http://www.amprs.org.br/arquivos/revista_artigo/arquivo_1273861260.pdf. Acesso: em 12 set. 2019.

WHITTAKER, Zack. **Hackers are spreading Islamic State propaganda by hijacking dormant Twitter accounts** 02 jan. 2019. Disponível em: https://techcrunch.com/2019/01/02/hackers-islamic-state-propaganda-twitter/. Acesso em: 10 set. 2019.

ZORZETTI, C. Alexandre T (2015): **Mão negra, o grupo terrorista da unidade sérvia que assassinou Francisco Ferdinando**. Disponível em: https://wp.me/p4uypD-5F Acesso em: 16 out 2019.