UNIVERSIDADE ESTADUAL DA PARAIBA
CAMPUS V – MINISTRO ALCIDES CARNEIRO
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
BACHARELADO EM RELAÇÕES INTERNACIONAIS

MORGANA SANTOS DAS CHAGAS

CIBERTERRORISMO: AS POSSIBILIDADES DA EXPANSÃO DO TERROR NAS RELAÇÕES INTERNACIONAIS

JOÃO PESSOA - PB
2012

MORGANA SANTOS DAS CHAGAS

CIBERTERRORISMO: AS POSSIBILIDADES DA EXPANSÃO DO TERROR NAS RELAÇÕES INTERNACIONAIS

Monografia apresentada ao Curso de Bacharelado em Relações Internacionais da Universidade Estadual da Paraíba - UEPB, em cumprimento à exigência para obtenção do grau de Bacharel.

Orientador: Prof. Dr. Paulo Roberto Loyolla Kuhlmann – UEPB

João Pessoa – PB
2012

F ICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA SETORIAL CAMPUS V – UEPB

C426c Chagas, Morgana Santos das.
Ciberterrorismo: as possibilidades da expansão do terror nas relações internacionais. / Morgana Santos das Chagas. – João Pessoa, 2012.
52f

Digitado.
Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) – Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, Curso de Relações Internacionais, 2011.
"Orientação: Profº. Dr Paulo Roberto Loyolla Kuhlmann, Curso de Relações Internacionais".

1. Terrorismo. 2. Ciberterrorismo. 3. Relações internacionais. 4. Tecnologia. I. Título.

21. ed. CDD 327.810960

UNIVERSIDADE ESTADUAL DA PARAÍBA

CURSO DE BACHARELADO EM RELAÇÕES INTERNACIONAIS

FOLHA DE DEFESA COM OS MEMBROS DA BANCA

ALUNO(A): MORGANA SANTOS DAS CHAGAS
MATRÍCULA: 072526416

CIBERTERRORISMO: AS POSSIBILIDADES DA EXPANSÃO DO TERROR NAS RELAÇÕES INTERNACIONAIS

Monografia apresentada ao Curso de Relações Internacionais da Universidade Estadual da Paraíba.

Professor(a) Paulo Roberto Loyolla Kuhlmann (Orientador(a)) - UEPB

Professor(a) Gabriela Gonçalves Barbosa - UEPB

Professor(a) Ana Paula Maielo Silva - UFPB

João Pessoa, 29 de junho de 2012.

DEDICATÓRIA

Aos meus pais e heróis: Marinalva e Evanderly.

AGRADECIMENTOS

Ao meu paizão Deus, sempre fiel e misericordioso. À Jesus Cristo, minha inspiração, meu salvador, meu tudo. Ao Santo Espírito por andar sempre ao meu lado me guiando e protegendo. Aos três agradeço pela vida.

À minha mãe e amiga Marinalva, que chora comigo na angústia e pula na alegria. Se não fosse por ela eu não estaria nem perto dessa conquista. Agradeço por ter sempre lutado por mim e pelo exemplo que ela é. Com ela aprendi a levantar sempre que caio, "pois só não cai quem já está no chão". Agradeço também ao meu pai Evanderly, que sempre me apoia em tudo que faço. Obrigada pelas caronas até a universidade e por sempre acreditar em mim. Ambos são guerreiros que lutam diariamente pela minha vida e à eles eu sou eternamente agradecida.

Ao meu orientador e excelente professor Paulo Kuhlmann que aceitou me ajudar nesta conquista e também por toda bibliografia me fornecida. À ele sou muito agradecida; o admiro como pessoa e professor. Agradeço também a professora Ana Paula, gente finíssima, que muito me ajudou me emprestando livros e por ter aceito de imediato fazer parte da banca. Também agradeço a professora Gabriela Gonçalves por aceitar este desafio.

À toda minha família. Em especial meus tios Sandro e Evaldo que penteavam meu fuá pra que eu fosse pra escola bonita (infelizmente agora ninguém faz mais isso e eu vou assanhada mesmo), além de fazerem aviãozinho sempre aos almoços (olha o meu tamanho agora!). À minha tia Evania por me acompanhar desde antes de eu nascer e estar sempre ao meu lado nas conquistas juntamente com seu esposo Marquinho. À minha tia Dôra por avisar em um diálogo há quase 17 anos que eu deveria ir à escola mesmo já sabendo o "ABC". À Tânia, pelo carinho e preocupação em saber se eu me alimentava durante a elaboração deste trabalho.

Ao Aurélio (caba véi fêi) que tanto me ajudou e torceu por mim, para que eu concluísse esse curso. Valeu por ter aguentado meu abuso diário e por ter estado sempre junto nas dificuldades que surgiam. Aos meus colegas Jane Eyre, Alexandre, Wemblley, Lídia Bruna, Suênia, Manú, Emilayne, Wesley e Amanda Salazar pelas boas gargalhadas. Thanks to Jonathan Salomon for the help. À Adriana e Dona Fátima por estarem sempre presentes como parte da família. Aos amigos e irmãos Sandra e Nicó pelas batalhas que juntos lutamos. E a todos que de alguma forma acrescentaram algo em minha vida.

“São mais felizes os que já morreram do que os que ainda vivem. Melhor do que ambos é aquele que ainda não nasceu, aquele que não viu as obras más que se fazem debaixo do sol. Vi que todo trabalho e toda obra que o homem executa causa inveja do seu próximo. Isso também é vaidade e aflição de espírito.”

(Ec. 4.1-4)

RESUMO

Com pouco mais de dois bilhões de usuários, a internet cresce e evolui rapidamente tornando o mundo físico cada vez mais envolvido e adaptado às maquinas. Porém, a internet é apenas uma das tantas outras ferramentas que operam no ciberespaço. A modernização trouxe praticidade, comunicação instantânea, entre outros, ultrapassando as fronteiras entre os Estados e o que consta entre elas. Apesar dos benefícios trazidos pela tecnologia à sociedade, a segurança é algo ainda em ameaça, pois os ciberataques se tornam cada vez mais comuns, evidenciando a possibilidade da expansão do terrorismo através dos mesmos. Em razão disso, o presente estudo visa analisar o ciberterrorismo enquanto uma grande possibilidade de ameaça real à Segurança Internacional nos dias atuais.

Palavras-chave: terrorismo, ciberterrorismo, relações internacionais, tecnologia

ABSTRACT

The world has just over 2 billion Internet users globally and is growing and evolving rapidly. Due to this the physical world is increasingly adapting and involving with machines. However, the internet is just one of many other tools that operate in cyberspace. The modernization has brought convenience, instant communication, among others, crossing the boundaries between States and between what is in it. But despite the benefits brought to society by technology the security is still threated because cyber-attacks are becoming more common and it has shown the possibility of expansion of terrorism therethrough. Because of it, this study aims to analyses cyber-terrorism as a strong possibility of a real threat to international security today.

Keywords: terrorism, cyber-terrorism, international relations, technology

SUMÁRIO

INTRODUÇÃO.....10

CAPÍTULO I - TERRORISMO: História, Tipologia e Definições.....12

1.1 O Terrorismo Na História 12

1.1.1 Terrorismo Pré-Moderno 12

1.1.2 Terrorismo Moderno 13

1.1.3 Pós 11 de Setembro 16

1.2 Definições 17

1.2.1 11 de Setembro, Choque de Civilizações? 21

1.3 Classificação Tipológica Do Terrorismo 22

1.3.1 Neo-terrorismo 24

1.4 Visão não-ocidentalista 25

1.5 Considerações 26

CAPÍTULO II - CIBERTERRORISMO: Possibilidades do acontecimento de ataques em grande escala e as mudanças trazidas por essas possibilidades à Comunidade Internacional.....28

2.1 Entendendo o Ciberterrorismo 28

2.1.1 Definições 29

2.1.2 Ciberespaço: como atua o ciberterrorismo 31

2.2 Ciberterrorismo: Por quê? 32

2.2.1 As possiblidades de ataques em grande escala 35

2.2.2 O caso da Estônia 40

2.2.3 As duas principais mudanças trazidas pela possibilidade do acontecimento do ciberterrorismo à comunidade internacional 42

Considerações finais.....**45**

Bibliografia.....**47**

Glossário.....**52**

INTRODUÇÃO

A revolução da tecnologia da informação - que segundo Furtado (2002), é todo recurso tecnológico e computacional destinado à coleta, manipulação, armazenamento e processamento de dados e/ou informações dentro de uma organização - constituiu-se nos EUA, difundiu-se pela cultura libertária cultivada nos anos 1960, mas foi na década de 1970 que um novo paradigma constituiu-se quando houve a interação entre os EUA, a economia global e a geopolítica mundial, que trouxe um novo estilo de produção, comunicação, gerenciamento e vida. Esta década foi marcada por estar relacionada, neste segmento, à liberdade de expressão, iniciativa empreendedora e inovação individual, diferente das décadas anteriores. Porém, quando esta se espalhou para Estados de culturas, organizações e objetivos diferentes, isso resultou na sua utilização em diferentes aplicações desta tecnologia (CASTELLS, 1999, p. 43).

A internet em si, originou-se nos anos 1960, como um aparato militar (assim como o computador) produzido pela Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos (DARPA – Defense Advanced Research Projects Agency). Tinha a princípio, o objetivo de impedir que a URSS tomasse ou destruísse os meios de comunicação da América do Norte em caso de uma possível guerra nuclear. Mais tarde, a internet foi compartilhada no mundo inteiro. A arquitetura da mesma foi baseada de maneira que não houvesse um centro de controle de comando, mas que fosse composta por milhares de computadores autônomos com inúmeras formas de conexão, contornando barreiras eletrônicas (id., 1999, p. 44). Por conta desta arquitetura, os Estados mais desenvolvidos que dependem do uso de redes sofrem com riscos ocasionados pela possibilidade de ataques. Quanto maior a "tecnodependência", pior o "*backfire*", ou seja, a capacidade dessa tecnologia voltasse contra si.

Os anos de 1990 foram marcados pela utilização destas novas tendências tecnológicas cultivadas desde a década de 1960. A exemplo, a internet, fruto da tecnologia desenvolvida nos anos 1960, teve um papel instrumental no crescimento da seita chinesa Falun Gong, que desafiou o partido comunista da China em 1999. A mesma também difundiu o protesto contra a Organização Mundial do Comércio (OMC) em Seattle neste mesmo ano. O subcomandante Marcos, líder dos zapatistas de Chiapas (movimento contra o regime autocrático de Porfirio Díaz, que encadeou a Revolução

Mexicana), estabeleceu comunicação com o mundo todo e com a mídia também através da rede. (CASTELLS, 1999, p. 44). O uso da internet para fins de propaganda pelo movimento zapatista mexicano foi tão bem-sucedido que os militares norte-americanos transformaram em exemplo numa cartilha para estudos acerca da internet e fizeram dele a base de sua estratégia contra os ciberterroristas, pois assim como este movimento espalhou sua ideologia e conseguiu audiência através da internet, os ciberterroristas também podem fazer (MATTELART, 2003, p. 131 apud KUMAR, 1997. p. 242).

A crescente dependência da tecnologia pela sociedade torna possível para grupos de crime organizado e ciberterroristas a realização de sérios danos na economia e na segurança dos Estados. “Quanto mais nos tornamos tecnologicamente sofisticados, mais somos alvos vulneráveis de possíveis ataques” (GORI; PAPARELA, 2006, p. 5). O ciberterrorismo é uma oportunidade para que terroristas, através da utilização de ferramentas tecnológicas cause danos à sociedade de modo geral, pois este fenômeno visa expandir o terrorismo tradicional ao ciberespaço e assim abranger a esfera global de maneira mais eficaz para a realização do terror.

Tendo em vista as possibilidades do acontecimento de ataques ciberterroristas, principalmente em grande escala, este estudo tem como objetivo analisar as divergências sobre o terrorismo e debates sobre o ciberterrorismo, assim como os riscos de sua ocorrência. O mesmo foi dividido em duas partes: no capitulo 1, serão abordados a história, tipologia e definições acerca do terrorismo, bem como seu impacto trazido às relações internacionais; no capitulo 2, a argumentação é construída em torno do ciberterrorismo (uma extensão do terrorismo que vem tomando espaço nas discursões atuais sobre segurança internacional), suas definições, o plano em que atua e as mudanças decorrentes do possível acontecimento desse fenômeno. A metodologia qualitativa foi utilizada para o desenvolvimento deste trabalho.

CAPÍTULO I

TERRORISMO: História, Tipologia e Definições

Perante o ciberterrorismo, assunto este presente nas últimas discussões sobre segurança internacional, é de tamanha necessidade que entendamos o que é terrorismo. Por isso, argumentarmos sobre o mesmo é de extrema importância para o presente trabalho.

1.1 O Terrorismo Na História

É quase impossível argumentar sobre terrorismo, sem discutir o contexto histórico da campanha terrorista. É interessante que uma pequena e simples retrospectiva dos acontecimentos ocorridos ao longo da história sejam relembrados para que possamos observar as devidas modificações do terrorismo quanto aos objetivos; às diferentes maneiras de causar terror; aos lugares dos acontecimentos e às causas. Assim como também perceber que não é um problema surgido no nosso século, mas muito antes. A divisão se baseia na separação histórica feita por White (2012) e os exemplos citados abaixo foram fatos classificados para melhor exemplificar esta separação histórica, portanto, não é defendido aqui que todos estes foram os principais fatos na história do terrorismo, pois não convém a este estudo avaliá-los como tais ou estudar um ou mais casos neste capítulo, nem os precursores do terror ou a natureza dos propósitos adotados, mas situar o leitor no assunto.

1.1.1 Terrorismo Pré-Moderno

Sean e Stephen (2009) em sua cronologia sobre o terrorismo cita que nos anos de 66 a 70 d.C., o movimento judeu político-religioso denominado "Zelota" revolta-se contra a dominação romana rejeitando o pagamento de tributo dos israelitas à um imperador pagão, levando à destruição de Jerusalém pelos romanos, do Segundo Templo (por conta da invasão romana) e o suicídio em massa[1] dos zelotas. Adagas foram utilizadas como arma na luta deste grupo de judeus extremistas para promover

[1] Para não serem pegos, estes cometeram suicídio em massa.

execuções e suicídios na estratégia política para se desprender das obrigações implicadas pelos romanos, ou seja, do pagamento dos tributos; e por isso, este instrumento tornou-se naquela época um símbolo de terror, mais tarde adotado pelos assassinos de encomenda (HOBSBAWM, 2007, p. 123). Comparando aos dias de hoje, estes judeus extremistas seriam como os atuais homens-bomba, pois, os mesmos utilizavam-se de suas adagas em lugares públicos lotados para assassinar e assim, promover o terror. Segundo Zalman (2010), o movimento era o mesmo, porém os chamados sicários (homens da adaga) costumavam atacar judeus notáveis e elites associadas ao sacerdócio que concordavam e até colaboravam com a imposição romana, distinguindo-se dos chamados zelotas, que visavam a sua violência contra os romanos. M. Hengel (1989 apud SELAND, 1995, p. 217) afirma que "Zelota" era o movimento judeu que abraçava todas as atividades revolucionárias praticadas pelos judeus nesse período. Porém, não cabe a este estudo uma análise mais detalhada das diferenças entres tais grupos, mas sim, a observância de suas ações e táticas terroristas. Eis abaixo uma tradução livre da citação de Hosley, em seu artigo *The Sicarii: Ancient Jewish "Terrorists"*:

> (...) um tipo diferente de bandido surgiu em Jerusalém, os denominados sicários, que mataram homens em plena luz do dia no coração da cidade. Especialmente durante festivais, pois estes se misturavam com a multidão, levando adagas escondidas sob suas roupas, com a qual esfaqueavam seus inimigos. Então, quando os inimigos caíram, os assassinos participavam dos gritos de indignação e, através deste comportamento plausível, evitavam serem descobertos. (HORSLEY, 1979, p. 436)

Não apenas este movimento judeu é exemplo de terrorismo pré-moderno, podemos citar a Ordem dos Assassinos (Isma'ili Fedayeen), pois conduziram uma campanha de terror contra o império islâmico Abássidas durante 1090–1256; o terrorismo feito pelo czar Ivan IV, durante 1530 – 1584, que ficou conhecido como "o terrível" por suas ações, pois o ele torturava, bania e a executava quem conspirasse contra ele; entre outros (ANDERSON; SLOAN, 2009, p. 29).

1.1.2 Terrorismo Moderno

O terrorismo moderno é considerado por Laqueur (1999) a forma tradicional do terrorismo. White (2012) afirma que o terrorismo moderno se originou em meados da Revolução Francesa (1789 - 1799). Era um termo para descrever as ações do governo francês, como por exemplo, a medida tomada pelo Comitê de Salvação Pública, em

maio de 1793, que comprometia o expurgo de inimigos por suspeita de revolução, liderando 300.000 detenções arbitrárias e 17.000 execuções.

Em 1848, o significado do termo mudou, sendo usado para descrever revolucionários violentos que se revoltaram contra os governos (WHITE, 2012). Do final de 1800 até o início de 1900, o terrorismo foi usado para descrever as atividades violentas de vários grupos, incluindo organizações de trabalhadores, anarquistas, grupos nacionalistas que se revoltaram contra as potências estrangeiras, e organizações políticas ultranacionalistas. Eis alguns exemplos: em Março de 1881, o grupo revolucionário Narodnaya Volya, conhecido como "A vontade do povo" (grupo revolucionário russo contrário ao regime), implantou uma bomba na carruagem do czar Alexandre II. No dia 4 de Maio de 1886, na Praça Haymarket, em Chicago, enquanto 180 policiais confrontavam 1.300 trabalhadores que protestavam para trabalharem oito horas por dia, uma bomba explodiu matando oito e ferindo muitos outros. Em 01 de outubro de 1910, durante uma greve, o edifício sede do sindicato *Los Angeles Times* foi dinamitado e entrou em chamas; pelo menos 20 morreram. O assassinato que repercutiria na mudança da história mundial, ocorrido em 28 de junho de 1914, do arquiduque austríaco Francisco Ferdinando em Sarajevo na Bósnia, desencadeara a primeira Guerra Mundial. Nos anos 1920, Michael Collins empregou métodos de terror em prol da causa nacionalista irlandesa. Mais tarde, por volta dos anos 1930, Stalin adotou uma grande campanha de terror político para dirigir a União Soviética – URSS (ANDERSON; SLOAN, 2009, p. 29-31).

Após a Segunda Guerra Mundial (1939-1945), ainda segundo White (2012), o significado de terrorismo mudou novamente. As pessoas começaram a se revoltar contra a dominação europeia no mundo e assim fora dada mais ênfase nos grupos nacionalistas, que eram vistos como grupos terroristas. Hobsbawm (2007) destaca três grandes episódios do surgimento da violência: o primeiro, denominado de neoblanquismo, ocorrido entre as décadas de 1960 e 1970, se caracterizou por grupos pequenos de elites que tentaram derrubar regimes ou alcançar objetivos nacionalista-separatistas por meio da luta armada, como ETA, Brigadas Vermelhas, entre outros. Para Hobsbawm (2007), o segundo episódio do surgimento da violência se caracteriza mais pela ideologia ética e religiosa, expandiu-se no fim dos anos 1970 e consolidou-se nos anos 1980, em razão dos chamados "grupos de ódio" - que praticam a violência contra membros de uma raça, etnia, religião, sexo, orientação sexual, profissão, etc. - e da Revolução Iraniana; e é a partir desta época que foi categorizado o inicio do que é

entendido atualmente como "terrorismo religioso"[2]. Também nesta época, o terrorismo foi associado à tomada de reféns. Esse momento marca uma nova "estrutura" do terrorismo, com a utilização de ferramentas e meios que propagam com maior eficácia o terror; como o terrorismo suicida dos homens-bomba, descrito por Hobsbawm (2007) a seguir:

> Tem origem como uma derivação da revolução iraniana de 1979, impregnado da poderosa ideologia islâmica xiita, que idealiza o martírio, e foi empregado pela primeira vez com objetivo de produzir efeitos decisivos em 1983, contra os americanos, pelo Hezbollah, no Líbano. Sua eficácia foi tão clara que a prática se estendeu aos Tigres Tâmeis em 1987, ao Hamas em 1993 e à Al Qaeda e outros grupos extremistas islâmicos na Caxemira e na Chechênia entre 1998-2000 (HOBSBAWM, 2007, p 130 – 131).

Na ilha Sri Lanka, constituída por cingaleses budistas que formam 75% da população, e por uma minoria tâmil, constituindo os outros 25%, a violência eclodiu rapidamente, apesar de tanto os cingaleses (budistas) quanto tâmeis (hinduístas) terem ideologias que se opunham à violência. Após a independência o país seguiu a ideologia socialista que resultou numa boa expectativa de vida e bem-estar perante o padrão asiático até antes dos anos 1970. Porém, por motivos seculares de outrora - como a troca da língua inglesa pelo cingalês como idioma oficial partindo do conceito de superioridade racial - um movimento separatista surgiu disseminado pelo ressentimento dos tâmeis, em 1970. Segundo Hobsbawm (2007), estes pioneiros do movimento separatista no Sri Lanka - organização armada antecessora do atual grupo de libertação "Tigres Tâmeis" (que luta desde 1980) - são provavelmente os maiores realizadores de operações "homem-bomba" no mundo. Além disso, um movimento baseado nas ideias castristas e no maoismo surgiu na ilha, no fim dos anos 1960, por causa de um grupo de jovens desempregados (em sua maioria cingalesa) e esquerdistas que procuravam melhores empregos e que tinham grande ressentimento contra a velha elite sociopolítica. Estes jovens organizaram uma mal sucedida insurreição, levando posteriormente ao surgimento de uma organização militante e terrorista que o autor vem a descrever como "uma organização baseada no campo e que modulava o maoismo original com um apaixonado e exagerado patriotismo cingalês racista e budista". Esse grupo, mais tarde em 1980, utilizou-se do terror para dominar aldeias e vilas e desencadeou uma campanha de assassinatos sistemáticos contra adversários políticos (HOBSBAWM, 2007, p. 122-123).

[2] Ver tópico 1.3 deste estudo.

O aumento da violência politica desde então, segundo Hobsbawm (2007), foi notável e o surto de violência politica pode acontecer em países com tradição de não violência politica e social como o Sri Lanka. Ainda para o autor, os grupos pequenos têm aterrorizado com assassinatos indiscriminados, prática essa ignorada por movimentos mais antigos e evitadas por movimentos como ETA e IRA. Ao contrario dos neoblanquistas, a maioria dos grupos ativistas tinham o apoio popular, como o Hamas, Hezbollah, Jihad Islâmica da Palestina, entre outros. Além do apoio popular, havia uma fonte permanente de recrutamento, o que ocasionava a não prática do terror individual por esses movimentos, obviamente, com exceções (quando essa era a única resposta ao poder militar esmagador do Estado ocupante ou em guerras civis cujo armamento era desequilibrado). Para White (2012), até então, o terrorismo era visto como um conflito subnacional.

1.1.3 Pós 11 de Setembro

À medida que o milênio virou, as definições do terrorismo mudaram mais uma vez e surgimento de novos conceitos no meio acadêmico eclodiu (WHITE, 2012, p. 8). O que antes era visto como subnacional passou a ser tratado de forma diferente, como um assunto global. O terceiro episódio do aumento da violência desacatado por Hobsbawm (2007), cuja fase predomina no início do século atual, é a fase onde a violência tornou-se global, a exemplo da Al Qaeda, cujo movimento é descentralizado, na qual as células não precisam de apoio nem base territorial.

Os atentados de 11 de Setembro representaram a passagem para o terrorismo pós-moderno e modificaram o cenário internacional em razão da ameaça à paz e a segurança que há tanto tempo vem tentando ser estabelecida. Esse fato trouxe mudanças na agenda internacional, assim como influenciou o surgimento de novas variáveis de estudos comprometendo este campo. Foi a partir desta data que o terrorismo fundamentalista islâmico passou a receber tamanha, senão, quase que total atenção. E deste então, a palavra “terrorismo” passou a ser relacionada (pelos ocidentais) aos acontecimentos desta data e à fé islâmica em sua forma fundamentalista. Não se pode negar que a repercussão dos atentados da Al Qaeda obteve a atenção do mundo, assim como o aterrorizou, sendo até mesmo considerado o maior atentado terrorista da história (DYSON, 2008, p. 3).

Tanto a história das relações internacionais como o pensamento para com futuro dela mudou, pois as velhas regras do estadismo, da guerra e da diplomacia têm sido inoperantes diante dos terroristas. Para Derian (2002), a própria escala, âmbito e impacto causado pelos ataques são parcialmente responsáveis pela escassez, bem como a pobreza da resposta pelo campo das Relações Internacionais e, o choque causado pelos atentados mostra que é ilusão por parte dos americanos acharem que são imunes, de alguma maneira, ao terrorismo, que por sinal atormenta muitos outros países. A diferença entre os dois ataques às Torres Gêmeas, o primeiro em 1993 - no dia 26 de fevereiro, cujo World Trade Center foi danificado quando um carro-bomba plantado por terroristas islâmicos seguidores de Sheikh Omar Abdul Rahman, um líder exilado de um grupo fundamentalista islâmico egípcio que pregou na área de Nova York na época do atentado, em uma das garagens subterrânea explodiu deixando seis mortos e cerca de mil feridos (WEINBERG; EUBANK, 2006, p. 1) - e o segundo em 2001, é que o último desafiou a imaginação pública, a capacidade intelectual da comunidade, burlou leis federais, a segurança dos aeroportos, a inteligência militar e ainda as agencias governamentais. Foi realmente chocante e surpreendente, além de representar uma "porta aberta" para a imensidão da capacidade terrorista. Além disso, os atentados de 2001 marcam não apenas a imensidão dos ataques e a criação das políticas para conter o terrorismo, mas também os ciclos de violência desencadeados a partir desta data.

1.2 Definições

Terrorismo tem o significado bastante amplo, não é fácil contextualizar e defini-lo, pois não existe um conceito universal justamente pelo mesmo possuir diferentes raízes e motivações, sendo ainda considerado um fenômeno de antigas datas que vem se modificando ao longo do tempo, ou seja, sua definição também é influenciada pelo seu contexto histórico.

É um fator elementar a informação de que nenhuma definição dada neste presente trabalho é neutra, mas carrega em si o posicionamento dos autores que são, em sua maioria, pertencentes à sociedade Ocidental. A presente seleção de definições feita com posicionamentos ocidentalistas não foi proposital, mas provinda da falta de fontes orientais em línguas acessíveis para o desenvolvimento do mesmo.

O significado dado pela primeira vez ao termo "terrorismo" foi em 1798, descrito pelo dicionário da Academia Francesa como sistema ou regime de terror; mas

anteriormente a esta data, os Jacobinos já se definiam como terroristas, porém com um sentido considerado por eles positivo, mas não demorou muito para o termo ser associado à implicações negativas (LAQUEUR, 2001, p. 6). Para Derian (2002), a menos que os ataques forem firmemente situados em uma posição patriota, ideológica ou religiosa, é intelectualmente e politicamente difícil o significado de um conflito que não siga uma linha contínua, ou seja, defasado, com ciclos novos.

Ramsbotham e Woodhouse (2011) utilizam conceitos de Wallensteen (2003) e Wardlow (1982) para definir terrorismo. Wardlow (1982), afirma que o terrorismo é o uso ou ameaça do uso da violência por um individuo ou grupo para agir em favor ou em oposição à autoridade estabelecida, quando este ato é designado pra criar extrema ansiedade ou medo, induzindo efeitos em um grupo alvo, com propósito de coagir o grupo alvo a aderi às demandas políticas dos autores do terror. Já Wallensteen (2003) afirma que este termo tem sido recentemente usado para abranger diferentes condutas, tais como atividades criminais e bandidismo, bem como propósitos políticos tradicionais. E este é frequentemente direcionado contra civis, contra símbolos sociais e também governamentais.

Para Saint-Pierre (1996), um sul-americano que possui uma visão notavelmente diferenciada, 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 efeito do ato terrorista é justamente causar terror ou pavor incontrolável, sendo assim, o objetivo não é a vítima atingida diretamente pela ação, classificada pelo autor como vítima direta, mas os indivíduos que possuem ou que poderiam ser confundidos com aqueles que possuem algum elemento que os liga, ou seja, que os identificam à vítima. Estes indivíduos, o autor chama de vítimas indiretas, pois apesar de não terem sido atingidas diretamente, as mesmas se sentem expostas e vulneráveis a outros atentados por conta dessa identidade em comum. A eficácia do ato está no grau de identificação com a vítima direta. Para o autor, quando menos identificável seja a vítima direta, quanto mais geral e comum sejam suas características identificatórias, maior será o número de vítimas indiretas e, consequentemente, maior o objetivo atingido.

Porém, há outros casos cujo objetivo visado pode ser procurar uma identificação negativa, ou seja, “o oposto”, o considerado específico, cujas medidas táticas aplicadas levem à cumplicidade entre os terroristas que cometem o atentado e parte da população, resultando na realização de seus desejos de justiça ou de mera vingança. Para que seja

satisfatório o resultado neste caso de identificação, as características procuradas para identificar “o oposto”, o inimigo, devem ser claras e suficientemente conhecidas e odiadas por parte da população, pois são as mesmas que representarão "simbolicamente" a linha divisória entre os propagadores do terror e as vítimas. Assim, para o Saint-Pierre (1996), este tipo de ação procura atingir mais uma eficácia simbólica do que tática ou estratégica. Dentro deste argumento, o autor resgata as palavras de Guevara a respeito do terrorismo:

> O terrorismo deve ser considerado como fator valioso quando se o utiliza para justiçar algum renomado dirigente das forças opressoras, caracterizado pela sua crueldade, por sua eficiência na repressão, por uma série de qualidades que fazem de sua supressão algo útil (CHE Guevara. Esencia de la lucha, estrategia y táctica guerrilleras, p. 51-52 apud SAINT-PIERRE, 1996, p. 6).

Um exemplo da utilização do terror para identificar negativamente os atores envolvidos foram os atentados de 11 de Setembro protagonizados pela Al Qaeda. Os alvos selecionados simbolizavam o poderio dos EUA perante o mundo (e consequentemente seu imperialismo): o World Trate Center, simbolizava o poderio econômico; o Pentágono, o poderio militar; e a Casa Branca, o poderio político. Estes foram alvos estrategicamente escolhidos para representar melhor o sentimento por parte do grupo terrorista. Para Saint-Pierre, este tipo de atentado, exemplificado aqui pelos acontecimentos de 11 de Setembro, tem por objetivo chamar a atenção da opinião pública para despertar a simpatia de parte da população com relação à justiça da "causa" do grupo, da população para com o grupo ou simplesmente coagir o inimigo através do medo. Para o autor, o terrorismo tanto pode procurar impactar a opinião pública em geral, quanto pode visar apenas um grupo específico como alvo definido, constituindo o que o autor vem a chamar de "grupos de risco". Estes “grupos de risco” são o oposto dos “grupos de ódio”, ou seja, as vítimas deste último. “Grupos de risco” podem ser grupos religiosos, étnicos, de determinada classe social, funcionários do governo, militares, homossexuais, prostitutas, imigrantes, entre outros.

Depois de 11 de Setembro o governo dos Estados Unidos, Estado que mais propaga que o terrorismo deve ser detido, definiu terrorismo, obviamente segundo suas intenções de contra-ataque a este fenômeno, como violência politico-motivada praticada contra civis por um grupo subnacional ou agentes clandestinos que normalmente pretende influenciar o público. Ainda, o termo “grupo terrorista” significa grupos ou subgrupos que praticam terrorismo internacional (RAMSBOTHAM; WOODHOUSE,

2011, p. 82). Seixas (2008) traduz o conceito dado por Laqueur no livro "The New Terrorism": "[...] é o uso da violência por parte de um grupo para fins políticos, normalmente dirigido contra um governo, mas por vezes contra outro grupo étnico, classe, raça, religião ou movimento político". Já segundo Dyson (2008), o termo usado para definir terrorismo hoje em dia, é o de que o mesmo trata-se do uso extremo e ilegal da força e violência com o proposito de coagir uma entidade governamental ou população a fim de modificar sua filosofia e direção. Vejamos que o conceito de Laqueur (1999) e Dyson (2008) é condizente ao de Wardlow (1982), porém mais abrangentes.

Os atos terroristas podem ser utilizados para fins políticos ou não, podendo também ter fins econômicos, religiosos, entre outros. Um fato interessante acerca do fenômeno é que não é preciso o uso real da violência para aterrorizar. Há casos em que só a ameaça basta para chegar ao objetivo, por ser, muitas vezes, improvável determinar se é um blefe ou uma ameaça real (SAINT-PIERRE, 1996, p. 3).

Laqueur (1999) considera que terrorismo é violência, mas nem toda forma de violência é terrorismo. Para ele, chegar à conclusão definitiva do que se considera terrorismo conduz a conclusões equivocadas. Embora seja difícil de definir, é sempre visto negativamente sendo considerado, seja qual for a sua forma, moralmente errado. O autor argumenta ainda que terroristas se autoconsideram salvadores da liberdade e justiça de uma maneira psicologicamente insana, diferentemente dos rebeldes contra a real "tirania'.

O terrorismo diferencia-se de outros tipos de luta, segundo Saint-Pierre (1996), porque tem como objetivo principal a utilização do terror para conseguir um determinado fim. Em outras lutas, como a revolucionária, o terrorismo pode ser implementado, e assim agir de maneira complementar, secundária, mas nunca sendo o principal. O autor afirma que toda ação revolucionária é política, porém, nem toda ação terrorista é política. O terrorismo distingue-se também da sabotagem, cujo objetivo pode ser desestabilizar o governo que está no poder, seja nas suas bases administrativas, econômicas (com atentados contra indústrias, bancos, bolsas de valores, etc.) ou bases energéticas (atingindo hidrelétricas, poços de petróleo, entre outros); ou simplesmente desestabilizar a tropa inimiga, sabotando seus suprimentos, arsenais, linhas de comunicação, etc. Porém a grande diferença é que a sabotagem é geralmente utilizada como estratégia de guerra (podendo ser utilizada em conflitos já desencadeados).

No livro “Guerra Irregular”, Visacro (2009), também sul-americano, argumenta que há aquilo que é terrorismo de fato e o que chamamos de terrorismo. Para o autor, são dois conceitos distintos, sendo o primeiro, relacionado ao pragmatismo das organizações militantes que utilizam-se do recurso operacional do terror e importam-se apenas com os resultados relativo às ações terroristas. E o segundo, que dar-se a respeito do Estado e da sociedade civil, sendo este utilizado para certa utilidade política (por exemplo, terrorismo de Estado). Ainda para o autor, há a existência do terrorismo intitulado “autotélico”. Este carece de motivações politicas, religiosas ou ideológicas e geralmente está associado ao fenômeno do bandidismo, à segregação social, ao fanatismo de seitas radicais, e à disputa por poder local entre tribos e grupos étnicos distintos.

1.2.1 11 de Setembro, Choque de Civilizações?

Quando usamos o termo “choque de civilizações” estamos nos referindo ao que Samuel Huntington descreve como conflitos culturais entre as oito civilizações dominantes no mundo (Ocidental, Sínica, Japonesa, Islâmica, Hindu, Eslavo-Ortodoxa, Latino Americana e Africana) definidas por costumes, valores, comportamentos, estruturas sociais e sistemas econômicos; tendo a religião como um fator essencial na definição das mesmas. Huntington acredita que a paz internacional é alvo de ameaça por países divididos, ou seja, que compartilham diferenças desencadeando assim um choque.

Ao ver as imagens da queda das Torres Gêmeas e, posteriormente, o discurso do presidente norte-americano Bush Filho de conter esta ação, houve a ilusão por parte da população em se pensar que este quadro referia-se a uma guerra entre lado A e lado B, contra o bem e o mal, a Sociedade Ocidental contra a Oriental. Já em 1993, após o primeiro atentado ao World Trate Center, se afirmava que a tentativa norte-americana de fornecer a liderança (que eles consideram necessária) em um mundo fragmentado e propenso às crises poderia receber como resposta as atuações inimagináveis de terroristas (DERIAN, 2002). E por isso, resgatamos a ideia do choque de civilizações abordado por Huntington para analisar tal argumentação.

Para Baudrillard (2002), o terrorismo não se trata de um choque de civilizações ou de religiões, e vai muito além da dicotomia construída entre a América e o islamismo. Aqui vemos que, na verdade, a “inexistência” das fronteiras para o

terrorismo é fruto do próprio processo de globalização, que tem experimentado um gosto amargo de sua própria evolução. Chomsky (2006) rejeita a ideia do choque, pois, segundo ele, os acadêmicos e os políticos estão à procura de uma grande argumentação para explicar o conflito, mas o mundo é muito complicado e está em constante mudança para uma teoria ser simplesmente aplicada e validada. Além disso, os defensores do paradigma do choque de civilizações argumentam que os conflitos étnicos e culturais em erupção após o colapso da União Soviética são novos. Isso é incorreto de acordo com o autor, pois para ele os conflitos não são novos, a maioria antecedeu o fim da Guerra Fria: "dizer que um conflito surge assim de repente é errôneo, pois sempre há uma historia que explique o desencadeamento de um" (CHOMSKY, 2006 apud WHITE, 2012, p. 41-42). O autor acredita ainda que não há choque entre o Mundo Islâmico e Ocidental, pois a Indonésia, por exemplo, cuja grande maioria da população é mulçumana, tem uma longa história de relações positivas com o Ocidente. Assim também a Arábia Saudita, que é um Estado fundamentalista, mas que investe fortemente em instituições financeiras ocidentais. Para o autor, as evidências não comprovam a veracidade do argumento de Huntington.

1.3 Classificação Tipológica Do Terrorismo

Existem várias classificações quanto à tipologia, pois o terrorismo é composto de uma variedade de atividades, não por uma ação isolada. A tipologia capta o leque de atividades terroristas melhor do que a maioria das definições e ajuda a identificar que tipo de terrorismo está sendo examinado. Mas, tipologias não solucionam todos os problemas enfrentados quando se tenta definir o terrorismo, simplesmente porque o mesmo está num estado constante de mudança. As tipologias descrevem apenas padrões entre os eventos, mas podem aumentar a nossa compreensão acerca do fenômeno. Porém, cada incidente terrorista deve ser compreendido em suas especificidades sociais, históricas e políticas, pois quando o nível de terrorismo é identificado, o nível de resposta pode ser determinado.

Quantitativamente, o terrorismo pode ser classificado em ações individuais, quando o planejamento e a execução do atentado são realizados por apenas uma pessoa, esta, sem ligação com nenhuma organização (com raras exceções). O terrorismo pode também ser classificado por ações grupais, quando a organização e realização do atentado são de responsabilidade de um grupo ou organização, seja esta, política,

religiosa, étnica, etc. Por último temos ações estatais, cujo próprio nome já afirma, é o caso de terrorismo cuja autoria e realização do atentado é o próprio Estado, a exemplo da ditadura na América Latina. No terrorismo de Estado, a propaganda das atrocidades cometidas pelos exércitos durante o período de guerra ou conflito contra as populações locais é usada para causar pânico, terror na população e se for o caso, forçar sua retirada da região que está sendo ocupada (SAINT-PIERRE, 1996, p. 4-5).

Em nível territorial pode ser de cunho nacional, quando realizado no território do próprio Estado (Tigres Tâmeis, IRA, ETA, etc.); e em nível internacional, quando transcende as linhas nacionais ou quando o ataque é destinado à instituições e organismos estrangeiros em Estado nacional. As ferramentas utilizadas para a realização das ações terroristas podem ser qualquer uma, desde uma adaga, como no caso dos Zelotas até artefatos nucleares como no caso dos "rebeldes" chechenos contra a Rússia. O objetivo que se quer alcançar com a utilização do terror também pode ser motivado por diferentes causas, estas podem ser religiosa, econômica, política, entre outros. Quando não há objetivo claro, pode ser classificado como patológico. Geralmente este tipo de terrorismo é caracterizado por ações individuais, cujo motivo da ação é de ordem psicopatológica (SAINT-PIERRE, 1996).

Quanto aos danos Visacro (2009) afirma que podem ser de caráter seletivo, cujo emprego do terror e a realização de ataques pode ser à alvos específicos, limitando algumas vezes, danos colaterais à vítimas inocentes, tendenciando a maior aceitação da opinião pública. Este tipo, argumenta Laqueur (2003), é característica do “velho terrorismo”. Há também o terrorismo de caráter indiscriminado, sendo este o contrário do terrorismo seletivo, por ter o intuito de causar o maior número de vitimas possível. Saint-Pierre (1996) que analisa o fenômeno sob a óptica da vítima, descreve melhor esse tipo de terror. Para ele, o terrorismo indiscriminado ou aleatório, é aquele cujas vítimas não são escolhidas especificamente, nem obedece qualquer seleção sistemática ou política. Quando trata-se deste caso, quanto maior o número de vítimas, mais suscetível este é, pois seu alvo é fazer vítimas inocentes indiscriminadamente, com a maior diferenciação social possível. Não importa o sexo, a cor, a idade, o segmento religioso; importa apenas que estas sejam pessoas comuns, vítimas inocentes. A eficácia desse tipo de terrorismo é grande pois como não há uma especificidade, maior e mais rápido o pânico espalhado na população, pois qualquer um pode ser a próxima vitima. O terrorismo sistemático ou discriminatório (que Visacro aborda como “seletivo”) descreve o tipo de terrorismo que tem vítimas específicas, determinadas por alguma

característica identificatória, seja esta a religião, a profissão, a cor, a etnia, etc. Este tipo se diferencia do aleatório, pois tem como base a eficácia na identificação da vítima, fazendo com que o objetivo que ocasionou uso do terror, seja nítido, identificado. Ou seja, a estratégia nesse caso é apontar, identificar "quem" é a vítima.

Por outro lado, há autores que minimizam as causas politicas e sociais do terrorismo e enfatizam o ato, como no caso de Michael Ignatieff:

> A natureza apocalíptica de seus objetivos torna absurdo acreditar que eles estão fazendo demandas politicas. Eles estão procurando a transformação violenta de um mal irremediável e um mundo injusto. O terror não expressa uma política, mas uma metafísica (conhecimento das causas primárias), um desejo de dar sentido ao tempo e história através de atos cada vez mais crescentes de violência na qual culmina em uma batalha final entre o bem e o mal. (MICHAEL IGNATIEFF, 2001 apud DERIAN, 2002, p. 102).

Laqueur (2004) critica a explicação do terrorismo segundo variáveis socioeconómicas, como pobreza, explosão demográfica, alto índice de desemprego e baixos níveis de educação. Porém estes fatores podem ajudar a influenciar a execução de atos terroristas, inclusive os suicidas, mas não são fatores diretos. Pelo contrário, o autor afirma que os cinquenta países mais pobres não tem índice de graves ataques terroristas. E que terroristas não são pessoas pobres e não provêm de sociedades pobres, como por exemplo, o caso ocorrido em Punjab em razão de movimentos separatistas, área prospera da na Índia, onde possui uma taxa de pobreza de 3,5% em comparação com a média nacional de 26%. Sendo assim, de modo geral, invalidada a relação de que pobreza é um dos fatores que causam terrorismo, segundo o autor.

1.3.1 Neo-terrorismo

O novo terrorismo, chamado muitas vezes de "neoterrorismo" está normalmente relacionado às mudanças e evoluções do terrorismo num contexto pós 11 de Setembro, apesar de Laqueur já ter tido usado este termo, no mínimo, dois anos antes deste acontecimento devido ao bombardeio em 1993 do World Trade Center em Nova York, bem como o ataque com gás no metrô de Tóquio em 1995.

Para Laqueur (2003), o novo terrorismo está relacionado ao uso de violência em grande escala com intuito de causar maior destruição e envolve diferentes atores, motivações, objetivos, táticas e ações, em comparação ao antigo do terrorismo usado em

meados do século XX. O novo terrorismo difere-se ainda do velho por suas características inovadoras.

Witker (2005) descreve cinco aspectos no quais nos faz afirmar que estamos presenciando uma fase que ele denomina de "neoterrorismo": um crescente caráter transnacional, um poderoso embasamento religioso e nacionalista, um aumento na frequência do uso de ataques suicidas, alta letalidade dos ataques e marcada orientação antiocidental, especialmente nos grupos fundamentalistas islâmicos. Porém esta última afirmação é recusada por outras argumentações como as de Baudrillard e Chomsky[3], que negam a característica de que o terrorismo se baseia nas questões que envolvem o choque de civilizações. O antiocidentalismo pode sim existir, mas que não é o fator central que desencadeia o terrorismo.

Laqueur (2003) afirma, em seus estudos pós 11 de setembro, que o novo terrorismo é diferente em caráter, visando não claramente reivindicações políticas definidas, mas à destruição da sociedade ou de grande parte de sua população. Segundo ele, os "velhos terroristas" tendem a atacar apenas alvos selecionados, enquanto que no novo terrorismo o alvo de ataque tornou-se cada vez mais indiscriminado, além de tentar causar o menor nível possível de casualidade. Ou seja, é uma nova fase do terror que tende a se propagar em grande escala, tornando-se mais letal, com terroristas dispostos a usar a força ilimitada para causar grande número de vítimas. Os ataques diminuíram, mas a proporção de destruição elevou-se, principalmente porque atualmente se pode contar com a ajuda de aparatos tecnológicos.

1.4 Visão não-ocidentalista

Contrapondo algumas afirmações citadas acimas, esta parte do trabalho visa abranger argumentos não tão ocidentalistas a respeito do terrorismo. Isto não implica dizer que os autores citados nesse tópico sejam pertencentes à Sociedade Oriental, mas que abordam sobre o terrorismo partindo do ponto de vista diferenciado, ou seja, visto a partir de um outro ângulo que não seja associado à definição de terrorismo dada pelo governo dos Estados Unidos, por exemplo, que segundo Booth e Dunne (2012) têm "americanizado" o mundo (BOOTH; DUNNE, 2012, p. 95).

Noam Chomsky (2002) afirma que "contraterrorismo muitas vezes, produz mais violência e sofrimento do que as ações dos próprios terroristas" (CHOMSKY, 2002,

[3] Ver tópico 1.2.1 deste estudo.

apud WHITE, 2012, p. 228), e se o terrorismo é definido (por Laqueur, 1999, e outros autores citados ao longo deste capitulo) pelo uso ou ameaça do uso da violência, o "contraterrorismo" ou "guerra contra o terror" também pode ser considerado terrorismo, uma vez que usa da violência até mesmo contra civis (pois não mira apenas os suspeitos, mas todo o país) para combater tal fenômeno. Com ironia Chomsky escreve que "temos que qualificar a definição de "terrorismo" em fontes oficiais, porém o termo se aplica apenas ao terrorismo contra os EUA, não ao terrorismo que os EUA realizam contra os demais" (CHOMSKY, 2002, p. 131).

Said (2001), palestino-americano, argumentou que existem pouquíssimos jornalistas para relatar o ponto de vista oriental, pois as manchetes veiculadas na mídia são em sua maioria elaborada por jornalistas com viés "pró-ocidental". Segundo o autor, centenas de mortes são ignoradas pelos relatórios do *Human Rights Watch*, dos comitês das Nações Unidas e da Agência da ONU para Refugiados. Para o autor, a busca incessante do terrorismo é quase criminosa, pois permite que os Estados Unidos façam o que quiser em qualquer lugar do mundo. Ainda para o autor, os argumentos de Samuel Huntington servem como ferramenta para manter a população com medo e insegura, e justificar as ações dos Estados Unidos.

Segundo Said (2001), atualmente há a criminalização dos movimentos sociais de resistência contra a miséria, contra o desemprego, contra a perda de recursos naturais, ente outros; e estes têm sido chamados de terrorismo (mesmo que não se utilizem do terror). Havendo assim, a "banalização" do verdadeiro significado do termo terrorismo por parte de alguns. Isto se dá também, por questões midiáticas. Por fim, o autor argumentou que o terrorismo feito por grupos como a Al Qaeda, por exemplo, são enfatizados para obscurecer os danos feitos pelos Estados Unidos ao mundo; tanto militarmente, ambientalmente ou economicamente, que são muito superiores aos danos que o terrorismo pode causar.

1.5 Considerações

O terrorismo é sem sombra de dúvidas uma estratégia poderosíssima para alcançar um determinado fim ou propósito, principalmente por parte dos mais fracos. Porém, definir o que de fato seja terrorismo nem sempre ajuda, pois as intepretações acerca do mesmo provêm da construção social que cada povo tem. O mesmo tanto serve

como uma máscara para cobrir os interesses de Estados como os Estados Unidos e ao mesmo tempo, como estratégia por parte de indivíduos, grupos ou da própria população.

Atualmente, como afirma Said (2001), qualquer resistência por parte de grupos menores tem sido chamada de terrorismo, principalmente pela mídia, talvez, para atrair a atenção do público em geral. “A grande maioria concorda que terrorismo é um problema, e é notável um problema na definição desse problema” (COOPER 1976 apud WHITE, 2012, p. 4).

O terrorismo teve várias formas, objetivos, motivações, vítimas e ferramentas ao longo da história, “enjaulá-lo” num conceito exato ocasionaria na perda de todo o sentido histórico do fenômeno, que como vimos, não é novo e frequentemente muda de forma.

CAPÍTULO II

CIBERTERRORISMO: Possibilidades do acontecimento de ataques em grande escala e as mudanças trazidas por essas possibilidades à Comunidade Internacional

O que aconteceria se os semáforos da cidade de Nova York fossem desligados por cinco minutos? Ou se houvesse uma invasão no sistema de alguma torre de controle de tráfego de aeronaves? E se as comportas de uma hidroelétrica fossem abertas simultaneamente por um ou mais indivíduos não autorizados, causando impacto ambiental ou risco à população local?

Do desligamento de semáforos, causando o caos e consequentemente o medo à população local (porque tal ação pode gerar acidentes e também o sentimento de insegurança) à abertura de comportas de uma hidroelétrica (ocasionando danos ou até mortes) são exemplos do danos que o ciberterrorismo pode causar.

2.1 Entendendo o Ciberterrorismo

Como foi visto no capítulo I, o terrorismo não é um fenômeno novo, pelo contrário, é muito antigo, mas está sempre se modificando e se adaptando de acordo com a evolução do mundo. A globalização, por sua vez, trouxe, principalmente entre os anos 1960 e 1980, uma gama de possibilidades em razão da revolução da tecnologia. As pessoas de diferentes partes do mundo podiam se comunicar em tempo real, empresas puderam deixar de lado o papel e utilizar computadores para controlar seu funcionamento, arquivar dados, entre outros (CASTELLS, 1999, p. 44).

As raízes do ciberterrorismo foram percebidas no início dos anos 1990, quando o rápido crescimento do uso da internet e o debate sobre a "sociedade da informação" provocaram vários estudos sobre os riscos potenciais enfrentados pela alta conectividade em rede e pela alta “tecnodependência” dos Estados, especialmente os Estados Unidos (WEIMANN, 2004, p. 2). Segundo Colarik e Janczewski (2008), o termo “ciberterrorismo” passou a ser usado a partir da reunião do G8 realizada em Lyon, na França, no fim da década de 1990, onde foram analisados e discutidos os crimes promovidos via aparelhos eletrônicos ou a disseminação de informações pela internet. É nesse contexto que Castells (1999) afirma que a sociedade não escreve o

curso da transformação tecnológica, uma vez que diversos fatores intervêm no processo de descoberta científica, inovação cientifica e aplicações sociais, sendo o resultado disto totalmente dependente de um complexo padrão interativo. Segundo o autor, "a tecnologia é a sociedade, e a sociedade não pode ser entendida ou representada sem suas ferramentas tecnológicas" (CASTELLS, 1999, p. 43).

A interligação da sociedade com a tecnologia e o aumento da dependência pela mesma deu ao terrorismo a oportunidade de explorar novos recursos; e consequentemente, foi crescendo o receio de que frutos de deficiências tecnológicas tornasse possível a execução de ataques ciberterroristas.

2.1.1 Definições

Segundo Shimeall (SHIMEALL, 2002 apud LIMA, 2006), entendemos por ciberterrorismo o uso do ciberespaço com o objetivo de aterrorizar através de ataques que possam causar a destruição, ou distorção deliberada de dados digitais e fluxos de informação, por motivos religiosos, políticos ou ideológicos.

> 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 intencional de informação eletrônica com o objetivo de descredito público da instituição (SHIMEALL, 2002 apud LIMA, 2006, p. 40).

Porém, quando o autor cita "acesso não autorizado à informação classificada em formato eletrônico" está descrevendo também um outro tipo de "ciberatuação" que pode ser bastante confundida com o ciberterrorismo, que são as invasões de hackers sem propósitos terroristas; neste caso considerado cibercrime. Para distinguir uma invasão ciberterrorista de uma invasão não ligada ao terrorismo, usaremos como exemplo a invasão de sistemas bancários. Seria considerado como cibercrime se a invasão fosse realizada com o intuito de efetuar verdadeiros furtos a bancos e/ou a correntistas. As ações que ocasionam estes furtos são motivadas por inúmeras razões não ideológicas. No caso dos ciberterroristas, os ataques a sistemas bancários e desvio de dinheiro tem o intuito de arrecadar fundos para financiar diversas outras ações terroristas, principalmente as cometidas "off-line"[4], mesmo assim, não deixam de ser consideradas

[4] Neste caso a autora Shimeall (apud LIMA, 2006), refere-se "fora da rede", ou seja, sem utilizar algum aparato tecnológico.

como cibercrimes (LEMOS, 2005, p. 267). Portanto, um cibercrime pode ser um ato terrorista desde que o mesmo esteja vinculado de alguma maneira ao terrorismo.

Lima (2006) afirma que o ciberterrorismo é uma extensão natural do terrorismo, e que este se aproveita da dependência que a sociedade tem da tecnologia, em especial da internet. E por ser um tipo de terrorismo, assim como os demais, planeja os atos (geralmente aplicados contra sistemas civis) motivados por alguma razão (ideológica, politica, religiosa, etc.). Ainda segundo o autor, este tipo de terrorismo pode funcionar desde atos como a disseminação de vírus ao público quanto à execução de ataques maiores, que obviamente terá consequências maiores. Para Che (2007), os ataques graves contra infraestruturas críticas, dependendo de seu impacto, podem ser atos de terrorismo. Já para Lemos (2005), o ciberterrorismo tem como objetivo causar sérios danos, como perdas econômicas ou até mesmo mortes.

Segundo Denning (2000), ciberterrorismo é a associação do ciberespaço e do terrorismo. Trata-se de ataques ou da ameaça de ataques ilegais a computadores, redes e às informações armazenadas no sistema em que estes atuam, quando feito para intimidar ou coagir um governo ou seu povo em prol de objetivos políticos ou sociais. Além disso, para se qualificar como ciberterrorismo, um ataque deve resultar na violência contra pessoas ou bens, ou pelo menos causar sérios danos para gerar medo. Os ataques que levam à morte ou lesão corporal, explosões, ou perdas econômicas graves seriam exemplos. Já os ataques que interrompem os serviços não essenciais ou os que são geralmente considerados apenas incômodos não seriam ataques ciberterroristas (DENNING, 2000 apud WEIMANN, 2004, p. 4).

Este conceito da Denning (2000) leva-nos a distinguir as ações do ciberterrorismo às do hacktivismo, por exemplo, que geralmente são incômodos a rede no geral, pois este último tanto visa ataques pessoais (por querer roubar senhas, vingar-se de alguém hackeando emails, etc.) quanto ataques numa escala maior (congestionar sites, invadir páginas de corporações ou do governo para expor mensagens, etc.).

O hacktivismo é um termo usado por estudiosos para descrever a união de hacking com ativismo político (DENNING, 1999 apud CHE, 2007, p. 8). Embora politicamente motivado, o hacktivismo difere-se do ciberterrorismo, por visar protestar e destruir ou atrapalhar o funcionamento de sites, fóruns, etc., mas, não visa matar, ferir fisicamente ou aterrorizar. Um exemplo de hacktivismo é a interrupção das operações normais de um site, como acontecido em Janeiro de 2012, quando os Anonymous

(grupo de hackers ativistas) derrubaram o site do FBI em protesto contra o fechamento do site de armazenamento de arquivos Megaupload.

Um ciberterrorista se difere de um terrorista que usa a tecnologia. Ciberterrorismo consiste em um ataque à um fator tecnológico usando outro fator tecnológico, sendo o feitor do ciberterrorismo um ciberterrorista. Isso é diferente de um terrorista utilizando a tecnologia para cometer um ato tradicional do terrorismo, e também é diferente de um terrorista usando meios não tecnológicos para cometer um ato de terrorismo contra uma rede de sistema de computador. Por exemplo, um ato de terrorismo cibernético ocorre quando um indivíduo ou uma organização usa uma rede de computadores para sobrecarregar e destruir um sistema de gerenciamento de energia nacional. O ciberterrorismo não ocorre quando um suicida (homem-bomba) destrói uma rede elétrica ou usa a internet para adquirir informações sobre como construir uma arma química (CHE, 2007, p. 8).

Na informática, os ataques sempre obtém uma parcela de sucesso, mesmo que estes não alcancem o resultado desejado. Isso acontece porque a fraqueza do sistema é revelada a partir do momento que é atacado. Para que o ataque ocorra, alguma "barreira" deve ser burlada ou quebrada, e isso significa que o alvo estava susceptível a isto de alguma forma, ou seja, não estava preparado, não tinha capacidade suficiente para fazer com que o ataque não passasse de uma tentativa de ataque.

2.1.2 Ciberespaço: como atua o ciberterrorismo

Como vimos, Shimeall (2002) e Danning (2000) afirmam que o ciberterrorismo atua no ciberespaço. Para que entendamos melhor como o ciberterrorismo funciona, é essencial sabermos o que é ciberespaço. A palavra "cyberspace" foi primeiramente designada em 1984, por William Gibson, um escritor de ficção científica (LÉVY, 1998, p. 104).

O ciberespaço, para Lévy (1998), constitui um campo vasto, aberto, ainda parcialmente indeterminado. Pode ser ainda, conceituado como um ambiente virtual que se utiliza de aparatos de comunicação para o estabelecimento de relações virtuais ou fenômeno que vai além da comunicação no sentido estrito do termo (JUNGBLUT, 2004; GUIMARÃES, 1999 apud GONTIJO; MENDES-SILVA; VIGGIANO; PAIXÃO, 2012). Para Lessig (1998), o ciberespaço é inevitável e irregular, e nenhuma nação pode viver sem ele, mas nenhuma nação será capaz de controlar o comportamento

dele. “O ciberespaço é o lugar onde os indivíduos são, por natureza, livres do controle dos soberanos do espaço real.” (LESSIG, 1998, p. 3).

Para Leão (2003):

> O ciberespaço é explorável e visualizável em tempo real. O ciberespaço engloba: as redes de computadores interligados no planeta (incluindo seus documentos, programas e dados); as pessoas, grupos e instituições que participam dessa interconectividade e, finalmente, o espaço (virtual, social, informacional, cultural e comunitário) que se desdobra das inter-relações homem-máquina (LEÃO apud GARCIA; NOJOSA, 2003, p. 155-157).

Segundo Gori e Paparela (2006), o ciberespaço é para as nossas sociedades como o sistema nervoso é para nossos corpos, onde todas as partes estão interligadas. O ciberespaço pode ser entendido como um espaço sem fronteira, que tráz à tona novas possibilidades para a propagação do terror, pois este é de certa forma, uma extensão do mundo real, sendo mais difícil de controlar, pois sua capacidade vai além da geografia.

2.2 Ciberterrorismo: Por quê?

O ciberterrorismo tem suas vantagens, uma delas é “invisibilidade”, pois de imediato não se sabe realmente quem está do outro lado ou o que pode este realmente fazer (apesar das especulações), limitando assim, a defesa ou contra-ataque por parte da vítima. Uma outra vantagem é que, por norma, não existem mortes do lado de quem ataca (LIMA, 2006, p. 42). Em razão disso, tornou-se uma estratégia interessante para a propagação do terrorismo, pois difere-se de outras táticas terroristas, como os ataques suicidas, por exemplo. Portanto, o ciberterrorismo é, com certeza, uma opção atraente para terroristas tecnologicamente modernos que procuram anonimato e o potencial de infligir danos maciços, causar impacto psicológico e utilizar-se dos recursos de mídia.

A internet tem sido uma ferramenta utilizada pelos terroristas para formularem planos de ataque, financiamento de atividades, propaganda de suas atividades[5], recrutamento de novos terroristas[6], comunicar-se, etc. (LIMA,2006, p. 42). Desde antes dos ataques de 11 de Setembro, o email tem sido ferramenta de comunicação dos terroristas, porém com uma diferença: são criptografados, ou seja, em códigos e até embutidos em imagens, por exemplo. Grupos terroristas maiores se comunicam com grupos pequenos espalhados em todo o globo através da internet. (DERIAN, 2002, p.

[5] Results of 7 Years Of The Crusades: <http://www.theunjustmedia.com/clips/saz/11908/11908.htm> Acessado em Junho de 2012.
[6] A exemplo do site: <alfidaa.org/vb>

110). Embora o fluxo de informações acessíveis através da internet e a utilização da rede por si só não seja considerado ciberterrorismo, as informações obtidas podem sim ser utilizadas para a realização do ciberterrorismo.

Sistemas militares sensíveis (como os que controlam armas nucleares), bem como os sistemas de computadores da CIA e do FBI são "air-gapped", ou seja, extremamente protegidos, tornando-os quase “inacessíveis”. Já os sistemas do setor privado tendem a ser bem menos protegidos, mas isso não significa que são indefesos, os mesmos são dotados de certo nível de segurança, porém não tão blindado como os “air-gapped”. Weimann, israelita, publicou em 2004, em um artigo[7], que os “contos” aterrorizantes sobre a vulnerabilidade dos sistemas informáticos do setor privado tendem a ser em grande parte apócrifa, sem provas reais. Porém sistemas podem ser “quebrados”, manipulados, burlados.

Para exemplificar a vulnerabilidade dos sistemas, eis alguns exemplos: em maio de 2009 um hacker francês invadiu o sistema administrativo do twitter, uma rede social, o que lhe daria acesso a todas as contas dos usuários, inclusive a do presidente Barak Obama, ou de qualquer um outro político ou celebridade com conta no microblog. Apesar das contas nesta rede não possuírem informações pessoais, ainda assim os usuários de todo o mundo teriam acesso ao que fosse postado pelo hacker em nome de alguém, ou seja, ele teria a capacidade de se expressar passando-se por alguém, e até que o post fosse negado pela informação de invasão de conta, a mensagem dada poderia ter causado alguma repercussão imediata. O hacker não chegou a alterar nada, porém se o mesmo tivesse ligações com organizações terroristas, essa seria uma oportunidade de propagar mensagens, por exemplo. Mais de dez mil contas de clientes cadastrados na Sony Online, serviços de jogos online, ficaram expostas ao roubo de números de cartões de créditos e dados como endereço, nome e identificações de usuários no fim de Abril de 2011. Em Junho de 2012 usuários da LinkedIn, rede social para profissionais, tiveram suas senhas roubadas e supostamente divulgadas, sendo elas cerca de 6 milhões. Obviamente esses são apenas alguns exemplos de que o acesso a dados de usuários tanto no setor privado como em redes sociais é possível. Para Weimann (2004), as redes sociais seriam um eficiente meio para a propagação de mensagens terroristas, uma vez que milhares de usuários em todo o mundo teriam acesso.

[7] WEIMANN, Gabriel. “Cyberterrorism. How Real Is the Threat?” Washington: United States Institute Of Peace, 2004.

Nenhum desses casos citados acima (incluindo a derrubada do site do FBI pelos Anonymous) são ocorrências de terrorismo, mas são exemplos de que a ameaça ciberterrorista pode ser real. Um dos fatores que dificultam o acontecimento do terrorismo no plano cibernético é o de que os hackers (pelo menos é o que se acredita) não estão associados à grupos terroristas e nem esses grupos tenham capacidade técnica para fazerem atentados virtuais no momento. A solução para esses grupos seria a de conseguir filiar-se a um ou mais hackers ou desenvolver a capacidade técnica que necessitam. Mas por razões de desconfianças e ideologias diferentes, a primeira alternativa seria descartada uma vez que os hackers poderiam se associar a outros organismos. Então, investir no próprio hacker seria a opção mais viável, porém necessita-se muito tempo, além de condições tecnológicas avançadas. Portanto não é algo imediato, sendo pouco provável em curto prazo.[8]

Para Weimann (2002), o ciberterrorismo é uma opção atraente por várias possíveis razões. Primeiro porque pode ser mais barato do que os métodos tradicionais, uma vez que não precisam comprar armas e explosivos; em vez disso, eles podem criar e enviar vírus de computador através de uma conexão. Em segundo lugar, ciberterrorismo é mais anônimo do que os tradicionais métodos terroristas. Podem usar "proxy anônimo", o que dificulta para as agências de segurança e forças policiais o rastreamento da identidade real dos terroristas. Além disso, no ciberespaço não existem barreiras físicas, tais como postos de controle para navegar e não existem fronteiras para cruzar. Em terceiro lugar, a variedade e o número de alvos são enormes. Os ciberterroristas poderiam ter como alvo os computadores e redes de computadores de governos, indivíduos, serviços públicos, companhias aéreas privadas, e assim por diante. O grande número e a complexidade de alvos potenciais permitem que os terroristas encontrem fraquezas e vulnerabilidades para explorar. As infraestruturas críticas, como redes de energia elétrica e serviços de emergência, são vulneráveis a um ataque ciberterrorista porque as infraestruturas e os sistemas de computadores que os executam são altamente complexos, tornando-se efetivamente impossível eliminar todas as fraquezas. Em quarto lugar, ciberterrorismo pode ser realizado remotamente, uma característica que é especialmente atraente para terroristas, pois, o ciberterrorismo requer menos treinamento físico e investimento psicológico, porque o risco de mortalidade das formas convencionais de terrorismo é aqui excluído, tornando mais fácil para as organizações terroristas a recrutar e reter seguidores. Em quinto lugar, o

[8] Informação contida no documentário: Cyberterrorism, History Channel, 2003.

vírus “I LOVE YOU” (que segundo Grego, 2000, infectou milhares de computadores e causou perdas de 6,7 bilhões de dólares em 1999) mostrou que há a possibilidade do ciberterrorismo afetar diretamente um número maior de pessoas do que os métodos tradicionais de terroristas, gerando uma maior cobertura da mídia.

2.2.1 As possiblidades de ataques em grande escala

Como podemos ver, ciberataques em componentes críticos de infraestruturas nacionais não são incomuns, mas eles não foram realizados por terroristas e não buscaram infligir o tipo de dano que se possa qualificar como ciberterrorismo. Lima (2006) argumenta que as consequências mais prováveis de um ataque ciberterrorista são maioritariamente econômicas ou psicológicas, mas não podem ser resumidas apenas a estas. Para ele os terroristas podem se infiltrar no controle de metrôs, de navios e até mesmo no sistema de torres de controle aéreo, provocando caos. Porém, o ciberterrorismo só é possível ser realizado por meios de aparatos tecnológicos em ambas as partes, tanto por parte do terrorista quanto da vítima.

A potencial ameaça representada pelo terrorismo cibernético tem provocado um “efeito alarme” nos Estados desenvolvidos. Robert Mueller, diretor do FBI, em entrevista à Fox News em março de 2012, afirmou que ciberterroristas estão constantemente envolvidos em ações de lavagem de dinheiro para financiar as suas investidas e que a preocupação é que os ataques terroristas saiam do campo digital e cheguem ao campo de batalha, prejudicando ou interferindo as operações nacionais. Foram confiscados nos EUA em dezembro de 2001, bens de uma instituição de caridade, pois o governo afirmava que esta tinha relações com o Hamas (FRIEDMAN, 2007, p. 507).

De fato, as infraestruturas mais importantes nas sociedades ocidentais estão conectadas em rede através de computadores, portanto, a ameaça potencial do ciberterrorismo é, com certeza, muito preocupante. Embora os Hackers (de maneira geral) não sejam motivados pelos mesmos objetivos que inspiram terroristas, estes demonstram que se pode ter acesso à informações sensíveis, importantes e ao funcionamento de serviços vitais. Os terroristas poderiam também romper sistemas de computadores particulares ou governamentais, prejudicar ou pelo menos desativar os sistemas do setor militar, financeiro e de serviço nos Estados mais desenvolvidos, pois é crescente a dependência das sociedades para com a tecnologia, e essa, não só nos trouxe

eficiência, eficácia e desenvolvimento, mas também vulnerabilidade, dando aos terroristas a oportunidade de alcançar alvos que seriam inatacáveis, como os sistemas nacionais de defesa, sistemas de controle de tráfego aéreo, entre outros.

Quanto mais tecnologicamente desenvolvido for um Estado e mais hackers houver, mais vulnerável é, e por outro lado, mais propício para executar ciberataques contra infraestruturas. Pois, quanto mais aparatos tecnológicos tiverem funcionando e dependendo o Estado, maior possibilidade de acessos aos mesmos. Pouco seria o despertar de interesse (ou mesmo a impossibilidade) para a execução de ciberataques em um Estado pouco desenvolvido, cujas infraestruturas são de certo modo arcaicas, diferentemente dos Estados potências que, em sua maioria, têm infraestruturas controladas quase que completamente por sistemas de computadores.

Depois dos ataques de 11 de Setembro a Al Qaeda anunciou em seus websites sobre um (suposto) ataque iminente em grande escala contra alvos dos EUA. A mídia, então, ajudou a propagar a sensação de terror e insegurança promovidos por esses anúncios, não só aos EUA, mas a todo o mundo. A internet expandiu a oportunidade dos terroristas de fazerem publicidade, antes disso, eles tentavam atrair a atenção do radio, TV, ou jornal escrito. Mas como a internet é um meio aberto a maiores chances de publicação, nem sempre essas mensagens publicitárias por parte dos terroristas são levadas a sério, pelo crescente número das mesmas. Porém nem sempre esses websites são utilizados pelos terroristas para publicitar seus atos, mas também para argumentar sobre a liberdade de expressão e o destino dos companheiros que são prisioneiros políticos. Deste modo, repercutem aos que lhe apoiam ou chama a atenção dos ocidentais que apoiam a liberdade de expressão (FRIEDMAN, 2007, p. 506-507).

A internet foi usada para arrecadar fundos, e além de solicitar ajuda financeira online, os terroristas recrutaram adeptos utilizando toda a gama de tecnologias de website (áudio, vídeo, etc.). Foi possível encontrar também, provas de que operadores da Al Qaeda navegavam em sites que continham informações sobre softwares que controlam redes de infraestruturas vitais, como vias fluviais e marítimas, redes elétricas, etc. Friedman (2007) afirma que um computador que foi capturado da Al Qaeda continha características estruturais de engenharia e arquitetura de uma represa. Essas informações tinham sido baixadas da internet e podiam fornecer aos organizadores um planejamento de ataques em grande escala, revelando as possiblidades do ciberterrorismo acontecer. Um manual de treinamento da Al Qaeda, encontrado no Afeganistão informa que “utilizando fontes públicas e sem recursos a meios ilegais, é

possível reunir pelo menos 80% das informações sobre o inimigo". Estes fatos nos levam a pensar no interesse que os grupos terroristas têm em utilizar a tecnologia para realizar seus objetivos, inclusive, através do ciberterrorismo (FRIEDMAN, 2007, p. 506-507). Acredita-se que Osama Bin Laden estudava um ataque cibernético, pois em uma entrevista realizada em novembro de 2002, Sheikh Omar Bakri Muhammad, que se auto proclamava porta-voz da Al Qaeda, afirmou que este e outros grupos tinham interesse em usar a internet como arma para defender suas ideologias e realizar ataques em todo o mundo.

Barry Collin (COLLIN apud ADAMS, 1999, p. 260) cita alguns exemplos do que um ciberterrorista é capaz de fazer. Para ele, este individuo estando em um outro lugar é capaz de invadir o sistema de controle de um fabricante de cereais e modificar os níveis de complemento de ferro no alimento, ocasionando intoxicação e até a morte de crianças que consumirem estes produtos. Outro exemplo é o de que o terrorista pode colocar bombas com controles em diversos pontos da cidade com todas transmitindo sinais umas às outras e, quanto uma parar de mandar este sinal, todas explodem simultaneamente. Trazendo o mesmo exemplo para um contexto mais atual, para que essas bombas explodissem bastava executar o comando para a explosão através do envio de uma mensagem de texto ou uma chamada telefônica, pois, o circuito da bomba pode ser ligado ao sistema de vibração do celular, sendo assim acionado quando o telefone vibra. O aparelho pode estar perto da bomba em um carro, por exemplo. São várias as alternativas para executar essa ação, mas segundo Gordon Corera (2012), especialista em segurança da BBC, "a alternativa de usar um telefone celular para detonar a bomba não existe dentro de um avião, onde a cobertura do sinal é limitada. Esse tipo de explosivo ainda está mais no campo da tese do que da prática". Porém segundo o mesmo, a Al Qaeda tem recorrido aos métodos mais criativos para conseguir atingir seus objetivos.

O segundo exemplo é interessantíssimo, pois nos faz sair do foco da internet. Para que celulares usados na explosão da bomba se conectem não é preciso a conexão da internet, como alguns autores argumentam que é pelo uso dela que se pode acontecer o ciberterrorismo (por invasões, etc.). Porém é importante diferenciar que um homem-bomba com os explosivos anexados a si mesmo, podendo estes serem ativados por um clique no botão detonador não é considerado ciberterrorismo, pois para que seja, tem que ser usado o ciberespaço. No caso do terrorista acionando a bomba através do botão detonador que geralmente está conectado diretamente a bomba através de fios, não

utiliza-se o ciberespaço, diferentemente da bomba conectada ao sistema de vibração do celular, que para poder explodir, o celular terá que vibrar, seja recebendo uma chamada telefônica ou torpedo (sms), que geralmente é distribuído por antenas. Mas há tecnologias alternativas, como o bluetooth, que faz o celular vibrar toda vez que pede permissão para compartilhar um arquivo, mas não seria "vantajoso" uma vez que as conexões bluetooth não funcionam a longa distância e a vantagem da utilização desse recurso é justamente porque o terrorista não precisar estar por perto para executar o atentado. Além disso, várias bombas podem ser implantadas em diferentes pontos da cidade e detonadas ao mesmo tempo por um único terrorista por meio de um controle ou mesmo do celular. Isso traria dificuldades para desativar de imediato as mesmas, se descobertas, pois enquanto uma estivesse sendo procurada e desarmada, outras estariam disponíveis para executar a explosão.

Um terceiro exemplo dado por Collin (COLLIN apud ADAMS, 1999, p. 260), são os transtornos ocasionados em bancos, transações financeiras e bolsas de valores, que como já citado anteriormente são cibercrimes, mas podem estar associado ao terrorismo. Existe ainda a possibilidade do ataque aos sistemas de controle de tráfico aéreo para provocar o choque de grandes aviões (não particulares), a invasão a laboratórios medicinais com o intuito de modificar formulas que se não contidas poderiam conduzir a morte daqueles que ingerissem os medicamentos modificados. Há ainda a possibilidade de modificação da pressão dos dutos de gás, o que provocaria falha em alguma válvula explodindo talvez uma quadra inteira. O mesmo poderia acontecer em uma rede elétrica com a sobrecarga da rede. Para o autor, estas hipóteses são realistas, mas a invasão de sistemas federais ou similares seria pouco provável por ser muito difíceis de neles penetrarem.

Porém Collin (apud id., 1999, p. 262) atinge o extremo ao defender que o ciberterrorismo pode ocasionar que a população de um Estado seja prejudicada o suficiente a não ter acesso à comida, bebida, viajar ou viver. Há a possibilidade de que navios cargueiros (transportando alimentos), por exemplo, sejam desviados (devido à confusão nos radares) por atentados ciberterroristas ou que algum recurso indispensável seja danificado (reservatórios de água, etc.), mas esta questão defendida pelo Collin é improvável, pois os ciberataques caracterizam-se por produzir danos imediatos, como invadir o sistema de uma estação de metrô, modificando os trilhos (moveis) fazendo com que haja um choque entre metrôs, ocasionando vítimas imediatas e assim produzir medo através do choque causado pela surpresa do ataque. Para que uma população fique

sem o básico para a sobrevivência deveriam ser atacadas quase, senão todas as principais estruturas vitais que mantém o lugar funcionando (portos, desorientando seus radares ou ferramentas de comunicação; estações de tratamento de água, etc.) e ainda assim, não tem como assegurar que essa população enfrentaria o caos citado pelo autor, simplesmente porque para que uma ação terrorista como esta seja executada, o Estado deve possuir aparatos tecnológicos fortemente desenvolvidos para manipular tais estruturas e os mesmos, obviamente, possuem certo nível de segurança em seus sistemas que podem ser modificados em pouco tempo, “fechando as brechas” da vulnerabilidade do momento, evitando a continuação de danos em curto prazo.

Collin chega a ser contraditório por defender este último argumento, pois ele acha pouco provável a invasão de sistemas federais e governamentais (nos EUA geralmente as estruturas responsáveis pelo fornecimento de recursos vitais são privadas), mas defende que o ciberterrorismo prejudique o acesso da população à comida, bebida, etc. Há a possibilidade de atentados ciberterroristas em grande escala proporcionados pelos veículos tecnológicos e pelos avanços da globalização, mas há tanto quem não considera a possibilidade desta ocorrência atualmente, a exemplo do James Corley (COUTO, 2005. p. 96), como também quem, como no caso do Collin, chegue próximo à ficção (COLLIN apud ADAMS, 1999, p. 260-262).

A ameaça de ataques não deve ser ignorada. Qualquer possibilidade de danos à vida humana é de responsabilidade do Estado, que visa garantir o bem estar de sua população. Os Estados que utilizam-se da tecnologia para o funcionamento de suas estruturas vitais devem investir na segurança tecnológica visando maior seguridade à população e assim evitar danos. Por mais que os sistemas que controlam as estruturas dos Estados sejam considerados seguros, quando se trata de tecnologia há sempre a possibilidade de superar a atual circunstância e evoluir para uma outra situação. Che (2007), assim como Collin (COLLIN apud ADAMS, 1999, p. 260-262), argumentam que os ataques contra redes militares seriam ineficazes, pois os principais sistemas militares, como o Departamento Canadense de Defesa Nacional, o Pentágono e instalações nucleares são "air-gapped" (LIBICKI, 1996; GREEN, 2002; MITCHELL, 2005 apud CHE, 2007). Isto é, não são fisicamente ligadas às redes externas, tais como a internet. Mas temos o exemplo do ocorrido em 2008, onde algumas redes de computadores do Departamento Americano de Defesa (Pentágono) foram infectadas por um "vírus global", assim, contrariando a afirmação de Che e expandindo as

possibilidades de acontecimentos maiores, pois apesar de toda segurança, estão suscetíveis a vírus e invasões.

O ciberterrorismo não é estratégia exclusiva de indivíduos ou grupos terroristas (orientais). Países tecnologicamente desenvolvidos, como os EUA, podem trazer ameaças aos demais, pois os mesmos podem ter acesso às redes de infraestrutura dos demais, aos mapas territoriais, entre outros recursos; o que num conflito pode ser extremamente vantajoso. Portanto, a ameaça pode não provir exclusivamente de organizações terroristas ou de indivíduos, mas os Estados podem utilizar-se do artefato tecnológico para aterrorizar.

Segundo Denning (2001), como retaliação aos atentados de 11 de Setembro, os *Dispatchers* – um grupo de 60 pessoas liderados por um jovem hacker de Ohio, EUA – executaram ciberataques contra alvos como o ministério do Interior iraniano, o Palácio Presidencial do Afeganistão e o ISPs (Código Internacional para proteção de Navios e Instalações Portuárias) palestino. O grupo anunciou que destruiria servidores Web e interromperia o acesso à Internet no Afeganistão e nos Estados que, segundo eles, apoiavam terroristas. A autora afirma que tem sido crescente o uso da internet como campo de batalha.

Apesar desse evento não ter sido considerado ciberterrorismo, podemos ver que as ameaças não provém do lado oriental apenas; cidadãos da sociedade Ocidental podem ciberatacar e ainda serem realizadores do ciberterrorismo, além disso, os Estados não estão destinados a serem apenas vítimas.

2.2.2 O caso da Estônia

A Estônia lidera no papel de um e-Estado (Estado eletrônico), não apenas porque desenvolveu os novos e atrativos e-serviços (serviços online), mas porque os cidadãos daquele Estado aceitaram a internet como um direito humano e como um fator comum ao padrão de vida dos cidadãos. Em 2007, 98% do território da Estónia tinha acesso à internet, apenas algumas pequenas áreas ficaram fora da cobertura por causa das peculiaridades desfavoráveis do lugar. Em Outubro de 2005, a Estónia tornou-se o primeiro país no mundo a permitir a votação pela internet. Em 2007, o país tinha 150 sistemas de informação do setor público à disposição. Porém, a grande disponibilidade de serviços públicos eletrônicos e de acessibilidade à internet teve um efeito negativo, pois fez do país um alvo atraente para ataques cibernéticos. A dependência da

população e o fácil acesso à serviços online tornou o Estado mais vulnerável às ataques em larga escala (TIKK, Eneken; KASKA, Kadri; VIHUL, Liis, 2010, p. 16).

O país passou por três semanas de ataques que foram considerados emocionalmente motivados. O fato iniciou-se logo após a remoção da estátua de bronze de um soldado soviético do centro de Tallinn, a capital do país, para transportá-la para um cemitério militar. O governo russo e estonianos descendentes de russos pronunciaram-se contra a mudança, e estes últimos iniciaram um protesto onde 150 pessoas ficaram feridas. Segundo a Rússia, a estátua é uma homenagem àqueles que lutaram contra o nazismo, mas os estonianos a veem como um símbolo da ocupação soviética. Esses ataques deixaram diversos sites inacessíveis, incluindo os do parlamento, ministérios, bancos e páginas de notícias, abalando a economia local em razão da inacessibilidade de instituições importantes (como bancos e empresas); e impossibilitando até que os membros do governo se comunicassem por email, pois estes ataques foram direcionados aos servidores de instituições que são responsáveis pela a infraestrutura da internet do país (TIKK, Eneken; KASKA, Kadri; VIHUL, Liis, 2010, p. 20).

Ajuda internacional foi oferecida por vários países para limitar os ataques. A OTAN enviou alguns de seus principais especialistas em ciberterrorismo à Tallin para investigar e ajudar os estonianos a reforçarem suas defesas eletrônicas. A Finlândia foi especialmente útil providenciando contatos e assistência à Estônia. Mas somente após a publicação de uma notícia sobre a cooperação de autoridades estrangeiras ao país com o objetivo localizar os criminosos e levá-los a julgamento, os números de ataques espontâneos começaram a diminuir (TIKK, Eneken; KASKA, Kadri; VIHUL, Liis, 2010, p. 24).

Esses ataques à Estônia foram considerados ciberterrorismo? Alguns autores como Tikk, Kaska E Vihul citam o caso da Estônia como exemplo de ciberterrorismo, mas esse termo empregado a esses ataques foi intitulado mais pela mídia. A Rússia foi acusada pelos estonianos como a responsável pelo ocorrido, mas esta acusação não foi confirmada. Se fosse, alguns autores teriam afirmado a ocorrência de ciberguerra[9]. A definição de guerra da informação dada por Colarick e Janczewski (2008) é de que trata-se de um ataque planejado por países ou seus agentes contra à informação,

[9] As expressões: "guerra da informação", "ciberguerra", "guerra cibernética", entre outras, são consideradas sinônimos pela falta de um consenso entre autores que escrevem sobre o tema. MANDARINO Jr, Raphael, 2009, p. 48.

sistemas e programas de computadores e dados que resultam em perdas ao inimigo (COLARICK; JANCZEWSKI, 2008, p. 15). Já Para Raphael Mergui, a ciberguerra não consiste em destruir o campo de batalha do adversário, mas paralisar os sistemas de informação através da invasão via internet, deixando o inimigo inoperante diante de suas estruturas tecnológicas (MERGUI, 2005 apud CAROU; PASTOR, 2006, p. 57).

Ciberguerra significa romper ou destruir informações e/ou sistemas. "Pode envolver diversas tecnologias para obter coleta de informações privilegiadas, processamento e distribuição destas informações, ainda a identificação de amigo ou inimigo", entre outros. É considerada "de nível militar", diferente dos ciberataques normais (ARQUILLA; RONFELDT, 1993, p. 30), como considerado por este estudo os ocorridos na Estônia; que não teve características militares, mas criminais cujos ataques não foram executados por hackers ligados ao governo, descartando a ocorrência da ciberguerra. É importante lembrar que a mesma utiliza-se do ciberespaço assim como o ciberterrorismo e pode ser associada às guerras ou conflitos convencionais. Obviamente a ciberguerra pode ser uma estratégia para o não uso da violência e para a provocação entre os Estados, mas não convém neste estudo, uma abordagem mais sólida sobre o que é ciberguerra e seus objetivos.

Houve especulações de que os ataques tinham sido provocados não pelo governo russo, mas por russos e estonianos descendentes de russos como protesto. Nesse caso, poderia sim ter sido considerado ciberterrorismo se tivesse aterrorizado a população, o que não aconteceu, pelo próprio nível dos ataques. Por faltam de provas sobre a essência dos ataques (não foi possível saber se foi mesmo protestos ou se os ataques foram realmente ocasionados pela retirada da estatua), não podemos classificar o acontecimento além de "ciberataques".

2.2.3 As duas principais mudanças trazidas pela possibilidade do acontecimento do ciberterrorismo à comunidade internacional

A primeira mudança é sem sombra de dúvidas, o aumento da segurança para evitar ou barrar ataques cibernéticos. Como é sabido, os ataques só podem acontecer se os Estados tiverem certo desenvolvimento tecnológico. O nível do ataque (se em grande escala ou não) vai depender da "tecnodependência" que o Estado tem.

A possibilidade de existência deste acontecimento causou preocupação por parte dos Estados que agora investem em medidas contra ciberataques, a exemplo dos EUA,

que desde a presidência de George W. Bush a Iniciativa Integral de Segurança Cibernética Nacional (CNCI - Comprehensive National Cybersecurity Initiative) reforçou as atividades que envolviam cibersegurança e estabeleceu metas para ajudar a estabelecer segurança no ciberespaço norte-americano. A primeira meta é estabelecer uma linha de defesa contra as ameaças imediatas atuais através da criação ou aumento da consciência da existência das vulnerabilidades da rede, ameaças e eventos ao governo e setor privado, promovendo a capacidade de agir rapidamente na redução das vulnerabilidades atuais e evitar invasões. Uma outra meta proposta é a defesa contra as ameaças, reforçando as capacidades de contraespionagem dos EUA e aumentando a segurança com para as tecnologias da informação (TI). E por último, reforçar o futuro da segurança cibernética expandindo a educação cibernética através da coordenação e orientação de pesquisas e, ainda, buscar definir e desenvolver estratégias para deter a atividade hostil ou maliciosa no ciberespaço. Essas metas podem ser implantadas em outros Estados em prol da segurança, como no caso do Brasil pela Polícia Federal[10], apesar de já existir o Centro de Defesa Cibernética (CDCiber), que como o propor nome já diz, é responsável pela defesa no âmbito cibernético.

A segunda mudança foi a tendência à cooperação, já que não existem fronteiras para o ciberterrorismo. Sendo assim, o alvo pode ser qualquer um dos Estados, ou vários simultaneamente. Por isso, há o interesse entre os Estados em unir-se através de acordos. Che (2007) argumenta que acordos internacionais são necessários para enfrentar a ameaça terrorista e há dois componentes a serem considerados: o direito internacional e harmonização de políticas.

O direito internacional, segundo o autor, pode tratar com mais sucesso o ciberterrorismo (do que a harmonização de políticas). Primeiro porque embora tenha havido desacordo a respeito de uma definição universal de terrorismo, as Nações Unidas tentam estabelecer medidas para conter o terrorismo internacional. Porém, para que haja maior eficiência na contenção do ciberterrorismo uma definição (oficial) do que constitui um ato ciberterrorista deve ser estabelecida. Em segundo lugar, uma designação de quais ações são requeridas para uma resposta legítima deve ser determinada. Em terceiro lugar, o acordo deverá promover a cooperação transnacional, assim, os interesses nacionais devem ser minimizados (CHE, 2007, p. 15-16).

[10] O Brasil inaugurou no mês de Junho o centro contra ataques cibernéticos. O centro funcionará em regime de plantão durante a Conferência Rio + 20, a Copa do Mundo 2014 e Olimpíadas 2016. Se a ameaça não fosse real, os Estados não estavam se prevenindo.

Harmonização de políticas é uma consequência das circunstâncias comuns aos Estados no cenário internacional. Para Che (2007), requisitos internacionais para legislar políticas nacionais contra o ciberterrorismo aumentam a seguridade no âmbito internacional e ajudam a cooperação transnacional. Um exemplo disso é o tratado realizado a partir da convenção de Budapeste, que abrange as ciberameaças. O tratado tem como objetivo proporcionar uma união mais estreita entre os signatários, intensificando a cooperação e tendo com objetivo proteger a sociedade contra as ameaças no ciberespaço (CONVENÇÃO SOBRE O CIBERCRIME, p.1).

Considerações finais

Pudemos perceber ao longo do estudo que o terrorismo não é um fato recente e muito menos desencadeado a partir dos eventos do dia 11 de Setembro. Apesar da ênfase sobre o terrorismo nestes últimos anos ter sido dada pelos novos rumos, objetivos, estratégias e ferramentas, inclusive virtuais, o mesmo é bem mais antigo do que os acontecimentos ocorridos no século XXI e vai muito além do terror produzido pelos fundamentalistas islâmicos que ficaram reconhecidos mundialmente pela ênfase da mídia nos ataques de 2001, nos Estados Unidos.

Quando se aborda acerca do terrorismo, entramos em um campo de discussão abrangente de certa forma complicado, pois é um tipo de conflito que leva consigo características de outros conflitos, se adapta muito bem às ferramentas atuais, pode acontecer em qualquer parte do mundo, inclusive, simultaneamente e, é basicamente um conflito "mutante", que possui várias formas de agir que mudam de acordo com a questão em relevância e com a situação. O porquê do terror nos leva a análise complexa que muitas vezes não são respondidas a modo satisfatório pela maioria dos autores, pela própria natureza do conflito, que muitas vezes leva ao discurso de que a explicação é identificada como exoneração. Portanto, nenhuma definição de terrorismo cobrirá realmente todas as variedades que tem aparecido ao longo da história. E a definição de ciberterrorismo é simplesmente uma reinterpretação de caracterizações tradicionais de terrorismo infundidos com a terminologia tecnológica.

É importante relatar que os autores (utilizados na bibliografia deste estudo) que escreveram sobre o ciberterrorismo até o presente, enfatizam que nenhum ataque ciberterrorista tinha sido relatado e que isso conduzia à questionamentos sobre o ciberterrorismo ser ou não uma ameaça real, pois, já existe a possibilidade da utilização do terrorismo cibernético e o avanço da tecnologia e globalização oferecem aos terroristas condições para a execução destes atentados, mas não se vê por parte destes nenhuma ação, diferentemente do hacktivismo. Além disso, estes autores argumentavam sobre a possibilidade do acontecimento do ciberterrorismo, muitas vezes, com certa apatia, não empenhando-se para desenvolver abordagens mais inovadoras, mesmo que contraditórias a possibilidade deste evento. A escassez do desenvolvimento de ideias contra ou a favor, levando-nos a pensar na hipótese de que no campo acadêmico, as abordagens sobre o assunto só venham a crescer se houver um "11 de Setembro" cibernético.

Porque não há atos de ciberterrorismo ocorrendo, não implica necessariamente que a potencial ameaça ciberterrorista não deva ser tratada como um risco, pelo contrário, nenhum país está livre da ameaça terrorista (KOLLER, 2000 apud LIMA, 2006, p. 43). A natureza da segurança a respeito do terrorismo é preventiva e não remediável, sendo possível impedir execuções do terrorismo, incluindo o ciberterrorismo, antes que eles ocorram. A utilização da tecnologia informática como uma arma ofensiva é uma estratégia diferente da utilizada pela Al Qaeda nos ataques de setembro de 2001 e muito mais poderosa, pois enquanto um homem-bomba pode matar centenas, um ataque terrorista cibernético pode matar milhares.

O exagero e a manipulação ideológica nos faz pensar que revoluções e movimentos tecnológicos tendem a ser feitas "hoje", "agora" e que as novidades neste ramo trazem mudanças imediatas. Pode ocorrer em certos casos, mas não façamos destes uma regra. Essa intolerância com relação ao tempo faz com que algumas pessoas acreditem que ataques desse tipo não poderão acontecer, mas é importante entender que os computadores, programações e sistemas de informações são uma extensão da mente humana.

Os países estão se prevenindo, e talvez a razão do ciberterrorismo não ter acontecido ainda é que os Estados possam estar um passo a frente. Além do investimento interno contra ataques, pudemos observar a cooperação internacional no caso da Estônia e na ratificação da convenção de Budapeste[11]. É interessante perceber que com a evolução do terrorismo à uma esfera global, houve certas mudanças de atitude por parte dos Estados, fazendo com que estes também optassem por meios de se tornarem mais seguros, e isso não é ocasionado apenas pelo investimento interno contra os ciberataques, mas na cooperação que vem sendo visualizada em prol da luta antiterrorista, pois de fato, este fenômeno trouxe tensões ao cenário internacional. Portanto, a resposta momentânea para o ciberterrorismo e para suas possíveis ameaças em grande escala é olhar para o futuro, já que ainda não houve nenhum caso e, permanecer em alerta para os perigos reais que este fenômeno pode causar.

[11] A União Europeia e mais 44 Estados (dos quais não inclui o Brasil) ratificaram a convenção de Budapeste, em 2001, para cooperarem entre si contra os crimes no plano cibernético.

Bibliografia

ABCNews. **The Smoke Over Flame: Who Is Behind Super Cyber Spy Tool?** Disponível em: <http://abcnews.go.com/Blotter/flame-israel-us-super-cyber-spy-tool/story?id=16459456#.T-gy8hdRSSp> Acesso em Junho de 2012.

ADAMS, James. **La Próxima Guerra Mundial: Los Ordenadores Son Las Armas y el Frente Está en todas partes.** Ediciones Granica S.A. Buenos Aires: 1999. p. 260

ANDESON, Sean K; SLOAN, Stephen. Historical Dictionary of Terrorism. Ed. 3rd. Toronto: The Scarecrow Press, 2009.

ARQUILLA, John; RONFELDT, David. **Cyberwar is Coming**! Comparative Strategy, Vol 12, No. 2,1993, p. 30.

AXELROD, Evan M. **Violence Goes to the Internet: Avoiding the Snare of the Net**. p. 185

BAUDRILLARD, Jean. **O Espírito do Terrorismo**. São Paulo: Campos das Letras, 2002.

BOOTH, Ken; DUNNE, Tim. **America**. In: Terror In Our Time. New York: Routledge, 2012, p. 95-109.

CAMPI, Monica. **Sony confirma roubo de dados na Sony Online**. Info Online. Disponível em: <http://info.abril.com.br/noticias/seguranca/sony-confirma-roubo-de-dados-na-sony-online-03052011-11.shl> Acesso em Junho de 2012.

_____. **LinkedIn confirma roubo de senhas**. Info Online. Disponível em: <http://info.abril.com.br/noticias/seguranca/linkedin-confirma-roubo-de-senhas-07062012-10.shl> Acesso em Junho de 2012.

CAROU, Heriberto Cairo; PASTOR, Jaime. **Geopolítica, Guerras y Resistencias.** Madrid: Trama Editoral, 2006. p. 57.

CASTELLS, Manuel. **A Era da Informação: economia, sociedade e cultura**. vol. 3, São Paulo: Paz e terra, 1999.

_____. **A sociedade em rede** – volume I: A era da informação: economia, sociedade e cultura. 8ª ed. São Paulo: Paz e Terra, 1999.

Ccomgex. **Exército brasileiro prepara sistema para prevenir ataques cibernéticos**. Disponível em: <http://www.ccomgex.eb.mil.br/index.php?option=com_content&view=category&layout=blog&id=89&Itemid=541> Acesso em Junho de 2012.

CHE, Eliot. **Securing A Network Society Cyber-Terrorism, International Cooperation And Transnational Surveillance. Research Paper**. Athens: 2007. p. 113

CHOMSKY, Noam. **Who are the Global Terrorists?** In: Worlds in Collision: Terror and the Future of Global Order. Booth, Ken; Dunne, Tim. Palgrave Macmillan, 2002

_____(2006). **The Clash of Civilizations**. Disponível em: <http://www.youtube.com/watch?v=qT64TNho59I>. Acesso em Junho de 2012.

COLARIK, Andrew M; JANCZEWSKI, Lech J. **Cyber Warfare and Cyber Terrorism.** Hershey: IGI Global, 2008. p. 13-15.

CONVENÇÃO SOBRE O CIBERCRIME. Disponível em: <http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf> Acesso em Junho de 2012

CORERA, Gordon. **Bombas escondidas dentro do corpo: Uma nova fronteira para a Al Qaeda?** BBC Brasil. Disponível em: <http://www.bbc.co.uk/portuguese/noticias/2012/05/120523_bombas_alqaeda_dg.shtml > Acesso em Junho de 2012.

COUTO, Sérgio Pereira. **Decifrando a Fortaleza Digital**. Universo dos Livros. 1ª ed. 2005. p. 96.

CROSS, Michael. **Scene of the Cybercrime**. Syngress, 2008.

DERIAN, James Der. **In Terrorem: Before and after 9/11.** In 'Worlds in Colision'. New York: Newsweek, 2002.

DENNING, Dorothy E. **Is Cyber Terror Next?** Disponível em: <http://essays.ssrc.org/sept11/essays/denning.htm> Acesso em Junho de 2012.

Exame. **Anonymous derruba site do FBI após fechamento do Megaupload**. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/anonymous-derruba-site-do-fbi-apos-fechamento-do-megaupload> acesso em Janeiro de 2012.

FAGUNDES, Renan Dissenha. **Ciberterrorismo e as guerras virtuais preocupam governos.** Época. Disponível em: <http://revistaepoca.globo.com/revista/epoca/0,,emi105832-15227-2,00-ciberterrorismo+e+guerras+virtuais+preocupam+governos.html> Acesso em Maio de 2012

FRIEDMAN, Thomas L. **O Mundo é plano**. Objetiva. 2007. p. 505-508.

FURTADO, Vasco. **Tecnologia e gestão da informação na segurança pública**. Editora Garamond, 2002. p. 24.

G1. **Polícia Federal inaugura centro contra ataques cibernéticos.** Disponível em: <http://g1.globo.com/brasil/noticia/2012/06/policia-federal-inaugura-centro-contra-ataques-ciberneticos.html> Acesso em Julho de 2012.

___. **Hacker rouba senha e invade sistema administrativo do Twitter**. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1107777-6174,00-

hacker+rouba+senha+e+invade+sistema+administrativo+do+ttwitte.html> Acesso em Junho de 2012

___. **Pentágono admite ocorrência de vírus em seus computadores**. Disponível em: <http://g1.globo.com/Noticias/tecnologia/0,,mul871412-6174,00-pentagono+admite+ocorrencia+de+virus+em+seus+computadores.html> Acesso: em Junho de 2012.

GLOBAL SECURITY. The Comprehensive National Cybersecurity Initiative. Disponível em: < http://www.globalsecurity.org/security/library/policy/national/cnci_2010.htm> acesso: Junho de 2012.

GONTIJO, MENDES-SILVA; VIGGIANO; PAIXÃO. Cynthia Rúbia Braga; Ivone Maria; Adalci Righi; Edmilson Leite**. Ciberespaço: Que Território É Esse?** Disponível em: <http://ticsproeja.pbworks.com/f/Ciberespaco.pdf> Acesso em Março de 2012.

GORI, Umberto; PAPARELA, Ivo. **Invisible Threats: Financial and Information Technology Crimes and National Security**. IOS Press, 2006

GREGO, Maurício. **Ciberterrorismo**. Infoonline, 2000. Disponível em: < http://info.abril.com.br/edicoes/172/arquivos/2627_1.shl>. Acesso em Junho de 2012

History**. Cyberterrorism**. A&E Television Networks, 2003. (Documentário em DVD)

HOBSBAWM, Eric. **Globalização democracia e terrorismo**. São Paulo: Companhia das Letras, 2007. cap 8.

HOFFMAN, B**. Inside terrorism**. New York: Columbia University Press, 2006. p. 432

HORSLEY, Richard. **The Sicarii: Ancient Jewish Terrorists**. The Journal of Religion, Vol. 59, No. 4, 1979, p. 435-458.

KUMAR, Krishan **Da Sociedade Pos-Industrial A Pos-Moderna: Novas Teorias Sobre Mundo**. Rio De Janeiro: J. Zahar, 1997. p. 242

LANDIM, Wikerson. **EUA sofrerão grande ataque cibernético em breve, afirma FBI**. Disponível em: <http://www.tecmundo.com.br/ataque-hacker/20491-eua-sofrerao-grande-ataque-cibernetico-em-breve-afirma-fbi.htm> Acessado em Março de 2012.

LEÃO, Lúcia. **O labirinto e a arquitetura do ciberespaço**. (IN) GARCIA, Wilton e NOJOSA, Urbano. *Comunicação e Tecnologia*. São Paulo: U.N Nojsa, 2003. p. 155-157

LESSIG, Lawrence. **The Laws of Cyberspace.** Disponível em: <http://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf> Acesso em Março de 2012.

LEMOS, André. **Ciberurbe: A Cidade Na Sociedade Da Informação**. 2005 p. 251-267.

LÉVY, Pierre. A inteligência coletiva: por uma antropologia do ciberespaço. Loyola, 1998. p. 103-105.

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

MANDARINO Jr, Raphael. **Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro**. Brasília: UNB, 2009, p. 48.

NUNES, Paulo Fernandes Viegas. **Ciberterrorismo: Aspectos de Segurança.** Revista militar <http://www.revistamilitar.pt/modules/articles/article.php?id=428> Acessado em Março de 2012.

ONÇA, Fabiano. **O homem-bomba**. Disponível em: <http://guiadoestudante.abril.com.br/estudar/historia/homem-bomba-434600.shtml>. Acesso em Junho de 2012.

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 Junho de 2012.

RAMSBOTHAM, Oliver; WOODHOUSE, Tom; MIALL, Hugh. **Contemporary Conflict Resolution.** Ed. 3rd. Cambridge: Polity Press, 2011.

SAID, Edward W. **They call all resistance "terrorism"**. Disponível em: <http://www.thirdworldtraveler.com/Terrorism/Resistance_Terrorism_Said.html> Acesso em Junho de 2012.

SAINT-PIERRE, Héctor Luis. **Terrorismo: uma abordagem tipológica**. ANPOCS, 1996.

SEIXAS, Eunice Castro. **"Terrorismos": uma exploração conceitual**. Rev. Sociol. Polít., Curitiba, v. 16, número suplementar, agosto de 2008, p. 9.

SELAND, Torrey. **Establishment Violence in Philo and Luke: A Study of Non-Conformity to the Torah and Jewish Vigilante Reactions**. BRILL, 1995, p. 217.

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

SONY**. Customer Service Notification**. Disponível em: <http://www.soe.com/securityupdate/> Acesso em Junho de 2012.

TIKK, Eneken; KASKA, Kadri; VIHUL, Liis. **International Cyber Incidents: Legal Considerations.** Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010, p. 16-24.

TIKK, Eneken; OORN, Reet. **Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism.** In 'Responses to Cyber Terrorism'. COE DAT, 2008. Pp. 89-103.

VISACRO, Alessandro. **Guerra irregular: terrorismo, guerrilha e movimentos de resistência ao longo da História**. São Paulo: Contexto, 2009.

VERTON, Dan. **Al-Qaeda poses threat to net: pay heed to warning from bin laden associate, experts say**. Disponível em: < http://www.accessmylibrary.com/article-1G1-99601910/al-qaeda-poses-threat.html>. Acesso em Novembro de 2011.

WALTER, Laqueur. **A History of Terrorism**. Transaction Publishers, 2001.

_____**The New Terrorism: Fanaticism and the Arms of Mass Destruction**, Oxford University Press, 1999.

_____**The Terrorism to Come**. Hoover Institution, 2004.

_____**No End To War: Terrorism In The Twenty-first Century.** Continuum International Publishing Group, 2003.

WEINBERG, Leonard; EUBANK, William L. **What Is Terrorism?** New York: Infobase Publishing, 2006.

WEIMANN, Gabriel. **Cyberterrorism: How Real Is the Threat?** Special Research Report, Washington DC: United States Institute of Peace, 2004.

WHITE, Jonathan R. **Terrorism Homeland and Security**. Ed.7th .Wadsworth: Cengage Learning. 2012.

WITKER, Ivan. **Occidente Ante Las Nuevas Tipologías** Del Terrorismo. Estudios Públicos, 2005.

ZALMAN, Amy. **The History of Terrorism**. 2010. Disponível em: <http://terrorism.about.com/od/whatisterroris1/p/Terrorism.htm>. Acesso em Junho de 2012.

Glossário

Ciberataques – Ataques que utilizam o ciberespaço.

Cibercrimes – Crimes cometidos usando computadores e internet. Pode ser entendido também como uma subcategoria de crime.

Ciberterroristas – Terroristas que estão ligados à prática do terrorismo no ciberespaço, ou no caso de ataques, a junção do terrorismo e o ciberespaço juntamente com a cibernética (ferramentas) para a pretensão ou realização dos mesmos (ataques).

Hackers - Especialistas em computadores.

Proxy anônimo - É utilizado para proteger as informações pessoais ao ocultar a identificação do computador de origem, não mostrando seu verdadeiro IP ou burlar restrições de acesso. Ou seja, é como uma "maquiagem" para que o local real do computador não seja exibido.

Tecnodependência - Do inglês "tech dependence", termo designado para descrever a dependência da tecnologia.

Vírus – É um programa de computador criado para provocar algum dano nos computadores.