UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS ECONÔMICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ESTUDOS ESTRATÉGICOS INTERNACIONAIS

BRUNA TOSO DE ALCÂNTARA

INTERNET, TERROR E CIBERTERRORISMO: UMA ANÁLISE COMPARATIVA

Porto Alegre
2018

BRUNA TOSO DE ALCÂNTARA

INTERNET, TERROR E CIBERTERRORISMO: UMA ANÁLISE COMPARATIVA

Dissertação submetida ao Programa de Pós-Graduação em Estudos Estratégicos Internacionais da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título de Mestre em Estudos Estratégicos Internacionais.

Orientador: Prof. Dr. Érico Esteves Duarte

Porto Alegre

2018

CIP - Catalogação na Publicação

Alcântara, Bruna Toso de
Internet, Terror e Ciberterrorismo: uma análise comparativa / Bruna Toso de Alcântara. -- 2018.
142 f.
Orientador: Érico Esteves Duarte.

Dissertação (Mestrado) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Programa de Pós-Graduação em Estudos Estratégicos Internacionais, Porto Alegre, BR-RS, 2018.

1. Ciberespaço. 2. Terror. 3. Internet. I. Duarte, Érico Esteves, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

BRUNA TOSO DE ALCÂNTARA

INTERNET, TERROR E CIBERTERRORISMO: UMA ANÁLISE COMPARATIVA

Dissertação submetida ao Programa de Pós-Graduação em Estudos Estratégicos Internacionais da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título de Mestre em Estudos Estratégicos Internacionais.

Aprovada em: Porto Alegre, 14 de março de 2018.

BANCA EXAMINADORA:

_____

Prof. Dr. Érico Esteves Duarte - Orientador

UFRGS

_____

Prof. Dr. Marco Aurélio Chaves Cepik

UFRGS

_____

Profa. Dra. Danielle Jacon Ayres Pinto

UFSM

_____

Prof. Dr. Gills Vilar Lopes

UNIR

"In the end, defining cyberterrorism is an act of faith and a dedication to reason, It is faith in those who make policies and laws, in the agencies dedicated to stopping these activities, and in the power of reason over the passion of violence"
(BALLARD; HORNIK; MCKENZIE, 2002, p.994)

AGRADECIMENTOS

Agradeço à Universidade Federal do Rio Grande do Sul que, por meio do do Programa de Pós-Graduação em Estudos Estratégicos Internacionais, forneceu a mim estrutura e suporte necessário para a construção dessa pesquisa, bem como à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior por financiá-la.

Agradeço ao meu orientador, Prof. Dr. Érico Esteves Duarte, que sempre me incentivou e deu todo apoio intelectual necessário para o desenvolvimento da pesquisa. De modo semelhante, agradeço aos professores do programa que, de forma direta ou indireta, me auxiliaram a perceber novas perspectivas para o estudo das Relações Internacionais Cibernéticas (CiberRI).

Por fim, mas não menos importante, eu agradeço a minha mãe, Rosane Beatriz Toso, por todo seu esforço e aconselhamentos em diversos momentos da minha pesquisa e aos meus amigos por todas as ideias que proporcionaram debates frutíferos.

RESUMO

Com o objetivo de identificar a diferença entre o uso da Internet por terroristas e o uso do ciberespaço com fins políticos para o terror, a pesquisa proposta se desenvolve em cinco capítulos, além da introdução e conclusão. O capítulo 2 busca elucidar como os mundos físico e virtual se entrelaçam, explicando a vulnerabilidade das Infraestruturas Críticas aos ataques cibernéticos que geram o medo sobre o ciberterrorismo. Seguindo, no capítulo 3 explica-se o debate sobre a percepção acadêmica acerca do uso do ciberespaço por terroristas e, no capítulo 4, uma amostra de países relevantes para o combate ao terrorismo é posta em comparação, a fim de se entender as percepções políticas acerca do uso terrorista do ciberespaço. Nesse sentido, o estudo em voga, hipotético-dedutivo com caráter qualitativo em meio às análises e comparações, validou a hipótese de que, embora pertencentes a paletas do mesmo escopo, o uso da Internet por terroristas e o ciberterrorismo possuem diferenças significativas, sendo elas elencadas dentro de quatro categorias analíticas: Utilidade do ciberespaço, Foco Operacional, Uso de violência e Objetivo Último. Por fim, essas diferenças foram postas na conclusão como propostas de tipologias para a definição do fenômeno do ciberterrorismo e do uso terrorista da Internet, partindo da conceituação de terrorismo proposta por Eugênio Diniz (2002).

Palavras-chave: Ciberespaço. Terror. Internet.

ABSTRACT

In order to identify the difference between the use of the Internet by terrorists and the use of cyberspace for political purposes for terror, this research developes itself in five chapters, in which, in addition to the introduction and conclusion, in chapter 2, it seeks to elucidate how the physical and virtual worlds intertwine, explaining the vulnerability of Critical Infrastructures to cyberattacks that generate fear about cyberterrorism. Chapter 3 explains the debate about the academic perception of the use of cyberspace by terrorists and, chapter 4, a sample of countries that are relevant to the fight against terrorism is compared in order to understand the perceptions about the terrorist use of cyberspace. In this sense, the present hypothetical-deductive study with a qualitative character, in the midst of the analyzes and acquisitions validated the hypothesis that although belonging to palettes of the same scope, the use of the Internet by terrorists and cyberterrorism have significant differences, and they are listed within four analytical categories: Usefulness of cyberspace, Operational Focus, Use of violence and Last Objective. Finally, these differences were put in the conclusion as typology proposals for the definition of the phenomenon of cyberterrorism and the terrorist use of the Internet, rooted in the conceptualization of terrorism proposed by Eugênio Diniz (2002).

Keywords: Cyberspace. Terror. Internet.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

O termo ciberterrorismo apareceu pela primeira vez em um artigo de Barry Collin, nos anos 1980, significando o perigo de ataques conduzidos a distância, como consequência da interseção entre mundo físico e virtual, tendo como alvos Infraestruturas Críticas de um Estado (COLLIN, 1997). Contudo, foi somente no início da década de 1990 que grupos terroristas começaram a operar no mundo virtual com seus websites (WEIMANN, 2015), bem como declarações alarmistas emergiram como no caso do Conselho de Pesquisa Nacional dos Estados Unidos: "Os terroristas de amanhã poderão ser aptos a fazer mais danos com um teclado do que com uma bomba" (NATIONAL RESEARCH COUNCIL - NRC, 1991, p.07, tradução nossa).

Não obstante, foi com a proclamação da Guerra ao Terror pelos Estados Unidos que questões de terrorismo começaram a ter um maior peso nas agendas políticas mundiais, principalmente considerando a Resolução do Conselho de Segurança das Nações Unidas de 1373, a qual obrigou os Estados-Membros a se engajarem em medidas preventivas ao terrorismo. Dessa forma, em alguns casos como do Reino Unido, Canadá, Nova Zelândia e Austrália, as legislações antiterroristas têm um escopo amplo o suficiente para permitir inferências sobre a possibilidade de ação ciberterrorista (HARDY; WILLIAMS, 2014).

Apesar disso, no momento ainda não existe uma definição internacional padrão para esse fenômeno. Com isos, o debate acerca das ameaças que o ciberterrorismo apresenta continua vivo e ganhando cada vez mais relevância. Um exemplo disso foi o estudo conduzido em 2013 pela Swansea University no qual 36% dos entrevistados admitiram ser muito importante que tomadores de decisão *(policymakers*) tivessem uma resolução das questões de definição em torno de terrorismo, bem como 35% marcaram como quase essencial a necessidade de uma definição específica de ciberterrorismo. Além disso, 87% dos entrevistados consideraram como elemento característico do ciberterrorismo a motivação política e ideológica (MACDONALD; JARVIS; CHEN, 2013).

Diante de tal indefinição, diferentes conceitos e percepções de ataques cibernéticos, que são atribuídos como ciberterrorismo, somam-se para bloquear um melhor entendimento acerca do fenômeno. Na mídia sensacionalista, as diferentes expertises de autores que tentam conceituar o fenômeno (LUIIJF, 2014) e o próprio fato de que o termo terrorismo, em sua forma clássica, também não possui uma definição acordada internacionalmente, são alguns dos fatores que contribuem com a falta de compreensão sobre o que vem a ser o

ciberterrorismo. Essa falta de compreensão não apenas desnorteia a população de maneira geral, como também dificulta a construção de estratégias para combater o fenômeno, impactando diretamente nas tomadas de decisões, uma vez que subotimiza o conhecimento situacional.

Apesar desse cenário, Taliham (2010) aponta para uma divisão geral quanto ao ciberterrorismo, com duas orientações diferentes: uma para ferramentas (*tool-oriented)* e outra para os alvos (*target-oriented*). Em outras palavras, o segundo grupo coloca o ciberterrorismo como "todos os ataques politicamente ou socialmente motivados contra computadores, redes e informações, seja conduzidos por meio de outros computadores ou fisicamente, quando causam lesões, derramamento de sangue, dano grave ou medo" (TALIHAM, 2010, p.63, tradução nossa). Já para o primeiro grupo, o ciberterrorismo englobaria "todas as ações usando a Internet ou computadores para organizar e completar ações terroristas como terrorismo cibernético" (TALIHAM, 2010, p.63-64, tradução nossa). Weimann (2015), por outro lado, faz uma distinção entre o uso da Internet por terroristas com dois propósitos diferentes: um instrumental, que englobaria o treinamento e ensinamento; e o outro comunicativo, que envolveria a propaganda, a radicalização, campanha de guerra psicológica e a segurança das comunicações internas.

O que se entende das percepções desses dois autores é que parece haver, sendo necessária, uma diferenciação entre o ciberterrorismo e as outras ações levadas a cabo por terroristas na Internet. Nesse sentido, com a indefinição e a aparentes clivagens em abordagens, os discursos que vêm se desenvolvendo na esfera internacional são dispersos.

De fato, Maura Conway (2002, p. 06), por exemplo, coloca explicitamente que o uso terrorista da Internet se limitaria ao uso de tecnologias como facilitador de atividades enquanto o ciberterrorismo se caracterizaria pelo uso terrorista envolvendo a tecnologia informática como arma e/ou alvo. Já o relatório do Escritório de Drogas e Crime das Nações Unidas (UNODC), se dirige ao uso terrorista da Internet abrangendo uma abordagem "funcional" e englobando seis categorias: "propaganda (incluindo recrutamento, radicalização e incitamento ao terrorismo); financiamento; treinamento; planejamento (inclusive por intermédio de comunicação secreta e informações de fonte aberta); execução e ataques cibernéticos" (UNODC, 2012, p.3, tradução nossa). Salienta-se que alguns autores acadêmicos tendem a buscar explicações em raízes mais sociais e psicológicas para o fenômeno.

Charvat (2009), por exemplo, evidencia os motivos que impulsionam atividades terroristas a partir de quatro categorias:

a) terroristas com só um foco (ou seja, a motivação deles vêm de um assunto em particular, como os direitos dos animais);
b) terroristas ideológicos (que usam da violência para promover sua ideologia política, a qual se pauta nos extremos da direita ou da esquerda);
c) terroristas nacionalistas (os quais buscam independência de um dado Estado ou entrar de um Estado para outro por razões étnicas ou geográficas); e
d) terroristas político-religiosos (que podem se tornar letais dado que entendem suas ações como atos sob as ordens divinas).

De maneira parecida, Hardy e Williams (2014, p.21, tradução nossa), ao fazer uma análise legal entre alguns países da Commonwhealth Britânica, indicam em suas conclusões que o ciberterrorismo seria uma conduta:

> [...] envolvendo computadores ou tecnologia da Internet que (1) seja realizada com o objetivo de promover uma causa política, religiosa ou ideológica; (2) destina-se a intimidar uma seção do público, ou obrigar um governo a fazer ou abster-se de fazer qualquer ato; e (3) causa intencionalmente uma séria interferência com um serviço, instalação ou sistema essencial, se tal interferência puser em perigo a vida ou causar danos econômicos ou ambientais significativos.

Dentro desse último ponto, Denning (2001, p. 269, tradução nossa) também ressalta que o ciberterrorismo, para ocorrer, deve conter uma violência contra pessoas, ou propriedades, como resultado do ataque, "ou pelo menos causar danos suficientes para gerar medo". Sendo que, dependendo dos impactos do ataque na Infraestrutura Crítica, esses poderiam ser enquadrados dentro do fenômeno. Para entender ainda essa dinâmica dispersa, a perspectiva de Weimann (2005, p. 133) parece auxiliar na medida em que ele descreve o uso de computadores feito por terroristas como um "facilitador de suas atividades, seja para propaganda, recrutamento, difamação de comunicações ou outros propósitos que não simplesmente o ciberterrorismo".

Nota-se com o debate que a possibilidade de diferenciação não só parece factível como também pode ser analisada sob um prisma estratégico, tático e operacional. Afinal, como Yannakogeorgos (2014, p.60) coloca "muitas organizações terroristas estão aumentando o uso do ciberespaço para convergir seus objetivos táticos, operacionais e estratégicos" Assim, evitando, para além da inércia internacional em ações legais, duas grandes preocupações sociais: uma em relação ao nível de monitoramento de atividades digitais com base no discurso de combate ao ciberterrorismo e outra no tocante à possibilidade de não diferenciação entre hacktivismo e ciberterrorismo.

Awan (2014, p.2) explica que "tipos de comportamento podem ser ligados aos problemas e movimentos sociais, isso nos permite olhar para o ciberterrorismo através das lentes da mudança social". Contudo, como alerta Weimann (2004, p.5), a confusão entre atividades de hacktivismo e ciberterrorismo faz com que atos menores tomem proporções maiores a partir da mídia, contribuindo com a indefinição do fenômeno. Não obstante, o autor ressalta que "[...] mesmo assim o hacktivismo realça a ameaça do ciberterrorismo", uma vez que os terroristas podem se utilizar "dos caminhos já trilhados pelos hacktivistas, mas para alcançar seus propósitos de atingir governos". Segundo o autor, zonas cinzentas podem existir entre essas duas modalidades no ciberespaço se os terroristas forem capazes de recrutar ou contratar hacktivistas ou se hacktivistas decidirem ir mais além e operar no nível de Infraestruturas Críticas.

Assim, diante desse cenário, a pesquisa proposta focalizou o seguinte problema: Qual a diferença no uso da Internet por terrorismo e para o terror? Colocando como hipótese principal que, embora pertençam ao mesmo escopo, o uso da Internet por terroristas e o ciberterrorismo possuem diferenças significativas. Sendo essas diferenças empiricamente visíveis por intermédio das percepções estatais do *Five Eyes*.

Sendo assim, foram elaboradas como hipóteses auxiliares:

a) as diferenças significativas entre os fenômenos analisados estão, majoritariamente, na esfera estratégica e tática, implicando uso de diferentes recursos para a viabilidade organizacional e política dos grupos terroristas;
b) a percepção dos países quanto ao fenômeno do uso da Internet por terroristas molda as ações de grupos, tanto no uso da Internet quanto em manobras de ciberterrorismo.

A escolha pelo *Five Eyes* (Aliança ou Comunidade dos Cinco Olhos em português) se deu porque a questão do monitoramento, a indefinição sobre o que vem ocorrendo na Rede e o rótulo de ciberterrorismo em muitas atividades, dão margem para ações de *sniffing*[1] que, se não limitadas, podem cercear a privacidade da Internet. Assim, o *Five Eyes* se torna relevante já que tem um histórico de monitoramento que data desde a Segunda Guerra Mundial e, em particular depois dos anos 2001, constatou-se a existência de inúmeros programas digitais de vigilância operados de modo conjunto por esse grupo, incluindo programa Tempora e

[1] "Sniffing é a prática que, utilizando uma ferramenta genericamente chamada sniffer, intercepta e registra tráfego de dados e é capaz de decodificar o conteúdo trocado entre computadores de uma rede [...]. Um sniffer é um software que pode facilmente ser configurado para capturar fluxos específicos como sessões de telefonia por internet ou de e-mail. Uma vez que o tráfego é capturado, os crackers conseguem extrair rapidamente a informação que quiserem – logins, senhas e textos de mensagens" (PETRACIOLI, 2008).

Xkeyscore. Além disso, identificar o que os países dessa aliança estão propondo enquanto ações antiterroristas, com foco no ciberespaço, dialoga com Hardy e Williams (2014) em sua análise sobre legislação doméstica de quatro dos cinco membros do grupo.

Portanto, a pesquisa em voga foi moldada a partir do caráter básico e natureza qualitativa, com foco hipotético-dedutivo, bem como apresemta a divisão em dois níveis de análise: exploratória e descritiva. Ela é exploratória no sentido de fornecer maior familiarida com os conceitos propostos, com objetivo de torná-los mais claros. Ao mesmo tempo, ela se torna descritiva ao buscar descrever o fenômeno do ciberterrorismo na realidade.

Dessa forma, o estudo apresenta três procedimentos: revisão bibliográfica, revisão documental e análise comparativa de países membros da Aliança dos Cinco Olhos. A Revisão bibliográfica foi organizada com base na produção acadêmica levantada sobre o assunto sendo que, em específico sobre a definição de ciberterrorismo, as análises partirão de três autores: Dorothy Denning, Gabriel Weimann e Maura Conway. Todos são considerados expoentes acadêmicos na área, bem como evidenciam ideias ora complementares ora opostas sobre o fenômeno. Além disso, suas ideias serão complementadas por uma série de outros autores que contribuem com concepções próprias para o debate.

A análise comparativa tomou por base a amostra referente a Aliança dos Cinco Olhos (*Five Eyes*), a qual compreende os seguintes países: Estados Unidos, Reino Unido, Austrália, Nova Zelândia e Canadá. Essa aliança se trona relevante para refletir percepções políticas mundiais acerca do ciberterrorismo já que têm um histórico de monitoramento que data desde a Segunda Guerra Mundial e, em particular, depois dos documentos vazados por Edward Snowden, os países se enveredaram em uma série de polêmicas sobre a segurança cibernética se dar em detrimento à privacidade on-line.

Quanto à revisão documental, essa se dará principalmente com base nas estratégias nacionais cibernéticas e/ ou documentos oficias sobre o terrorismo e a Internet dos cinco países escolhidos, podendo incluir outros documentos e estratégias de defesa, como forma de aprofundar a contextualização desses países e suas percepções acerca do fenômeno do ciberterrorismo.

A pesquisa fez uso também do ecletismo teórico dividido em três blocos: Relações Internacionais (com foco na Escola de Copenhague e seu debate com a Escola de Paris), Estudos Estratégicos (com o debate sobre terrorismo e a utilização de uma base conceitual, advida da proposta de Eugênio Diniz) e Sociológico (ao se contextualizar a sociedade como Sociedade de Informação e Sociedade de Risco).

Sendo assim, o estudo evidencia como objetivo principal identificar o que diferencia o uso da Internet por terroristas e o uso com fins políticos para o terror. Para tanto, foram pensados nos seguintes objetivos específicos:

a) identificar como terroristas vem usando Internetcomo recurso para suas viabilidades organizacional e política;
b) evidenciar como o ciberespaço poder ser utilizado para provocar paralisia psicológica diante do terror;
c) destacar como o ciberespaço pode ser utilizado para uso de violência física;
d) constatar como os países percebem e reagem ao uso da Internet por terroristas.

O trabalho em voga apresenta quatro capítulos, contando com o da introdução. Assim, o Capítulo 2 busca contextualizar a questão da segurança cibernética para depois elucidar como o terrorismo cibernético é atrelado ao medo de ataques a Infraestruturas Críticas, detalhando como os mundos físico e virtual interagem e como as Infraestruturas Críticas se tornam vulneráveis no campo cibernético. O Capítulo 3 detalha a perspectiva acadêmica sobre como os grupos terroristas vêm utilizando o ciberespaço. Dessa forma, o capítulo desenvolve como essa perspectiva verifica, ou não, a afirmação de que o uso terrorista da Internet e o ciberterrorismo são percebidos como fenômenos diferentes, além de explicar como o conceito de ciberterrorismo deriva de percepções sobre o terrorismo e como, tanto o fenômeno do terrorismo quanto o ciberterrorismo, são diferenciados de outros fenômenos conflitivos. Por fim, o Capítulo 4 faz a composição da parte prática sobre as elaborações referentes aos fenômenos ao detalhar como as características do ciberterrorismo estão sendo discutidas e abordadas no cenário internacional, via análise das percepções governamentais acerca do assunto, a partir de uma amostra de países relevante: o *Five Eyes*.

Ressalta-se que a preocupação da pesquisa, de maneira geral, é elucidar até que ponto pode-se falar em uma nova modalidade de terrorismo que necessita de mecanismos de proteção diferenciados e próprios. Sendo assim, acredita-se que contribua academicamente com o debate sobre a caracterização do ciberterrorismo, já que pretende diferenciá-lo de outras ações terroristas, de menor impacto, que se dão no ciberespaço, além de procurar entender quais elementos das agendas políticas se dirigem ao fenômeno.

Quanto à justificativa social, a pesquisa se torna relevante, pois não só visa contribuir com o aclaramento do termo *per se*, mas também tem como objetivo alcançar o público em geral e quiçá os tomadores de decisão para que tomem consciência sobre o debate do terrorismo cibernético, possam tomar medidas proporcionais ou entrar em consenso quanto à elaboração de normas internacionais sobre o assunto.

As reflexões propostas são justificadas, também, por incitar o desenvolvimento de novos estudos dentro da seara do terrorismo e ciberespaço para que um diálogo mais profundo, com diversas perspectivas, aflore e permita o entendimento de ações humanas na seara cibernética.

Como última ressalva, coloca-se que quaisquer erros contidos na investigação são de resposnsabilidade da autora, bem como espera-se não esgotar o debate sobre o fenômeno do ciberterrorismo, mas abrir janelas de oportunidades para que novas pesquisas acerca do assunto surjam no mundo e no Brasil.

2 RECORTE TEÓRICO: CIBERESPAÇO, SEGURANÇA E INFRAESTRUTURAS CRÍTICAS

Para se entender como o terrorismo cibernético é atrelado ao medo de ataques a Infraestruturas Críticas, é necessário entender como o ciberespaço funciona; como os mundos físico e virtual se entrelaçam; e como as Infraestruturas Críticas se tornam tão vulneráveis e, no caso, alvos preferidos por grupos terroristas. Assim, eias as questões que o capítulo busca desvendar, antes de partir para a análise do fenômeno do terrorismo cibernético *per se*, realizado no capítulo 3.

2.1 O CIBERESPAÇO

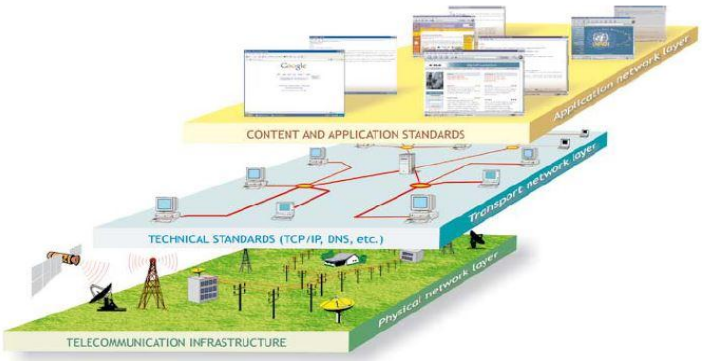
O mundo virtual começou a existir a partir da necessidade de comunicação a distância. Assim, foi com base na primeira conexão entre dois pontos de uma rede via computadores, nos Estados Unidos, em 1969, desenvolvida dentro do Âmbito da ARPANET [2] que a Internet nasceu. Contudo, foi em meados dos anos 1980, extrapolando o âmbito militar, e nos anos 1990, se espalhando mundialmente, que o modelo de Internet que conhecemos hoje se desenvolveu (LUCERO, 2011).

Segundo Kurbalija (2010, p.35-36), o ciberespaço é constituído por três camadas (ver Figura 01). A primeira é a camada física das redes, englobando a infraestrutura de telecomunicações, na qual todos os fluxos de internet fluem; a segunda é a camada lógica, que contém as normas e serviços técnicos da Internet para que ela funcione a exemplo do protocolo TCP/IP; a terceira é a camada de conteúdos e aplicação da rede, na qual se desenvolve padrões de aplicações a exemplo do HTML (Hyper Text Markup Language) e XML (Xtensible Markup Language). Conforme Canabarro (2014, p.70), uma quarta camada poderia ser adicionada, ou seja, a do:

[2]A ARPANET, acrônimo em inglês para *Advanced Research Projects Agency Network*, foi a primeira rede operacional de computadores à base de comutação de pacotes do Departamento de Defesa dos Estados Unidos, criada no âmbito da Guerra Fria, e somente para fins militares. Assim, apenas em 1983, quando o Departamento de Defesa criou uma rede exclusiva para uso militar (MILNET) a estrutura da rede (*backbones*) foi liberada para uso civil, em um primeiro momento para uso acadêmico, via a Fundação Nacional de Ciências (NSF) e depois com o advento da World Wide Web (WWW), com alcance mais generalizado (LUCERO, 2011; KUROSE, ROSS, 2012).

> [...] domínio das dinâmicas sociais, resultante do emprego da Rede como instrumento de forma de acesso àa divulgação e troca de informações; e como uma plataforma para a realização de transações econômicas, sociais e políticas diversas.

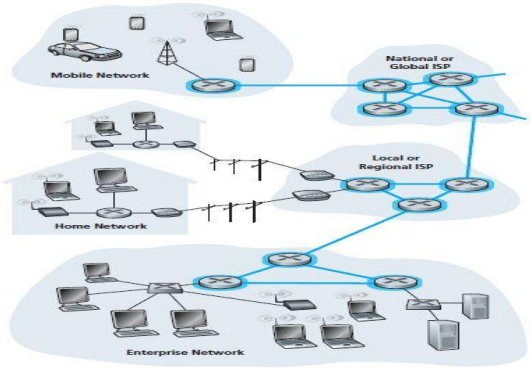
Figura 1 - Rede em Camadas



Fonte: Kurbalija (2010, p.35)

Por outro lado, Kurose e Ross (2012) entendem a infraestrutura da Internet de forma mais horizontalizada, como um sistema que envolve um centro e uma periferia. De maneira resumida, a periferia da Rede seria composta por outras redes de menor alcance e, individualmente, funcionariam como um sistema autônomo da Internet, sob a responsabilidade de um ou mais operadores periféricos.

Figura 2 - Comunicação Cliente-Servidor



Fonte: Kurose e Ross (2012, p.23)

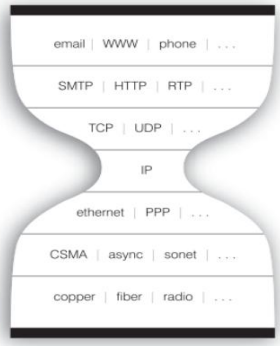
Assim, dentro da lógica cliente-servidor, uma aplicação cliente solicitaria e receberia informações de uma aplicação servidora, sendo cada rede identificada por um código de numeração para que as redes pudessem serem identificadas enquanto caminhos: parciais (intermediários) e finais (ver Figura 02).

Vale ressaltar que essa comunicação entre centro-periferia se dá via protocolos. Nesse sentido, a ideia de Zittrain (2008 p. 68) sobre um modelo do tipo ampulheta (Figura 03), explica melhor esse funcionamento, uma vez que parte de uma concepção da Internet dividida em camadas, como se fossem divisões de trabalho nas quais não são necessariamente os protocolos que precisariam ser coordenados ou entender uns aos outros. Isso faria com que não houvesse a necessidade dos usuários diferenciarem o tipo de conexão física empregada, por exemplo, "alguém pode escrever um novo aplicativo de mensagem instantânea sem ter que saber se seus usuários estarão conectados à rede por modem ou banda larga". Assim,

> o Protocolo incorporou tão poucos pressupostos sobre a natureza e do meio utilizado que o tornava sem fio que não violava nenhum deles. A grande variedade de formas de conexão física é representada pela ampla base para a ampulheta. Da mesma forma, os autores do Protocolo da Internet fizeram poucos pressupostos sobre os melhores usos da rede. Eles apenas forneceram um esquema de empacotamento e movimentação de dados, seja qual for o propósito. Este esquema permitiu uma proliferação de aplicativos de qualquer fonte interessada e talentosa, [...]. Assim, o topo da ampulheta também é amplo. É apenas o meio que é estreito, contendo o Protocolo da Internet, porque ele deve ser tão livre de recursos quanto possível. Ele simplesmente descreve como mover dados, e seus parâmetros básicos evoluíram lentamente ao longo dos anos (ZITTRAIN, 2008, p.69, tradução nossa).

Portanto, conforme Canabarro (2014, p.72), esse modelo explica a centralidade do *Internet Protocol* (IP), uma vez que a comunicação "apenas precisaria respeitar a lógica de funcionamento do IP- para a produção e a partilha de informações a partir da interconexão de redes distintas".

Figura 3 - Modelo Ampulheta do funcionamento do Internet Protocol



Fonte: Zittrain (2008, p.68)

Assim, de maneira simplificada, vale a explicação de Singer e Friedman (2014, p.23) sobre o funcionamento da comunicação dentro da Internet, dividida em sete passos:

a) se clica em um link em sua aplicação de navegador web, que traduz o clique em um pedido no protocolo HTTP;
b) as solicitação HTTP do aplicativo é cortada pelo sistema operacional em pequenos pacotes de IP direcionados individualmente;
c) o computador envia pacotes para a rede local;
d) cada pacote é encaminhado individualmente para uma rede maior, sendo que pacotes na mesma mensagem pode seguir caminhos diferentes;
e) Tier1 ou "back-bone" e redes encaminham tráfego para outros nós que estão mais próximos do endereço IP de destino;
f) o IPS (*Internet Service Provider*) do site envia o tráfego para o servidor web e
g) o servidor web reagrupa os pacotes e interpreta a solicitação HTTP para enviar o conteúdo da Web.

Em resumo, a visão de Kurbalija (2010) nos ajuda a entender que há um encontro entre o físico e virtual quando se fala em ciberespaço, já que diferencia uma camada da infraestrutura de telecomunicações. Ao mesmo tempo, a análise de Kurose e Ross (2012) nos permite entender a interdependência da Rede, com suas várias conexões. Zittrain (2008) também nos ajuda a entender, pensando em aspectos securitários, que o IP não foi desenvolvido com mecanismos de autoproteção, pois simplesmente buscava facilitar a comunicação, não se preocupando com quem a enviava ou qual informação estava sendo enviada. Por fim, Singer e Friedman (2014, p.25) apontam, de forma pertinente, que a partir do entendimento da arquitetura descentralizada da Internet se tiram 02 *insights* sobre a segurança cibernética:

a) oferece apreciação de como Internet funciona sem coordenação de cima para baixo;
b) a importância dos usuários e *gatekeepers* se comportando propriamente e como certos pontos de estrangulamento construídos podem criar grandes vulnerabilidades, caso esses mesmos usuários não apresentem comportamento apropriado.

Logo, como o foco da pesquisa é um aspecto conflituoso do ciberespaço, é interessante adentrar questões de segurança cibernética e também verificar como essa interdependência está relacionada não somente com os sistemas de rede, mas também com o lado físico do mundo.

2.2 SEGURANÇA CIBERNÉTICA

Vive-se atualmente em um mundo no qual vários aspectos da vida social estão ligados às tecnologias. Nesse sentido, o ciberespaço e sua interação com os seres humanos, levaram, segundo Radu (2014, p.06) ao desenvolvimento de duas escolas de pensamento: deterministas técnicos (os quais veem as tecnologias como principal motor da sociedade e valores culturais) e os construtivistas sociais (entendem a tecnologia como socialmente construída). Sendo que no meio dessas perspectivas surge uma abordagem sociotecnológica, a qual a dinâmica das mudanças tecnológicas é potencializada por escolhas individuais e refletem relações de poder subjacentes.

Uma percepção parecida é feita por Lango (2016), para o qual há duas escolas de pensamento quanto à percepção securitária do ciberespaço: os revolucionários e os tradicionalistas. Os primeiros têm um pensamento expansivo e positivo sobre tecnologias no conflito, admitindo que elas podem alterar tudo, inclusive o modo de se fazer guerra. Por isso, diante das potencialidades dos conflitos cibernéticos de alta escala (i.e. guerra e terrorismo) sua retórica se torna mais alarmista. Já os tradicionalistas veem o ciberespaço e ataques cibernéticos como diferentes ferramentas para o que já é conhecido; ficam relutantes em descartar conceitos, doutrinas e políticas já existentes de forma prematura; são mais céticos em relação ao grau de transformações tecnológicas, embora admitam que haja potencial para conflitos de alto impacto, explicam que ele ainda não é foi desenvolvido na realidade. Contudo, existem algumas tendências acadêmicas culminando em uma terceira via: os ambientalistas, os quais mantêm como foco as características e traços próprios do ciberespaço tendo o poder no âmago de suas pesquisas.

Dessa forma, independente da escola de pensamento, vale entender que a dependência das tecnologias criou um círculo viciante que atrela cada vez mais a sociedade, inclusive o aparato estatal, as tecnologias de informação (TICs). Isso se dá porque:

> [...] as inovações técnicas são uma consequência da demanda da sociedade, assim como o desenvolvimento de inúmeras ferramentas para facilitar a vida na Rede e a emergência de novas formas de interação entre os usuários da Internet, o que novamente cria novas demandas e inovações tecnológicas (CALVETY, 2002, p.69, tradução nossa).

Por isso, a sociedade do século XXI é apontada por vários autores da Sociedade de Informação. Contudo, dada as escolas de pensamento explicitadas, alguns estudiosos

perceberam a sociedade contemporânea sob perspectivas diferentes em relação à tecnologia. Assim, por questões técnicas, na pesquisa em voga considera-se o conceito de Cavelty (2002, p.71, tradução nossa) sobre Sociedade de Informação, ou seja,

> a Sociedade de Informação é aquela parte da sociedade que experimenta uma revolução da informação. É uma sociedade cada vez mais dependente das TIC e em que a utilização regular das TIC é o padrão. Isso depende principalmente das TIC para o trabalho, das transações econômicas, da vida cotidiana, do bem-estar, do conforto e da interação pessoal.

Tal definição ajuda a entender a correlação de dependência entre o mundo físico e digital, via as dependências humanas. Consequentemente, como os seres humanos se organizam, em sua maioria, de forma institucional, a "a administração de toda e qualquer infraestrutura social" (MANDARINO, 2010, p.22) também entra nessa equação de dependência, ou seja, uma primeira perspectiva sobre o atrelamento do Estado para com as TICs nos é fornecida.

Igualmente, pelo ciberespaço ser um ambiente totalmente produzido pelo ser humano cabe a ideia de Sociedade de Risco de Ulrich Beck. Para esse autor, a sociedade estaria vivendo uma segunda modernidade, diferente da primeira modernidade que se baseava nas relações sociais e as redes e as comunidades assumiam um caráter territorial (i.e. local). Assim, a sociedade industrial foi substituída por uma sociedade de risco, em que tais teriam uma distribuição global não correspondente às diferenças sociais, econômicas e geográficas. Em outras palavras, o risco contemporâneo seria "uma forma sistemática de lidar com riscos e inseguranças induzidas e introduzidas pela própria modernização" (BECK, 1992, p.21, tradução nossa). Dessa forma, as sociedades seriam construídas em torno da percepção de ameaças que determinariam forma de se pensar e agir (LEVITAS, 2000, p.213). Portanto, em que pese Beck tenha se centrado nos riscos do setor ambiental para embasar sua teoria, Radu (2014, p.9) coloca que essa determinação de pensamento e ação faz com que representações discursivas da segurança cibernética tornem-se "fundamentais para criar a realidade e para determinar a percepção de risco no nível global". Afinal, ao tratar da Sociedade de Risco, focalizam-se os hibridismos[3], o que o ciberespaço vem provocando em matéria de conflitos, uma vez que, segundo Beck (2002, p. 221, tradução nossa): "risco não é apenas uma noção

[3] Conforme Beck (2000, p.221, tradução nossa): "os riscos são híbridos artificiais. Incluem e combinam política, ética, matemática, mídia de massa, tecnologias, definições culturais e percepções; e, o mais importante de tudo, não pode separar esses aspectos e "realidades" quando se deseja entender as dinâmicas culturais e políticas da sociedade de risco mundial."

que é usada em um assunto central por disciplinas muito diferentes, é também a forma como a "sociedade híbrida" observa, descreve, valoriza e critica sua própria hibridez".

Diante dessas colocações, percebe-se a falta de consenso sobre como se interpretar e, consequentemente, agir em prol da segurança cibernética. Isso gera várias inconsistências conceituais, que fazem as pesquisas avançarem "em analogias insatisfatórias" e "criarem quadros analíticos sem consistência teórica, lógica e empírica" (CANABARRO; BORNE, 2013, p.5). Além disso, prejudicam análises mais apuradas sobre os conflitos cibernéticos, bem como suas complexidades vêm se agravando com a intensificação do processo de securitização do ciberespaço (CEPIK; CANABARRO; BORNE, 2014, p.179).

Sendo assim, esse alto grau de variação quanto às definições, uma vez entendida a lógica da sociedade em relação às tecnologias (da Sociedade de Informação) e que essa sociedade age em conformidade com as ameaças de riscos percebidas (da Sociedade de Risco), pode-se entender melhor como a segurança cibernética vem se desenvolvendo no âmbito internacional. De maneira geral, podemos dizer que ela "tenta garantir a obtenção e manutenção das propriedades de segurança da organização e dos recursos dos usuários contra riscos de segurança relevantes no ambiente cibernético" (MUNK, 2015, p.47, tradução nossa).

De acordo com Nye (2010, p.16), esses riscos de segurança foram traduzidos em quatro principais ameaças cibernéticas: espionagem econômica, crime, guerra cibernética e terrorismo cibernético, cada qual com uma solução e um horizonte de tempo diferente. Todavia, de uma maneira um pouco mais metódica, vale a explicação do modelo expandido de Mccamber, com base no qual a garantia de informação deveria ser analisada em quatro dimensões: Informação de Estados, Segurança de Serviços, Segurança de Contramedidas e Tempo (SHAKARIAN; SHAKARIAN; RUEF, p.6).

Enquanto a informação de Estados lidaria com os aspectos da informação (estocada, transmitida e processada), a segurança de sistemas teria como objetivos gerais garantir a disponibilidade, integridade, confidencialidade, autenticação e o não repúdio[4]. A segurança de contramedidas faz referência a atenção que pessoas, operações e tecnologia devem receber, enquanto possíveis vulnerabilidades. Por fim, a questão temporal indica a mutabilidade e evolução do meio digital que afeta, de maneira dinâmica, as outras três dimensões (SAKARIAN; SHAKARIAN; RUEF, 2013, p.6-7)

[4] A disponibilidade se refere ao fato das redes estarem aptas a ser utilizadas, ou seja, estão disponíveis aos usuários; a integridade se refere ao funcionamento sem interferências externas; a confidencialidade se refere ao sigilo das informações, resguardando a privacidade dos usuários sem que terceiros as obtenham; a autenticação se refere à verificação dos comandos enviados, e o não-repúdio refere-se à garantia de que o remetente dos dados é fornecido com comprovante de entrega e o destinatário é fornecido com prova da identidade do remetente (SHAKARIAN; SHAKARIAN; RUEF, 2013 p. 7-8).

Tendo essas dimensões em mente, entende-se que o ciberespaço é totalmente interligado, percebe-se que não apenas atores estatais, mas não-estatais se envolvem na interação com o mundo virtual. Não obstante, quando se trata de ameaças cibernéticas, os Estados se mobilizam de maneira mais organizada, ainda que descompassada com a evolução das ameaças. Alguns dados da *International Teleccomunication Union* (ITU) acerca da segurança cibernética (*Global Cyber Security Index*) revelam aspectos internacionais valiosos.

O Index Global de Segurança Cibernética foi desenvolvido sob a égide da Resolução 130 (Rev. Busan, 2014) [5] pautando-se conforme a Agenda Global de Segurança Cibernética da União e seus cinco pilares, a saber: legal, técnico, organizacional, formação de capacidades e cooperação (ITU, 2017). Igualmente relevante é que a elaboração do Index foi conjunta com ABI Research[6]. Assim, até o momento, foram gerados dois indexes: o primeiro em 2014 e o segundo em 2017.

Comparando os dois indexes, nota-se a diferença de classificação dos três primeiros colocados e os três últimos colocados. Quanto aos primeiros lugares, em 2014, eles pertenciam respectivamente os Estados Unidos, Canadá e Austrália, e, em 2017, passaram a pertencer a Singapura, Estados Unidos e Malásia. Já os últimos colocados, em 2014, eram respectivamente Namíbia, São Vicente e Granadinas e Timor-Leste, e, em 2017, a República Centro-Africana, Iémen e Guiné Equatorial. Essa realocação permite inferir que houve uma mudança internacional acerca de aspectos securitário ao ciberespaço, uma vez que regiões orientais começaram a se preocupar com o assunto. Outrossim, dada a variação da penetrabilidade da Internet[7], percebe-se que as ações dos países em prol da segurança do ciberespaço são diretamente proporcionais ao grau de conectividade à rede, considerando os últimos lugares.

Ademais, o Index de 2017 avança nas análises quando evidencia que, em um universo de 193 países apenas 38% possuem uma estratégia de segurança cibernética publicada, sendo que apenas 11% possuem uma estratégia dedicada à área de forma autônoma, e só outros 12%

---

5 Sobre o fortalecimento do papel da ITU na criação de confiança e segurança no uso das TICs.

6 "A ABI Research é uma empresa de inteligência de mercado especializada em mercados globais de tecnologia a partir de previsão quantitativa e análise de métricas e tendências chave. Com competência exclusiva para fornecer visão de futuro e pontos de dados atuais, atecipados e reais no setor de tecnologia, a ABI Research possui conjuntos de habilidades principais em desenvolvimento de estratégia, inteligência competitiva, planejamento de negócios, desenvolvimento e priorização, avaliação de tecnologia e benchmarking do setor" (ABI RESEARCH, 2017, tradução nossa).

7 Segundo o site da Internet World Stats (2017), a penetrabilidade da Internet e, consequentemente, junto a Rede varia ao redor o mundo. Sendo que dados de 30 de junho de 2017, além de demonstrarem que a média mundial de penetrabilidade da Internet é de 51,7%, demonstraram que na África ela representa 31,2%; na Ásia 46,7%; na Europa 80,2%; na América Latina e Caribenha 62,4% ; Oriente Médio 58,7% , na América do Norte 88,1% e na Oceania 69,6%.

tem uma estratégia de segurança cibernética em desenvolvimento. Em outras palavras, isso significa que 50% dos países analisados não desenvolveram documentos que "descreva [m] como o país irá preparar e responder a ataques contra suas redes digitais" (ITU, 2017, p.17).

Apesar disso, como mostra Nascimento (2015), os países que se preocupam com o desenvolvimento de estratégias adotam estruturas civis ou civis e militares para tratar de conflitos cibernéticos. Todavia, como o mapa demonstra (Figura 04), há um grande envolvimento de países tanto na região asiática, quanto europeia e americana que optam pelo atrelamento militar no tocante à segurança cibernética. Isso evidencia uma tendência não só da securitização do ciberespaço como também a sua spossível militarização.

Esse debate sobre securitização e militarização do ambiente cibernético é interessante, pois levou repercussões acadêmicas dentro dos estudos de segurança, principalmente ao se falar em um ambiente que tem uma parte intangível. Essa repercussão se desenvolve na proposta de Hansen e Nissenbaum (2009) em expandir os setores de securitização postos pela Escola de Copenhague, colocando o setor cibernético junto à lista, ao lado dos setores: militar, político, econômico, ambiental e societal (BUZAN, 1991).

A Escola de Copenhague, tendo como expoentes Buzan, Waever e Wilde (1998), buscou dentro do contexto pós-Guerra Fria ampliar e definir assuntos sobre Segurança Internacional. Daí o uso de uma concepção de segurança abrangente contendo as cinco áreas explicitadas acima. Nesse sentido, com foco no discurso como agente transformador, a estrutura de análise dos assuntos de segurança seria definida pelas Unidades de Análise em Segurança, compreendendo: Objeto Referência, ou seja, a coisa existencialmente ameaçada; o Ator securitizador, que securitiza o tema e declara que o Objeto de Referência está ameaçado; e o Ator Funcional que nem sempre está presente, mas faz referência aos atores que influenciam (como uma variável interveniente) os debates sobre segurança (BUZAN; WAEVER; WILDE, 1998, p.36).

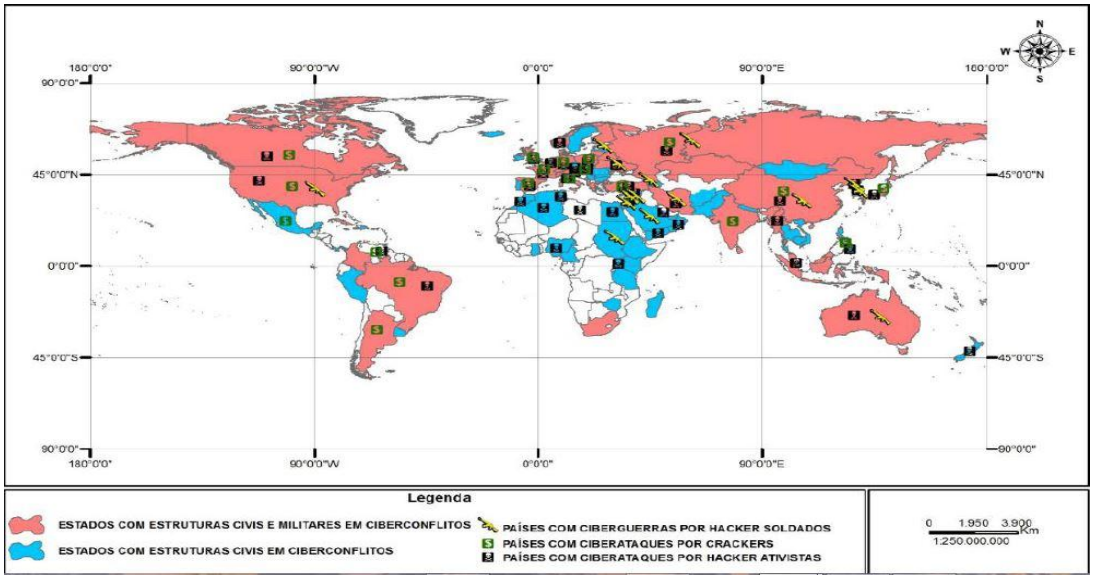
A ideia central dessa Escola é que ameaças existenciais aos Estados e sistemas de redes podem gerar a mudança de um tema de uma agenda política (tema politizado) para a agenda de segurança. Esse movimento de mudança é o que Buzan, Waever e Wilde (1998) chamam de securitização. Então, uma questão poderia se encontrar dentro em três categorias: não politizado (fora da agenda política), politizado (dentro da agenda e do debate político) e securitizado (dentro da agenda de segurança) (BUZAN; WAEVER; WILDE, 1998, pp. 23-24).

De forma resumida, a securitização de um tema começaria com um movimento de securitização, que somente seria efetivado caso uma audiência aceitasse como legítima a

demanda do agente securitizador, proporcionando que a ameaça fosse estabelecida com relevância suficiente para justificar a quebra de regras normais da política, como forma de contrabalancear a ameaça em questão (BUZAN; WAEVER; WILDE, 1998, p.25).

Hansen e Nissembaum (2009, p. 1157) usam da ideia de securitização para aplicá-la ao ciberespaço, colocando como evidências dessa securitização desenvolvimentos institucionais, por exemplo: a criação pelo presidente Clinton da Comissão sobre Proteção de Infraestruturas Críticas, em 1996; a localização proeminente da segurança cibernética no Departamento de Segurança Interna; a formulação do presidente Bush da Estratégia Nacional de Segurança do Ciberespaço, em 2003; e a criação de um centro de defesa cibernética apoiado pela Organização do Tratado Atlântico Norte na Estônia, em 2008. Atualmente, outros desenvolvimentos institucionais também corroborariam a ideia de securitização exitosa do ciberespaço e, desde 2009 até 2015, o mapa de Nascimento (2015) embasa ainda mais essa visão.

Figura 4 - Mapa de estruturas estatais de conflitos cibernéticos no mundo



Fonte: Nascimento (2015, p.40)

Uma vez entendida que há a securitização do setor, Hansen e Nissembaum (2009) consideram que a segurança da rede e a segurança individual se tornam objetos referentes significativos, mas com sua importância política surgindo das conexões aos objetos referentes coletivos do Estado, sociedade, nação e a economia. Assim, a articulação dos objetos

referentes como ameaçados se daria a patir de três formas distintas de securitização: hipersecuritização, práticas diárias de segurança e tecnificação.

Na hipersecuritização, o discurso toma um tom mais exagerado e, dentro da segurança cibernética, "depende de cenários de desastres cibernéticos multidimensionais, que embalam uma longa lista de ameaças graves em uma sequência de cascata monumental e o fato de que nenhum desses cenários ocorreu até agora" (HANSEN;, NISSEMBAUM, 2009, p.1164). Essa multidimensionalidade faz referência às consequências militares, financeiras e sociais que ataques cibernéticos podem provocar.

As práticas diárias apresentam relação com a forma e os agentes securitizadores, o que inclui atores não-estatais, mobilizam as experiências normais de indivíduo em prol da garantia da parceria na proteção, segurança das redes e tornar os cenários de hipersecuritização mais factíveis, ao ligarem "elementos do cenário do desastre para experiências familiares da vida cotidiana" (HANSEN; NISSEMBAUM, 2009, p.1165, tradução nossa). Em outras palavras, essa forma se concentraria na ideia de aceitação da audiência, que fica facilitada com o uso de um vocabulário próximo ao biológico, no caso, o uso de termos como "vírus e infecções" (HANSEN; NISSEMBAUM, 2009, p.1166, tradução nossa).

Por fim, a tecnificação se referiria ao espaço que a área cibernética deixa para discursos técnicos. Essa categoria surgiria da própria lógica de securitização já que "se a segurança cibernética é tão crucial que não deve ser deixada aos amadores" (HANSEN; NISSEMBAUM, 2009, p.1167, tradução nossa). Nesse sentido, as autoras alertam para o conhecimento técnico que se sobressai em relação ao da segurança internacional que leva progressivamente a despolitização do assunto, uma vez que se restringiria a uma visão técnica (HANSEN; NISSEMBAUM, 2009, p.1668).

A proposta de Hansen e Nissembaum (2009) foi uma das poucas alternativas teóricas específicas voltadas ao ciberespaço, o que demonstra a necessidade de estudos adicionais nessa seara. Isso não significa que alguns debates teóricos não ocorram. Nesse sentido, é relevante a discussão feita por Munk (2015).

Para Munk (2015), o papel teórico da Escola de Copenhague se deu de forma marginal no entendimento das dinâmicas conflitivas do ciberespaço. Mais relevante seria a abordagem da Escola de Paris por não ser estatocêntrica, compreendendo grupos e indivíduos em particular e ao afirmar que a segurança também diz respeito à identidade e à cultura de sociedades particulares, comunidades locais ou religiões. Principalmente ao se pensar na falta de fronteiras dentro no ciberespaço (MUNK, 2015, p.100).

A segurança cibernética necessitaria de um arcabouço baseado na resiliência e preparação, ligados à gestão de risco e práticas de governança antecipatória (preventiva) (MUNK, 2015, p.46). Dessa forma, a resistência aos ataques cobriria a cooperação de aspectos operacionais e políticos de organizações governamentais, harmonização via cooperação, legislação internacional e o envolvimento de atores não-estatais (MUNK, 2015, p.178). Em outras palavras, em que pese que a securitização dê ao Estado o poder, enquanto agente securitizador, de escolher quais são as ameaças passíveis de entrarem na agenda de segurança, o entendimento de securitização segundo à Escola de Copenhage não aborda de uma maneira eficaz a parte privada da equação.

Nesse sentido, Munk coloca que a Escola de Paris vê uma agenda de segurança expandida e profunda já que a ameaça não é mais externa, ou seja, há a diluição da divisão entre ameaças externas e internas, e os problemas de execução da segurança cibernética se relacionam com o aumento do uso das tecnologias no dia a dia resultando em riscos possíveis para grupos e indivíduos (MUNK, 2015, p.100). Ainda, para corroborar sua linha de raciocínio, ele usa como ilustrações as questões do crime cibernético e ciberterrorismo. Em específico quanto ao ciberterrorismo, na sua visão, atualmente ataques ciberterroristas não são somente dirigidos aos Estados, mas também contra populações civis (MUNK, 2015, p. 171) e implicações políticas e militares afetam a sociedade, uma vez que é ela é dependente das novas tecnologias. Dessa forma, para o autor, a tensão na governança em relação ao ciberespaço vem de medidas centradas no Estado em um ambiente que é composto por múltiplos atores securitários (MUNK, 2015, p. 185).

Ainda ao nível teórico, mas menos específico ao setor cibernético, existem três outras escolas com visões acerca do ciberespaço e suas inseguranças: Realismo, Liberalismo/Neoliberalismo e Escola Inglesa (ERIKSSON; GIACOMELLO, 2006; ACACIO, 2016). As quais estão sintetizadas no Quadro 01.

Quanto ao Realismo, por se tratar de uma teoria estatocêntrica, vê na anarquia internacional a necessidade do Estado estar sempre alerta para garantir sua sobrevivência, agindo como um ator racional; seus pensadores vão entender o domínio digital como mais um espaço para se apropriar e projetar poder, ganhado maior influencia perante outros Estados (ACACIO, 2016, p.41) Ainda, um entendimento restrito de segurança vai prevalecer (área militar) fazendo com que considerem que as “ameaças de segurança relacionadas à TI são em grande parte uma questão econômica, não necessariamente afetando a segurança dos estados e não em si mesmas ameaças de segurança”(ERIKSSON; GIACOMELLO, 2006, p.229, tradução nossa).

O Neoliberalismo, por lidar com uma visão de mundo mais cooperativa advinda do liberalismo clássico, enfatiza a influência das instituições internacionais, aceitando em sua análise a inclusão de atores não estatais. De fato, assim como as organizações e regimes internacionais servem como ferramentas influenciadoras dos Estados, a arquitetura aberta do ciberespaço força uma governança na Internet *par excellence* pela criação de regimes internacionais e instituições de fomento e cooperação internacional em matéria de defesa e segurança internacional (ACACIO, 2016, p.48). Com isso, traços de liberalismo podem ser entendidos quando a ênfase das ações se coloca nas parcerias público-privadas (ERIKSSON,; GIACOMELO, 2006, p.231), uma vez que, no ciberespaço, a divisão entre militar e civil se esvai, já que a Rede permeia os dois setores, muitas vezes cruzando-os.

Por fim, para a Escola Inglesa, o ciberespaço permite ser usado pelo estadista como ferramenta, sendo possível traçar um perfil do estadista por trás de ações securitárias no ciberespaço. Além disso, o equilíbrio de poder também é projetado no ciberespaço, já que nem todos os Estados veem a questão de segurança e defesa desse ambiente da mesma maneira, gerando, muitas vezes, "a justificativa para a tomada de determinadas ações estratégicas o ciberespaço" (ACACIO, 2016, p.45) Além do debate sobre uma Guerra Fria cibernética ganhar espaço nessa perspectiva teórica, uma vez que Wright, um dos expoentes teóricos, considera que uma crise se caracteriza, entre outras coisas, por uma corrida armamentista (ACACIO, 2016).

Quadro 1 - As teorias de Relações Internacionais e o Ciberespaço

Escopo quanto à insegurança do ciberespaço	Abordagem teórica	O que dizem (ou podem dizer) sobre a insegurança do ciberespaço
Mais geral (ontológico)	Realismo	- ciberespaço é novo domínio operacional no qual Estados devem agir para mitigar insegurança ocasionada por ameaças a suas infraestruturas críticas, buscando projetar poder e influência, maximizando seus interesses.
	Escola Inglesa	- ciberespaço enquanto instituição efetiva da sociedade da informação
Mais específico (pragmático)	Neoliberalismo	- Direito internacional, regimes internacionais e organizações internacionais (OEA, OTAN, ONU) podem fomentar cooperação internacional - *cyber Power*
	Escola de Copenhague	- temática da Segurança Cibernética é passível de Securitização por Estados

Fonte: Acacio (2016, p.56)

Diante de todas essas possibilidades teóricas, adota-se, na dissertação em voga, uma abordagem mais próxima da Escola de Copenhague para a pesquisa, a qual embora não análise o processo de securitização do ciberespaço em si, o considera como dado. Nesse sentido, vale uma reflexão mais profunda acerca da proposta de Munk (2015), o qual exagera na análise colocando que a Escola de Copenhague retém pouco valor ao se debater sobre a segurança cibernética. Embora se deva reconhecer a relevância de atores não-estatais no domínio digital, principalmente depois de episódios como a Primavera Árabe (2010) e Snowden (2013), ataques a uma população significam ataques a um Estado, principalmente se o alvo for escolhido por motivação política (como o caso do ciberterrorismo); eles não se destinguem, principalmente em razão de não haver limites definidos entre público e privado no ciberespaço. Ademais, se pensarmos na Escola de Paris como base de análise, as variáveis já em alta quantidade se tornam ainda maiores, dificultando a viabilidade científica. Afinal, quer queiramos ou não, em que pese o ciberespaço possa dar uma luz para a sociedade cosmopolita ao modo kantiano (*netzens*), sua parte atrelada ao mundo físico não parece demonstrar nenhum avanço nesse sentido. Talvez, por isso, Munk (2015) não descarte totalmente a Escola de Copenhague. Tal dualidade virtual-física coloca o Estado no estudo do ciberespaço desde que este último ainda é produzido a partir da alocação de recursos. Entende-se que isso não permite uma visão mais aberta em relação à centralidade das grandes potências e, por hora, do papel do Estado como uma última instância de tomada de decisão na securitização do ciberespaço. Dessa forma, concorda-se com Drezner (2007) quando ele coloca que os Estados têm seu poder aumentado na Era Digital devido a estratégias no ciberespaço que continuam a visar seus interesses próprios. Em outras palavras,

> [...] os estados podem e substituirão diferentes estruturas de governança dentro de um complexo de regime comum, e eles substituirão diferentes ferramentas políticas para criar essas estruturas, dependendo da aparência do interesse da grande potência (DREZNER , 2007, p.92, tradução nossa).

Todavia, isso não significa que os outros atores internacionais não tenham peso ou relevância, ou que não possam digladiar-se entre si. Apenas significa que sob a visão da pesquisa proposta, pensando em uma visão macro (internacional) e em uma escala conflitiva maior (se pensarmos em guerra e terrorismo cibernéticos), os atores não estatais se tornam mais “peões do que reis ou rainhas” dentro do jogo de poder internacional, já que normalmente vão significar uma afronta a uma hierarquia maior, ou seja, o Estado. Dessa forma, análises individuais são excelentes para que seja possível traçar perfis desviantes ou

entender contextos que levaram a o ataque X ou Y, não para delinear estratégias *per se*. O que se torna, sim, passível é a abrangência pelos Estados de cooperações público-privadas, mas sob a organização última do Estado.

Além disso, como Calvety (2007, p.22) coloca, o debate sobre ameaças cibernéticas sempre foi altamente político, envolvendo a preparação dos tomadores de decisão (i.e. Estados) dentro de uma lógica probabilística de riscos futuros, com uma míriade de narrativas sobre o que irá acontecer e como irá acontecer. Essas diversas narrativas, que incluem a questão do ciberterrorismo, não deixam de se colocar em um formato conflitivo envolvendo relações de poder, que internacionalmente direcionariam, então, para aos Estados e suas posições diante das ameaças cibernéticas, gerando o que Nye (2010), por exemplo, propõe como poder cibernético. De qualquer forma, o que aqui se enfoca é que assumindo o viés contrutivista da pesquisa e a importância do Estado perante às questões de segurança e defesa do ciberespaço a percepção estatal acerca de ameaças, como o ciberterroismo, se torna relevante e parte do mundo empírico, uma vez que essas percepções vão gerar ações concretas.

Por fim, como o ciberespaço tem uma camada física ele se atrela impreterivelmente ao Estado, como coloca Nye (2010, p.15, tradução nossa), ele se torna um "bem comum imperfeito ou um condomínio de propriedade conjunta sem regras bem desenvolvidas", afinal essa infraestrutura passa por um território soberano, onde na impossibilidade de qualquer alternativa viável o Estado ainda detem o monopólio da força. Assim, em específico, a relação do Estado com a questão do ciberterrorismo, só pode ser entendida a partir de seu medo oriundo de ataques a Infraestruturas Críticas nacionais.

2.3 INFRAESTRUTURAS CRÍTICAS

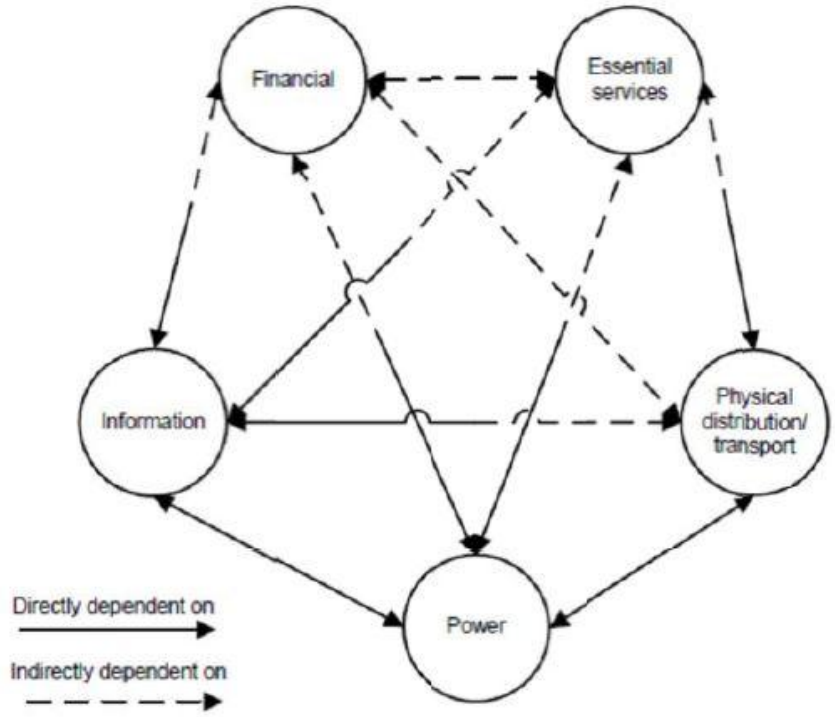
A importância do Estado e sua relação com o ciberespaço ficam mais esclarecidas se adentrarmos na noção de Infraestrutura de Telecomunicações Global, teorizada por Edward Waltz (1998, p.175), a qual ele considera ser a camada de conexão entre o complexo de comunicações de transmissão, telecomunicações e computadores que fornecem comunicações globais, comércio, mídia, navegação e serviços de rede e as Infraestruturas Nacionais de Informação. Em outras palavras, podemos fazer referência à Internet como *de facto* tal Infraestrutura, mas a questão de interdependência vai para além da explicação de como a própria Rede funciona, e a palavra-chave nesse sentido é Infraestrutura Crítica.

Segundo Clemente (2013, p.17), uma Infraestrutura Crítica é mais do que uma mera infraestrutura, ela inclui informação que é crítica ao funcionamento de tal estrutura, chegando ao ponto de estarmos nos aproximando de uma distinção irrelevante entre infraestrutura e infraestrutura de informação. Niekerk e Maharaj (2011, p.101, tradução nossa) apontam que essas infraestruturas seriam consideradas críticas por serem "vitais para o bem-estar e o funcionamento de uma organização, sociedade ou nação". Sendo que "qualquer perturbação dessas infraestruturas resultará em uma grave degradação ou prevenção de capacidades operacionais e prestação de serviços".

Johnson (2012, p.8-9) reforça essa ideia de manutenção da coesão social pelas Infraestruturas Críticas ao enfatizar que uma perturbação nelas causaria resultados desastrosos e economicamente devastadores, dando como exemplos de tais infraestruturas: a malha energética, satélites, centros de dados, redes e sistemas governamentais e comando e sistemas de controle militares. Por isso, se pensarmos na Internet das coisas e em sua interconectividade, cenários como "ataques cibernéticos que levam satélites a girar fora de controle, tomar o controle de aviões, desligar usinas de energia e quebrar economias" (MUNK, 2015, p.176, tradução nossa) se tornam passíveis de serem imaginados. Em um modelo visual mais claro (Figura 05), essas interdependências, são desenhadas.

Apesar do tom pessimista e exagerado, a suposição de tais cenários explica um pouco da interdependência que existe entre as Infraestruturas Críticas, o Estado e a população. Um processo que vem sendo aprofundado, segundo Pope (2008, p.4), deixando as Infraestruturas Críticas mais complexas e interdependentes, pela a inovação tecnológica e a desregulamentação e imperativos econômicos. Em outras palavras, o problema da proteção de Infraestruturas entra em paralelo com as grandes preocupações da globalização. Afinal, ambas se dão fora do controle total do Estado ao mesmo tempo em que afetam a relação entre todos eles (CLEMENTE, 2013, p.24).

Figura 5 - Interdependências de Infraestrutura



Fonte: Niekerk e Maharaj (2011, p.102)

Assim, podemos apontar que há um envolvimento Estatal mais forte em relação à parte física do ciberespaço, principalmente das infraestruturas de telecomunicações que perpassam territórios soberanos e interligam suas infraestruturas críticas à Rede. Portanto, como o Estado detém o monopólio da força e em suas funções primordiais está a defesa de seu território, ele *par default* é coagido a agir diante das ameaças cibernéticas. Contudo, o paradoxo se instala, na medida em que se a parte física perpassa os Estados, a parte virtual não respeita fronteiras. Afinal, quando se originou a ideia de comunicação em rede ela não previa a criação de mecanismos de segurança, até porque a finalidade principal era a comunicação e não a verificação da informação passada.

Então, se essa Infraestrutura Global de Comunicações, se os Estados estão preocupados com a questão, conforme demonstram os dados aqui mencionados do Index Global de Segurança (ITU, 2017) de onde exatamente vem a potencialidade das ameaças às Infraestruturas Críticas? Obviamente, da inter-relação entre espaço físico e virtual, que, como elucidamos, vêm da interdependência de vários setores com a sociedade. Mas, tecnicamente,

como essa relação se forma? Para isso, é necessário entendermos um pouco a diferença entre sistemas de tecnologia de informação e sistema de controle industrial.

2.3 1 Sistema de Controle Industrial e Sistemas de Tecnologia de Informação

Sistema de Controle Industrial é o termo usado para descrever vários tipos de sistemas de controle de processos industriais de larga escala, indo desde fábricas até oleodutos (SINGER; FRIEDMAN, 2014, p.296). Esses vários sistemas podem ser do tipo Controle de Supervisão e Aquisição de Dados (SCADA), Sistemas de Controle Distribuídos (DCS) e Controladores Lógicos Programáveis (PLCs) (SHAKARIAN; SHAKARIAN; RUEF, 2013, p.200).

Os sistemas SCADA são usados frequentemente para o "monitoramento remoto em uma grande área geográfica e para transmitir comandos para recursos remotos, como válvulas e interruptores". Os Sistemas DCS geralmente "fornecem informações processadas, ou uma série de comandos de uma localização central" (SHEA, 2004, p.2, tradução nossa). Já os PLCs são "uma forma especial de controlador baseado em microprocessador que usa memória programável para armazenar instruções e implementar funções como lógica, sequenciamento, temporização, contagem e aritmética no controle de máquinas" (BOLTON, 2009, p.3, tradução nossa). Assim, tecnologias do Sistema de Controle Industrial são, muitas vezes, empregadas em indústrias de infraestrutura "para permitir que um único centro de controle gerencie vários lugares" (SHEA, 2004, p.3, tradução nossa).

Como originalmente esses sistemas foram implementados como redes separadas e isoladas, eles eram vistos como sistemas de segurança física de infraestruturas afastadas (SHEA, 2004, p.3). Contudo, à medida que a produção industrial foi aumentando sua escala, em grande parte pelas demandas do mercado globalizado, e se conectando à Internet, esses sistemas se tornaram muito vulneráveis, ainda mais por serem considerados sistemas de legado, ou seja, não projetados para trabalhar em uma miríade de conexões, muito menos terem mecanismos de segurança próprios. Em outras palavras, "os sistemas legados referem-se aos sistemas que são obsoletos ou o fornecedor não mais suporta hardware e / ou software desatualizado" sendo que a maioria desses sistemas não está criptografada e nem autenticada (SMITH, 2014, p.24, tradução nossa).

Não obstante, ainda que simples soluções de TI pudessem resolver muitos dos problemas dos Sistemas de Controle Industriais, fazê-lo seria custoso, poderia quebrar com uma lógica de mercado de atualizações de prateleira (*off-the-shelf*) e demandaria um manejo

diferente (SHEA, 2004; SHAKARIAN; SHAKARIAN; RUEF, 2013). Isso se dá porque Sistemas de Controle Industriais possuem características próprias, mas principalmente por serem sistemas ciber-físicos, ou seja, unirem, de fato, o mundo virtual ao físico (MACKINNON et al, 2013, p.250).

A lógica por trás desses sistemas se torna mais clara sob a análise de Shakarian, Shakarian e Ruef (2013), na qual, com base em um relatório do Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos, descrevem dentro de 13 categorias as principais diferenças entre esses sistemas e sistemas comuns de tecnologia de informação, um compilado dessas diferenças pode ser visto no Quadro 02.

Contudo, ressalta-se algumas diferenças marcantes dentro desse universo, como o fato dos Sistemas de Controle Industrial terem uma expectativa de funcionamento bem longa (entre 15 e 20 anos); sua demanda de serviço ser contínua, ou seja, pensar em parar a ITAIPU mesmo que por pouco tempo, não é algo viável, ao passo que reiniciar um notebook é as vezes algo corriqueiro; e a questão do desempenho, para a qual o tempo de demora para se receber uma informação (*delay*) e variação estatística do atraso na entrega de dados da rede usada (*jitter*) são maiores em relação aos sistemas comuns de TI.

Quadro 2 - Tecnologia de Informação (TI) Vs. Sistema de Controle Industrial (SCI)

Categoria de Análise	TI	SCI
Desempenho	Requisitos mais leves para delay e jitter e, solicitação de garantias à largura de banda.	Requisitos fortes para delay e jitter e exigências menos rigorosas à largura de banda.
Disponibilidade	Possibilidade de interrupções na demanda	Demanda contínua de serviço
Gestão de riscos	Sistemas e dados	Sistemas, dados e pessoas.
Arquitetura	Repositórios centralizados	Repositórios descentralizados
Interação física	Mundo virtual	Mundo virtual e físico
Resposta em tempo crítico	Rápida	Lenta
Operacionalização do sistema	Conhecimento técnico abrangente	Conhecimento técnico específico
Limitação de recursos	Inexistente	Existente
Protocolos de comunicação	Simples	Proprietários
Atualizações	Rápidas e simples	Lentas e complexas
Suporte técnico	Múltiplos fornecedores	Único fornecedor
Tempo de vida de componentes	De 3 a 5 anos	De 15 a 20 anos
Acesso a componentes	Local e/ou de fácil acesso	Localização remota e/ou de difícil acesso

Fonte: Elaboração própria, com base em Shakarian, Shakarian e Ruef (2013)

Ao ser compreendida a diferença entre Sistemas de Controle Industrial e Sistemas de Tecnologia de Informação é interessante perceber que as vulnerabilidades colocadas foram testadas, seja por meio de testes voluntários, como no caso do Black Ice, ou ataque cibernético, como foi o caso do Stuxnet e da indústria Maroochy Water Services. Assim, descreveremos esses eventos como formas empíricas que dão respaldo ao temor dos Estados em relação às vulnerabilidades digitais de suas Infraestruturas Críticas.

Em preparação aos Jogos Olímpicos de 2002, o Departamento de Energia dos EUA e o Comando Olímpico de Segurança Pública de Utah realizaram o primeiro grande exercício de interdependência de infraestrutura. Esse exercício teve como intuito preparar funcionários federais, estaduais, locais e privados para as consequências inesperadas de ataques terroristas ou uma série de ataques na área que envolvesse o evento, como o agravamento de desastres naturais. Sendo assim, simulações de ataques cibernéticos mostraram que o modo de ataque não é importante. Afinal, quando um sistema falha, outros logo seguirão em razão da interdependência da Rede (SMITH, 2014, p.15-16; AXELROD, 2009, p.177).

Em 2007, o Teste Aurora foi desenhado para determinar a viabilidade de um ataque cibernético contra um gerador de energia real. Assim, conduzido pelo Laboratório Nacional de Idaho do Departamento Nacional de Energia um gerador a diesel foi submetido aos ataques cibernéticos (SHAKARIAN; SHAKARIAN; RUEF, 2013, p.213).

O teste basicamente se focou em fazer com que o vírus controlasse a abertura e o fechamento de disjuntores, o que resultou em um sincronismo fora de fase. Isso colocou estresse sobre os componentes mecânicos do equipamento rotativo no gerador, fazendo com que eles falhassem (SALMON et. al. 2010).

Como resultado, o teste demonstrou a possibilidade de ataques virtuais com repercussões físicas. Vale salientar que, embora tenha igualmente demonstrado que caso um ataque desses ocorra, o hacker teria que saber sobre a vulnerabilidade específica, ou descobri-la por acaso, para, então, obter acesso físico ao sistema de controle, burlando como no teste, os protocolos de segurança do operador e passando de forma despercebida (BURKHART, 2008).

O sistema Maroochy Water Services sofreu um ataque real a seus sistemas, os quais eram do tipo SCADA formado por duas estações de monitoramento utilizando três frequências de rádio para controlar 142 estações de bombeamento de esgoto. Em outras palavras, a indústria lidava com o manejo de rejeitos de Queensland's Sunshine Coast, na Austrália (SHAKARIAN; SHAKARIAN; RUEF, 2013, p 206).

O fato é que, frustrado por não conseguir um emprego no Conselho Maroochy Shire, Vitek Boden, um homem de 40 anos que trabalhou para uma empresa australiana (Hunter Watertech) na instalação do equipamento de esgoto radioelétrico SCADA invadiu o sistema remotamente a partir de equipamento de rádio. Assim, em posse de controle do sistema no ano de 2000, entre fevereiro e abril, ele liberou 800 mil litros de esgoto bruto para atingir parques locais, rios e até mesmo os terrenos de um hotel Hyatt Regency. Ele só foi apanhado porque um policial o abordou por uma infração de trânsito depois de um de seus ataques (ABRAM; WEIZZ, 2008, p.1).

Assim, ele foi condenado a dois anos de prisão e a reembolsar o Conselho pela limpeza. Independente da sentença, "o ataque de Boden tornou-se o primeiro exemplo amplamente conhecido de alguém invadindo maliciosamente um sistema de controle" (ABRAM e WEIZZ, 2008, p.1, tradução nossa). Além disso, levantou algumas dificuldades na proteção do sistema como: dificuldade de se identificar o ataque, vulnerabilidade a ameaças internas e os efeitos desses ataques em infraestruturas causa mais danos para as pessoas do que aos sistemas digitais (SHAKARIAN; SHAKARIAN; RUEF, 2013, p.206-207).

O caso do *worm* Stuxnet é bem documentado e, para muitos, inclusive a autora, é considerado um *turning point* em relação aos ataques cibernéticos, a primeira arma cibernética do mundo. Independente dessa afirmação e da especulação do que foi o ocorrido, seja um ato de Guerra Cibernética ou de Terrorismo Cibernético, o fato é que ele demonstrou em que medida um ataque aos Sistemas de Controle Industrial pode ser perpetrado a fim de atingir objetivos maiores dentro do jogo de poder das relações internacionais.

Desenhado para atingir um tipo de programa usado por um software de controle da Siemens o WinCC/PCS 7 SCADA, o Stuxnet foi descoberto por uma empresa da Bielo-Rússia chamada VirusBlockAda, a qual pesquisava um *worm* cibernético de origem desconhecida que estava se espalhando por todo o mundo, mas com 60% das infeções concentradas no Irã, bem como sendo incorporado aos sistemas de controle (SINGER; FRIEDMAN, 2014, p.115). Após a descoberta do vírus, a comunidade científica passou a relacionar o epicentro de ataques do vírus (Irã) com o mau funcionamento das centrífugas em Natanz. Assim, em novembro de 2010, o então presidente iraniano, Mahmoud Ahmadinejad, reconheceu publicamente que um *worm* estava limitando o funcionamento das centrífugas (SHAKARIAN; SHAKARIAN; RUEF, 2013, p.224).

O Stuxnet se diferenciava não apenas por ter 04 novos "dias-zero", mas também utilizar assinaturas digitais com chaves privadas de 02 certificados roubados de companhias

reconhecidas, além de poder operar em qualquer sistema operacional Windows até a edição do Windows 95 (SINGER e FRIEDMAN, 2014, p.115). Igualmente, ele possuía um sistema de autodestruição para apagá-lo em 2012 (SINGER; FRIEDMAN, 2014, p.116), sendo sua função dentro das centrífugas uma mudança de rotina que hora acelerava hora diminuía, ao mesmo tempo em que encobria seu rastro para que os cientistas não pudessem detectar o que estava fazendo, as peças da instalação quebra ou as máquinas literalmente explodirem (SINGER; FRIEDMAN, 2014, p.117).

Ao final, com a descoberta do vírus o governo iraniano, segundo o ministro da inteligência do Irã, Heydar Moslehi, prendeu um número não especificado de espiões nucleares em conexão com Stuxnet (SHAKARIAN; SHAKARIAN; RUEF, 2013, p.232), o programa nuclear fora atrasado pelo menos 05 anos (ROHR, 2011) e o mundo teve certeza de que assinaturas digitais não eram garantia de segurança, muito menos um Sistema de Controle Industrial não conectado a Rede (*air-gripped*) (SHAKARIAN; SHAKARIAN; RUEF, 2013, p.233).

2.4 TERRORISMO E INFRAESTRUTURAS CRÍTICAS

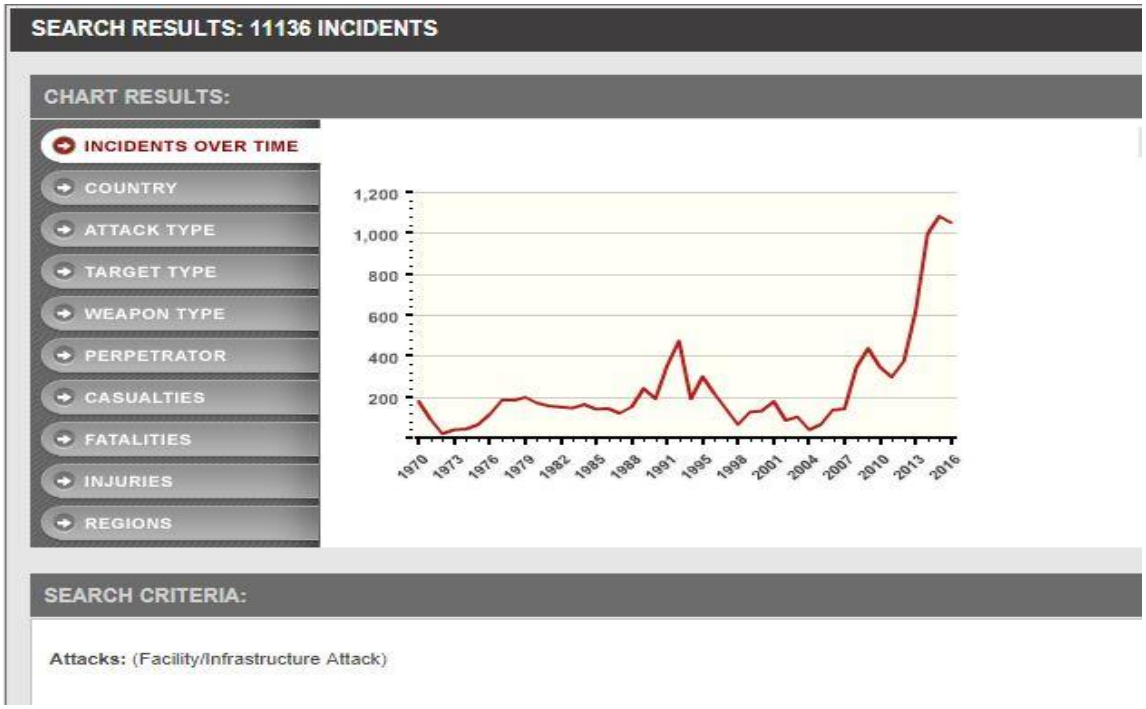
O terrorismo é um fenômeno social de longa data, mas os ataques de 11 de Setembro marcariam para sempre como o mundo veria esse fenômeno no decorrer do século XX e XXI. A securitização do ciberespaço nos Estados Unidos e na Europa solicitou a proteção das Infraestruturas Críticas do terrorismo (CLEMENTE, 2013, p.6, tradução nossa), “principalmente o terrorismo extremista não estatal, em oposição ao terrorismo patrocinado pelo Estado”, que passou a encabeçar listas de ameaças quanto à infraestrutura. Como visto anteriormente, a preocupação com essas infraestruturas ocorre em função das suas vulnerabilidades. No entanto, mesmo antes dos Sistemas de Controle Industrial fazerem conexão com a Rede, ou trabalharem em grandes e complexas escalas, eles já eram alvos de ataques terroristas, contudo anterior ao advento da Internet, de uma maneira física.

Essa busca das Infraestruturas Críticas pelos terroristas se dá exatamente por seus efeitos imediatos perante a população, chamando atenção estatal e proporcionando um palco considerável, ainda que muitas vezes local, a causa do perpetrador. Em outras palavras, como o objetivo dos terroristas é espalhar medo, ansiedade e pânico, criar a percepção de que todo cidadão e nó crítico da infraestrutura de um país, estando vulnerável aos ataques (COUNTER TERRORISM COMMITTEE EXECUTIVE DIRECTORATE - CTED, 2017, p.4) em sua maneira de agir e pensar. Ainda como Jinga (2017, tradução nossa) explica:

> É geralmente aceito que, a nível nacional, se destruído, degradado ou tornado indisponível, a infraestrutura crítica afetaria significativamente o bem-estar social e econômico de uma nação ou afetaria sua capacidade de garantir a defesa e a segurança nacionais.

Dados do *Global Terrorism Database*, disponível pelo Consórcio Nacional de Estudo de terrorismo e respostas ao terrorismo (START, em inglês), com um compilado de 170.000 casos de terrorismo (perpetrados somente por atores não estatais) mostram essa realidade de ataque a infraestruturas de maneira geral, datando desde 1970 até 2016, conforme mostra o gráfico na Figura 06.

Figura 6 - Ataques a Infraestruturas entre 1970-2016

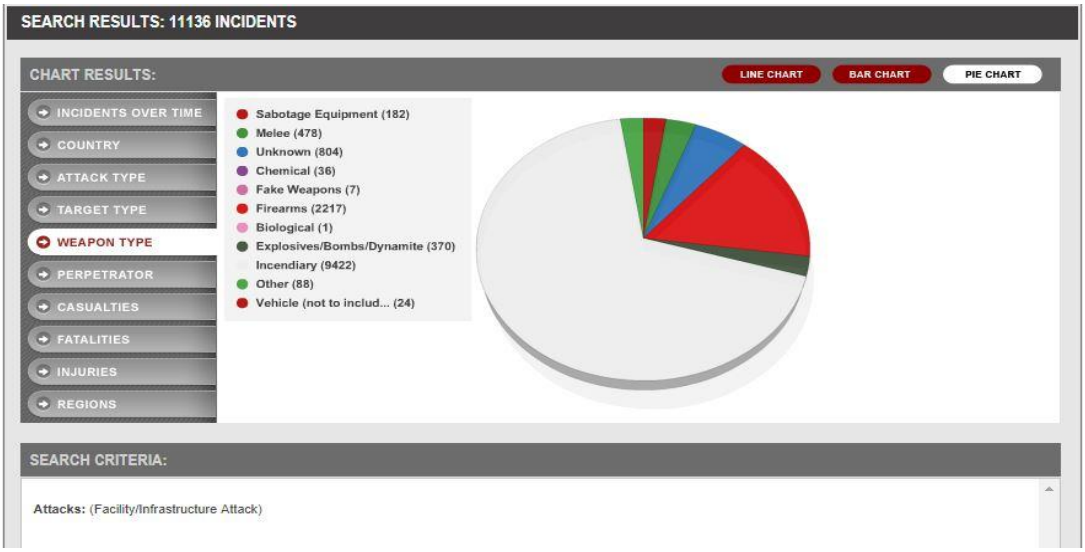


Fonte: START (2017)

Analisando o gráfico é possível perceber dois grandes picos desse tipo de ataque nos anos 90 e outro nos anos 2000. Todavia, em que pese ambos os picos se encontrem já dentro de um contexto cibernético, os dados revelam que a maioria dos ataques foi incendiária, totalizando 84,6% deles (conforme Figura 07), o que não exclui por completo a

vulnerabilidade das infraestruturas aos ataques cibernéticos, o ponto aqui é a "tradição" das infraestruturas serem alvos terroristas.

Figura 7 - Tipo de armas usadas em ataques à Infraestruturas (entre 1970-2016)



Fonte: START (2017)

Se observarmos ainda os tipos de infraestrutura que foram atacadas, os dados revelam que as maiores incidências foram: infraestruturas de governo geral (13%), sem contar as diplomáticas; propriedades privadas (21,25%); e Indústrias (27,5%) (START, 2017). Ademais dados de entre 2010 e 2014 do mesmo banco de dados, mostram que dentro do setor energético e de mineração, a maioria dos ataques foi contra as infraestruturas (74%), corroborando com a ideia de que as Infraestruturas Críticas são preferidas dentro do rol de ação dos terroristas (CTED, 2017, p.5).

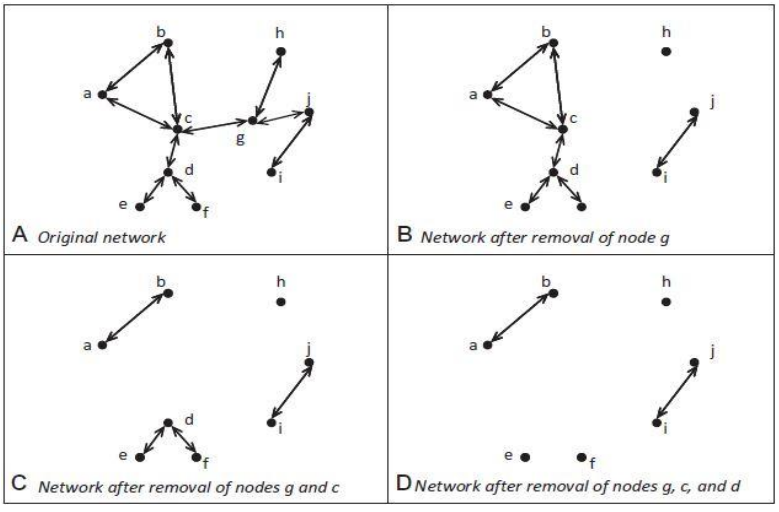
Dessa forma, uma vez estabelecido que existam razões de cunho histórico para os Estados se preocuparem com a proteção de suas infraestruturas, em especial as que são críticas, cabe a colocação de Singer e Friedman (2014, p.97, tradução nossa):

> Deixe-nos ser claros: as preocupações com as vulnerabilidades em infraestrutura crítica para o ataque cibernético têm validade real. De 2011 a 2013, sondas e intrusões nas redes informáticas de infraestrutura crítica nos Estados Unidos subiu 1700 por cento. E as preocupações dos ciberterroristas que prejudicam esta infraestrutura são certamente uma preocupação real.

Diante desses dados, é ainda interessante perceber o medo no tocante às Infraestruturas Críticas quanto aos ataques físicos. Essa combinação seria o pior cenário possível entre especialistas, já que o ataque cibernético funcionaria como um multiplicador de força terrorista (SHEA, 2004, p.10). Todavia, é curioso que essa hipótese, do ciberespaço ser um multiplicador de força, permeia conflitos no ciberespaço de forma geral, uma vez que qualquer objeto conectado à Rede ou operando com um sistema de rede pode possuir falha e, portanto, ser passível de enganado/invadido. Isso com uma previsão para que até 2020 existam 50 bilhões de coisas conectadas à Internet (CLEMENTE, 2013, p.4) pode levar a incertezas que se refletem na preocupação dos Estados com suas infraestruturas.

Outro ponto que aqui aprofundamos, é a questão da interdependência da rede, que uma vez atacada pode se fragmentar ou sofrer falhas em cascata. A possibilidade da fragmentação pode se dar mediante ataques cibernéticos em nós de uma rede de sistema, os quais cortam a comunicação entre a rede, causando falhas (ver Figura 08). Em redes elétricas, por exemplo, ataques a nós resultam na distribuição isolada de subestações, tornando-a incapaz de receber qualquer energia do gerador, consequentemente, deixando os clientes associados a tal subestação em condições de apagão (SHAKARIAN; SHAKARIAN; RUEF, 2013, p.204).

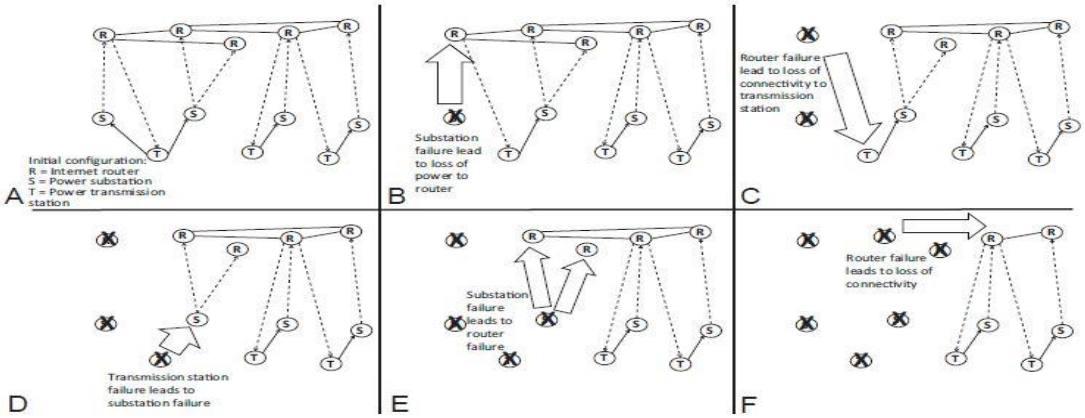
Figura 8 - Exemplo de Rede e efeito de fragmentação na remoção de nós selecionados



Fonte: Shakarian, Shakarian e Ruef (2013, p.204)

Quanto à falha em cascata, ela nada se refere ao resultado de ataques que vão impossibilitando a comunicação da rede gerando falhas em uma sequência progressiva. Assim, tomando novamente o exemplo das redes elétricas, uma "interrupção em uma subestação levará a uma interrupção em certos roteadores na Internet, o que poderia potencialmente deixar uma estação de transmissão ou controle incapaz de se comunicar e assim causar mais interrupções na subestação" (SHAKARIAN; SHAKARIAN; RUEF, 2013, p.220).

Figura 9 - Efeito Cascata em Rede Elétrica ligada a Internet (modelo Buldyrev)



Fonte: Shakarian.Shakarian e Ruef (2013, p.220)

Por fim, essa preocupação entre interface física e virtual, ainda abala os Estados de outra forma: sua falta de controle direto sobre elas. De acordo com o relatório de tendências do Comitê Contra o Terrorismo das Nações Unidas, 80% das Infraestruturas Críticas em países ocidentais representam propriedade e operação privada (CTED, 2017, p.02). Nesse sentido, para valer fazer seus interesses e conseguir proteger sua população, os Estados devem começar a pensar em parcerias-público privadas, tendo em mente que a lógica do mercado deverá fazer parte dessa equação.

Em tal ponto, é válida a ponderação sobre a multiplicidade de atores internacionais que repercute internacionalmente em um *gap* legislativo. Em outras palavras, a questão da atribuição de responsabilidade.

A atribuição de responsabilidade se torna relevante aqui porque, em se tratando de ciberespaço, o uso de infraestruturas cibernéticas nacionais, deixa dúvidas acerca de quem começou a lançar ataques. Tal dúvida, além de gerar inação, pode comprometer avaliações

sobre retaliações proporcionais no ciberespaço. Talvez essas indagações sejam melhor explicadas por Schimitt e Watts (2016, p.596, tradução nossa), para os quais:

> As operações cibernéticas, no entanto, parecem apresentar oportunidades grandemente acrescidas para os atores não estatais combinarem e, em alguns casos, até superar, a supremacia estatal. Atores não estatais capazes de montar operações cibernéticas que afetam profundamente a segurança dos estados e as circunstâncias em que os atores não estatais exigem tanto ou mais atenção do que outros estados, não são mais futuristas ou exageradas - são a realidade do ciberespaço. Além de constituir um novo domínio de guerra entre estados, o ciberespaço também parece representar um domínio significativamente contestado entre estados e atores não estatais. Como exemplo, um recente relatório revela que os EUA recorreram à operação cibernética ofensiva em seus esforços contra as forças do Estado islâmico que operam na Síria e no Iraque.

Conforme explica Tsagourias (2016, p.458, tradução nossa), existe na vigente legislação internacional um déficit quanto à responsabilidade Estatal em lugares não governados. Por lugares não governados o autor entende "uma situação em que há perda total e geral de capacidade estatal em termos geográficos e de governança, mas também situações em que a capacidade do estado gradualmente ou de repente recua de partes de um estado de funcionamento". Assim, o ciberespaço entraria nesse contexto.

Tal falta de responsabilização se dá basicamente porque, ao mesmo tempo em que o Estado não pode aplicar suas obrigações legais se sofrerem de não governabilidade, os atores não estatais, mesmo operando em seu território e usando da infraestrutura cibernética para perpetrar atividades virtuais, não podem ser parte em tratados internacionais não podendo, portanto, ser responsabilizados por obrigações que não foram incumbidas a eles (TSAGOURIAS, 2016, p.461-462). A situação se agrava mais se pensarmos que toda a legislação internacional é baseada na noção de estadismo e na premissa de uma clara divisão entre público e privado (TSAGOURIAS, 2016).

Outro fator que complica a questão de responsabilidade no ciberespaço é a dificuldade de identificação dos atacantes, uma vez que o anonimato na Rede é amplo e de fácil acesso. Além disso, atores estatais podem ter uma plausível negação de responsabilidade agindo por meio de *proxies*, fazendo com que, em última instância, a atribuição seja uma decisão política (MAURER, 2016, p.393). Por isso, essa atribuição por questões políticas não deixa de ser um reflexo de jogos de poder internacionais e com relação às ações terroristas, não deixa de ficar centrada em definições sobre o terrorismo que as potências mais poderosas poderão ter.

Ainda no tocante à questão de atribuição, ela é importante diante do terrorismo de Estado, ou seja, haveria possibilidade de se pensar em um terrorismo cibernético de Estado? Ou do terrorismo disfarçar uma Guerra Cibernética?

Segundo Kallberg e Thuraisingham (2013, p.233, tradução nossa), uma Guerra Cibernética terceirizada por *proxy* do ator estadual por terroristas cibernéticos, operaria nas mesmas linhas que as armas cibernéticas de grau militar dispersas para grupos violentos e grupos políticos militantes, ou seja, criariam uma grande incerteza. "Essa incerteza baseia-se no que um agressor pode fazer, e não o que eles realmente fazem".

Contudo, lembrando que existem várias escolas de pensamento sobre esse assunto, bem como a pesquisa em evidência apresente a visão de centralidade do Estado como detentor do monopólio de poder e, portanto, em última instância, responsável pela segurança nacional, respostas para essas duas perguntas devem ser muito bem analisadas.

Em primeiro lugar, a fluidez dos conflitos cibernéticos permite que criminosos terroristas e Estados usem a Rede de maneira igualitária, ou seja, a um custo de entrada baixo. Dessa forma, a princípio, nada impede que vários conflitos se imiscuam, até como uma questão estratégica. Por exemplo, um ataque de *randsomware* servir para acumular *bitcoins* com objetivo de comprar armas cibernéticas de outro Estado e, com isso, atingir uma infraestrutura crítica de um terceiro. Em outras palavras, um crime cibernético servir para um fim maior, pois como mexe com infraestruturas pode desencadear uma guerra virtual ou em terrorismo cibernético.

Em segundo lugar, o fato de não se saber quem está por trás ou não dos ataques, verdadeiramente, ou seja, a questão dos *proxies* força a escolha de conceitos com uma base mais sólida, ou seja, o mundo considerará o um Estado usando um grupo terrorista para atingir outro Estado um ato de guerra ou terrorismo? Quem afinal pode fazer uma guerra ou terrorismo cibernético? Nesse sentido, o próximo capítulo vai buscar apoiar a ideia de que definições do uso terrorista e ciberterrorismo são necessárias.

2.5 CONSIDERAÇÕES PARCIAIS

Partindo de uma visão de mundo sobre uma Sociedade de Informação, altamente dependente das Tecnologias de Informação (TICs), que, em um contexto securitário, percebe o ciberespaço como um lugar de potenciais ameaças hibridas (Sociedade de Risco), as quais fazem com que o ciberespaço se torne um tema progressivamente securitizado (Escola de

Copenhague), o capítulo em evidência buscou informar ao leitor sobre o funcionamento e as diversas contribuições teóricas e técnicas que compõem as visões sobre vulnerabilidades do ciberespaço.

Assim, em forma de um apanhado teórico generalizado, buscou-se explicar como é a natureza do ciberespaço, como a segurança cibernética vê a questão das vulnerabilidades sob diversas perspectivas, seja em escolas próprias ou dentro de teorias já mais consolidadas das Relações Internacionais e, por fim, foram levantados alguns questionamentos que pudessem tentar explicar de onde vem a preocupação com os terroristas, com o ciberespaço e como complicações legais internacionais e conceituais colocam desafios maiores em toda essa discussão.

Nesse sentido, chegou-se à conclusão que duas são as principais preocupações com relação ao terrorismo cibernético e o ciberespaço: a proteção de Infraestruturas Críticas e a possibilidade de grupos terroristas serem usados por Estados. Com isso em mente, o próximo capítulo se voltará ao debate em si do conceito de terrorismo cibernético, tentando elucidar como essas preocupações estão sendo desenvolvidas na academia.

3 TERRORISMO E CIBERESPAÇO: NOVAS AMEAÇAS E INTERPRETAÇÕES

Este capítulo busca explorar a perspectiva acadêmica sobre como os grupos terroristas vêm utilizando o ciberespaço. Dessa forma, apresenta como essa perspectiva pode verificar a afirmação de que o uso terrorista da Internet e o ciberterrorismo, ainda que fenômenos muito próximos, são diferentes. Ademais, o capítulo elucida como o conceito de ciberterrorismo deriva de percepções sobre o terrorismo, e como tanto o fenômeno do terrorismo quanto do ciberterrorismo se diferenciam de outros fenômenos conflitivos.

Ao contextualizarmos a sociedade do século XXI enquanto uma Sociedade de Informação, ao mesmo tempo que uma Sociedade de Risco, entendemos a importância que ameaças percebidas detêm no imaginário coletivo, mais ainda, se considerarmos potencialidades de ameaças à Infraestruturas Críticas. Nesse sentido, a lógica de securitização acerca das ameaças que o ciberespaço coloca, se torna, muitas vezes, nebulosa para o entendimento de muitos, colocando entraves diante de pesquisas mais rígidas metodologicamente acerca do fenômeno do ciberterrorismo.

De fato, vários autores consideram quais os maiores entraves para uma definição mais concreta sobre o termo. Luijif (2014, p.11-12), por exemplo, identifica que o problema sobre a incoerência de definições está na sua origem, que vêm de campos de especialidades bem diferentes, e na imprensa popular, que cria ainda mais confusão.

De maneira semelhante, Conway (2007, p. 77) aponta como o tema é conduzido pela mídia popular, de maneira que seus termos são mal-usados (de forma excessiva e crônica) e há a tendência de adicionar o prefixo “cyber” aos fenômenos relacionados com os computadores. Por fim, a falta de definição geral sobre o termo terrorismo adiciona camadas de inconsistências conceituais. Ballard, Hornik e Mckenzie (2002, p.994, tradução nossa) comentam o que pesquisadores devem considerar, quanto aos estudos sobre o ciberterrorismo, questões “relacionadas com o viés do pesquisador, o suporte hegemônico para as estruturas de poder existentes, a validade e a confiabilidade dos dados contidos na tipologia e o tempo de atraso no reconhecimento das inovações tecnológicas”.

Dentro desse contexto de inconsistência conceitual, um estudo do tipo *survey* feito por Jarvis, Macdonal e Nouri (2014)[8] revelou dados valiosos sobre o estado da arte dos estudos acerca desse fenômeno. Como o fato de que 58% dos pesquisadores afirmam que o ciberterrorismo é uma ameaça, mas conseguem diferir quem seria ameaçado, indo desde Governos e Infraestruturas Críticas (maioria das respostas) até eleições políticas. Igualmente a pesquisa reforça a ideia de que o background dos pesquisadores influencia suas percepções acerca do fenômeno (ver Tabela 01), uma vez que diferentes áreas percebem a materialidade do fenômeno de modos singulares. Assim, enquanto a maioria dos pesquisadores de Ciências Políticas e Relações Internacionais acreditam que não houve casos de ciberterrorismo, pesquisadores da área do Direito acham que já. Essa diferença, e em específico a discordância entre essas duas áreas, é mais um indicativo de que indefinições não são um bom caminho para o entendimento de tomadores de decisão, os quais influenciam direta ou indiretamente a construção de leis para combater o fenômeno.

Tabela 1 - Ranking de respostas baseado no background acadêmico dos pesquisadores

Has a cyberterrorist attack ever taken place? (By disciplinary background)

	All respondents	Those respondents that said a cyberterrorist attack has taken place	Those respondents that said a cyberterrorist attack has not taken place
Group A (Political Science, International Relations, et al.)	50%	34%	69%
Group B (Law, Criminology, et al.)	11%	20%	0%
Group C (Economics, Business, et al.)	1%	3%	0%
Group D (Engineering, Computer Science, Cyber, et al.)	12%	15%	10%
Group E (Psychology, Anthropology, et al.)	15%	16%	12%
Group F (Literature, Arts, History, et al.)	7%	5%	7%
Group G (Independent Researchers, Analysts, et al.)	4%	7%	2%

Fonte: Jarvis, Macdonald e Nouri (2014, p.80)

[8] Nesse estudo, foram abordadas 118 respostas de 24 países que abrangem seis continentes. Todavia vale ressaltar que a maioria dos pesquisadores concentrava-se em países anglófonos (i.e. 35% Estados Unidos da América 27% Reino Unido, 6% Austrália e 3% no Canadá).

Assim, Flemming e Stohl (2001, p. 36, tradução nossa) resumem muito bem as consequências dessas indefinições, a saber:

> [...] para o formulador de políticas, isso significa que as expedições políticas muitas vezes ditarão o que devem ser medidas pragmáticas. No caso do analista, a ambiguidade na delimitação do crime cibernético pelo ciberterrorismo dá origem ao pseudoestudo do último. Por último, também é essencial lembrar que para a vítima, o tipo de agressor por trás do ataque é muitas vezes menos importante do que as consequências do ataque.

Diante desse quadro, compreender como o uso terrorista da Internet vem evoluindo e sendo percebido parece uma alternativa viável para aclarar o fenômeno do ciberterrorismo. Em realidade, segundo Jarvis, Nouri e Whiting (2014, p.26), a tensão quanto à definição do tema gera três caminhos possíveis:

a) Simplesmente abandonar o conceito de ciberterrorismo como inapropriado ou um inapropriado alongamento da linguagem do terrorismo;

b) Envolver-se em mais trabalho de definição para melhor esclarecer os tipos de atividade a que o rótulo de ciberterrorismo pode se referir, e

c) Explorar o ciberterrorismo como uma construção social em vez de um fenômeno ontológico coerente e estável.

Dessa forma, entendemos que ao se buscar esclarecer um fenômeno, deve-se partir de uma base conceitual, a fim de que uma rede nomológica de abrangência aceitável torne possível seu entendimento. Em outras palavras, essa seção focar-se-á no segundo caminho proposto por Jarvis, Nouri e Whiting (2014).

Assim, antes de se falar em uma tipologia de terrorismo a qual é caracterizada pelo uso do ciberespaço (i.e. ciberterrorismo), é preciso fragmentar o conceito, ou seja, entender de um lado o que vem a ser o terrorismo e do outro o que vem a ser o ciberespaço. Quanto à questão do ciberespaço, ela foi abordada com mais detalhes no capítulo anterior, portanto, cabe aqui desvendar como a parte conceitual de terrorismo se desenvolve em tal equação.

3.1 TERRORISMO CLÁSSICO: UM PROBLEMA CONCEITUAL

A palavra terror deriva da palavra em latim *terrere* que significa “trazer alguém para tremer através de um grande medo”, ou seja, “se refere a um estado de espírito caracterizado pelo intenso medo de um perigo ameaçador em umnível individual e por um clima de medo ao nível coletivo”. Já terrorismo, de uma maneira objetiva, se refere “uma atividade, método

ou tática que, como resultado psicológico, visa produzir terror" (SCHMIDT, 2011, p.3, tradução nossa). Contudo, exatamente como as atividades terroristas se desenvolvem? O que elas são exatamente?

Em que pese o terrorismo não seja um fenômeno novo[9], uma definição consensual internacional sobre ele ainda não foi desenvolvida. O que não significa que não existam estudos consistentes sobre o fenômeno, ou que não tenham existido, ao longo da história, tentativas de uma definição legal internacional.

Em realidade, a primeira tentativa de uma definição legal internacional se deu em 1937 no âmbito da Liga das Nações[10], para a qual atos de terrorismo seriam "atos criminosos dirigidos contra um Estado e com a intenção calculada de criar um estado de terror nas mentes de pessoas específicas ou de um grupo de pessoas ou do público em geral" (LoN, 1937, p.22, tradução nossa). A convenção especificava ainda os tipos de ações antiestatais que eram considerados atos de terror (i.e. atacar funcionários públicos, chefes de Estado e suas famílias ou destruir instalações públicas) (LoN, 1937, p.23), bem como demandava que Estados signatários promulgassem leis que tornassem os, então, atos terroristas, como ofensas passíveis de extradição caso seus cidadãos cometessem o crime em um país estrangeiro (LoN, 1937, p.25). Todavia, interesses estatais diversos dificultaram a ratificação da convenção, principalmente centrados nas partes concernentes à extradição, o que fez com que ela nunca se tornasse efetiva (WORLD DIGITAL LIBRARY- WDL, 2017).

Os embates com a questão do terror e do terrorismo provém de longa dada, uma vez que o conceito sofreu modificações ao longo da história humana. Afinal, no século XVIII, o terror foi usado como instrumento da Revolução Francesa e seu uso significava um meio legítimo de defesa da ordem social, para depois, com a morte de Robespierre, significar o "abuso do poder governamental com implicações criminosas abertas" (HOFFMANN, 2006, p.3-4, tradução nossa).

No século seguinte, com o advento do nacionalismo que levou até "noções de Estado e cidadania baseadas na identidade comum de um povo e não na linhagem de uma família real" o terrorismo passou a ter conotações antiestatais e revolucionárias, principalmente pela ideia

---

[9] "Acredita-se que o terrorismo como uma prática tenha começado na Judéia do primeiro século, onde os homens judeus usariam um punhal curto (sica) para cortar a garganta dos romanos e seus colaboradores em plena visão do público. Sicarri, como esses apontadores eram chamados, também atacariam judeus ricos e sequestrariam seus servos por resgate. Os Sicarri faziam parte de um grupo conhecido como zelotes, que procuravam derrubar os romanos. O termo Zealot é derivado do nome desse movimento. Mais tarde, na Índia do século VII, membros do culto de Thuggee ritualmente estrangulavam suas vítimas em um aparente ato de sacrifício para a deusa Hindu Kali". (KUSHNER, 2003, p.360, tradução nossa).

[10] O governo francês propôs após o assassinato do Rei Alexandre I da Iugoslávia, em Marselha, por separatistas croatas e macedônios, que a Liga adotasse uma convenção sobre terrorismo. (WDL, 2017).

de “propaganda via feitos” de Carlo Pisacane, para o qual a “violência era necessária não só para chamar a atenção para, ou gerar publicidade para, uma causa, mas também para informar, educar e, finalmente, reunir as massas por trás da revolução” (HOFFMANN, 2006, p.05, tradução nossa). Assim, “na virada do século XIX, o terrorismo sob a forma de assassinato político tornou-se um fenômeno global importante” (KUSHNER, 2003, p.360, tradução nossa), considerando o assassinato do Arquiduque Habsburgo Francisco Ferdinado que culminou na Primeira Guerra Mundial.

Após a Primeira Guerra, “o terrorismo individual foi um anátema tanto fascista quanto comunista de pontos de vista” (KUSHNER, 2003, p. 360, tradução nossa), visto que essas ideologias totalitárias empregavam o terrorismo coletivo do Estado, ou seja, o terrorismo passou a descrever “as práticas de repressão em massa empregadas pelos Estados totalitários e seus líderes ditatoriais contra seus próprios cidadãos” e, portanto, “recuperando suas antigas conotações de abuso de poder pelo governo” (HOFFMAN, 2006, p.14, tradução nossa).

No pós II Guerra, o terrorismo tornou-se “uma estratégia de escolha para grupos nacionalistas no Oriente Médio, África do Norte e Ásia em sua luta por independência”, culminando no uso de táticas terroristas pelas guerras de guerrilha (KRUSHNER, 2003, p.360, tradução nossa). Nos anos de 1960-70 retomaram o caráter revolucionário do terrorismo incluindo “grupos separatistas nacionalistas e étnicos fora de uma estrutura colonialista ou neocolonial, bem como organizações radicais motivadas inteiramente ideologicamente”, como grupos étnicos nacionalistas/separatistas. (HOFFMANN, 2006, p.16-17, tradução nossa).

Depois, nos anos 1980, dentro de um contexto de Guerra Fria, o terrorismo passou a ser “considerado como um meio calculado para desestabilizar o Ocidente como parte de uma vasta conspiração global”, sendo que na metade da década com os bombardeamentos suicidas de embaixadas e alvos militares norte-americanos, principalmente no Oriente Médio, a ameaça de terrorismo apoiado pelo Estado ressurgiu. Assim, o terrorismo tornou-se associado “a um tipo de guerra secreta ou substituta, em que Estados mais fracos poderiam enfrentar rivais maiores e mais poderosos sem o risco de retribuição” (HOFFMANN, 2006, p.17, tradução nossa).

Já na década de 1990, como narcotráfico e o fenômeno da área cinzenta o terrorismo começou a se tornar um conceito mais borrado, ou seja, “o terrorismo voltou a mudar seu significado de um fenômeno individual de violência subnacional a um dos vários elementos, ou parte de um padrão mais amplo, de um conflito não estatal” (HOFFMANN, 2006, p.18, tradução nossa). Afinal, atores não estatais (criminosos) estavam “forjando alianças

estratégicas com organizações terroristas e guerrilhas ou empregando eles mesmos a violência para fins especificamente políticos" (HOFFMANN, 2006, p.18, tradução nossa).

Por fim, os atentados de 11 de Setembro de 2001 às Torres Gêmeas do *World Trade Center* nos Estados Unidos provocaram outra mudança em relação à percepção do fenômeno, uma vez que a proclamação da "Guerra ao Terror", pelo então presidente norte-americano George W. Bush, colocou um caráter de cruzada contra um mal externo ao fenômeno. Com isso, criando, ao mesmo tempo, o medo de que forças malignas se levantassem e ameaçassem a civilização (HOFFMAN, 2006, p.20).

A breve contextualização de percepções acerca do significado do terrorismo (resumida no quadro 3) serve ao propósito de favorecer a mutabilidade da sua percepção. Dessa forma, fica claro quando Best e Nocella II (2004, p.03, tradução nossa) argumentam que o terrorismo é um termo "subjetivo, altamente carregado política e emocionalmente, cujo significado é relativo a uma agenda e ideologia política, ou mesmo a uma cultura". Ademais, entende-se quando Laquer (1996, p.24) menciona que, no momento, vivemos vários tipos de terrorismos. Afinal, se o terrorismo é percebido como uma força maligna, ela pode ganhar várias formas, incluindo lobos solitários, o uso do ciberespaço (terrorismo cibernético) ou mesmo do meio ambiente (terrorismo ambiental).

Dentro desse quadro de mutabilidade, parece lógico que indefinições acerca do fenômeno foram surgindo. Elas são exacerbadas, muitas vezes, pela mídia sensacionalista que, em raras ocasições, conceitua de forma criteriosa atos cunhados como terroristas.

Em contrapartida, dentro do âmbito acadêmico esforços para uma conceituação ou formas de se compreender o fenômeno de forma mais rigorosa são enormes. Assim, ainda que não se tenha uma teoria propriamente dita sobre o fenômeno do terrorismo, muitos pesquisadores enquadram o fenômeno dentro de algumas interpretações (*frameworks*) e apostam no uso de tipologias.

Quadro 3 - Mudança de percepção sobre terrorismo na história

Período	**Caráter**	**Ponto de Mudança**
Século XVIII	Abuso de poder governamental (controle da população)	Morte de Robespierre
Meados século XIX	Revolucionário e Antiestatal	Nacionalismo (noção de Estado e cidadania)

Período	Caráter	Ponto de Mudança
Década 1930	Abuso do poder governamental (fascismo, nazismo, comunismo)	Fim I Guerra Mundial
Década 1940-50	Revolucionário e anticolonialista	Fim II Guerra Mundial
Década 1960-70	Revolucionário e antiestatal (separatista)	Descolonização
Década 1980	Abuso de poder governamental (com o Estado apoiando grupos terroristas)	Guerra Fria
Década 1990	Revolucionário e antiestatal (majoritariamente atores não estatais)	Narcotráfico e fenômeno da área cinzenta
Anos 2000	Inimigo externo antiestatal	Ataques de 11 de Setembro de 2001

Fonte: Elaboração própria com base em Hoffmann (2006) e Kushner (2003)

Segundo Schmidt (2011, p.2), essas interpretações podem ser divididas em cinco categorias. Assim, atos de terrorismo poderiam ser vistos como: crime, política, guerra, comunicação e cruzada religiosa/jihad. Contudo, nenhuma dessas interpretações sozinhas seria suficiente, uma vez que:

> um ato de violência terrorista pode ser criminoso e político ao mesmo tempo, tornando-se um crime político ou uma infração criminal com repercussões políticas. Um ato de terrorismo pode ser cometido no contexto da guerra e constituir uma violação grave das leis da guerra - um crime de guerra. Um ato de terrorismo pode ser principalmente um impulso de comunicação propagandista para impressionar um público ou para chegar a outras audiências que, de outra forma, não poderiam "ouvir" protestos menos violentos. Um ato de violência terrorista também pode ser interpretado como um sacrifício com conotações religiosas, pelo qual o terrorista oferece vidas inocentes pela causa sagrada ou vê-se como um mártir. À medida que as tendências no uso do terrorismo mudam, um tipo de interpretação pode se tornar mais apropriado do que outro. O terrorismo muda à medida que os instrumentos de violência e comunicação mudam e à medida que os contextos evoluem (SCHMIDT, 2011, p.02, tradução nossa).

Ainda, segundo Marsden e Schimidt (2011, p.192), a maioria das definições sobre terrorismo tem um cunho dedutivo, e seu poder explicativo pode se enquadrar em uma das seguintes perguntas:

a) quem são os terroristas?
b) por que os terroristas agem?
c) onde os terroristas operam?
d) quando os terroristas mudam?

e) como eles operam?

Nesse sentido, entram as tipologias, as quais buscam na medida do possível engendrar as interpretações mencionadas umas nas outras, buscando focalmente responder a alguma dessas perguntas explicitadas acerca do fenômeno.

Logo, o fato de existirem mais de 100 definições diferentes para o terrorismo não surpreende, uma vez que a possibilidade de arranjos passíveis de serem feitos é enorme. Ainda mais quanto à questão de quem são os atores terroristas e como eles agem, já que existem vários autores que discutem o assunto, sendo que em relação à forma de ação terrorista as tipologias consideradas ficam "sob as rubricas de motivação, causa, propósito e objetivo" (MARSDEN; SCHIMIDT, 2011, p.179, tradução nossa).

Um exemplo interessante é a proposta de Combs e Slann (2007, p.320, tradução nossa) que colocam como componentes cruciais do terrorismo: violência, audiência, estado de medo, vítimas e motivação política. Nesse sentido, para eles, o termo é definido como "uma síntese da guerra e do teatro, uma dramatização do tipo de violência mais proscrita - que é perpetrado em vítimas inocentes – atuada diante de uma audiência com a esperança de criar um clima de medo para fins políticos". Assim, nessa definição é relevante: o enquadramento das vítimas enquanto inocentes, o foco na percepção da audiência, uma vez que o fenômeno é "essencialmente um teatro" e a motivação como política (COMBS; SLANN, 2007, p. 321).

Outra definição interessante é proposta por Peter Chalk (2013, p xii, tradução nossa) que entende o terrorismo:

> [...] como o uso ou a ameaça de violência ilegítima empregada por atores subsestatais como meio de alcançar fins políticos específicos (com os objetivos diferindo de acordo com a organização em questão). É uma tática psicológica que procura gerar medo generalizado através da busca indiscriminada de vítimas não combatentes. Nesse sentido, o terrorismo pode ser considerado como um meio de diálogo político extremo que visa influenciar o comportamento através da precipitação de um estado geral de medo e colapso. A fim de cumprir eficazmente esta função comunicativa, o terrorismo deve visar maximizar a publicidade e os perpetradores precisam reivindicar a responsabilidade por suas ações.

Em outras palavras, o autor considera o terrorismo como uma atividade política que, embora politicamente motivada dentro do rol de atividades criminosas, as quais incluem atores subestatais, tem como alvos os não combatentes. Ademais, percebe-se que essa definição se apresenta com um enquadramento do fenômeno como um tipo comunicação.

De outro lado, Hoffmann (2006, p.39-40, tradução nossa) entende o terrorismo

> [...] como a criação deliberada e a exploração do medo através da violência ou a ameaça de violência na busca de mudanças políticas. Todos os atos terroristas envolvem violência ou a ameaça de violência. O terrorismo é projetado especificamente para ter efeitos psicológicos de longo alcance além da (s) vítima (s) imediata (s) ou objeto do ataque terrorista. É a intenção de inculcar medo dentro e, assim, intimidar, um "público-alvo" mais amplo que possa incluir um grupo étnico ou religioso rival, um país inteiro, um governo nacional ou um partido político ou a opinião pública em geral. O terrorismo é projetado para criar o poder onde não existe ou para consolidar o poder, onde há muito pouco. Através da publicidade gerada por sua violência, os terroristas procuram obter o alavancagem, a influência e o poder que, de outra forma, não têm para afetar mudanças políticas, tanto a nível local como internacional.

Assim, é interessante a percepção quanto aos atores, os quais seriam não estatais e que, politicamente motivados, poderiam atacar a mídia (opinião púbica), Estados ou entidades estatais além de grupos populacionais específicos. Outra questão relevante é o aspecto psicológico, aqui percebido com o fato de ser de longo prazo.

Encontramos, ainda, a proposta de Diniz (2002, p.13), para o qual o terrorismo figura como o:

> [...] emprego do terror contra um determinado público, cuja meta é induzir (e não compelir nem dissuadir) num outro público (que pode, mas não precisa, coincidir com o primeiro) um determinado comportamento cujo resultado esperado é alterar a relação de forças em favor do ator que emprega o terrorismo, permitindo-lhe no futuro alcançar seu objetivo político — qualquer que este seja.

Ainda dentro da abordagem do autor, o emprego de terror seria factível tanto para atores não estatais (emprego político terrorista do terror) quanto para atores estatais (emprego político não terrorista do terror) sendo que, no terrorismo, não há vinculação direta entre o objetivo e o emprego do terror (seria um estratagema). Ademais, a motivação seria política, sendo os alvos terroristas entendidos enquanto coletividade e a repercussão dos atos mais almejada do que fazer-se valer de meios de comunicação de massa em si (mídia em si). (DINIZ, 2002).

Por fim, é relevante a proposta de Schmidt (2011) de um conceito acadêmico consensual, baseado na análise de mais de 100 definições de terrorismo e um *survey* que teve três modelações, a primeira em 1984, a segunda em 1988 e a última em 2011[11]. Assim, a última atualização, com críticas ao conceito anterior estabelece que:

[11] Nesse último estudo foram analisadas respostas qualitativas de 91 indivíduos e cerca de 250 definições sobre terrorismo.

> o terrorismo refere-se, por um lado, a uma doutrina sobre a presumida eficácia de uma forma especial ou tática de violência política coerente e geradora de medo e, por outro lado, de uma prática conspiradora de ação violenta direta, demonstrativa e violência sem direito ou restrições morais, visando principalmente civis e não combatentes, realizadas por seus efeitos propagandísticos e psicológicos em vários públicos e partes do conflito (SCHMIDT, 2011, p.86, tradução nossa).

Ainda dentro da concepção de terrorismo do autor e dentro de outros pontos levantados, os alvos podem ser civis, não combatentes e outras pessoas inocentes e indefesas; as motivações cobrem um amplo espectro (desde vingança até objetivos religiosos ou nacionais); e as fontes de violência podem vir de indivíduos, pequenos grupos, redes difusas transnacionais e atores estatais ou agentes clandestinos patrocinados pelo Estado (SCHMIDT, 2011).

Diante dessas definições, de forma geral, percebe-se que a classificação dos atores e como eles agem levam as respostas com vários desdobramentos, diferentes enquadramentos e supressões ou explicação de alguns elementos. Contudo, na tentativa de se explicar o fenômeno de outras maneiras, algumas explicações acadêmicas são mais aceitas do que outras, como a explicação do terrorismo em ondas de Rappoport (que responde pergunta "d"), a divisão entre novo e velho terrorismo, a proposta de Arquilla e Ronfeldt de Guerra de Rede (que responde a pergunta "e") e a ideia de terrorismo internacional e/ou transnacional (que responde a pergunta "c").

A explicação de Rapoport (2002, tradução nossa) é que o terrorismo se dá em ondas, sendo que, ao longo da história, pode-se identificar quatro dessas ondas (ver Quadro 4). A primeira onda seria de natureza anarquista, surgindo na década de 1880 e durando 40 anos antes da nova onda, anticolonial, surgir na década de 1920. A onda anticolonial durará até a década de 1960, quando substituída pela onda da Nova Direita, que vai até a década de 1990, "deixando apenas alguns grupos ativos no Siri Lanka, Espanha, Perue Colômbia". A partir daí, e tendo principalmente sua gênese com a Revolução Iraniana, surge a última onda: a religiosa, a qual apesar de ter o islã como religião mais proeminente, não descarta o uso do terror por outras religiões.

Dentro desse quadro, a explicação de Rapoport é o mais próximo a uma teoria nos estudos sobre terrorismo. Contudo, sua teoria ainda é passível de críticas, a exemplo das apontadas por McAllister e Schmidt (2011, p.233, tradução nossa): "ao falar de movimentos e não de grupos individuais, existem ambiguidades em sua contabilidade para casos particulares de violência política". Assim, a maior falha na "teoria" seria que ele "exclui os grupos não estatais que conseguiram assumir o poder do Estado - como no caso dos fascistas e dos

comunistas - e se envolver com sucesso em terrorismo de grande porte por longos períodos de tempo" (MCALLISTER; SCHMIDT, 2011, p.233, tradução nossa).

Quadro 4 -Teoria de Ondas de Rapoport

Focus	*Primary strategy*	*Target identity*	*Precipitant*	*Special characteristics*
Anarchists, 1870–1920s	Elite assassinations, bank robberies	Primary European states	Failure/slowness of political reform	Developed basic terrorism strategies and rationales
Nationalists, 1920s–1960s	Guerrilla attacks on police and military	European empires	Post-1919 de-legitimization of empire	Increased international support (UN and diaspora)
New Left/Marxist, 1960s–1980s	Hijackings, kidnappings, assassination	Governments in general; increasing focus on USA	Viet Cong successes	Increased international training/cooperation/ sponsorship
Religious, 1970s–2020s	Suicide bombings	USA, Israel, and secular regimes with Muslim populations	Iranian Revolution, Soviet invasion of Afghanistan	Casualty escalation. Decline in the number of terrorist groups

Fonte: Mcallister e Schmidt (2011, p.229).

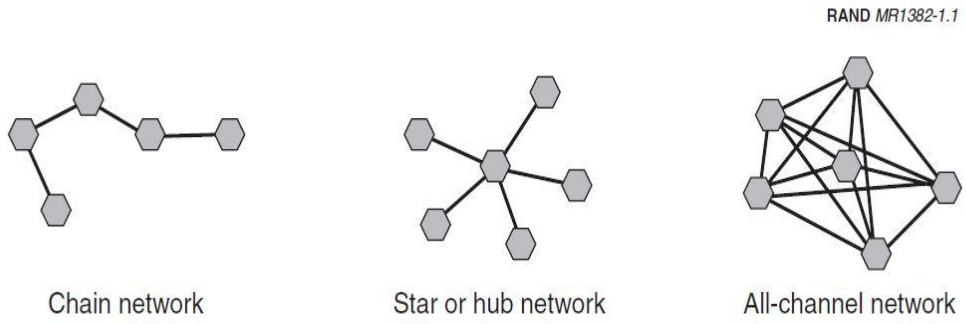
Nesse sentido autores como Burnett e Whyte (2005), Laqueur (1999), Neumann (2009), Schmid e Jongman (1988) preferem optar pela ideia de divisão entre novo e velho terrorismo, sendo que o terrorismo considerado velho faria referência aos grupos terroristas mais tradicionais, ou seja, motivados politicamente, hierarquizados e que, geralmente, utilizam métodos violentos contra seus alvos legítimos. Já o terrorismo novo faria referência aos grupos transnacionais, organizados em rede, com inspiração religiosa, comprometidos com uso excessivo de violência (JARVIS; NOURI; WHITING, 2014, p 31).

Dentro dessa ideia de rede, tem-se a proposta de Arquilla e Ronfeldt (2001, p. 06, tradução nossa) de Guerra de Rede que, embora receba o nome de "guerra", faz referência a um modo "emergente de conflito (e crime) e níveis sociais, à falta de guerra militar tradicional, em que os protagonistas utilizam formas de organização em redes e doutrinas, estratégias e tecnologias relacionadas em sintonia com a Era da Informação". Assim, uma Guerra em Rede teria duas faces: a terrorista e criminosa e a de ativistas sociais, indicando uma migração de poder para atores não estatais, mas não restringindo esse poder a elesA

Afinal, o poder ficaria em última instância para controlar as redes (ARQUILLA; RONFELDT, 1997, p.40).

Ainda colocando que existem inúmeros tipos de formatos para redes, Arquilla e Ronfeldt (2001, p.08) colocam que o formato nuclear dos terroristas (e criminosos) seria do tipo estrela (ver Figura 10). Nesse sentido, ao se pensar no terrorismo, a ideia de rede, mais descentralizada e horizontal que instituições hierarquizadas como o Estado, ajuda a ter uma perspectiva sobre medidas antiterroristas, bem como em que medida elas podem ser trabalhadas.

Figura 10 - Tipos de Rede



Fonte: Arquillla e Rondfeldt (2001, p.8)

Por fim, a ideia de terrorismo internacional e transnacional, principalmente depois da globalização e Revolução de Informação, tem ganho campo em muitas definições e explicações. Como Kushner (2003, p.365, tradução nossa) coloca esse termo serve para denominar grupos "militantes de múltiplasnacionalidades e que operam em muitos países de uma vez. Além disso, às vezes é usado de forma sinônima como terrorismo internacional ou terrorismo que envolve cidadãos ou o território de mais de um país".

Diante de todas essas indefinições e possibilidades, reforça-se aqui, então, como a pesquisa buscou entender esse lado mais "convencional" do terrorismo para depois seguir com a tipologia de ciberterrorismo. Nesse sentido, dentro das perspectivas de análise, se descartará a do terrorismo como guerra.

Essa preferência se dá uma vez que a escolha da definição de terrorismo para a pesquisa se pautará em Diniz (2002, p.15), o qual, ao relacionar os fins e os meios das ações terroristas, coloca que o terrorismo:

> [...] difere de outras formas de emprego da força pela maneira específica como a emprega (o terror) e de outras formas de emprego do terror por não visar nem a compelir nem a dissuadir, mas sim a induzir no inimigo um comportamento que altere a relação de forças em favor do grupo terrorista.

Outrossim, em sua proposta de definição há uma dissociação entre alvo tático e efeito/oponente político, elucidada no que ele chama de emprego político não terrorista do terror e emprego político terrorista do terror. Em outras palavras, ao exemplificar o emprego político não terrorista do terror com os bombardeios estratégicos, percebe-se que, em que pese o alvo tático do emprego do terror seja a população, o oponente político é outro Estado. Dessa forma, ainda que se verifique uma vinculação direta entre o objetivo último e o emprego do terror, alvos e oponentes não coincidem. De maneira similar, o emprego político terrorista do terror, embora tenha uma vinculação indireta entre objetivo último e emprego do terror (uma vez que o objetivo último dos terroristas é a mudança de forças a seu favor), não necessariamente tem seus alvos táticos coincidindo com o os oponentes.

Essa diferenciação com outros fenômenos conflitivos se dá de maneira clara, quando usamos uma abordagem clausewitziana de Guerra, adotada nesse trabalho. Para Clausewitz (1993, p. 83, tradução nossa), a guerra é "um ato de força para compelir nosso oponente a fazer a nossa vontade". Assim,

> O "ato de força" delimita o fenômeno em termos de seus *meios* – a força –, separando-o de outras manifestações em que meios exclusivamente não violentos sejam empregados. "Compelir" indica a necessidade de dobrar o oponente, obrigá-lo a algo a que ele naturalmente se opõe. E "nossa vontade" diz respeito ao objeto de toda a ação, o motivo que levou ao emprego do meio força e que causou a oposição do outro, que por isso mesmo se tornou um oponente (MENDES, 2014, p.98).

A guerra requerer períodos de ação e inação nos quais combates são desenvolvidos, gerando tanto táticas (uso da força no combate) quanto estratégias (uso dos combates para alcançar objetivos da guerra). Igualmente, vale lembrar o caráter político do conflito. Afinal, a "a guerra é meramente a continuação da política por outros meios" (CLAUSEWITZ, 1993, p. 99, tradução nossa).

Ressalta-se aqui que mesmo a Guerrilha se difere do terrorismo (embora possa fazer uso de táticas terroristas no intuito de mudar a correlação de forças) porque a guerrilha se manifesta pela combinação entre defesa estratégica e ofensiva tática dentro da concepção clausewitziana. É que a principal diferença entre guerra e terrorismo, sob a perspectiva de Diniz, se centra na vinculação entre o ato e o objetivo político final. Em outras palavras,

enquanto na guerra há uma vinculação direta, possibilitando constitui uma estratégia, no terrorismo não há essa possibilidade, daí a ideia de ele ser um estratagema (DINIZ, 2002; MENDES, 2014).

Vale ainda indicar que, ao se trabalhar com uma tipologia que use como meio o ciberespaço, a ideia de rede e de fenômeno transnacional é válida para a pesquisa. Afinal, o ciberespaço interliga o mundo, ou pelo menos boa parte dele, uma vez que a penetrabilidade média da Internet a nível mundial é de 51,7% (INTERNET WORLD STATS, 2017), fazendo com que narrativas terroristas cheguem mito mais longe e alargando pontos nodais das redes terroristas.

3.2 O ADVENTO DA INTERNET E SEU USO POR GRUPOS TERRORISTAS

Com a expansão da Internet, na década de 1990[12], várias pessoas passaram a utilizar o ciberespaço de maneira crescente, fomentando tanto o desenvolvimento de atividades produtivas para a sociedade quanto o de atividades desviantes. Segundo Wykes e Harcus (2010, p.216, tradução nossa):

> Agora, o advento e o crescimento exponencial da Internet desempenham um papel fundamental no mundo em que vivemos. É o espaço público do século XXI. O alcance global, a estrutura caótica, a facilidade de acesso, o anonimato e a nossa crescente dependência para a informação, a educação, o entretenimento e a comunicação que oferece fazem parecer ser uma ferramenta perfeita para terroristas e locais de atividade terrorista em todo o mundo.

Dessa forma, ideias da década de 1980 de terceira onda de Toffler (1980)[13]e sobre a possibilidade de terroristas perpetrarem ataques destrutivos a distância, ganharam força. Em realidade, essa ideia de ataques a distância surge pela primeira vez com Barry Collin (1997), que cunhou o termo ciberterrorismo pela primeira vez significando exatamente esse perigo como consequência da interseção entre mundo físico e virtual, tendo como alvos Infraestruturas Críticas de um Estado. Na visão de Collin, ciberterroristas se tornariam um perigo, uma vez que poderiam invadir o sistema de controle de tráfego aéreo fazendo aviões

---

[12] Com o CERN (Organização Europeia para a Pesquisa Nuclear) colocando em domínio público software da World Wide Web (WWW) e a proliferação de navegadores da Internet (LUCERO, 2011).

[13] De acordo com Alvin Toffler (1984), a primeira onda trata da Revolução Agrícola; a segunda apresenta as modificações ocorridas na sociedade com base na Revolução Industrial, já a terceira onda é a "Era da Informação", em que mente, informação, conhecimento e alta tecnologia são tipos de capital essenciais ao sucesso das corporações.

colidirem, ou invadir sistemas industriais de alimentação mudando a composição dos alimentos, ou ainda desestabilizar sistemas bancários, transações financeiras e bolsas de valores.

Nesse contexto de novas tecnologias e com tais visões alarmistas sobre o uso da Internet por atores não estatais, interpretações como a do Conselho de Pesquisa Nacional dos Estados Unidos emergiram, constatando que "Os terroristas de amanhã poderão ser aptos a fazer mais danos com um teclado do que com uma bomba" (NRC, 1991, p.7, tradução nossa). Essas interpretações acabaram ganhando um maior terreno após os ataques de 11 de Setembro e a ideia de Guerra ao Terror. Segundo Denning (2010, p.216), o que houve foi uma reinterpretação sobre o significado do terrorismo, que começou um pouco antes, mas foi acelerada com o 11 de Setembro, gerando uma sobrevalorização diante do risco do terrorismo, uma vez que o fenômeno foi transferido de uma significação de motivação política com uso de violência para representar ameaças contra a soberania Estatal.

Todavia, como exatamente os terroristas passaram a se apropriar do ciberespaço? Em definitivo, o que levou a manutenção de seu uso? E quais as possibilidades que eles enxergam para o ciberespaço?

O uso da Internet por grupos terroristas começou no final da década de 1990, quando a Al Qaeda lançou pioneiramente seu primeiro website: www.alneda.com (WEIMANN, 2008, p.64). Além disso, desde 1995, o grupo possuía uma lista de e-mails para disseminação de informações (ATWAN, 2015, p.16).

Concretamente, de acordo com Weimann (2015, p.35), em 1990, havia em torno de 12 websites terroristas, sendo que em 2003 esse número subiu para 2.600 e, em 2013, um pouco mais de 10.000 websites foram contabilizados. Segundo Denning (2010, p. 195), em 1998, 12 dos 30 grupos da lista de organizações terroristas do Departamento de Estado dos EUA teriam websites, sendo que, em 2002, pesquisadores da Universidade de Haifa, em Israel, encontraram 29 sites de 18 organizações na lista do Departamento de Estado de 2000.

Essa proliferação de websites não tinha como interesse revelar qualquer informação sobre atividades violentas, mas sim começar a espalhar uma narrativa de legitimação. Afinal, os grupos explicitam que foram deixados sem escolha alguma a não ser a via violenta, mostrando-se enquanto oprimidos, uma vez que "são perseguidos, seus líderes submetidos a tentativas de assassinato e seus apoiadores são massacrados" (CURRAN; CONCANNON; MCKEEVER, 2008, p. 2, tradução nossa).

Aliado a esse discurso sobre opressão, a religião foi colocada como outra variável de legitimação e, em 2003, foi a primeira vez que o termo *cyber jihad* apareceu nos "39 Princípios da Jihad" que a Al Qaeda circulava em suas redes de comunicação (ATWAN, 2015, p.16). Assim, com viés religioso, esse termo representaria uma forte ação interativa das plataformas digitais pelos terroristas, "evoluindo de sites estáticos, fóruns de bate-papo e revistas on-line para fazer uso eficiente das plataformas de mídia sociais interativas e de ritmo acelerado de hoje" (LIANG, 2015, p.2, tradução nossa).

Em 2005, Ayman al Zawahiri, líder da Al Qaeda, declarou que mais da metade da batalha travada estria na mídia e que, "nessa batalha de mídia, estamos na corrida pelos corações e mentes da nossa Umma". Não obstante, segundo Atwan (2015, p.17), Anwar al-Awlaki foi o primeiro a pensar em usar as plataformas sociais "para espalhar o material jihadista mais amplamente e alcançar novos nichos de recrutamento". Ele criou um blog, conta no Facebook e canal no Youtube próprios para distribuir a revista digital "Inspire", a qual oferece conselhos sobre a fabricação de bombas, criptografia, fabricação de venenos, realização de vigilância, comentários do Alcorão e uma propaganda mais crua da Al Qaeda (THE GUARDIAN, 2013).

Assim, os anos 2000 vão representar a ascensão cada vez maior dos grupos a essas plataformas on-line, à medida que elas foram aparecendo, como foi o caso do *Orkut*, *Facebook*, do *Youtube* e do *Twitter*. A título de curiosidade, em 2006, o *Orkut* tinha "ao menos 10 comunidades dedicadas a louvar Bin Laden, Al-Qaeda, ou a jihad contra os Estados Unidos, com uma comunidade desenhando mais de 2.000 membros" (DENNING, 2010, p.197, tradução nossa). Entretanto, o grande salto quantitativo se deu com o Estado Islâmico, que, no ano de 2014, tinha em sua conta do *Facebook* cerca de 829 milhões de usuários ativos e mais de 284 milhões de usuários registrados no *Twitter*, publicando 500 milhões de *tweets* por dia, bem como suportando mais de 35 idiomas (LIANG, 2015, p.5, tradução nossa). De fato, o Estado Islâmico elevou o uso de mídias sociais, recebendo muitas vezes a alcunha de Califado Digital, que, para além do uso do Instagram e Skype, usa meios de mensagens anônimas por plataformas Android para comunicações, postagens de materiais, vídeos desenhados e alimentados via "uso inteligente de hashtags" (ATWAN, 2015, p.18, tradução nossa).

Para manter um discurso amplo, tais grupos se apropriam de ferramentas de criptografia. Contudo, se no passado essas ferramentas eram obtidas do setor privado, a exemplo do PGP (*Pretty Good Privace*) ou o *TrueCrypt*, os riscos de que poderiam haver potenciais *backdoors* governamentais nos softwares fez com que os grupos desenvolvessem

suas próprias ferramentas. Exemplo disso, foi o desenvolvimento do *Mujahideen Secrets* e o *Mujahideen Serets 2*, lançados pela *Global Islamic Media Front* (Frente Global da Mídia Islâmica- GIMF) em 2007 e 2008, e, mais recentemente, em 2013, o *Asrar al-Dardashah*, também lançado pelo GIMF, que implementa uma camada de criptografia em serviços já existentes da Internet, a exemplo do Google, Talk, MSN, AOL, Instant Messenger e Jabber / XMPP e o *Amn al-Mujahid,* lançado pelo *Al-Fajr Media Centre* (Centro de Mídia Al-Fajr), que permite aos usuários escolher entre um conjunto de algoritmos de criptografia bem conhecidos e gerar pares de chaves (HALOPEAU, 2014, p.126-127).

Outra forma de ocultação de mensagens que vem sendo utilizada crescentemente é a esteganografia que visa ocultar mensagens dentro de imagens (BALLARD; HORNIK; MCKENZIE, 2002, 989). Além do uso do espaço da Deep Web[14] e Dark Web[15], existe a facilidade de acesso aos mecanismos como VPN/GhostVPN, Tor (The OnionRouter) e serviços de e-mail já criptografados como o Bitmessage (ATWAN, 2015).

Quanto aos modos de disseminação de narrativas, não apenas o ciberespaço é usado, mas o desenvolvimento de videogames também é uma ferramenta - a exemplo do *Kaboom* (jogo de bombardeio suicida), *Special Forces* (do Hezzbollah, o qual jogadores atacam Israel e forças pró-israelenses) e *The Way to Al Quads* (Caminho para Jerusalém, ou seja, um jogo de crianças em que se ganha pontos ao se atingir helicópteros israelenses) (AXELROD, 2009, p.175). No que tange ao Estado Islâmico, por exemplo, sua versão própria do Facebook, o Muslimbook, bem como aplicativos para celulares (apps) próprios, como é o caso do *Dawn of Glad Tidings*, que atualiza os usuários sobre notícias do ISIS e "usa suas contas de Twitter automaticamente para disseminar informação, achar novos financiadores", são eficazes (ATWAN, 2015. p.19, tradução nossa).

O alcance das narrativas terroristas, nesse sentido, deve ser levado em consideração, já que dois casos ilustram o que podem gerar: a radicalização. Esses casos são o da estudante universitária Roshnara Choudry, que esfaqueou um membro do Parlamento britânico com uma faca em 2010 (SEAMARK, 2010) e dos Irmãos Tsarnaev, que plantaram bombas na maratona de Boston em abril de 2013, sendo condenados em 2015 (G1, 2013).

Vale ressaltar que não apenas a questão da comunicação foi se desenvolvendo com os grupos terroristas, mas também o modo de invasão dos sistemas. Em 2003, por exemplo, o culto japonês Aum Shinrikyo ("Suprema Verdade") realizou um ataque cibernético complexo,

---

[14] A Deep Web faz referência ao conteúdo da World Wide Web que não é indexado por mecanismos de busca padrão (GREENBERG, 2014).

[15] A Dark Web faz referência aos servidores de rede inalcançáveis na Internet, por demandar softwares, configurações ou autorizações específicas para o acesso (GREENBER, 2014).

incluindo a obtenção de informações confidenciais sobre instalações nucleares na Rússia, Ucrânia, Japão e outros países como parte de uma tentativa de atacar os sistemas de segurança da informação dessas instalações. Contudo, a tentativa foi frustrada pelo confisco da informação antes de que qualquer ação se desse efetivamente. Outro exemplo pode ser visto em 2013, quando um grupo de hackers palestinos chamado o I*zzad-Din al-Qassam Cyber Fighters,* identificado com a seção militar do Hamas, reivindicou a responsabilidade por um ataque no site da American Express que interrompeu serviços financeiros por duas horas (COHEN, 2014, p166-67). Em 2015, desde o mês anterior ao Massacre de *Charlie Hebdo*[16], 25.000 ataques cibernéticos de pelo menos 27 grupos de hackers advogando aliança ao Estado Islâmico foram dirigidos à França, representando a maior onda de ataques que o país já havia presenciado - com a maioria dos grupos hacker com origem do Norte da África e da região do Sahel, e sendo a maioria dos ataques do tipo Negação de Serviço (DoS), os quais bloqueiam o tráfego de informações de websites e, portanto, seu funcionamento (ATWAN, 2015, p.27-28).

Diante do exposto, não é de se espantar os cenários alarmantes, formados em torno do ciberespaço e de grupos terroristas. Ainda mais com os exemplos acima mencionados, em que hackers dos grupos estão sendo incentivados. O que demonstra uma tendência preconizada no início dos anos 2000 por Verton (2003, p.18, tradução nossa, grifo nosso):

> a próxima geração de terroristas não será uma horda de bandidos acéfalos vivendo no aperto existente no Afeganistão. **As jovens crianças que eles estão radicalizando hoje estão estudando matemática, ciência da computação e engenharia.** Eles crescerão e perceberão "Eu sou muito valioso para colocar dinamite ao redor da minha cintura e caminhar até um café lotado". E eles irão pensar muito diferentemente sobre como eles podem atacar seus inimigos percebidos. **"A Internet será outra ferramenta na sua caixa de ferramentas"**

Assim, a geração do século XXI, que cresceu em um ambiente já digitalizado, compõe as células terroristas. Em sua maioria, esses jovens têm não só a familiaridade, mas igual dependência das tecnologias da informação. Padrão que tende a crescer com o passar do tempo e muito provavelmente seguirá tendência de uso e desenvolvimento de ferramentas concomitantes ao lançamento de novidades digitais.

Além disso, como McGuire (2014, p.79, tradução nossa) coloca, vale lembrar que a Internet é "apenas mais uma ferramenta para o mau uso da hiperconectividade, uma vez que os terroristas têm acesso aos aparelhos como GPS e tecnologia de satélites que fornecem suas

[16] Massacre do *Charlie Hebdo* foi um atentado terrorista que atingiu o jornal satírico francês *Charlie Hebdo* em 7 de janeiro de 2015, em Paris, resultando em doze pessoas mortas e cinco feridas gravemente.

próprias opções". Em outras palavras, o uso terrorista da Internet não abrange todas as possibilidades que o ciberespaço proporciona aos grupos terroristas, principalmente se recordarmos que o ciberespaço, para além de uma camada de conteúdos e aplicação, possui uma parte física e outra lógica. Nesse sentido, em que medida é válido o uso terrorista da Internet como representação do ciberterrorismo? Seriam os dois conceitos iguais? Para responder a essa questão, talvez seja mais profícuo detalhar melhor o que a Internet proporciona aos grupos terroristas, para, então, avaliar os dois termos.

Segundo Calafato e Caruana (2015, p.210, tradução nossa), "a transição da adaga para a bomba, para ataques suicidas e para uso da internet para atender seus objetivos, indica como os terroristas evoluem seus métodos de acordo com as circunstâncias circundantes". Denning (2010, p.194) comenta que os grupos terroristas usam a Rede basicamente do mesmo modo que outros usuários, mas as formas pelas quais os terroristas divulgam documentos, propaganda, recrutam, treinam novos membros e causam dano às vítimas vêm se modificando. Fato comprovado pela exposição anterior sobre a evolução do uso da Internet pelos terroristas. Mas, em resumo, o que a Internet traz de vantagem aos grupos terroristas?

Alguns pontos já foram levantados como a questão da comunicação e o anonimato, mas diferentes autores especificam alguns pontos a mais. Weimann (2015, p.55-56), por exemplo, separa o uso da Internet em dois tipos: instrumental e para comunicação, colocando que os usos mais comuns das plataformas digitais por grupos terroristas são: guerra psicológica, propaganda, doutrinação on-line, recrutamento e mobilização, extração de dados, treinamento virtual, planejamento, coordenação cibernéticos e financiamento. De maneira semelhante, Wykes e Harcus (2010, p.220-221) colocam o ciberespaço como um local para a coleta de informações, publicidade, propaganda e guerra psicológica, recrutamento, meio de treinamento (incluindo planejamento e networking), levantamento de fundos e ataques a outros terroristas.

Nesse sentido, diante do exposto acerca do desenvolvimento do uso terrorista da Internet, fica clara, em primeiro lugar, a questão do ciberespaço enquanto meio de comunicação e aprendizado para os grupos terroristas. Internamente os meios de comunicação instantânea, de fácil acesso (basta uma máquina/aparelho e um ponto de conexão) e de fácil manipulação, garantindo anonimato, são atrativos para os grupos terroristas. Ademais, como Weimann (2015, p.58) coloca, esses grupos têm controle direto sobre o conteúdo de sua mensagem, oferecendo ótimas oportunidades para que eles moldem como são percebidos por diferentes audiências, manipulem sua própria imagem e a imagem de seus inimigos, normalmente via discurso dos oprimidos e opressores.

A abrangência para espalhar sua narrativa atingindo o maior número possível de recrutas é possibilitada pelo alcance mundial da Rede, proporcionando formas de radicalização. Essa radicalização se dá em quatro etapas segundo Halopeau (2014, p.125):

a) o indivíduo é atraído por intermédio do compartilhamento de vídeos em websites, como o Youtube, isto é, com uma conta que se refere a um URL que leva a um fórum de debates especifico;
b) membros juniores que entram no grupo são testados para completar tarefas e, a medida que vão tendo bons resultados, eles ganham além de privilégios, posições de destaque dentro do fórum;
c) depois de um tempo, o membro sênior é convidado a conhecer fisicamente o administrador do grupo para validar e aprofundar o acesso do novo membro;
d) depois do encontro, o membro é introduzido a uma pequena rede de indivíduos muito mais radicais (via VoIP, Skype ou PalTalk) e é quando o candidato é confiado com informações de planejamento de ataques e quais são os alvos das operações.

Dentro dessas etapas, é interessante a parte off-line (i.e. física) do recrutamento. Entretanto, ela não exclui que a validação aconteça de forma on-line. Como coloca Yannakogeorgos (2014, p.49, tradução nossa), a doutrinação ocorre quando "o indivíduo simpatizante começa a dedicar tempo a explorar sites terroristas e a formar relacionamentos on-line com indivíduos que promovem ideologias extremas" sendo que a radicalização se completa quando "indivíduo influenciado se move da pirâmide de opinião para o domínio de apoiar ativamente um ato de terrorismo específico ou facilitá-lo de maneira material além do campo das ideias". Assim, vale o estudo da RAND Corporation de 2013 (BEHR et al, 2013), pois coloca que a Internet pode aumentar as oportunidades para a radicalização[17]. Contudo, não necessariamente acelerando o processo e não necessariamente substituindo o contato físico necessário para a própria radicalização (*self-radicalisation).*

Nesse sentido, a questão da narrativa ganha relevância, na maneira em que percepções são moldadas, e como o conteúdo da narrativa é legitimado. Conforme mencionado anteriormente, essa legitimação vem do discurso de oprimidos e opressores e de um viés religioso muito forte. Esse viés religioso se traduz através da citação de *fatwas* (opinião legal

[17] No estudo feito se usa o termo radicalização com base na definição do governo britânico aplicada a sua estratégia de prevenção ("processo pelo qual uma pessoa vem a apoiar o terrorismo e formas de extremismo que levam ao terrorismo"). Logo, sua definição sobre radicalização on-line é a seguinte: "processo onde interações virtuais e exposição ao conteúdo da Internet fazem com que indivíduos vejam a violência como método legítimo de resolver conflitos político sociais" (BEHR et al. 2013, p. 2-3, tradução nossa).

ou interpretação interpretada que não é vinculante, mas autoritária, como se fossem regras religiosas) e em menções a jihad (guerra aos infiéis). Como Weimann (2015, p 215, tradução nossa) coloca:

> embora a maioria das fatwas on-line não estejam relacionadas ao terrorismo, à violência, ao radicalismo ou à jihad, grupos terroristas têm usado a Internet para publicar fatwas radicais. [...] Muitos dessas fatwas on-line fornecem justificação moral e religiosa para o uso do terrorismo e se relacionam com questões terroristas incluindo a definição e identificação do espaço de batalha em que os atos devem ser executados, a identidade das vítimas legítimas, os meios de ação adequados e a legitimidade dos ataques suicidas.

Igualmente, fóruns de discussão e websites dão vazão para não apenas a sondagem de membros, mas também para o processo de mostrar e moldar uma percepção a audiências, a exemplo do: *Mujahidat* (grupo para mulheres que querem participar da jihad criado em 2004), *Musilm Net* (website que acusa EU de uso de armas químicas no Iraque); *Palestinian Forum* (website do Hamas que chama audiência para a destruição de Israel) (AXELROD, 2009, p.174). Além de servirem para a disseminação de informações, proporcionando aprendizado para simpatizantes e membros.

Dessa forma, vale a colocação de que os terroristas são trabalhadores de conhecimento e que grupos terroristas são organizações de conhecimento (ARIELY, 2008). Afinal, a troca de informações sobre construção de bombas, químicos, mapas, planos entre outros não deixa de concretizar um verdadeiro campo de treinamento on-line para os membros dos grupos terroristas, com revistas, manuais e websites contendo informações. Toda essa comunicação se dá de forma a se manter o anonimato, conforme já mencionado, seja pelo uso do espaço da Deep Weeb e Dark Web, seja por ferramentas de mensagem criptografadas disponíveis ou desenhadas.

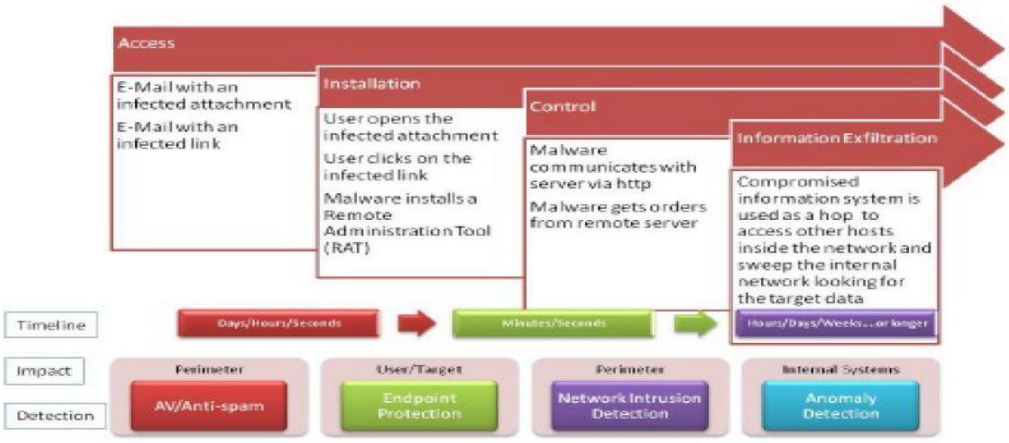
Para além da comunicação interna, a comunicação externa também é importante para a causa dos grupos terroristas, uma vez que facilita a arrecadação de fundos, proporcionando financiamento. Esses financiamentos se dão por meio de e-commerce ou doações explícitas nos websites dos grupos, mas algumas vezes elas são feitas sob a fachada de websites de organizações de caridade (WEIMANN, 2015, p.77). Ainda, o angariamento de fundos pode se dar por intermédio de vários crimes cibernéticos, como roubo de identidade e fraude de cartão de crédito (WEIMANN, 2015, p.78; DENNING, 2010, p.206).

Outra questão que conta a favor do uso da Internet é a facilidade de acesso a dados abertos que podem ser úteis aos planos terroristas. Acesso aos mapas pelo Google Earth,

websites com descrição de funcionários contendo fotos, ou mesmo documentos de domínio público são de grande valia para o planejamento de operações dos grupos terroristas. Contudo, para além dessa receptação de informações de forma passiva, os grupos terroristas vêm desenvolvendo formas ativas de coleta de dados, ou seja, eles também invadem sistemas, desenvolvendo não apenas softwares próprios como já comentado, mas também por meio do que se chamam Ameaças Persistentes Avançadas (APT, em inglês) as quais têm um interesse simbiótico em manter o meio de onde eles se alimentam e são projetados para contornar a maioria dos detectores de malware (MEHAN, 2014, p. 85) perfazendo um ciclo de 04 fases: acesso, instalação, controle e extração de informações (ver Figura 11).

Nesse ponto, é factível se perguntar se essa invasão de sistemas, com uma potencialidade destrutiva pode ser considerada apenas uma extensão das atividades terroristas no ciberespaço ou se configura um novo fenômeno. Nesse sentido, a mesma pergunta é válida sobre a mobilização de massas, a guerra psicológica. Afinal, todas essas ações podem ser bem específicas e desenvolvidas de maneira praticamente independente de uma contraparte física.

Figura 11 - Ciclo de vida de um APT



Fonte: Mehan (2014, p.85)

Tanto questões de comunicação, recrutamento, radicalização e financiamento revertem para células terroristas físicas, de uma maneira mais direta com aporte de indivíduos ou de dinheiro. Contudo, questões psicológicas e a invasão de sistemas parecem ir além de extensões de atividades terroristas convencionais, dando uma nova forma a um fenômeno flexível. Essa nova forma e a questão da violência (psicológica e potencialmente física)

parecem dar margem a diferenciação do uso terrorista da Internet e do ciberterrorismo, mas, para entender essa aparente diferenciação, primeiro se faz necessário analisar mais a fundo o que a academia entende por ciberterrorismo.

3.3 CIBERTERRORISMO: (IN)DEFINIÇÕES

A questão sobre o ciberterrorismo, conforme já comentada, se revolve em um imbróglio conceitual. Isso se deve em parte devido à natureza híbrida do uso do ciberespaço por grupos terroristas. Como Talihärm (2010, p.63, tradução nossa) coloca:

> Na prática, enfrentamos ataques cibernéticos cada vez mais comuns que englobam alguns dos elementos substanciais do ciberterrorismo, como a motivação política ou o dano e o medo graves, bem como várias maneiras pelas quais os terroristas usam a Internet para apoiar e cumprir seus propósitos.

Nesse sentido, MacKinnon et al. (2013, p 234, tradução nossa) apontam que a maioria das conceitualizações contemporâneas segue três motes: motivação do perpetrador, sistema cibernético como alvo e o impacto em uma população identificada. Já Talihärm (2010, p.63-64) explica que há duas tendências para a conceitualização do fenômeno: uma orientada a seus alvos e outra orientada a ferramentas. A primeira tendência se refere aos ataques politicamente ou socialmente motivados contra computadores, redes e informações, que sejam conduzidos a partir de outros computadores ou fisicamente, quando causam lesões, derramamento de sangue ou dano grave ou medo. Já a segunda engloba todas as ações que usam a internet ou computadores para organizar e completar ações terroristas.

Em que pese haja essa diferenciação, a maioria dos acadêmicos considera o ciberterrorismo como mais preciso dentro da tendência orientada para ferramentas (TALIHÄRM, 2010, p 64) e, embasado na conceituação de Denning (2000, p.1, tradução nossa, grifo nosso), para a qual:

> o ciberterrorismo é a convergência do ciberespaço e do terrorismo. Refere-se aos **ataques ilegais e ameaças de ataque contra computadores, redes e as informações nele armazenadas quando são feitos para intimidar ou coagir um governo ou suas pessoas em busca de objetivos políticos ou sociais**. Além disso, para se qualificar de terrorismo cibernético, um ataque deve resultar em **violência contra pessoas ou propriedade, ou pelo menos causar danos suficientes para gerar medo**. Os ataques que levam à morte ou lesões corporais, explosões ou **perdas econômicas** severas seriam exemplos**. Ataques sérios contra as infraestruturas críticas** podem ser atos de ciberterrorismo, dependendo do seu impacto. Os ataques que perturbam os serviços não essenciais ou que são principalmente um incômodo caro não seriam [ciberterrorismo].

Todavia, com o passar do tempo essa definição foi levemente alterada, tanto com o objetivo de diferenciar o fenômeno da guerra cibernética, que para Denning (2007) se pautaria em uma dinâmica estatal, como de tentar reforçar a possibilidade de o fenômeno ocorrer diante das críticas de sua baixa probabilidade. Dessa forma, o fenômeno do ciberterrorismo seria constituído de:

> ataques altamente danificadores ou ameaças de ataque por **atores não estatais contra sistemas de informação** quando conduzidos para **intimidar ou coagir governos ou sociedades na busca de objetivos políticos ou sociais**. É a convergência do terrorismo com o ciberespaço, onde o ciberespaço se torna o meio de conduzir o ato terrorista. Em vez de cometer atos de violência contra pessoas ou propriedades físicas, o **ciberterrorista comete atos de destruição e destruição de propriedade digital** (DENNING, 2007, p. 124, tradução nossa, grifo nosso).

De maneira similar, Weimann (2005, p.130; 2016 p. 277, tradução nossa, grifo nosso) coloca que o fenômeno comumente faz referência ao "uso de ferramentas de rede informática para prejudicar ou **desligar infraestruturas críticas nacionais** (como energia, transporte, operações governamentais)". O autor explicita que quanto à "**distinção entre uso de tecnologia da informação e terrorismo que usa tecnologia informática como arma/ alvo**, apenas o último pode ser definido como o terrorismo cibernético" (WEIMANN, 2005, p. 133, tradução nossa, grifo nosso).

Nesse sentido, a separação entre uso terrorista da Internet e ciberterrorismo é enfatizada por Maura Conway (2002, p.6) para a qual ataques cibernéticos para serem caracterizados como terrorista devem ter por trás uma motivação política e resultar em algum tipo de violência. Assim, para Conway (2002, p.6, tradução nossa, grifo nosso).

> no que diz respeito à distinção entre uso terrorista de tecnologia da informação e **terrorismo envolvendo tecnologia informática como arma / alvo,** apenas o último pode ser definido como o terrorismo cibernético. O "uso" terrorista de computadores como facilitador de suas atividades, seja por propaganda, comunicação ou outros fins, é simplesmente isso: "uso".

Diante dessas colocações e entendendo que referências acadêmicas no estudo sobre o fenômeno do ciberterrorismo explicitam a necessidade de diferenciação do uso da Internet por terroristas e do ciberterrorismo, a questão que é deixada se resume em quais as características que exatamente distinguem as duas modalidades, dado que elas se interligam.

Com isso, Seddon (2002, p.1034) elucida um caminho, visto que, para o autor, os elementos chave para uma conceituação "precisa e legítima da ameaça do ciberterrorismo" seriam quatro:

a) Uma definição confiável de ciberterrorismo e termos relacionados;

b) Uma compreensão do tipo de hacking que está ocorrendo atualmente;

c) Uma compreensão da pior coisa que um ataque cibernético poderia fazer, o que um ataque cibernético não poderia fazer e a coisa mais provável que um ataque cibernético poderia fazer; e

d) Uma compreensão de como os computadores podem ser usados por organizações terroristas como táticas e multiplicadores de força.

No tocante à definição confiável, dada as várias interpretações sobre o ciberterrorismo, um consenso não aparece no horizonte. Contudo, conforme observado em Denning (2000; 2007), Weimann (2005, 2016) e Conway (2002) algumas características se repetem como:

a) utilização da tecnologia como arma ou alvo;

b) caráter destrutivo a propriedade (digital ou Infraestruturas Críticas) e

c) motivação política.

Obviamente, existem outras definições sobre o fenômeno que podem ajudar na busca de características em comum, as quais podem apontar diferenças valiosas com termos relacionados, isto é, hacktivismo, guerra e crime cibernéticos. Logo, um levantamento de conceitos é oportuno.

Flemming e Stohl (2001, p.31, tradução nossa, grifo nosso), por exemplo, acreditam que o ciberterrorismo é único na medida em que não existe além do relacionamento próximo com os computadores. Assim, ele é considerado:

> [...] como qualquer ato de terrorismo que use **sistemas de informação** ou tecnologia digital (computadores ou redes de computadores) como **um instrumento ou alvo**. Mais uma vez, os descritores qualificados podem ser usados para colocar o terrorismo cibernético em contextos mais específicos. O "terrorismo cibernético" pode ser "**internacional" "doméstico", "estatal" ou "político", mas o ato principal que envolve uma combinação do ato terrorista e dos computadores permanece sempre o mesmo**

Theohary e Rollins (2015, p.1, tradução nossa, grifo nosso) consideram o fenômeno como o uso "premeditado de atividades disruptivas, ou a ameaça, contra computadores e / ou redes, com a intenção de causar **danos ou outros aspectos sociais, ideológicos, religiosos, políticos ou objetivos semelhantes,** ou intimidar qualquer pessoa em cumprimento de tais

objetivos". Podendo ser perpetrado **tanto por atores estatais quanto não estatais** (THEORAHY; ROLLINS, 2015, p.2, tradução nossa, grifo nosso).

Luijif (2014, p.13) busca em sua análise do fenômeno agregar um contexto legal (usando o Reino Unido como base), explicitar: se o ciberespaço é usado como arma ou sendo um alvo, qual o objetivo do ato malicioso e qual a intenção combinada com objetivo de longo prazo. Nesse caso, o ciberterrorismo seria:

> O uso, preparação ou ameaça de ação projetada para causar uma mudança de ordem social, cria um **clima de medo ou intimidação** entre (parte de) o público em geral, ou **influenciar a tomada de decisões políticas** pelo governo ou uma organização governamental internacional; feito para o avanço de uma **causa política, religiosa, racial ou ideológica**; **afetando a integridade, confidencialidade e / ou disponibilidade de informações, sistemas de informação e redes**, ou por ações não autorizadas que afetam o **controle baseado na tecnologia da informação e da comunicação de processos físicos do mundo real**; e envolve ou causa:
> - **violência, sofrimento, lesões graves ou morte de (a) pessoa (s),**
> - **dano grave a uma propriedade,**
> - **um risco grave para a saúde e a segurança do público,**
> - **uma séria perda econômica,**
> - **uma violação grave da segurança ecológica,**
> - **uma grave violação da estabilidade social e política e da coesão de uma nação.**
>
> (LUIJIF, 2014, p.15-16, tradução nossa, grifo nosso)

Tombul e Akdogan (2016, p. 4) tem uma análise interessante quando explicitam que o ciberterrorismo causa uma **ansiedade política, econômica e psicológica**. Sendo que,

> O uso terrorista do computador para fazer propaganda, arrecadar dinheiro, recrutar novos apoiantes não pode ser totalmente definido como o terrorismo cibernético. Os ataques do ciberespaço devem **incluir elementos e atividades terroristas, como resultados de assassinatos ou danos em grande escala e as ações devem ser politicamente motivadas** para serem chamadas de terrorismo cibernético. (TOMBUL e AKDOGAN, 2016, p.6, tradução nossa, grifo nosso).

Combs e Slann (2007, p.71, tradução nossa, grifo nosso) apresentam dentro de sua "Enciclopédia sobre Terrorismo" o termo como "uso de recursos computacionais para **intimidar e / ou coagir outros ou uma sociedade inteira**". Destacando que essa seria uma atividade individual ou grupal, indicando sua perpetração **por atores não estatais.**

Dentro de uma Enciclopédia sobre Terrorismo também encontramos a definição de Kushner (2003, p.103, tradução nossa, grifo nosso), para o qual "o termo terrorismo cibernético refere-se à convergência do terrorismo e do ciberespaço - **a motivação política e sabotagem de sistemas de informação**". Colocando que "O ataque cibernético coordenado

contra certas infraestruturas, como os computadores que controlam e coordenam aviões ou os que operam no mercado de ações, podem causar estragos significativos" (KUSHNER, 2003, p.104, tradução nossa).

Por fim, tem-se Colarik (2006, p.47, tradução nossa, grifo nosso) que define ciberterrorismo como:

> [...] ato criminoso **premeditado e politicamente motivado**, por **grupos subnacionais** ou clandestinos contra a **informação e sistema de computadores, programa de computadores e dados**, que resultam em **violência física** onde o objetivo pretendido é **criar medo** em alvos não combatentes.

Diante dessa simples amostra de conceitos, fica evidente a dependência do termo em relação à concepção dos autores sobre o conceito de terrorismo. Assim, alguns aspectos de consideração do terrorismo, enquanto crime, política, guerra, comunicação e cruzada religiosa/jihad, podem ser observados. Ademais, mantem-se nos conceitos de uma forma maior ou menor:

a) tríade de utilização da tecnologia como arma ou alvo;
b) caráter destrutivo a propriedade (digital ou Infraestruturas Críticas);
c) motivação política.

Contudo, ainda resta a questão de diferenciação com outros fenômenos pares, que não é o objetivo dessa pesquisa *per se* e, por isso, a análise não será minuciosa.

Flemming e Stohl (2001, p.34, tradução nossa) colocam que "o crime cibernético é semelhante ao ciberterrorismo no uso de redes de computadores e sistemas de informação, mas claramente diferente em sua motivação e objetivos". Afinal os objetivos dos criminosos cibernéticos de acordo com Mehan (2014, p.68) são a maximização do lucro financeiro, ao mesmo tempo em que se minimizam riscos, e o desejo de ganhar poder por meio do controle de fontes ou da própria informação, enquanto que os objetivos dos ciberterroristas estariam relacionados a um alto impacto destruição com maior sigilo (MACKINNON et al, 2013, p.236).

Nesse sentido, Colarik (2006, p.53) argumenta que há duas principais diferenças entre criminosos e terroristas na Internet: a transferência de conhecimento dos sistemas e a destruição do sistema. Afinal, ainda que o compartilhamento de conhecimento seja eficaz para a narrativa dos grupos terroristas, certo grau de anonimato é requerido para que a invasão dos sistemas/coleta de informações possa ocorrer. Além disso, para perpetrarem suas ações, os

criminosos não podem permitir o bloqueio ou a destruição da Internet para si próprios. Afinal, ela é vista como uma ferramenta (CONWAY, 2007, p.14).

De modo estratégico, “os cibercriminosos tipicamente usam inúmeros alvos e não mantêm um controle prolongado sobre os servidores, pois o risco de detecção aumenta proporcionalmente” (MACKINNON et al. 2013, p.235, tradução nossa). Em outras palavras, quanto maior o anonimato melhor para os criminosos, mas o mesmo não pode ser dito para os ciberterroristas, que procuram um espaço para seu teatro, procurando o que aqui chamaremos de anonimato estratégico, ou seja, manter-se no anonimato até a reivindicação de autoria dos atos.

Dado esse caráter destrutivo e a necessidade do anonimato estratégico, pergunta-se até que ponto a viabilidade de contratações de criminosos ou mercenários cibernéticos é possível. Nesse sentido, Rattray (2001, p.85) coloca que estrategicamente a contratação de hackers de aluguel além de difícil, no sentido de conseguir indivíduos dispostos a cometer atos destrutivos no ciberespaço, seria arriscada, uma vez que eles não possuiriam a lealdade de membros do grupo, podendo converter-se em agentes duplos (agindo para governos) ou serem pegos, prejudicando o planejamento/informações do plano. Independente desses obstáculos, a vantagem da contratação estaria na expertise de “pronta entrega”, baixando custos e tempo para realização de uma operação.

Em resumo, o que se percebe em relação ao crime cibernético é que o ciberterrorismo é um tipo de crime, mas em um tom mais elevado. Afinal, ainda que o terrorismo cibernético não tenha como objetivo último o lucro, como o é normalmente nos crimes, ele pode gerar a ansiedade econômica caso ocorram invasões em operações virtuais de sistemas financeiros. .

Vale salientar a importância de diferenciar o ciberterrorismo de outro fenômeno social e com motivação política: o hacktivismo. Tal fenômeno é a junção das palavras “ativismo” e "hacker" com a “ideia de promover ou resistir a algum tipo de mudança política ou social através de meios de protesto não violentos, mas muitas vezes legalmente questionáveis” (SINGER; FRIEDMAN, 2014, p.77, tradução nossa)

Assim, os hacktivistas “usam seu conhecimento de sistemas informáticos para se envolver em atividades disruptivas na Internet na esperança de chamar a atenção para alguma causa política”, as quais podem ser: ataques de "negação de serviço" (DoS) que vinculam sites e outros servidores, "graffiti eletrônico" nas páginas do governo e sites corporativos, roubo e publicação de informações privadas na Internet (CONWAY, 2007, p.8). Contudo, de forma geral, o hacktivismo inclui quatro operações: protestos passivos e bloqueios virtuais (geralmente, do DoS), bombas automáticas de e-mail (enormes volumes de e-mail são

enviados para um endereço na tentativa de transbordar a caixa de correio ou sobrecarregar o servidor onde o endereço de e-mail está hospedado), invasões de Rede e de computador, e vírus e *worms (*WEIMANN, 2005, p.135; DENNING, 2001, p. 263). Os alvos dos hacktivistas são normalmente organizações ou fontes de informação específicas (MEHAN, 2014, p.82).

Os fenômenos do hacktivismo e do ciberterrorismo, nesse sentido, se aproximam pela questão das ações perpetradas por atores não estatais, com motivação política e ações que levam à espionagem e invasão de sistemas. Entretanto, há uma diferença fundamental entre os dois fenômenos: os hacktivistas ainda que usem ferramentas para invadir sistemas, possuem uma narrativa desprovida de terror. Como Weimann (2005, p.136, tradução nossa) evidencia: hacktivistas "querem protestar e perturbar; eles não querem matar ou mutilar ou aterrorizar".

Talvez a principal questão de separação entre os dois fenômenos se dê pela preservação de direitos humanos, ou seja, ainda que os hacktivistas apresentem uma conduta de desobediência social, muitas de suas bandeiras se centram em torno da transparência, excesso de vigilância na Internet e o direito a privacidade. Nesse sentido, caso as invasões dos sistemas entrem legalmente dentro de concepções ou categorizações de ciberterrorismo, podemos nos perguntar até que ponto os direitos e abusos, principalmente na Internet, seriam respeitados ou limitados.

Por fim, outra questão diferente surge ao se falar em guerra cibernética. Afinal, esse é outro conceito em aberto na academia. Nesse sentido, a aproximação do ciberterrorismo com a guerra cibernética, além de depender de qual viés se percebe o terrorismo, lembrando de que há um viés que o aproxima de guerra, vai se pautar muito no debate em relação aos atores internacionais envolvidos.

Segundo Stohl (2014, p. 90, tradução nossa), "os estados têm investido recursos crescentes no desenvolvimento de suas próprias capacidades de guerra cibernética, ao mesmo tempo em que encorajaram o setor privado a se envolver em segurança cibernética". Além disso, a doutrina estratégica com o advento do C4ISTAR (Comando, Controle, Comunicação, Computadores, Inteligência, Vigilância e Reconhecimento) coloca um componente militar no ciberespaço que, até julho de 2016, não era considerado pela OTAN (Organização do Tratado Norte Atlântico) como um novo domínio operacional de guerra (OTAN, 2017).

Com isso, o que pesa mais em relação à guerra cibernética é o acesso a armas cibernéticas. Afinal, "se um ator emprega uma arma cibernética para produzir efeitos cinéticos que possam justificar o poder de fogo sob outras circunstâncias, o uso desse armamento cibernético aumenta para o nível de uso da força" (THEORARY; ROLLINS,

2015, p.4, tradução nossa), configurando, assim, característica necessária à guerra. O alto investimento e necessidade de conhecimento para a construção de armas cibernéticas são atribuídos mais aos Estados. Por isso, há uma ênfase em relação a atores não estatais como agentes de ciberterrorismo em várias definições acadêmicas. Todavia, essas armas podem ser roubadas ou dadas (no caso do uso de ciberterroristas a emprego do Estado). Nesse sentido, como Stohl (2014, p.96, tradução nossa) salienta:

> assim como os Estados criticam o uso do terrorismo por atores não estatais, ao mesmo tempo que apoiam ou fecham a visão do uso do terrorismo por atores não estatais de quem eles aprovaram, os estados condenaram os ciberterroristas ao mesmo tempo que criaram suas próprias capacidades para se envolverem em comportamentos cibernéticos destrutivos.

Em outras palavras, os Estados são pragmáticos quanto aos seus interesses. Além disso, como a atribuição e a consequente responsabilização dos Estados, sob a jurisdição da atual legislação internacional, são dificultadas pelo anonimato que o ciberespaço proporciona, eles podem desempenhar um papel indireto no desenvolvimento de grupos ciberterroristas. Ainda, a questão da vigilância do ciberespaço enquanto uma forma de terrorismo de Estado é posta por Wykes e Harcus (2010, p.243, tradução nossa) quando eles mencionam que "se continuarmos a apoiar o vigilantismo, corremos o risco de nos tornarmos estados terroristas".

Igualmente, a falta de dinheiro e expertise não são impedimentos intransponíveis para que grupos terroristas desenvolvam tais armamentos. Como Munoz (2015, p. 5, tradução nossa) destaca, os terroristas buscam "melhorar suas habilidades na gestão da informação, comunicação, inteligência e avanço tecnológico no sentido de criar armas para a guerra cibernética". Então, como diferenciar os dois fenômenos?

Nesse ponto, para a pesquisa proposta, vale recordar a definição de Diniz (2002) sobre o terrorismo, aqui usado como o emprego do terror para induzir em outro público um comportamento que altere as forças a favor do ator que emprega o terrorismo. Dessa forma, colocando o ciberterrorismo como um tipo de terrorismo, que usa o ciberespaço, tanto atores estatais quanto não estatais podem fazer uso do emprego do terror cibernético.

Por isso, o emprego do terror, a capacidade de alcance psicológico do ciberterrorismo, que muitos acadêmicos colocam como guerra psicológica, talvez seja a chave da diferenciação. Afinal, aparenta ser fundamental para esse fenômeno e não para a guerra cibernética, que se pautará mais no uso de força virtual, a qual ainda tem poucos trabalhos desenvolvidos a respeito.

Em resumo, a diferenciação do fenômeno do ciberterrorismo com seus termos/fenômenos correlatos pode ter aclarado um pouco mais as características próprias do terrorismo cibernético, que começam a distanciá-lo do uso terrorista da Internet. Contudo, em especial com a questão do hacktivismo que tipos de hacking poderiam elucidar questões operacionais e táticas do ciberterrorismo?

Curran, Concannon, Mckeever (2008, p.2) explicam que ataques cibernéticos se dão contra dados (sabotagem) e sistemas de controle (infraestruturas). Tendo, segundo Heikerö (2008, p.6), três efeitos:

a) físicos, em que as estruturas de dados são destruídas ou se tornam inacessíveis;
b) de sintaxe, na qual a lógica de um sistema é distorcida (via atraso de informações ou comportamentos imprevisíveis); e
c) semânticos, em que a confiança em um sistema se altera pela manipulação, mudança e decepção de informações.

Dessa forma, há uma ampla janela de oportunidades para os ciberterroristas causarem insegurança e gerar medo. Tudo dependerá de suas capacidades ofensivas, as quais requerem, segundo Cohen (2014, p.170), a combinação de capacidades em três áreas: tecnológica, operacional e criação de diretrizes de inteligência para ajuste de objetivos (geração de alvos)

Assim, a área tecnológica, faz referência às ferramentas virtuais disponíveis para o alcance de objetivos (COHEN, 2014, p.170). Essas ferramentas podem ser construídas, compradas, roubadas ou ofertadas, mas no tocante aos sistemas de controle, solicitam alto grau de sofisticação tendo em vista que, especialmente os Sistemas de Controle Industrial, são autônomos, o que exige que cada sistema tenha um desenho próprio de arma cibernética para causar maiores impactos. Quanto à questão tecnológica, vale a observação de que os ataques aos DoS/DDoS parecem mais disruptivos do que destrutivos e não se pode fazer generalizações, uma vez que sobrecargas *SNMP(IP Simple Network Management Protocol)* são exemplos de ataques de DoS de sobrecarga sem rede, causando falhas na memória, e não na Rede do sistema. Fato que, consequentemente, gera uma falha física de infraestrutura (YANNAKOGEORGOS, 2014, p.54).

No tocante à criação de diretrizes de inteligência, elas vão depender da geração de alvos e da qualidade das ferramentas obtidas. Afinal, existem várias ferramentas de espionagem disponíveis no ciberespaço (COHEN, 2014, p.171). As mais conhecidas são o Duqu e Flame ambos desenhados com o paradigma de programação orientada para objetos (OOP), o que lhes confere lugar como software primos do Stuxnet, mesmo que tenham como

objetivo apenas a coleta, não a adulteração de informações dos sistemas infectados (SHAKARIAN; SHAKARIAN; RUEF, 2013, p.166-67).

Por fim, a questão de capacidade operacional se refere a uma "cadeia de ações realizadas pelos atacantes em que cada ação constitui um passo no caminho para o objetivo final, que geralmente inclui controle total ou parcial de um sistema de computador ou sistema de controle industrial" (COHEN, 2014, p.171). Colarik (2006, p.83) argumenta que são cinco fases pela qual um ataque cibernético bem-sucedido deve passar:

a) reconhecimento;
b) acesso;
c) expansão e identificação de capacidades internas;
d) dano no sistema;
e) remoção de evidências.

Dessa forma, após a coleta de informações, advinda da inteligência, o estágio mais importante é o primeiro: o acesso aos sistemas, que pode se dar de maneira interna e externa, principalmente via falsificações e engenharia social (COHEN, 2014, p.171). Internamente, esse acesso pode se dar via uso de portais (ex. e-mails, websites, browsers, vídeo streaming, software remoto) ou de elementos produzidos *(deliverables*, ex.vírus, *worms* ou scripts executáveis). Já externamente, o acesso pode se dar de maneira física (uma vez que o ciberespaço possui uma parte física, que pode ser acessada de alguma forma) ou por meio de engenharia social, que busca colher informações a partir de membros que já tenham acesso ao sistema (COLARIK, 2008).

A questão da engenharia social, no ciberterrorismo deve ser levada em consideração enquanto aspecto psicológico, uma vez que envolve um grau de manipulação mental. Assim, alvos potenciais dos ciberterroristas poderiam estar dentro de certos grupos como: desenvolvedores de TI, CEOs, usuários de TI da organização, pessoal de apoio de TI ou gerentes de projetos da organização, e até mesmo membros do público (MACKINNON et al 2013, p.249).

Em resumo, o tipo de hacking que caracteriza o ciberterrorismo, conforme a literatura, parece se centrar em invasões estratégicas, que requerem maior sofisticação, para gerar impactos pretendidos, mas não necessariamente descartando operações mais simples a exemplo da sobrecarga SNMP, que envolvem a manipulação do indivíduo específico, não aleatório como no caso do crime cibernético, como meio de acesso aos sistemas *airgripped* (fora da Rede).

Diante dessas informações ainda podemos nos perguntar sobre a questão psicológica do ciberterrorismo. Com isso, é oportuno frisar a capacidade de manipulação e geração de terror característica do terrorismo.

Como Ariely (2008, p. 8, tradução nossa) explica, “a bomba mais inteligente que as forças combatentes já inventaram, é a humana - a única bomba que se adapta a uma situação em mudança (além de ser "pré-programada"), cobrando também um preço psicológico”. Nesse sentido, uma vez que a informação é o bem valioso do ciberespaço, vale a ideia de que a informação certa vale mais ainda, ou seja, quem tem o conhecimento tem a vantagem estratégica.

Com o uso de seres humanos como meios para se alcançar dado objetivo em grupos terroristas, a manipulação de conhecimento passada para os membros e futuros membros de grupos terroristas aparenta ser algo recorrente, bem como esse aspecto parece ser replicado no ciberespaço. A diferença agora é que o alcance das informações se transforma em um multiplicador de força (SEDDON, 2002, 1035), seja por dar uma percepção maior de força (física ou virtual) que dado grupo terrorista possui ou pode combinar com ataques físicos. Além disso, essa manipulação pode ser mais direcionada, para grupos alvos, uma tendência que Weimann (2015) identifica como *narrowcasting*.

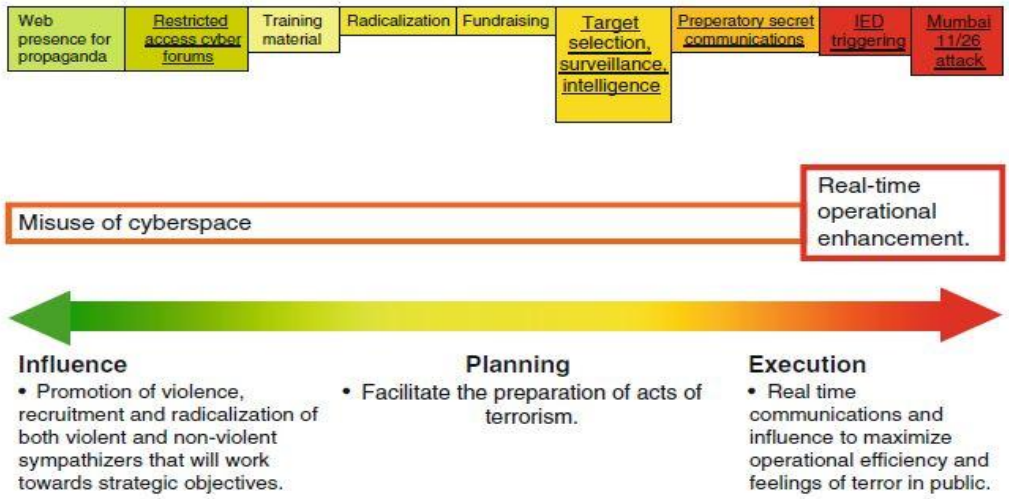
Ressalta-se que, se manipulação de informações ocorre com o uso terrorista da Internet, no ciberterrorismo essa manipulação se dá em torno dos sistemas e dos dados, algo já comentado anteriormente com a questão dos ataques cibernéticos. Todavia, a proposta de Yannakogeorgos (2014) pode esclarecer um pouco mais essa capacidade psicológica, uma vez que ele cria um espectro de operações cibernéticas, indo do mau uso da Internet até a capacidade de produzir terror e destruição com ataques cibernéticos.

A representação em espectro feita por Yannakogeorgos (2014) é interessante por reforçar a ideia de que uso da Internet por grupos terroristas e o ciberterrorismo podem ser vistos como gradientes diferentes dentro de uma mesma paleta de cores (ver Figura 12). Nesse sentido, o que deveria começar a preocupar os Estados seria a capacidade de intrusão dos grupos nos sistemas. No entanto, os mais perigosos grupos, para além de formar a opinião pública e aumentar o terror, seriam aqueles que também ganhariam informações em tempo real sobre a resposta do governo no meio do incidente para impulsionar a tomada de decisões operacionais. Fato que ocorreu de maneira embrionária nos Ataques de Mumbai, em

novembro de 2008, com o uso de tecnologia de informação (incluindo uso de plataformas sociais) pelo grupo Lashkar-e-Taiba[18] (YANNAKOGEORGOS, 2014, p.52).

As operações mais perigosas poderiam resultar em operações destrutivas, com dano à propriedade e/ou pessoas, ou serem o que ele cunha de *PsyberOperations* (operações psicológicas). Essas operações psicológicas focam a mente humana como alvo, sendo "aquela[s] em que os terroristas podem manipular a emoção pública em massa para criar esse efeito que faz com que indivíduos ou massas de pessoas se movam espontaneamente de maneira específica em resposta às mensagens (YANNAKOGEORGOS, 2014, p. 57). Como exemplo, podemos citar o fenômeno dos *Foreign Transnational Fighters* (Combatentes Estrangeiros Internacionais) que, por meio de informações disponíveis na Rede, mobilizam-se para ir ao encontro das célulasterroristas físicas, como no caso do Estado Islâmico, o qual com sua campanha nas redes sociais atraiu para sua causa uma modesta estimativa 30,000 combatentes estrangeiros, advindos de vários países (ATWAN, 2015, p.168).

Figura 12 - Espectro de Operações Cibernéticas



Fonte: Yannakogeorgos (2014, p. 46)

Por fim, resta a explicação do que o ciberterrorismo pode, não pode e poderia fazer. Nesse sentido, a maioria dos acadêmicos parece ser inclinada a possibilidade de que os grupos terroristas estejam desenvolvendo capacidades cibernéticas para conseguir concretizar atos de ciberterrorismo. No entanto, enquanto há autores como Conway (2014), que advogam a baixa

[18] O grupo é um dos movimentos clandestinos paquistaneses que afirmam lutar contra a ocupação indiana da Caxemira e contra o que chamam de perseguição à minoria muçulmana na Índia (SISSON, 2016)

e improvável probabilidade de um ataque ciberterrorista ocorrer, existem autores como Cohen (2014), que colocam tendências futuras que podem aumentar a possibilidade de ocorrência.

Conway (2014, p.107) explica que dado o peso de quatro fatores limitantes - a saber: custo, complexidade, destruição e impacto da mídia - os grupos terroristas seriam dissuadidos de irem pelo caminho do ciberterrorismo. O que a autora faz é, basicamente, um paralelo entre a utilização de carros bombas (Dispositivos Explosivos Improvisados de veículos) e o uso de ferramentas virtuais. Nesse sentido, ela coloca que é muito mais barato, simples, impactante e destrutivo a utilização de carros bombas que o desenvolvimento de armas cibernéticas para grupos terroristas, evidenciando uma tendência ao uso de velhas ferramentas ao invés de dispêndio de tempo e recursos com novas. No mais, dada a complexidade de ferramentas virtuais não apenas os terroristas perderiam controle sobre resultados, como também dado o anonimato da Rede poderiam perder o crédito pela ação, caso ela fosse bem-sucedida (CONNWAY, 2014, p.112).

Do outro lado está Cohen (2014) com a ideia de que os grupos terroristas podem: se beneficiar do desenvolvimento, estabilização e flexibilidade de criptomoedas (ex. Bitcoin) para conseguir financiamentos maiores e mais seguro; usar ainda mais a Darknet para manter suas operações mais seguras; utilizar a impressão 3D para obtenção de armas físicas (e aqui está a questão da tecnologia como multiplicador de força), bem como conseguir proteger suas comunicações utilizando somente canais de VPN (*Virtual Private Network*), algo possível como o NAS (*Network Attached Storage*), que são serviços adicionais fáceis de instalar e oferecem armazenamento. O autor conclui que um ataque ciberterrorista, nesse sentido, seria possível, mas fora de alcance e que o uso de tecnologias seria vantajoso para os grupos conseguirem escapar da lei. Com essas tendências e conclusões, ele abrange tanto o uso terrorista da Internet quanto o ciberterrorismo.

Assim, percebe-se que não há ao certo como saber em que grau a evolução do uso de tecnologia por terroristas pode levar ao ciberterrorismo. Afinal, existem atores limitantes e oportunidades. Entretanto, o que fica claro é a necessidade de se entender o fenômeno e saber que ele é passível de ocorrer em um futuro (seja ele distante ou não).

3.4 CONSIDERAÇÕES PARCIAIS

Diante do exposto no capítulo, verifica-se a existência da distinção entre o uso terrorista da Internet e o ciberterrorismo. Nesse sentido, ainda que os dois fenômenos se aproximem algumas características podem aclarar suas diferenças, principalmente se as

dividirmos em quatro categorias analíticas: Unidade do Ciberespaço, Foco Operacional, Uso da Violência e Objetivo Último (Quadro 5).

Tais categorias podem ser elencadas, uma vez que a base de conceituação do terrorismo, usada na pesquisa, considera o fenômeno em si como um estratagema. Assim, níveis mais profundos de estratégia são aqui descartados. Ademais, como os tipos de ataques têm uma variação muito grande, já que não apenas os complexos, mas alguns tipos mais simples podem ter consequências destrutivas, buscou-se concentrar em seu objetivo maior frente ao ciberespaço, incluindo os focos das operações citadas pelos autores analisados.

Dessa forma, percebe-se no uso terrorista da Internet o uso passivo do ciberespaço com operações focadas, principalmente em comunicação (interna e externa) e com o uso de uma violência indireta, seja em relação aos indivíduos, por meio do *narrowcasting*, de vias econômicas para o financiamento de operações e manutenção da célula terrorista (representada pelo símbolo $). Nesse sentido, o ciberespaço se torna um espaço logístico para as ações terroristas.

Quadro 5 - Diferenças entre Uso terrorista da Internet e Ciberterrorismo

Categoria	Uso Terrorista da Internet	Ciberterrorismo
Utilidade do ciberespaço	Logística - Uso passivo do ciberespaço	Logístico e Estratégico - Uso ativo do ciberespaço
Foco Operacional	Operações com foco em comunicação	Operações com foco na Mobilização de pessoas e invasão e destruição de dados esistemas tecnológicos.
Uso de violência	Indireta (psicológica ou física - $)	Direta (psicológica ou física- IC e indivíduos)
Objetivo último	Autofortalecimento	Enfraquecimento do Oponente

Fonte: Elaboração própria com base em nos autores analisados no capítulo

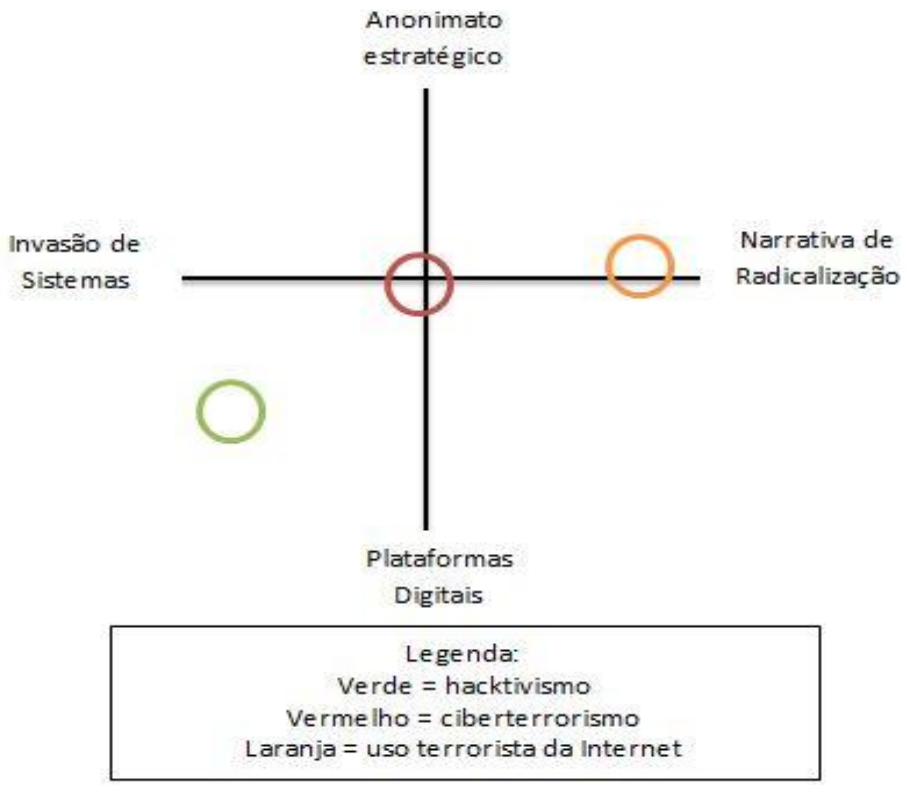
Do outro lado, o ciberterrorismo aparece com o uso ativo do ciberespaço, com operações focadas na mobilização de pessoas (alvo das ações é a mente humana) e na invasão e destruição de sistemas e dadostecnológicos, principalmente de Infraestruturas Críticas (IC). Em outras palavras, há um viés estratégico no uso do ciberespaço, objetivando o

enfraquecimento do oponente, e não apenas o uso do ciberespaço como um multiplicador de força.

Como existe também a possibilidade do emprego de hackers por terroristas, sendo que tanto hacktivistas quanto os grupos que usam a Internet e os ciberterroristas envolvem de alguma maneira a invasão de sistemas, seja para ataques pontuais ou por meio da coleta de informações (inteligência), uma maneira de diferenciar os fenômenos, tão próximos entre si, pode ser por intermédio de suas táticas empregadas.

Nesse sentido, a invasão de sistemas, o anonimato estratégico, as narrativas de radicalização e o uso de plataformas digitais (redes sociais e ferramentas virtuais) podem colocar os fenômenos em uma confguração que, para a autora, poderia ser representada pela Figura 13.

Figura 13 - Relação entre Uso Terrorista da Internet, Hacktivismo e Ciberterrorismo segundo métodos empregados



Fonte: Elaboração própria com base nos autres analisados no capítulo

Dessa forma, ainda que academicamente se perceba a diferenciação dos fenômenos, há que se considerar que o mundo não é apenas regido pela teoria, pois os Estados dão o tom e o compasso legal das respostas para as interpretações dos fenômenos cibernéticos. Logo, também produzindo reações nos próprios grupos terroristas, as quais vão moldando o desenvolvimento do ciberterrorismo e outros fenômenos on-line. O entendimento das interpretações de países será visto no próximo capítulo, a fim de apurar as características do que vem se desenvolvendo quanto ao terrorismo cibernético.

4 CIBERTERRORISMO E POLÍTICA: ANÁLISE DAS PERCEPÇÕES DO GRUPO *FIVE EYES*

O capítulo em voga busca compreender como as características do ciberterrorismo estão sendo discutidas e abordadas no cenário internacional. Para tanto, focaliza uma análise das percepções governamentais acerca do assunto, com base na amostragem de países relevantes: o grupo do *Five Eyes*. Dessa forma, a análise proposta evidencia, essencialmente a partir de documentos legais e relevantes na área de contraterrorismo, na legislação doméstica de combate aos crimes e documentos específicos para o domínio do ciberespaço.

O Grupo do *Five Eyes* foi criado durante a II Guerra Mundial com base em uma aliança entre Grã-Bretanha e Estados Unidos para coleta SIGINT[19] durante a guerra, interceptando as comunicações dos poderes do Eixo e gerando, por parte da Grã-Bretanha, a quebra do funcionamento do Enigma (máquina de criptografia alemã) e por parte dos Estados Unidos a quebra do Purple (máquina de criptografia japonesa). Depois da Guerra, em 1946, a aliança entre os dois Estados foi formalizada no tratado UKUSA, uma vez que no contexto da Guerra Fria a coleta de informações em tempos de paz poderia previnir potenciais conflitos, agora envolvendo uma maior parcela do mundo. Dessa forma, o Canadá se juntou a aliança, em 1948, e Austrália e Nova Zelândia, em 1956, gerando uma aliança de alcance global que passou a ser chamada de *Five Eyes* (DAILEY, 2017).

O *Five Eyes*, portanto, é uma coalizão de agências de inteligência independentes que trabalham de forma fluída, sendo dividida para ter alcance global: Estados Unidos vigia Caribe, China, Rússia, Oriente Médio e África; Reino Unido, a Europa e Ocidente de maneira geral; Austrália, emissões da Ásia do Sul e do Leste; Nova Zelândia cobre o Pacífico Sul e Sudeste Asiático (DAILEY, 2017, p.1). Como mostraram as revelações de Snowden. todos os documentos vazados incluiam a classificação "TOP SECRET // COMINT // REL TO USA, AUS, CAN, GBR,NZL "ou" TOP SECRET // COMINT // REL TO USA, FVEY", indicando relação com o grupo. Além disso, programas de coleta de informações no meio cibernético, a

[19] "SIGINT, um acrônimo para a Inteligência de Sinais, é uma espécie de forma dos vários tipos de inteligência, incluindo HUMINT (Human Intelligence), GEOINT (GeospatialIntelligence), MASINT (Medição e Inteligência de assinaturas) e OSINT (Open-SourceIntelligence). Como as transmissões de todos os tipos aumentaram, a SIGINT tornou-se mais valiosa. A globalização e a internet criaram um ambiente altamente conducente à sua coleta e análise. SIGINT é composto de múltiplos campos e práticas, incluindo criptoanálise, análise de tráfego, inteligência eletrônica, inteligência de comunicação e medição e inteligência de assinatura" (DAILEY, 2017, p.1, tradução nossa).

exemplo dos com o codinome de TEMPORA[20] e XKEYSCORE[21] levaram ao debate o quanto uma justificativa de combate a ameaças, incluindo o terrorismo, é válida diante do direto da privacidade (NYST; CROWE, 2014, p.51).

Nesse sentido, analisamos individualmente como cada país percebe a ameaça do uso terrorista da Internet e o ciberterrorismo, a fim de aclarar as percepções dos países quanto aos fenômenos que fazem com que precisem realizar tais coletas de informações.

4.1 ESTADOS UNIDOS

Com 76,2% dos indivíduos usando a Internet em 2016 (BRODBAND COMISSION FOR SUSTAINABLE DEVELOPMENT, 2017), o país que originou a Rede fica atrás de vários outros em penetrabilidade de conexões. No entanto, a população norte-americana é uma das que mais usa redes sociais, já que do total da população 68% de todos os adultos dos EUA são usuários do Facebook, enquanto 28% usam Instagram, 26% usam Pinterest, 25% utilizam o LinkedIn e 21% utilizam o Twitter (GREENWOOD; PERRIN; DUGAN,2016). Ainda mais impressinante é o número de norte-americanosque eram *smartphone only* em 2015 (13%), um acréscimo de 8% desde 2013 (HORRIGAN; DUGGAN, 2015), e a quantidade de embarques fabris do comércio eletrônico que chegaram a representar 63,2% de todos os embarques, em 2015, totalizando uma movimentação de US $ 3.506,9 bilhões (USA CENSUS BUREAU, 2015, p.1).

Dentro desse cenário de exposição e trânsito financeiro, o fato de que as infraestruturas do país possuam um domínio distribuído, ou seja, os governos estaduais e locais e o setor privado possuem 97% da infraestrutura não defensiva da nação, financiando 94% disso (EDWARDS, 2017) faz com que cerca da metade dos norte-americanos (49%) sintam que sua informação pessoal seja menos segura do que era há cinco anos (OLMSTEAD; SMITH, 2017).

Toda essa preocupação levou, e leva, o governo estadunidense à criação de arcabouços legais e de instituições específicas para a segurança cibernética. Sendo um de seus

---

[20] O Programa de codinome TEMPORA iniciou com a colocação de “torneiras” nos cabos submarinos de fibra óptica de estações chave do Reino Unido, podendo interceptar uma parte significativa das comunicações que atravessam o país. The Guardian informou que 300 analistas do GCHQ e 250 da NSA foram diretamente atribuídos para examinar o material coletado (NYST; CROWE, 2014, p.52).

[21] O XKEYSCORE “tem sido descrito por apresentações internas de NSA como "estrutura analítica" que permite uma única pesquisa para consultar um "buffer de rolamento de 3 dias" de "todos dados não filtrados" "armazenados em 150 sites globais em 700 bases de dados Servidores. O sistema NSAXKEYSCORE possui sites que aparece nos países dos Cinco Olhos” (NYST; CROWE, 2014, p.52, tradução nossa).

principais marcos, a Estratégia Nacional de Segurança do Ciberespaço de 2003, que estabeleceu três objetivos estratégicos para a segurança nacional do ciberespaço:

a) Prevenção de ataques cibernéticos contra infraestruturas críticas nacionais;

b) Redução da vulnerabilidade nacional aos ataques cibernéticos; e

c) Minimizaçãodos danos e o tempo de recuperação dos ataques cibernéticos que ocorrem (UNITED STATES OF AMERICA -USA, 2003a, p.14).

Sendo assim, a Estratégia coloca como prioridades: garantir sistemas e redes de computadores federais; desenvolvimento de um sistema de resposta; estabelecimento de um programa de redução de ameaças e vulnerabilidades; iniciação de um programa de conscientização e treinamento para a segurança cibernética; e desenvolvimento de um sistema de cooperação internacional (USA, 2003).

Dentro dessa estratégia, em que pese não haja uma seção específica para o uso terrorista da Internet, alguns indicativos da preocupação com terroristas usando o ciberespaço são identificáveis, por exemplo, a Estratégia coloca:

> atores maliciosos no ciberespaço podem levar muitas formas, incluindo indivíduos, cartéis criminais, terroristas ou Estados Nação. Enquanto os atacantes tomam muitas formas, todos procuram explorar vulnerabilidades criadas pelo desenho ou implementação de softwares, hardwares, redes e protocolos para alcançar uma ampla gama de efeitos políticos e econômicos. À medida que nossa dependência do ciberespaço aumenta assim também o alcance do dano que malicioso os atores podem impor (USA, 2003, p.27, tradução nossa).

Outrossim, há a menção de que tanto os terroristas quanto os Estados-Nação podem lançar ataques cibernéticos ou buscar a exploração dos sistemas eletrônicos, em tempos de paz por meio da espionagem e em tempos de guerra tentando atrasar o Departamento de Defesa (DoD) ou procurar "intimidar atacando infraestruturas críticas e funções econômicas chave ou prejudicar a confiança pública nas informações sistema" (USA, 2003, p.50).

Vale observar que A Estratégia de Segurança Nacional de 2010

> foi a primeira estratégia de segurança nacional dos Estados Unidos a dedicar atenção substancial às ameaças cibernéticas e também representou uma mudança na caracterização de ameaças cibernéticas pelo governo federal, com ênfase na mudança do terrorismo não-estatal para atividades patrocinadas pelo estado e de uma preocupação predominantemente política e econômica (PERNIK; WOJTKOWIAK; VERSCHOOR-KIRSS, 2016, p.8).

Tal tom de mudança repercutiu em outros documentos como a Estratégia Internacional para o Ciberespaço de 2011, a qual, ao mencionar terroristas, evidencia dentro do cumprimento da lei (l*aw enforcement*) ênfase em "**Negar terroristas e outros criminosos a capacidade de explorar Internet para planejamento operacional, financiamento ou ataques"** (USA, 2011a, p.20, grifo do documento) e na Estratégia de Segurança Cibernática de 2015 do DoD, na qual coloca que "Os atores estatais e não-estatais realizam operações cibernéticas para alcançar uma variedade de aspectos políticos, econômicos, ou objetivos militares" (USA, 2015, p.1, tradução nossa).

No entanto, a Estratégia de 2015 elucida mais as visões estadunidenses acerca do uso terrorista do ciberespaço ao colocar a disseminação de propaganda, o recrutamento de indivíduos e aquisição de capacidades diretivas e destrutivas que grupos terroristas, como o Estado Islâmico no Iraque e Levante (ISIL), demonstram (USA, 2015, p.9). Com isso, há menção de mistura de atores estatais e não-estatais no ciberespaço (US, 2015, p. 9) e a ideia de que atores estatais e não-estatais podem "comprar malwares destrutivos e outras capacidades no mercado negro", bem como " pagar especialistas para procurar vulnerabilidades e desenvolver explorações" (USA, 2015, p. 10, tradução nossa).

A Estratégia de Segurança Nacional de 2017, sob governo do presidente Donald Trump, colocou ênfase na questão religiosa terrorista da Internet, ao explicitar que "os terroristas jihadistas usam redes físicas e virtuais, ou seja, redes ao redor do mundo para radicalizar indivíduos, explorar populações vulneráveis, inspirar e direcionar tramas" (USA, 2017a, p.10, tradução nossa). Além disso, a Estratégia ressalta que:

> atores estatais e não estatais maliciosos usam ataques cibernéticos para extorsão, guerra de informações, desinformação e muito mais. Tais ataques têm a capacidade de prejudicar um grande número de pessoas e instituiçõescom um investimento comparativamente mínimo e um grau de desconfiança preocupante. Esses ataques podem prejudicar a fé e a confiança nas instituições democráticas e no sistema econômico global (USA, 2017b, p.31, tradução nossa).

No entanto, não apenas esses documentos explicam o entendimento do país acerca do fenômeno do ciberterrorismo e uso terrorista da Internet. Os Estados Unidos possuem mais de 50 estatutos abordando inúmeros aspectos da segurança cibernética (PERNIK; WOJTKOWIAK; VERSCHOOR-KIRSS, 2016, p. 7) com um amplo arcabouço institucional[22]

[22] De forma resumida, segundo Pernik, Wojtkowiak e Verschoor-Kirss (2016), em termos políticos, o principal papel de coordenação das políticas é assumido pelo Comitê de Política Interagencial de Infraestrutura de Informação e Comunicação (ICI-IPC) do Conselho de Segurança Nacional na Casa Branca. O ICI-IPC é co-presidido pelo Conselho de Segurança Interna e pelo Coordenador de Segurança Cibernética (CSC) no

dirigido a esses aspectos. Assim, alguns aspectos legislativos e dentro da documentação contraterrorista podem aclarar suas percepções

Dessa forma, é interessante ressaltar que os Estados Unidos têm no seu Ato Patriota (Act 18 U.S.C. 2332b), referente ao que constitui um crime federal de terrorismo, e na referência ao Ato de Fraude e Abuso de Computadores (18 U.S.C. 1030a-c.) alguns indicativos sobre o entendimento acerca do ciberterrorismo. Assim, de acordo, com Theohary e Rollins (2015, p.9, tradução nossa), as definições que parecem seguir algumas análises legais que especificam o ciberterrorismo como "o uso premeditado de atividades disruptivas, ou sua ameaça, contra computadores e / ou redes, com a intenção de causar danos ou outros objetivos sociais, ideológicos, religiosos, políticos ou similares, bem como intimidar qualquer pessoa em prol de tais objetivos".

Vale ressaltar que o Ato Patriota permite que os responsáveis pela aplicação da lei obtenham um mandado de busca em qualquer lugar que ocorra uma atividade relacionada ao terrorismo e que as vítimas de hacking de computador possam solicitar ajuda à aplicação da lei no monitoramento dos "intrusos" em seus computadores (USA, 2017b). Nesse sentido, é relevante observar documentos que falem de coleta de inteligência, no sentido de que o monitoramento do ciberespaço é pautado sob a justificativa de combate ao terrorismo.

Dessa forma, A Estratégia Nacional de Inteligência de 2014 destaca que, dentro de seus objetivos, se encontra a inteligência cibernética (IC), a qual “(...) também fornece conhecimentos necessários para defender as redes do governo dos EUA junto com outras redes de comunicações e a infraestrutura” (USA, 2014, p.8, tradução nossa). Por isso, a Estratégia elucida que:

Gabinete de Segurança Cibernética do Conselho de Segurança Nacional. O CSC lidera desenvolvimento interagências da estratégia e política nacionais de segurança cibernética e supervisiona a implementação dessas políticas pelas agências (...), o Departamento de Segurança Interna (DHS) é a principal instituição responsável pela cibersegurança dentro das fronteiras dos EUA (...) “O Departamento de Justiça (DoJ) é em grande parte responsável pela aplicação das leis relativas à segurança cibernética”. (p.16, tradução nossa) “O US-CERT responde a incidentes cibernéticos, fornece assistência técnica aos operadores e divulga notificações sobre ameaças atuais e potenciais” (p.19, tradução nossa). Já a parte militar cabe ao Departamento de Defesa que protege os dominios .mil, sendo que “As funções e responsabilidades operacionais do DoD em segurança cibernética são realizadas através do USCYBERCOM Joint Operations Center, da Agência de Segurança Nacional / Central Security Service Center, do Centro de Defesa da Criminalidade da Defesa e da Agência de Sistemas de Informação da Defesa (DISA) (p.19, tradução nossa) “Cada serviço militar possui um componente cibernético que relata ao US Cyber Command (USCYBERCOM), um comando subunificado sob US Command Estratégico (USSTRATCOM), localizado em Fort Meade Maryland e colocalizado com a sede da Agência Nacional de Segurança (NSA), sendo que o Diretor da NSA é também o Comandante do USCYBERCOM (p.20, tradução nossa).

> Os atores estatais e não-estatais usam tecnologias digitais para alcançar as vantagens políticas econômicas e militares, fomentar a instabilidade, aumentar o controle sobre o conteúdo no ciberespaço e alcançar outros objetivos estratégicos - muitas vezes mais rápido do que nossa capacidade de entender as implicações de segurança e mitigar os riscos potenciais (USA, 2014, p.8, tradução nossa).

Tal visão estratégica que os grupos terroristas parecem ter fica mais clara na Estratégia para Combater o Terrorismo de 2006 (*National Strategy for Combating Terrorism*) a qual coloca como desafios o fato de que "O uso cada vez mais sofisticado da Internet e da mídia permitiu que nossos inimigos terroristas se comunicassem, recrutassem, treinassem, reunissem apoio, catequizassem e propagassem sua propaganda sem arriscar o contato pessoal" (USA, 2006, p.4, tradução nossa). Igualmente define como prioridades dentro do curto prazo prevenir ataques por redes terroristas, destacando dentro de suas capacidades operacionais a comunicação, favorecida pela Internet. De acordo com a Estratégia:

> Nossos inimigos contam com mensageiros e contatos diretos com associados e tendem a usar o que é acessível em suas áreas locais, bem como o que eles podem pagar. Eles também usam tecnologias de hoje com crescente perspicácia e sofisticação. Isto é especialmente verdadeiro com a Internet, que exploram para criar e divulgar propaganda, recrutar novos membros, arrecadar fundos e outros recursos materiais, fornecer instruções sobre armas e táticas, e planejar operações. Sem uma capacidade de comunicação, os grupos terroristas não podem efetivamente organizar operações, executar ataques ou disseminar sua ideologia (USA, 2006, p.12, tradução nossa).

Além da questão comunicativa, a Estratégia de 2006 focou a eliminação de paraísos virtuais (*cybersafeheavens*). Como Judy (2011, p.36, tradução nossa) explica:

> A utilidade de um refúgio "virtual" está prevista como uma área não física por meio da qual a atividade ilícita é conquistada em apoio a operações terroristas através de uma rede de redes em meio a um ambiente relativamente seguro. O refúgio "virtual" é composto por componentes como a internet, sistemas de telefonia móvel, redes de satélite, redes de comunicação globais, mídia digital portátil, comércio eletrônico e bancos informais que possibilitam que indivíduos e pequenos grupos se comuniquem ou com massas anônimas sem o requisito de uma reunião física

Seguindo uma evolução no pensamento estadunidense acerca do fenômeno do terrorismo, já sob a então presidência de Barack Obama, a Estratégia Nacional de Contraterrorismo de 2011 (*National Strategy for Counterterrorism*) elucidou a necessidade de uma abordagem de "todo governo" (*wholeofgovernment approach*) (US, 2011b, p.7, tradução nossa) "concentrando-se mais nos aspectos operacionais da ameaça e nas capacidades

tangíveis da Al Qaeda, incluindo parcelas continuadas na pátria e a radicalização e alocação dos muçulmanos" (NELSON, 2011, tradução nossa).

Nesse novo documento, os Estados Unidos enfatizam que "os meios de comunicação de massa e a Internet, em particular, permitem o planejamento, facilitação e comunicação do terrorismo, e nós [EUA] continuaremos a combater a capacidade dos terroristas de explorá-los" (USA, 2011b, p.10). Com isso, especificando que independente dos meios tradicionais ou do ciberespaço, uma estratégia bem-sucedida "nesses domínios se concentrará em minar e inibir a ideologia de Al-Qaeda, ao mesmo tempo que diminui os fatores específicos que o tornam atraente como catalisador e justificativa para a violência" (USA, 2011b, p.17). Em outras palavras, há o enfoque na questão do cambate à radicalização e dos combatentes estrangeiros transnacionais presentes no documento.

O documento de 2016, chamado de Estratégia Nacional para Vencer a Guerra contra o Terror Islâmico (*National Strategy to Win the War Against Islamist Terror*), mais recentemente, dentro da administração do presidente Donald Trump, retoma a ideia de que terroristas estão fazendo uso de "santuários virtuais" (*virtual heavens*), além de elucidar que os "inimigos terroristas estão se aproximando do desenvolvimento de capacidades de hacking cibernético, de modo que o DHS deve priorizar a segurança cibernética das infraestruturas críticas" (USA, 2016, p.11, tradução nossa) e que os terroristas também estão melhorando em se comunicar de forma segura e escondendo seus traços on-line" (USA, 2016, p.20, tradução nossa).

Vale ressaltar que em uma audiência sobre Segurança Interna e Assuntos Governamentais do Senado (2017), a vice-secretária do Departamento de Segurança Interna (DHS), Elaine Duke, expôs que "com as violações de alto perfil das bases de dados Equifax e federais e os estragos causados por Wannacry e Petya ransomware, o ano passado marcou 'um ponto de viragem no domínio cibernético', colocando-o diretamente na consciência pública" (DUKE, apud ROCKWELL, 2017, tradução nossa). Em outras palavras, parece que os Estados Unidos a partir desses eventos entenderam a facilidade de acesso de atores menores (i.e. com menos recursos) `as ferramentas de alta performace, que, em um primeiro momento, seriam atribuídas aos Estados, em razão dos altos custos e expertise envolvida (ROCKWELL, 2017).

Nesse sentido, os Estados Unidos, em sua Estratégia de Defesa Nacional de 2018, salientaram a questão do uso de proxies para Estados de forma mais aberta, explicando que:

> Os Estados são os principais atores no cenário mundial, mas os atores não-estatais também ameaçam o ambiente de segurança com capacidades cada vez mais sofisticadas. Terroristas, organizações criminosos transnacionais, ciber hackers e outros atores maliciosos não estatais transformam assuntos globais com maior capacidade de ruptura em massa. Há um lado positivo disso, como nossos parceiros em manter a segurança também são mais do que apenas estados-nação: organizações multilaterais, organizações não-governamentais, corporações e influenciadores estratégicos oferecem oportunidades de colaboração e parceria. O terrorismo continua a ser uma condição persistente impulsionada pela ideologia e política e estruturas econômicas, apesar da derrota do califado físico do ISIS (USA, 2018, p.3, tradução nossa).

Em resumo, o que se pode analisar acerca da percepção norte-americana é que os terroristas usam o ciberespaço para atividades logísticas e estratégicas. No entanto, a diferenciação dessas atividades não aparece bem definida nos documentos, como dois fenômenos separados. Além disso, prevalece uma legislação abrangente ainda que faça referência aos ataques e sistemas, o faz sem mais indicativos de intensidade.

4.2 REINO UNIDO

Com 94,8% de indivíduos com acesso à Internet, um crescimento de 12.8% nos últimos cinco anos (BRODBAND COMISSION FOR DIGITAL DEVELOPMENT, 2012; BRODBAND COMISSION FOR SUSTAINABLE DEVELOPMENT, 2017), o Reino Unido se insere dentro de um contexto em que as Tecnologias de Informação já fazem parte do cotidiano dos cidadãos ingleses. De fato, já em 2010 a disponibilidade de serviços e governo eletrônico aos cidadãos e empresas era próximo de 100% (OSULA, 2015, p. 5). De acordo com dados do *Office for National Statistics*, em 2016, 62% das empresas com 1.000 ou mais funcionários se beneficiam da banda larga super rápida, com uma velocidade de 100, ou mais, megabits por segundo de Internet, movimentando no setor não financeiro £ 511 bilhões em vendas, £ 8 bilhões a mais do que em 2015 (PRESCOTT, 2017). Esses dados indicam não apenas que o ciberespaço representa para o país um domínio cheio de oportunidades, mas também desafios, especialmente porque, dados de 2013, já apontavam que 82% das infraestruturas críticas do país estavam sob controle privado (OSULA, 2015, p 17).

Diante desse cenário, o Reino Unido não poderia ficar inerte aos desafios que o ciberespaço coloca em matéria de segurança ao governo. Assim, ao longo dos anos lançou três Estratégias Cibernéticas: a primeira em 2009, a segunda em 2011 e a última, recentemente, em 2016. Sendo que a partir da segunda Estratégia a previsibilidade de atualização foi fixada em cinco anos. Dessa forma, seguindo a preocupação com ameaça de

ataques cibernéticos mencionada na Estratégia de Segurança Nacional de 2008 (OSULA, 2015, p.6), a primeira Estratégia Cibernética tinha como foco a seguridade, segurança e resiliência, com especial preocupação sobre como explorar as oportunidades no ciberespaço (UNITED KINGDOM - UK, 2009, p.7).

Já a Estratégia de 2011 colocou o foco uma visão prospectiva para que o país, em 2015, obtivesse "um enorme valor econômico e social a partir de um ciberespaço vibrante, resiliente e seguro" com ações, "guiadas pelos nossos valores fundamentais de liberdade, justiça, transparência e estado de direito". Com isso, explicita com base nos objetivos maior resiliência e melhor proteção dos interesses do país no ciberespaço (UK, 2011a, p.8, tradução nossa).

Por fim, a última Estratégia manteve o caráter prospectivo, já que visa período de 2016-2021, colocando como objetivo se tornar um país "seguro e resiliente às ameaças cibernéticas, próspero e confiante no mundo digital". Colocando como objetivos defender, deter as ameaças cibernéticas, bem como desenvolver a indústria e pesquisas sobre questões de seguraça cibernética, sempre buscando ação internacional (UK, 2016, p. 25, tradução nossa).

Dentro dessa evolução de pensamento, um arcabouço institucional foi sendo desenvolvido. Entretanto, merece destaque dentre as várias agências o *Cabinet Office*[23], que ficou como responsável geral das diretrizes estratégicas e coordenação intergovernamental sobre a segurança cibernética, o Centro de Segurança Cibernética Nacional (NCSC, em inglês), o qual, criado em 2016, é a agência autorizada para implementar a política de segurança cibernética, responsável por assessorar e coordenar a resposta de segurança cibernética em todo o governo e indústria[24](JOSHI, 2017, p.16). Outrossim, é possivel perceber que o Reino Unido teve, igualmente, uma evolução de pensamento quanto à percepção acerca dos terroristas e do ciberspaço, na medida em que toda as estratégias

[23] "A segurança cibernética é o mandato da Secretaria de Segurança Nacional no Cabinet Office, que apoia o Conselho de Segurança Nacional e o Primeiro Ministro em toda a gama de questões de segurança nacional em todo o governo. Dentro da Secretaria de Segurança Nacional, o órgão central de coordenação para a segurança cibernética é o Escritório de Segurança Cibernética e Garantia da Informação (OCSIA), que apóia o Ministro do Gabinete e do Conselho de Segurança Nacional na determinação das prioridades para garantir o ciberespaço. A unidade fornece orientação estratégica e coordena as ações relacionadas com a segurança cibernética e garantia de informações no Reino Unido, sendo também o proprietário e gerente do Programa Nacional de Segurança Cibernética (NCSP)" (OSULA, 2015, p.9, tradução nossa).

[24] O NCSC "(...) incorpora os papéis e funções do Grupo de Segurança de Comunicações-Eletrônicas que foi a ala de inteligência da Agência de Segurança Nacional do Reino Unido, o GCHQ, e também é responsável pelo funcionamento do CERT-UK, bem como o Centro de Avaliação Cibernética e as funções cibernéticas da proteção de infraestrutura crítica que foram realizadas pelo Centro de Proteção de Infraestrutura Nacional. O fato de o NCSC ser uma das duas alas do GCHQ, uma agência cuja principal responsabilidade é a segurança nacional figura como indicativo da ênfase na segurança nacional na política do Reino Unido" (JOSHI, 2017, p. 16, tradução nossa).

mencionam o uso terrorista da Internet para propaganda, comunicação, radicalização e fianciamento. Entretanto, a última Estratégia (2016-2021) além de contar com outras ameaças hacktivista e script kiddies[25], colocou em um box separado uma citação da ENISA (Agência da União Europeia para Segurança de Redes e Informação) explicitando que há diferenças entre ciberterrorismo e uso terrorista da Internet (UK, 2016, p. 19).

É relevante também a definição de ataque cibernético que consta na mais recente Estratégia (2016, p. 74, tradução nossa), ou seja, um ataque cibernético seria a "exploração deliberada de sistemas informáticos, empresas e redes dependentes digitalmente para causar danos". Essa relevância é caracterizada considerando que, embora as Estratégias não explicitem o termo "ciberterrorismo", elas evidenciam que o uso de ataques cibernéticos por grupos terroristas é tido como uma baixa ameaça, mesmo que possa acontecer.

Nesse sentido, para entender melhor como o país concebe, em específico, a questão terrorista no ciberespaço, outros documentos devem ser analisados: o Ato sobre Terrorismo de 2000 (*Terrorism Act 2000*) e de 2006 (*Terrorism Act 2006*), o Ato de Poderes Investigatórios (*Investigatory Powers Act 2016*) e as últimas Estratégias Contraterroristas que o país elaborou (2009 e 2011).

O Ato sobre Terrorismo inglês foi decretado 14 meses antes do 11 de Setembro, projetado para ter um escopo abrangente, a fim de incluir as ameaças de grupos terroristas estrangeiros, que viessem a atuar em solo inglês e, igualmente, incorporando novas ameaças, como o ciberterrorismo (HARDY; WILLIAMS, 2014, p.4). Dessa forma, a seção 1 do Ato sobre Terrorismo coloca:

> 1 .- (1) Neste Ato, "terrorismo" significa o uso ou ameaça de ação
> onde
> (a) a ação caia na subsecção (2),
> (b) **o uso ou ameaça** é projetado para **influenciar o governo, uma organização governamental internacional**, ou para intimidar o público ou uma seção do público, e
> (c) o uso ou ameaça é feito **com a finalidade de avançar uma causa de forma política, religiosa, racial ou ideológica**.
>
> (2) A ação cai dentro desta subseção se ela
> (a) envolve violência grave contra uma pessoa,
> (b) envolve danos sérios à propriedade,
> (c) põe em perigo a vida de uma pessoa, diferente da pessoacometendo a ação,
> (d) cria um risco grave para a saúde ou a segurança do público ou um
> seção do público, ou
> **(e) é projetado seriamente para interferir ou seriamente interromper um sistema eletrônico**.

[25] "Os chamados 'script kiddies' - geralmente indivíduos menos qualificados que usam scripts ou programas desenvolvidos por outros para realizar ataques cibernéticos" (UK, 2016, p.20, tradução nossa).

> (3) A utilização ou ameaça de ação abrangida pela subseção (2) que envolve o uso de armas de fogo ou explosivos é o terrorismo, seja ou não a subsecção (1) (b) satisfeita.
>
> (UK, 2000, tradução nossa, grifo nosso)

Como Hardy e Williams (2014, p.5) observam, o Ato possui três requerimentos:

a) intenção;

b) motivo;

c) dano.

Além disso, o fato de que a legislação coloca "uso ou ameaça", pode-se entender "que uma pessoa que ameaça cometer um ato de terrorismo ficaria sob a definição da mesma maneira como se ele ou ela realmente seguisse com a ação ameaçada". Nesse sentido, e pensando em um contexto cibernético, isso dá margem para que movimentos de menor impacto no ciberespaço, que não causariam uma séria interferência ou disrupção em sistemas eletrônicos, pudessem ser abarcados.

No entanto, é interessante que o Ato não específica o que seria uma séria interferência/disrupção de sistemas, nem discrimina esses sistemas eletrônicos. A questão de envolver os sistemas eletrônicos como base para motivações religiosas e ideológicas, permite o enquadramento de ações cibernéticas sob alcunha de "ciberjihad".

Continuando com a definição, e lembrando de seu escopo abrangente, vale ressaltar a subseção que expande o alcance da definição para além do Reino Unido. Segundo o Ato sobre Terrorismo:

> 4) Nesta seção:
>
> (**a) "ação" inclui ação fora do Reino Unido,**
> (b) uma referência a qualquer pessoa ou propriedade é uma referência a qualquer pessoa ou propriedade, onde quer que esteja situado,
> (c) uma referência ao público inclui uma referência ao público de um país diferente do Reino Unido, e
> (d) "governo" significa o governo do Reino Unido, de uma Parte do Reino Unido ou de um país diferente do Reino Unido.
>
> (5) Neste Ato, uma referência às ações tomadas para fins de terrorismo inclui uma referência às ações tomadas em benefício de uma organização proscrita.
>
> (UK,2000, tradução nossa, grifo nosso).

Dessa forma, aliando essa subseção com a questão posta a respeito da abrangência das organizações internacionais, há margem para se pensar na extensão de proteção à OTAN (Organização do Tratado Atlântico), uma vez que, como Brexit, em detrenimento da União

Eruropeia, em acordos bilaterias e alianças com outros formatos, exemplo da Aliança dos Cinco Olhos, ganham maior relevância para o Reino Unido.

O Ato sobre Terrorismo 2006 (*Terrorism Act 2006*) permite ao governo a retirada de conteúdo on-line, segundo as Seções 1 e 2, uma vez que divulguam encorajamento do terrorismo (seção 1) e a divulgação de publicações terroristas (seção 2) (UK, 2006, tradução nossa). Entretanto, em 2016, o Ato de Poderes Investigatórios foi aprovado, exigindo, entre outras coisas, que os provedores de serviços de comunicação assegurem que as mensagens transmitidas pelos seus serviços possam ser decompostas pelas agências de segurança (JOSHI, 2017, p.6) Dessa maneira, empresas como o Whatsapp, teriam o dever de permitir a coleta de dados em investigações criminosas.

Quanto à Estratégia Contraterrorista inglesa, é relevante comentar que três versões dela foram produzidas: a primeira em 2003 , mas publicizada apenas em 2006, a segunda em 2009 e a mais recente em 2011. De acordo com Gearson e Rosemont (2015, p.1040, tradução nossa), a Estratégia revisada de Contraterrorismo do Reino Unido foi inicialmente concebida e desenvolvida pelo *Cabinet Office* "a partir de novembro de 2002 e tornou-se conhecido como CONTEST, um acrônimo originalmente tirado de *Counter-Terrorism Strategy"*.

Dessa forma, é interessante notar que mesmo com suas atualizações a CONTEST continuou com a mesma estrutura, com os chamados 4Ps: Perseguir (no sentido de parar os ataques terroristas), Previnir (que pessoas se tornem ou apoiem terrroristas), Proteger (fortalecer proteção contra ataques terroristas) e Preparar (mitigar o impacto dos ataques terroristas) (UK, 2011b, p.10). Fato que pode ser explicado a partir de uma abordagem de gestão de riscos (GEARSON; ROSEMONT, 2015, p.1043).

Nesse sentido, é considerando o *Terrorism Act 2006*. Por isso, a CONTEST de 2009 explicita que "a Internet apresenta desafios significativos e, no geral, a Prevenção em particular" (UK,2009, p.15). Ooutrossim, especifica que:

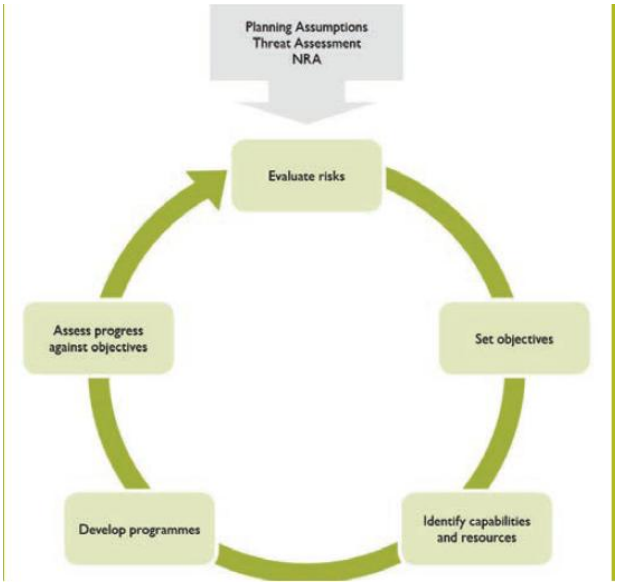
> 5.16 A revolução das comunicações também facilita um diálogo bidirecional entre organizações e seus membros potenciais. Esse diálogo permite **captação de recursos, recrutamento e algum treinamento e planejamento operacional: em grande medida, a internet tem substituído o campo de treinamento terrorista** (UK, 2009, p.43, tradução nossa, grifo nosso).

Em sentido prospectivo, destaca-se que o ciberterrorismo não parece uma grande ameaça, porém tal cenário poderia mudar. Sendo assim, há uma breve definição do que se

considera como ciberterrorismo “um ataque eletrônico por terroristas em nossas infraestruturas de informação e telecomunicação” (UK, 2009, p.116, tradução nossa).

Na CONTEST de 2011, diferentemente, há uma seção inteira sobre “Contraterrorismo e a Internet”, na qual as atividades que terroristas podem exercer on-line ficaram restringidas a 5 pontos: propaganda, radicalização e recrutamento, comunicação, planejamento de ataques e ataques cibernéticos (UK, 2011b, p.73-74). Outrossim, o uso de redes sociais pelos terroristas também é explicitado: websites, criptografia, Google Earth/Street, Darknet, Twitter e *Cloud Cpmputing* (UK, 2011b, p. 34-35).

Figura 14: Avaliação Nacional de Risco (NRA)



Fonte: UK (2011, p.42)

Em específico, quanto aos ataques cibernéticos, a CONTEST coloca a baixa probabilidade de que ocorram, mas alerta que “as ferramentas e técnicas necessárias para o ataque cibernético se tornam mais amplamente disponíveis e o sucesso das operações cibernéticas criminosas torna-se mais amplamente conhecido” (UK, 2011b, p.74). De fato, a CONTEST explicita que “nós continuamos a não ver evidência de ciberterrorismo **sistemático** (i.e. ataque terrorista em sistemasde TI [Tecnologia da Informação])” (UK, 2011b, p.34, tradução e grifo nosso) Nesse sentido, o uso de ataques cibernéticos por grupos ja é uma realidade, como o mesmo ponto explica:

> (...) Mas o primeiro incidente registrado de um ataque terrorista cibernético a sistemas de computadores corporativos ocorreram em 2010. O vírus chamado “here you have” (de responsabilidade que foi reivindicado pelas Brigadas Tariq bin Ziyad para Jihad eletrônico) foi relativamente pouco sofisticado, mas um indicador provável de uma tendência futura. Desde a morte de Osama Bin Laden, Al Qa'ida chamou-se explicitamente não só para atos de terrorismo solitário ou individual (ver ponto 2.22), mas também para “ciberjihad” (UK, 2011b, p.34, tradução nossa).

Todavia o ponto que comenta sobre o ciberterrorismo, com essa definição, não adentra muitos detalhes. Colocando mais uma explicação sobre funções de agências do que elaborando sobre o fenômeno. Conforme a CONTEST:

> 6.21 O Governo já se comprometeu a um aprimoramento significativo do trabalho para abordar oriscos de ataque cibernético. O Escritório de Segurança Cibernética e Garantia de Informação (OCSIA), com base no Cabinet Office, está supervisionando um programa para melhorar a nossa segurança cibernética nacional. O Programa Nacional de Segurança Cibernética (NCSP), entre outras coisas, eleva nosso nível de capacidade para detectar e nos defendemos de ameaças cibernéticas, construindo sobre o trabalho existente em todo o governo. O NCSP reduzirá nossa vulnerabilidade aos ataques cibernéticos independentemente da sua fonte. Mais detalhes serão contidos na Estratégia Nacional de Segurança Cibernética publicada no final deste ano (UK, 2011b, p.76, tradução nossa).

Por fim, a CONTEST, ao planejar hipóteses para 2011-2015, destacou que “haverá mais ciberterrorismo” e que grupos terroristas vão continuar se beneficiando de tecnologia off-shelf dando a eles poder logístico e, potencialmente letal, transformando a Internet e o espaço virtual “estrategicamente vitais” (UK, 2011b, p. 41, tradução nossa).

Em resumo, nota-se que o Reino Unido entende que há uma diferença entre o uso terrorista da Internet e o ciberterrrorismo, conforme a academia apregoa. Entretanto, o país entende que ataques cibernéticos terroristas, ainda que não de forma massiva, já estão ocorrendo, com uma baixa probabilidade de aumentar à curto prazo. Assim, a inteligência entra como ferramenta para contemplar a prevenção e perseguição dos terroristas.

4.3 AUSTRÁLIA

A Austrália é um país extremamente conectado, com uma tendência cada vez maior de presença no ciberespaço. Em cinco anos (2011-2016), a porcentagem de indivíduos usando a Internet subiu 9.2% (BRODBAND COMISSION FOR DIGITAL DEVELOPMENT, 2012; BRODBAND COMISSION FOR SUSTAINABLE DEVELOPMENT, 2017). Fato que repercutiu no setor comercial, uma vez que, segundo o Escritório de Estátistica Australiano (*Australian Bureau of Statistics*, em inglês), de 2013 até 2016, pela primeira vez mais da

metade de todas as empresas australianas apresentaram presença na web e 87% delas, no ano de 2015-16, divulgaram atividades financeiras virtuais, incluindo o banco on-line, o faturamento e a realização de pagamentos (AUSTRALIAN BUREAU OF STATISTICS, 2017a; 2017b). Sendo assim, essa digitalização fez com que 90% das infraestruturas críticas fossem encontradas sob domínio privado em 2016 (AUSTRALIAN STRATEGIC POLICY INSTITUTE- ASPI, 2016, p.4).

Esse cenário proporciona uma preocupação fundamentada do governo australiano com a questão da segurança cibernética. De fato, a percepção australiana sobre o domínio cibernético, com suas ameaças e potencial estratégico, começou em 2001, quando o governo lançou a Agenda Nacional de E-Segurança, a qual foi atualizada em 2006 e, posteriormente, sua Estratégia Nacional de Segurança Cibernética em 2009 (BROOKES, 2015, p.7), sendo também atualizada em 2016. Com isso, o governo australiano investiu na criação de instituições-chave para resguardar a Segurança Nacional do ciberespaço, como o CERT Austrália (Equipe de Resposta de Emergência de Computadores)[26] e o Centro de Segurança Cibernético Australiano (ACSC, em inglês)[27].

Conforme a Estratégia Nacional de Segurança Cibernética de 2009, no tocante à questão do terrorismo, coloca-se que as linhas entre as ameaças de atores tradicionais, incluindo o terrorismo, se tornem borradas (*blurred)* com a Internet, já que sua "natureza anônima e sem fronteiras" vem fazendo com que a atribuição da fonte de ataques seja difícil, e explicitando que:

> Os ataques aos sistemas informáticos críticos no governo e no setor privado estão sendo contemplados como uma forma alternativa de conduzir a guerra e um meio pelos quais criminosos, grupos **terroristas** e serviços de inteligência hostis podem prejudicar os interesses nacionais da Austrália (AUSTRÁLIA, 2009, p.3, tradução nossa, grifo nosso).

[26] Estabelecido em 2010 o CERT Austrália é "o ponto de contato governamental primário das grandes empresas australianas para: receber e responder relatórios de incidentes de segurança cibernética, receber apoio e conselhos para responder e atenuar incidentes cibernéticos, monitorar incidentes de segurança cibernética ou ataques para desenvolver uma imagem de ameaça e fornecer aconselhamento e alertas aos seus parceiros para melhorar sua resiliência de segurança cibernética". Outrossim, fornece "conselhos e suporte sobre ameaças cibernéticas e vulnerabilidades aos proprietários e operadores da infraestrutura crítica da Austrália e outros sistemas de interesse nacional (SNI)" (CERT AUSTRÁLIA, 2017, tradução nossa).

[27] Sucessor do Centro de Operações de Segurança Cibernética (CSOC, criado em 2011) e operacional desde 2014, o papel da ACSC é: "liderar a resposta operacional do governo australiano a incidentes de segurança cibernética, organizar operações e recursos nacionais de segurança cibernética, incentivar e receber relatórios de incidentes de segurança cibernética, conscientizar sobre o nível de ameaças cibernéticas para a Austrália e estudar e investigar ameaças cibernéticas" (ACSC, 2017, tradução nossa).

A estratégia coloca que cabe a Organização Australiana de Inteligência de Segurança (ASIO, em inglês) "investigar ataques eletrônicos realizados para espionagem, sabotagem, **terrorismo** ou outras formas de violência politicamente motivadas, ataques ao sistema de defesa e outros assuntos que caem sob mandato do Ato ASIO"[28], como parte dos Arranjos Operacionais Conjuntos (JOA)[29], os quais trabalhariam em conjunto com o CERT Austrália.

Em consonância, a Estratégia de Segurança Cibernética de 2016 destaca que "a atividade cibernética maliciosa é um desafio de segurança para todos os australianos. Organizações australianas em todo o setor público e privado foram comprometidas por atores patrocinados pelo Estado ou não estatais" (AUSTRÁLIA, 2016, p.4, tradução nossa). Por isos, a estratégia faz uso do termo "terrorista da Internet" ao mencionar seu engajamento "com parceiros internacionais para detectar e prevenir o uso da Internet pelos terroristas e combater o extremismo violento on-line" (AUSTRÁLIA, 2016, p.41, tradução nossa).

Observa-se que ambas as estratégias não usam o termo ciberterrorismo e, apesar de reconhecerem o uso terrorista da Internet, não discorreram muito sobre o assunto. Nesse sentido, para entender como o país percebe a movimentação terrorista virtualmente é relevante uma emenda[30] feita em 2002 (pós 11 de Setembro), chamada *Security Legislation Amendment (Terrorism) Act 2002*, que inseriu uma definição de terrorismo na Parte 5.3 da Lei do Código Penal de 1995.

---

[28] O Ato Legal da Organização Australiana de Inteligência de Segurança de 1979, confere uma seção inteira (Divisão 3) descrevendo poderes especiais da agência relacionados com as ofensas terroristas, possuindo várias emendas ao longo dos anos, sendo que a última, em 2016, possui entre vários tópicos uma *schedule* sobre interceptação de telecomunicações e uma sobre proteção de informações de segurança nacional em processos de ordem de controle. Para mais detalhes ver: Counter-Terrorism Legislation Amendment Act (nº. 1) 2016, nº 82, 2016.

[29] Segundo a própria estratégia, "os Arranjos de Operação Conjunta (JOA) foram estabelecidos pelo governo australiano, segundo o qual agências operacionais de segurança cibernética (DSD [Defence Signals Directorate], AFP [Australian Federal Police] e ASIO [Australian Security IntelligenceOrganisation's]) identificam, analisam e respondem ao cyber eventos de graves consequências nacionais. As agências JOA determinam qual a agência tem principal transporte de uma resposta de evento de segurança com base na natureza do evento e na agência individual responsabilidades. Pretende-se que este processo seja realizado dentro do CSOC [Cyber Security Operations Centre, antecessor do ACSC], com base em sua capacidades e pessoal, incorporado dentro das agências relevantes do governo australiano" (AUSTRÁLIA, 2009, p.30, tradução nossa).

[30] Como até o 11 de Setembro a Austrália não possuía leis nacionais em vigor para enfrentar a ameaça do terrorismo, e com a pressão da Resolução 1373 do Conselho de Segurança das Nações Unidas, que havia surgido em resposta aos ataques e exigia aos Estados-Membros que decretrassem ofensas de terrorismo e outras medidas preventivas, como restrições ao financiamento do terrorismo, o país se inspirou no Ato sobre Terrorismo de 2000 do Reino Unido (*Terrorism Act 2000*). Dessa forma, a principal resposta legislativa australiana ao 11 de Setembro foi um pacote de cinco projetos de lei promulgados em março de 2002 (HARDY e WILLIAMS, 2014, p.9). Outrossim, o governo australiano buscou progresso e cooperação entre inteligência e agências de *law enforcement* para responder aos ataques cibernéticos, vulnerabilidades e incidentes, incluindo a assinatura de um acordo como AusCERT (BEGGS, 2005,´474, tradução nossa).

Assim, o C*riminal Code Amendment (Terrorism) Act 2003 (CCA Act,)* coloca na Divisão 100.1:

> [...] Ato terrorista significa ação ou ameaça de ação em que:
>
> (a) a ação está incluída na subseção (2) e não se enquadra subsecção (2A); e
> (b) a **ação é feita ou a ameaça é feita** com a intenção de avançar uma causa política**, religiosa ou ideológica**; e
> (c) a ação é feita ou a ameaça é feita com a intenção de:
>
> (i) **coação ou influência por intimidação**, o Governo da Commonwealth ou de um Estado, Território ou país estrangeiro, ou de parte de um Estado, Território ou país estrangeiro; ou
> (ii) intimidar o público ou uma seção do público.
>
> (2) A ação cai dentro desta subseção se:
>
> (a) causa danos graves que são danos físicos a uma pessoa; ou
> (b) causa sérios danos à propriedade; ou
> (ba) causa a morte de uma pessoa; ou
> (c) põe em perigo a vida de uma pessoa, além da vida da pessoa tomando a ação; ou
> (d) cria um risco grave para a saúde ou a segurança do público ou um seção do público; ou
> **(e) interfere seriamente, interrompe ou destrói seriamente sistema eletrônico incluindo, mas não limitado a:**
>
> **(i) um sistema de informação; ou**
> **(ii) um sistema de telecomunicações; ou**
> **(iii) um sistema financeiro; ou**
> **(iv) um sistema usado para a entrega de serviços essenciais ao governo; ou**
> **(v) um sistema usado para, ou por, uma utilidade pública essencial; ou**
> **(vi) um sistema usado para, ou por, um sistema de transporte.**
>
> (AUSTRÁLIA, 2003, tradução nossa, grifo nosso).

Dessa forma, ao inserir em um componente cibernético a definição de terrorismo, indiretamente se abarca a questão do ciberterrorismo. Por isso, entende-se o fenômeno como algo mais agressivo aos sistemas digitais (i.e. ataques cibernéticos) do que o simples uso logístico do ciberespaço por grupos terroristas.

Em relação ao terrorismo, há uma parte demonstrando o que poderia cair no escopo das exceções aos atos terroristas. Assim, a parte 100.1 (3) inclui ações de:

> **(a) *adocacy*, protesto, dissidência ou ação industrial; e**
> **(b) não é intencional:**
>
> (i) causar danos graves que sejam danos físicos para uma pessoa; ou
> (ii) causar a morte de uma pessoa; ou

> (iii) pôr em perigo a vida de uma pessoa, diferente da pessoa tomando a ação; ou
> (iv) criar um risco sério para a saúde ou segurança do público ou uma seção do público.
>
> (AUSTRÁLIA, 2003, tradução nossa, grifo nosso).

Assim, percebe-se que o país tem uma preocupação em preservar direitos civis, que podem levar a *accountablity* de governos. Dessa forma, pensando no ciberespaço, uma divisão entre ações terroristas e atos hacktivistas é desenhada.

Por último, é válido ressaltar que a última parte coloca a possibilidade de extensão da definição para fora do país. Conforme a parte 101.1(4):

> (4) Nessa divisão:
>
> a) uma referência a qualquer pessoa ou propriedade é uma referência a qualquer pessoa ou propriedade, onde quer que seja, **dentro ou fora da Austrália**; e
> (b) uma referência ao público inclui uma referência ao público de um país diferente da Austrália.
>
> (AUSTRÁLIA, 2003, tradução nossa, grifo nosso).

Assim, de maneira geral, conforme Hardy e Williams (2014, p.11-12, tradução nossa), seis pontos podem ser retirados da definição em relação ao ambiente virtual:

> Em primeiro lugar, como a definição do Reino Unido, a definição australiana de terrorismo se aplicaria à ameaça de um ataque cibernético da mesma forma que se aplicaria a um ciberataque real. Em segundo lugar, a definição australiana não se aplicaria aos ataques cibernéticos destinados apenas a "influenciar" um governo. Um ataque cibernético precisaria ser intimidatório ou cair sob a definição australiana. Em terceiro lugar, a definição australiana provavelmente não abrangeria ataques cibernéticos contra a ONU, a OTAN ou órgãos similares, porque a subseção (1) (c) não inclui uma referência específica a "organizações governamentais internacionais" (como no Reino Unido defi nição). Em quarto lugar, para cair sob a definição australiana, um ataque cibernético precisaria causar séria interferência ou destruir um sistema eletrônico; não poderia simplesmente ser destinado a fazê-lo. Em quinto lugar, parece que a definição australiana se aplicaria aos ataques cibernéticos contra governos estrangeiros opressivos, embora a isenção de protesto político na subseção (3) limite o escopo da definição neste cenário. Por último, se um ataque cibernético pudesse ser classificado como protesto, dissidência ou ação industrial, ele ficaria sob a definição australiana somente se os manifestantes pretendessem causar um dos danos listados na subseção (3) (b).

Vale alientar também a observação de Roach (2007, p.58) ao apontar as motivações religiosas e ideológicas na definição australiana, as quais, segundo ele, têm um foco restritivo sobre crimes terroristas e não “sobre os efeitos discriminatórios que esses requisitos podem ter sobre os acusados e aqueles que podem compartilhar crenças políticas ou religiosas com

terroristas". Dessa forma, considerando o ciberespaço, categorias como a ciberjihad, podem ser pensadas.

Entretanto, a legislação australiana é só uma parte do entendimento sobre como o país percebe o fenômeno. Logo, é relevante para o complemento dessa percepção observar outros documentos como a Estratégia Contraterrorista Nacional e os relatórios do ACSC sobre ameaças, os *Treath Reports*.

A mais recente Estratégia Contraterrorista australiana se baseia em três princípios: a proteção de vidas é primordial, governo e comunidade devem se unir para lutar contra o terrorismo e o terrorismo é um ato criminoso que deve ser julgado dentro do sistema da justiça criminal (AUSTRÁLIA, 2015, p.V). Outrossim, o documento afirma que os esforços australianos estão focados na prevenção (AUSTRÁLIA, 2015, p.6), distribuindo-se em cinco elementos: desafiar ideologias violentas extremistas, frear o movimento das pessoas se tronarem terroristas, moldar o ambiente global, quebrar as atividades terroristas na Austrália e ter uma resposta efetiva e uma rápida recuperação dos ataques (representados na Figura 15).

Dessa forma, já no primeiro elemento há uma seção dedicada ao uso terrorista da Internet, na qual se reconhece que a Internet permite aos terroristas espalhar sua propaganda, conectando-se uns com os outros, preparar, recrutar pessoas, planejar e executar ataques terroristas (AUSTRÁLIA, 2015, p.7). Dessa maneira, evidencia-se o poder que mensagens e imagens gráficas têm no papel de radicalização dos indivíduos. Por isso, tem-se a ideia de um *continum*, partindo da prevenção até a disrupção de atividades.

Figura 15: Estratégia Contra Terrorista Australiana

Fonte: Austrália (2015, p. 6)

Assim, o foco da Estratégia é centrado na radicalização, incluindo a on-line, que é entendida na estratégia como: "indivíduos que vêm a aceitar o extremismo violento como meio legítimo de perseguir seus objetivos políticos, religiosos e ideológicos" (AUSTRÁLIA, 2015, p.7, tradução nossa). Com efeito, de maneira explicita não se abrange a questão de sistemas digitais, mas, faz-se a inclusão da restauração da normalidade de infraestruturas críticas dentro do elemento de recuperação, sem que os ataques aos sistemas possam gerar destruições físicas, como consta na legislação doméstica. Assim, se pode pensar em uma conexão indireta, com o ciberterrorismo.

A Estratégia coloca-se ainda dentro do elemento "Moldar o Ambiente Global", ou seja, a questão do uso do ciberespaço, de maneira geral, no sentido de "facilitar o uso de tecnologias avançadas para identificar, investigar, monitorar e combater o terrorismo" (AUSTRÁLIA, 2015, p.12, tradução nossa). Nesse sentido, não apenas o ciberespaço parece ser visto como passível de uso para os terroristas, mas também pelo governo, em sua batalha contraterrorista, principalmente como meio de coleta de informações.

Quanto aos relatórios, foram analisados os anos de 2015, 2016 e 2017. Com isso, notou-se que, em todos, a questão dos terroristas com intenção de conduzir ataques cibernéticos é posta. Apesar disso, todos mencionam a baixa probabilidade de que seja uma ameaça relevante a curto prazo. Sendo assim, embora não haja uma definição para o termo ciberterrorismo nos relatórios, ao associar o fenômeno com os ataques cibernéticos aos sistemas, é relevante a conceituação de ataque cibernético como um ato: "deliberado através do ciberespaço para manipular, interromper, negar, degradar ou destruir computadores ou redes ou a informação residente neles, com o efeito de sério comprometimento nacional da segurança, estabilidade ou prosperidade" (ACSC, 2017, p.52, tradução nossa).

Portanto, análises de baixo impacto são postas. Como o Relatório de 2015 (ASCS, 2015, p.8) evidencia: "embora alguns adversários não-estatais - como grupos terroristas e motivados por motivos – tenham expressado a intenção de conduzir ataques cibernéticos, eles provavelmente continuarão a usar a ruptura e o vandalismo para ganhar publicidade e promover suas causas". Além disso, como o Relatório de 2016 (ACSC, 2016, p.8-9, tradução nossa) destaca:

> Grupos terroristas que procuram prejudicar os interesses ocidentais atualmente representam baixa ameaça cibernética. Além de demonstrar uma compreensão das mídias sociais e explorar a internet para fins propagandisticos, as capacidades terroristas cibernéticas geralmente permanecem rudimentares e mostram poucos sinais de melhorar significativa num futuro próximo (...)

> No entanto, neste momento, os grupos terroristas são mais propensos a envergonhar os governos, impor custos financeiros e conquistar vitórias de propaganda comprometendo e afetando pobremente redes seguras.

De maneira um pouco mais sofisticada, o relatório de 2017 (ACSC, 2017, p.52, tradução nossa) concorda com o baixo impacto explicando que "a longo prazo, existe o potencial de tais grupos para desenvolver as capacidades necessárias, mas isso requer uma mudança de foco e recrutamento deliberado e esforços de treinamento".

Em resumo, percebe-se que a visão australiana do fenômeno do ciberterrorismo vai de encontro com a divisão proposta pela academia quanto ao uso terrorista da Internet e o ciberterrorismo, evidenciando um grau de intensidade maior para os ataques cibernéticos aos sistemas e o ciberterrorismo. Por isso, mesmo entendendo-o como uma possibilidade de ameaça futura, ao mesmo tempo, os documentos mostram a compreensão e preocupação com o combate ao uso terrorista da Internet, no sentido de eliminar principalmente as narrativas terroristas on-line, mas tentando prezar por uma diferenciação desses com atividades políticas que demandem, de maneira legal, *accountability* de governos e empresas.

4.4 CANADÁ

O Canadá apresentou um aumento de 6,8% na porcentagem de população usuária de Internet nos últimos cinco anos (2011-2016), porém a penetrabilidade da Internet mantém um patamar elevado, já que, em 2016, 89,8% da população estava conectada à Internet (BRODBAND COMISSION FOR DIGITAL DEVELOPMENT, 2012; BRODBAND COMISSION FOR SUSTAINABLE DEVELOPMENT, 2017). Essa conectividade levou ao incremento de companhias vendendo on-line que, segundo dados da *Statistics Canada*de 11%, em 201, subiram para 13, em 2013, sendo que o movimento de vendas on-line teve um aumento de 14 bilhões de dólares canadenses entre esses anos[31]. Segundo dados governamentais de 2004, 85% das infraestruturas críticas estão sob o domínio do setor privado (CANADÁ, 2004, p.5).

Dessa forma, o cenário cibernético ganhou relevância para o país, levando consequentemente o governo canadense a desenvolver, ao longo dos anos, um arcabouço jurídico legal que se procurasse endereçar a sua segurança cibernética. Nesse sentido, pode-se analisar a Lei Antiterrorismo de 2001 (ATA), a qual foi promulgada dois meses depois do 11

[31] Em 2012, foram 122 bilhões de dólares canadenses em vendas on-line e, em 2013, foram 136 bilhões de dólares canadenses (STATISTICS CANADÁ, 2014a; 2014b).

de Setembro, inspirando-se igualmente na legislação antiterrorista britânica e inserindo uma definição para terrorismo na seção 83.01 do Código Criminal Canadense de 1985 (HARDY e WILLIAMS, 2014, p.14). Assim, de acordo com a Lei o terrorismo é:

> [...]
>
> (b) um ato ou omissão, **dentro ou fora do Canadá**,
>
> (i) que está comprometido
>
> (A) no todo ou em parte para um **propósito objetivo ou causa política, religiosa ou ideológica**; e
> (B), no todo ou em parte, com a intenção de intimidar o público, ou um segmento do público, no que diz respeito à sua segurança, incluindo a sua segurança econômica, ou **compelir uma pessoa**, um governo ou uma **organização internacional** para fazer ou abster-se de fazer qualquer ato, seja ao público ou a pessoa, o governo ou a organização de dentro ou foraCanadá e
>
> **(ii) que intencionalmente**
>
> (A) cause morte ou dano corporal grave a uma pessoa pelo uso da violência;
> (B) põe em perigo a vida de uma pessoa;
> (C) provoque um risco grave para a saúde ou a segurança do público ou de qualquer segmentodo público;
> (D) cause danos substanciais à propriedade, seja para propriedade pública ou privada,se causar tal dano provavelmente resultará na conduta ou no danoreferido em qualquer das cláusulas (A) a (C); ou
> (E) **cause séria interferência ou grave interrupção de um serviço essencial, instalação ou sistema, seja público ou privado, outro que de um resultado de advocacy, protesto, dissidência ou paralisação do trabalho que não é destinado a resultar na conduta ou danos referidos em qualquer das cláusulas(A) a (C),** e que inclua uma conspiração, tentativa ou ameaça de cometer qualquer tal ato ou omissão, ou ser um acessório após o fato ou aconselhamento em relação a qualquer ato ou omissão, mas, para maior certeza, não inclui um ato ou omissão cometido durante uma conflito armado e que, no momento e no lugar de sua comissão, esteja de acordo com direito internacional consuetudinário ou lei internacional convencional aplicável ao conflito, ou as atividades realizadas por forças militares de um Estado no exercício de seus deveres oficiais, na medida em que essas atividades são regidas por outras regras do direito internacional.
>
> (CANADÁ, 2001, tradução nossa, grifo nosso).

Percebe-se aqui, camuflada em um elelemento cibernético, a definição do ponto (E), direcionado provavelmente para Infraestruturas Críticas, por restringir as ações dos serviços essenciais. Interessante notar que não apenas a intencionalidade, mas também um efeito fisico devem ser combinados, segundo a legislação, para que o ato esteja dentro do escopo de atividade terrorista, ou seja, em um contexto cibernético, essa restrição dá um tom mais intenso aos tipos de ataque que poderiam ser considerados ciberterrorismo.

Ressalta-se o foco das motivações políticas, religiosas e ideológicas na legislação, abrangendo em um contexto de ataques cibernéticos a questão da ciberjihad. A respeito de tal assunto, Roach (2007, p.59) ressalta que o governo canadense se preocupou com uma possível rotulação de terroristas quanto à religião. Dessa forma, o governo canadense adicionou uma cláusula interpretativa afirmando que "para maior certeza, a expressão de um político, religioso ou ideológico pensamento, crença ou opinião não vem dentro da definição de terrorista em atividade, a menos que constitua um ato ou omissão que satisfaça os critérios desse parágrafo" (CANADÁ, 1985, p.80).

Nota-se igualmente na definição a exclusão de protestos políticos, que não tenham intencionalide de causar dano ou pôr em risco a vida de uma pessoa. Como Hardy e Williams (2014) evidenciam, o alcance mais amplo de sua definição reduz o risco de que os usos menos sérios da informática e da tecnologia da Internet sejam alvo da legislação. Dessa forma, uma divisão com hacktivismo também pode ser delineada.

Por fim, vale ressaltar a questão da extensão do ato de compelir pessoas e/ou Organizações Internacionas, a qual permite, segundo Hardy e Williams (2014, p. 16, tradução nossa), "ser aplicada a ataques cibernéticos contra o Greenpeace, uma empresa doméstica de gás ou um ISP [provedor de serviço de Internet]". A definição canadense também pode ser plausivelmente aplicada a um ataque cibernético que obrigou um deputado a agir de forma particular".

Ainda um dos documentos mais relevantes quanto à segurança cibernética, é a Estratégia Nacional de Segurança Cibernética, que foi lançado em 2010, o qual é baseado em três princípios: proteger sistemas governamentais, fazer parcerias para proteger sistemas cibernéticos vitais, fora o governo federal, e ajudar os canadenses a ficar seguros on-line (CANADÁ, 2010, p.7).

De uma maneira geral, Adams (2016, p.2, tradução nossa) destaca que "a estratégia é digna de nota pelo fato de se limitar ao fortalecimento da capacidade do governo para detectar, dissuadir e defender contra-ataques cibernéticos, ao mesmo tempo que implanta a tecnologia cibernética para promover os interesses econômicos e de segurança nacional do Canadá". Nesse sentido, a Estratégia coloca três tipos de ameaças: espionagem e atividades militares cibernéticas financiadas por Estados, uso terrorista da Internet e crime cibernético (CANADÁ, 2010, p.5), sendo que a análise leva em consideração seus "alvos, métodos, motivações e intenções" (BARBAS, 2015, p.16, tradução nossa).

Dessa forma, no tocante ao uso terrorista da Internet a Estratégia reconhece que:

> Os terroristas estão conscientes do potencial para usar o Ocidente dependência mundial de sistemas cibernéticos como vulnerabilidade a ser explorado. Por exemplo, agora existem recursos on-line fornecendo conselhos aos terroristas sobre como defender os seus próprios sites enquanto lançam ataques cibernéticos a seus inimigos. **Além disso, vários grupos terroristas, incluindo a Al-Qaeda, expressaram sua intenção de lançar ataques cibernéticos contra estados ocidentais. Embora os especialistas duvidam de que terroristas atualmente têm a capacidade de causar sérios danos via ciber ataques, eles reconhecem que essa capacidade provavelmente irá desenvolver ao longo do tempo (**CANADÁ, 2010, p.5, tradução nossa, grifo nosso).

Assim, de forma mais esquemática Barbas (2015, p.16) identifica que dentro da Estratégia:

a) o histórico do uso terrorista da Internet advém da percepção de que o ciberespaço está sendo usado por redes terroristas porque eles reconhecem a dependência ocidental quanto às tecnologias;
b) a fonte dessa meaça são as redes terroristas;
c) o objetvo do uso terrorista da Internet é apoiar o recrutamento, levandar fundos e espalhar propaganda.

Para além da Estratégia de Segurança Cibernética, o Canadá possui, em particular, uma agência que se dirige a proteção dos canadenses contra riscos como desastres naturais, crime e terrorismo: a *Public Safety Canada*, a qual, apesar de ter sido criada em 2003 (para assegurar a coordenação em todos os departamentos e agências federais responsáveis pela segurança nacional e a segurança dos canadenses), foi designada pela Estratégia de Segurança Cibernética a: "projetar uma abordagem de todo o governo para informar sobre a implementação da Estratégia[32]" (CANADÁ, 2010, p.9, tradução nossa) trabalhando em conjunto com: Centro de Segurança das Comunicações Canadá (CSEC), Polícia Montada Real do Canadá (RCPM), Serviço Canadense de Inteligência de Segurança (CSIS), Departamento de Defesa Nacional (DND), Indústria Canadá (IC), Pesquisa e Desenvolvimento na Defesa Canadá (DRDC), Secretariado do Conselho do Tesouro (TBS), Serviços Compartilhados Canadá (SSC), Comissão Canadense de Radiotelevisão e

[32] É relevante colocar que o CERT Canadá está inserido dentro desse departamento, como a Estratégia coloca: "Dentro da Public Safety Canadá, o Centro Canadense de Resposta ao Incidente Cibernético [CERT] continuará a ser o foco ponto para monitorar e fornecer conselhos sobre atenuação do cyber ameaças e direcionar a resposta nacional a qualquer incidente cibernético e de segurança" (CANADÁ, 2010, p.10, tradução nossa).

Telecomunicações (CRTC), Escritório do Comitê de Privacidade do Canadá e o Centro Canadense de Combate Antifraude (CAFC) (PUBLIC SAFETY, 2017a; 2018).

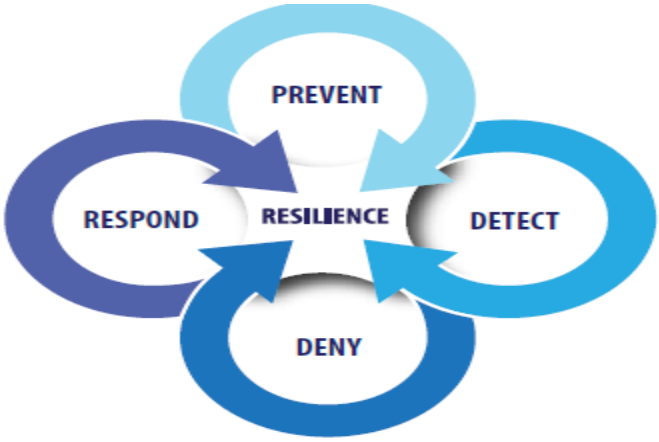
A partir dessa organização institucional, quanto à compreensão do país sobre o fenômeno do ciberterrorismo, outros documentos podem ser levantados como a Estratégia Nacional Contraterrorismo (2013) e os Relatórios Públicos sobre a Ameaça Terrorista no Canadá (2013; 2014; 2016; 2017).

A Estratégia de Contraterrorismo canadense possui seis princípios fundamentais:

a) construção de resiliência;
b) o terrorismo é um crime e será processado;
c) adesão à regra da lei;
d) cooperação e parcerias;
e) resposta proporcional e medida;
f) uma abordagem flexível e voltada para o futuro (CANADÁ, 2013a, p.11) e se baseia em quatro elementos: prevenir, detectar, negar e responder (conforme Figura 16).

Assim, dentro desse quadro, a questão da prevenção é focada no processo de radicalização dos indivíduos e, nesse caso, a questão do uso da Internet por terroristas é levantada. Segundo a Estratégia, "os grupos terroristas se comunicam com pessoas potencialmente suscetíveis à ideologia extremista violenta através de vários meios de comunicação, especialmente a Internet, que evoluiu como um fórum significativo para a comunicação e coordenação extremista violenta" (CANADÁ, 2013a, p.16, tradução nossa).

Figura 16 - Elementos da Estratégia Contra-Terrorismo Canadense



Fonte: Canada (2013a, p.14)

Seguindo para a parte de detecção, percebe-se que o papel da inteligência na esfera cibernética ganha um tom elevado, uma vez que a detecção "requer uma capacidade e competênciade inteligência sólidas" (CANADÁ, 2013a, p.17, tradução nossa). Sendo considerado o campo cibernético como área de atuação das agências envolvidas na coleta de informações, a exemplo do RCPM, o qual "opera uma equipe de inteligência de infraestrutura crítica que examina ameaças físicas e cibernéticas para infraestrutura crítica" (CANADÁ, 2013a, p. 19). Ainda a Estratégia coloca que a coleta de informações e dá igualmente fora do país:

> as atividades de coleta também ocorrem fora do Canadá. Por exemplo, a CSEC produz e divulga SIGINT estrangeiro para apoiar a tomada de decisões governamentais em diversas áreas, como segurança. O CSIS realiza coleta de inteligência de segurança e operações no exterior em apoio seu mandato e mantém relações fortes com agências estrangeiras com as quais regularmente troca informações sobre potenciais ameaças à segurança do Canadá. O DND/ CF pode fornecer reconhecimento estratégico para coletar ou verificar informações em apoio de outros governos departamentos. Através da ampla gama de contatos em sua rede no exterior, o DFAIT avalia desenvolvimentos sociais, econômicos, de segurança e políticos que ajudam a definir uma ameaça global meio Ambiente. O RCMP realiza investigações extraterritoriais de atividades terroristas quando cometido contra um cidadão canadense ou por um cidadão canadense no exterior (CANADÁ, 2013a, p.19, tradução nossa).

A parte de negação também traz um aspecto cibernético a Estratégia ao colocar que companhias privadas e outros níveis de governo "também são alvo de ciberterroristas, que procuram perturbar mercados financeiros e empresariais significativos" (CANADÁ, 2013a, p 26, tradução nossa). Igualmente compreendendo que:

> grupos terroristas manifestaram interesse em desenvolver as capacidades para ataques baseados em computador, contra a infraestrutura crítica. Pode ser difícil determinar os motivos por trás dos ataques cibernéticos que perpetram espionagem ou roubo. O mesmo modus operandi pode ser usado por oportunistas criminosos, concorrentes corporativos ou Estados-Nação estrangeiros. Os terroristas usam o ciberespaço para recrutar, comunicar e facilitar as operações. O Canadá deve negar-lhes os meios para operar neste domínio. Para esse fim, o Governo continua a implementar a Estratégia de Segurança Cibernética do Canadá (CANADÁ, 2013a, p.26, tradução nossa).

Por fim, quanto ao elemento de resposta, coloca a necessidade de cooperação entre os diversos setores incluindo "entre governos, empresas, indivíduos e ONGs para reconstruir

comunidades e trazer os responsáveis pela justiça" (CANADÁ, 2013a, p.28, tradução nossa). Assim, entendendo no contexto cibernético a necessidade de uma interação multinível.

De uma maneira geral, a Estratégia, segundo Findlay (2014, p.4, tradução nossa), "oferece um conjunto robusto de legislação nacional, estratégias, e quadro jurídico abrangentes que abordam crimes e atividades de terrorismo e atividades relacionadas ao uso e a ajuda do computador (*computer-relatedandcomputer-aided*)". Sendo que no nível governamental (mais alto) o Canadá abrange: "prevenção, detecção, resposta e interdição de atividades de ciberterrorismo em proteção, inteligência e vigilância de fronteiras, imigração, finanças e transporte através de vários departamentos e agências em todo o setor de segurança".

Quanto aos Relatórios Públicos sobre a Ameaça Terrorista no Canadá (2013; 2014; 2016; 2017). Eles indicam apenas uma aspiração terrorista quanto aos ataques cibernéticos e uma concreta utilização logística do ciberespaço pelos grupos. Além disso, é interessante a evolução da proporção das seções destinadas especificamente para as atividades terroristas da internet que, ao longo dos anos, foram ganhando maior refinamento.

O Relatório de 2013, por exemplo, apenas menciona que atividades terroristas na Internet continuam sendo um desafio. Expondo a seguinte percepção:

> o governo observou a crescente habilidade dos terroristas desde 2008 em benefício dos últimos desenvolvimentos em comunicações digitais, redes sociais e Internet para espalhar sua mensagem em todo o mundo, atrair adeptos à sua causa e planejar e controlar ataques. Alguns grupos terroristas mostraram interesse em incorporar ataques cibernéticos em suas atividades. Isso inclui aspirações para desenvolver capacidades cibernéticas para e interesses aliados. Os terroristas podem não ser capazes de causar sérios danos até ataques cibernéticos, mas sua capacidade provavelmente aumentará ao longo do tempo (CANADÁ, 2013b, p.27, tradução nossa).

Já no ano seguinte, o Relatório parece dar mais atenção aos Combatentes Transnacionais Estrangeiros (*Foreign Transnational Fighters*), destacando o uso de propaganda e das mídias sociais fatores que contribuem para o fenômeno desses combatentes e do meio virtual no processo de radicalização à violência (CANADÁ, 2014). O foco no relatório evidencia a repercussão, principalmente dos conflitos no início do ano, na Síria, Somália, Iraque e Afeganistão, aliados ao fato de que o governo detinha o conhecimento a respeito dos "130 indivíduos com conexões canadenses no exterior e que eram suspeitos de apoiar atividades relacionadas ao terrorismo de vários grupos" (CANADÁ, 2014, p.11, tradução nossa).

Nesse sentido, os Relatórios de 2016 e 2017 parecem mais detalhados na questão cibernética. Dessa forma, enquanto o Relatório de 2016 ainda continuou com uma explicação logística do uso do ciberespaço por terroristas, colocando a questão da violência on-line, radicalização, recrutamento e financiamento, o Relatório de 2017 traz uma definição de ataque cibernético, considerado como "esforços para danificar ou interromper um sistema informático ou eletrônico rede de comunicações", se diferenciando da exploração cibernética que "se refere à obtenção de informações em um sistema informático ou rede que de outra forma seria considerado privado" (CANADÁ, 2017, p.8, tradução nossa).

O Relatório de 2017, ainda, da ênfase ao grupo Daesh[33] considerado, junto da Al-Qaeda, como uma das principais ameaças ao país (CANADÁ, 2017, p.5). Salienta-se a dificuldade da luta contra o terrorismo que a criptografia usada pelos grupos terroristas vêm colocando, ou seja, a partir do uso do meio virtual para aumentar a segurança de suas atividades convencionais, além de explicitar que:

> [...] entidades terroristas aspiram a usar ciber-ferramentas como armas que podem causar danos físicos para redes e sistemas informáticos, o que seria um tipo de ataque cibernético muito mais sofisticado. Possuir capacidades suficientemente avançadas lhes permitiria interromper com sucesso serviços essenciais e infraestrutura crítica (como a rede elétrica, água, alimentos e transporte) (CANADÁ, 2017, p.9, tradução nossa).

Em resumo, percebe-se que o Canadá, com enfoque preventivo, direciona atenção para a legislação e entende o fenômeno do ciberterrorismo, do uso terrorista da Internet de formas diferentes, tentando restringir, dentro da legislação, o que seriam ataques cibernéticos mais sérios. Além disso, embora coloquem o enfoque na inteligência, preocupam-se com a questão da privacidade e os direitos civis que podem vir a reivindicar *accountability* do governo. Por fim, a ameaça de ataques físicos a infraestruturas críticas ainda que previsto na legislação tem um tom de longo prazo na narrativa canadense.

4.5 NOVA ZELÂNDIA

Com 88,5% dos indivíduos conectados à Internet (BRODBAND COMISSION FOR SUSTAINABLE DEVELOPMENT, 2017, p.95), quase a totalidade das indústrias usando Internet e um aumento de 67% nas conexões de fibra óptica em 2016 (STATSNZ, 2017a; 2017b) a Nova Zelândia é um país com uma alta conectividade. Com isso, existe a constante

[33]Sigla para a frase árabe *al-Dawla al-Islamiya al-Iraq al-Sham* (Estado islâmico do Iraque e Levante)

preocupação com sua segurança cibernética. Fato que se agrava, uma vez que, segundo Hyslop (2007, p.35, tradução nossa), “ o governo não possui ou controla diretamente grande parte da infraestrutura crítica da Nova Zelândia”, e mesmo o plano de Infraestrutra de 2015 do ´país se coloca que “em algumas áreas, o governo age como um regulador, enquanto em outras atua como financiador e proprietário da infraestrutura” (NEW ZEALAND - NZ, 2015a, p.52, tradução nossa) embora não as discrimine.

Dentro desse contexto, a Nova Zelândia desenvolveu, em 2011, sua Estratégia de Segurança cibernética, com planos de ação anuais. Assim, a Estratégia possui três areas prioritárias:

a) sensibilização crescente e segurança on-line;
b) proteção de sistemas e informações governamentais;
c) resposta e planejamento de incidentes.

Já os quatro objetivos são: resiliência cibernética, capacidade cibernética, cooperação internacional e abordagem do crime cibernético (NZ, 2015b; 2016) (ver Figura17).

Figura 17 - Objetivos da Estratégia de Segurança Cibernética da Nova Zelândia

Fonte: NZ (2016, p.4)

Dessa forma, é interessante notar que na Estratégia há um lugar para o debate sobre o uso terrorista da internet, visto como ameaça, em que se expressa que:

> os terroristas reconhecem a crescente dependência mundial dos sistemas cibernéticos e podem procurar aproveitar as vulnerabilidades que existem. É **provável que os terroristas continuem a desenvolver sua capacidade cibernética e uso da Internet para apoiar atividades de recrutamento e captação de recursos** (NZ, 2011, p.5, tradução nossa, grifo nosso).

Nos planos de ação, ainda, o de 2015 comenta a preocupação com o financiamento de criminosos e grupos terroristas de forma on-line.

> à medida que a imagem da ameaça evoluir, outras questões serão precisam ser considerados. Estes podem incluir considerar dar à policia as ferramentas para endereçar botnets; ampliando os poderes de execução para incluir a busca de informações sobre assuntos de proteção e proteção; **e o papel da Internet no financiamento ou no apoio a grupos criminosos ou terroristas organizados** (NZ, 2015b, p.8, tradução nossa, grifo nosso).

De fato, como a Nova Zelândia é um país com baixa atividade terrorista ele direciona atenção para ações de cooperação internacional, principalmente dentro das Nações Unidas e da Comunidade do *Five Eyes*. O que não significa que o Estado não possua instituições voltadas para a Segurança Cibernética, ou legislação que lide com o terrorismo.

Vale salientar as instituições que lidam com a Segurança Cibernética no país, por exemplo, são: Escritório Nacional de Política Cibernética (NCPO)[34],CERT NZ, Centro de Segurança Cibernética (NCSC), Polícia da Nova Zelândia, Departamento de Assuntos Internos (com a Equipe de Conformidade de Mensagens Eletrônicas), Oficial de governo do Escritório Digital (*The Government Chief Information Officer*) e Escritório do Comissário da Privacidade (CONNECTSMART, 2017). Outrossim, agências de inteligência ajudam no monitoramento das informações e, assim, na possibilidade dos ataques cibernéticos: Gabinete de Segurança das Comunicações do Governo (GCSB) e Serviço de Inteligência de Segurança da Nova Zelândia (NZSIS)[35].

Com todo esse aparato, é relevante colocar que, em 2017, o *Briefing* para o novo ministro destaca a ameaça das narrativas terroristas, no meio digital, como problema quanto à radicalização e os combatentes transnacionais estrangeiros. De acordo com o documento:

---

[34] "O Escritório Nacional de Política Cibernética (NCPO) no Departamento do Primeiro Ministroe o Gabinete (DPMC) lidera o desenvolvimento do conselho de políticas de segurança cibernética efornece assessoria ao governo para investir em atividades de segurança cibernética" (NZ, 2017, p.2, tradução nossa). Para descrição das outras agências ver: <https://www.connectsmart.govt.nz/about/more-about-cyber-security/>.

[35] "GCSB é responsável por SIGINT com foco estrangeiro. A agência não tem a habilidade legislativa de espionar os neozelandeses de forma independente, a menos que determinados critérios sejam atendidos, como o indivíduo sendo designado como "agente de uma potência estrangeira". O NZSIS é responsável pela coleção HUMINT da Nova Zelândia e é único entre os Cinco Olhos em termos de foco doméstico e estrangeiro" (GORDON, 2014, p.35, tradução nossa).

> a ideologia e mensagens extremistas violentas, acessadas principalmente através de plataformas de conteúdo e redes sociais em linha, continuam a ressoar com um pequeno número de indivíduos na Nova Zelândia. NZSIS continua ainvestigar indivíduos para apoiar ou tentar juntar ISIL na Síria e no Iraque. O NZSIS também fornece segurançainformações para apoiar cancelamentos de passaportes. A provisão desta informação ajuda a apoiar as Nações Unidas que impedem a viagem de combatentes terroristas estrangeiros (NZ, 2017, p.9, tradução nossa).

Quanto à legislação, ganha destaque o Ato de Supressão ao Terrorismo de 2002 (*Terrorism Supression Act 2002)*[36], o qual define o que é terrorismo na seção 5. Dessa forma:

> 5 Ato do terrorismo definido
>
> (1) Um ato é um ato terrorista para os fins deste Ato se
>
> (a) o ato cai na subsecção (2); ou
> (b) o ato é um ato contra uma convenção específica de terrorismo (conforme definido na seção 4 (1)); ou
> (c) o ato é um ato terrorista em conflito armado (conforme definido na seção 4 (1).
>
> (2) Um ato cai dentro desta subsecção se for destinado a causar, em qualquer 1 ou mais países, 1 ou mais dos resultados especificados na subseção (3), e é realizado com o objetivo de **promover uma causa ideológica, política ou religiosa** e com a seguinte **intenção**:
>
> (a) **induzir o terror** numa população civil; ou
> (b) forçar ou forçar indevidamente **um governo ou uma organização internacional** para fazer ou abster-se de fazer qualquer ato.
>
> (3) Os resultados referidos na subsecção (2) são
>
> (a) a morte de, ou outros ferimentos corporais graves, de uma ou mais pessoas (outrasdo que uma pessoa que executa o ato):
> (b) um risco grave para a saúde ou segurança de uma população:
> (c) destruição de, ou danos sérios bens de grande valor ou importância ou perda econômica importante, ou grande dano ambiental, se provávelpara resultar em 1 ou mais resultados especificados nos parágrafos (a), (b) e (d):
> (d) **interferência séria ou grave interrupção de uma infraestrutura, se for susceptível de pôr em perigo a vida humana**:
> (e) introdução ou libertação de um organismo portador de doenças, se for provável de devastar a economia nacional de um país.
>
> (4) No entanto, um ato não se enquadra na subseção (2) se ocorrer em uma situação de conflito armado e é, no momento e no lugar em que ocorre, conforme a regras de direito internacional aplicáveis ao conflito.

[36] "A TSA foi originalmente introduzida no Parlamento da Nova Zelândia antes do 11 de Setembro como a *Terrorism (BombingsandFinancing) Bill*. Após o 11 de Setembro, a Bill foi redirecionada e, posteriormente, promulgada em outubro de 2002. Embora a Nova Zelândia não tenha uma ameaça significativa de terrorismo, o governo da Nova Zelândia, como em muitas nações pequenas da Commonwealth, reconheceu a importância de se unir à comunidade internacional para denunciar e criminalizar o terrorismo" (HARDY; WILLIAMS, 2014, p.17).

> (5) Para evitar dúvidas, o fato de uma pessoa se envolver em qualquer **protesto, defesa ou dissidência,** ou se envolvre em qualquer greve, bloqueio ou outra ação industrial, não é, porém uma base suficiente para inferir que a pessoa-
>
> (a) está realizando um ato para um propósito, ou com uma intenção, especificada em subsecção (2); ou
> (b) pretende causar um resultado especificado na subseção (3).
>
> (NZ, 2002, tradução nossa, grifo nosso)

Dessa forma, observa-se que, diferentemente de outras legislações, o Ato de Supressão do Terrorismo 2002, não comenta sobre sistemas eletrônicos. Assim, Hardy e Williams (2014, p.19) explicam que tratando de ataques cibernéticos, seis pontos podem ser levantados:

a) a definição da Nova Zelândia não se aplicaria à ameaça de um ataque cibernético;
b) a definição apenas se aplicaria aos ataques cibernéticos destinados a obrigar indevidamente um governo ou induzir o terror em uma população;
c) a definição seria aplicável aos ataques cibernéticos contra organizações internacionais (incluindo ataques cibernéticos contra organizações governamentais internacionais como a ONU ou organizações não-governamentais como o Greenpeace);
d) a definição seria restrita aos ataques cibernéticos contra "infraestrutura", o que provavelmente não incluirá ataques cibernéticos sobre serviços essenciais (como gás ou eletricidade) ou sistemas, como uma coleção de servidores de site;
e) a definição exigiria que qualquer ataque cibernético contra uma infraestrutura fosse "susceptível de pôr em perigo a vida" (excluindo atos menos graves de hacktivismo);
f) a definição não abrangeria ataques cibernéticos que poderiam ser classificados como protesto, dissidência ou ação industrial.

Nesse sentido, a legislação da Nova Zelândia parece ser mais restritiva em alguns aspectos em relação aos ataques cibernéticos, lembrando que, para o país, um ataque cibernético seria: "uma tentativa de minar ou comprometer a função de um sistema baseado em computador, acessar informações, ou tentar rastrear os movimentos on-line de indivíduos sem sua permissão" (NZ, 2011, p.12, tradução nossa). Logo, a questão da espionagem ganha relevância para os neozelandeses e, portanto, é relevante comentar que existe legislação doméstica a qual permite que governo possa interceptar mensagens de telecomunicação: *o The Telecommunications (Interception Capability and Security) Act 2013*[37]. Em outras

[37] "O Ato de Telecomunicações (Capacidade e Segurança de Intercepção) de 2013 substituiu o Ato de Telecomunicações (Capacidade de Intercepção) de 2004. Esta Lei ampliou os poderes do Governo em

palavras, em se tratando de atos terroristas no ciberespaço, na prática, o governo neozelandês enfatiza a questão da espionagem.

De maneira geral, percebe-se que a Nova Zelândia não tem uma preocupação aparente muito específica no tocante à distinção entre uso terrorista da Internet e ciberterrorismo. No entanto, o pouco material analisado passa a impressão de que o governo entende essa diferença. Mas prefere se focar na invasão dos sistemas *per se* do que em outras modalidades cibernéticas.

4.6 CONSIDERAÇÕES PARCIAIS

Com o intuito de fazer uma análise específica dentro dos países da Comunidade dos Cinco Olhos, pode-se perceber que há um grau de coerência e consistência com o pensamento da comunidade acerca do fenômeno do ciberterrorismo e do uso terrorista da Internet. Contudo, são percebidas algumas pequenas variações que são mais visíveis se utilizarmos as categorias de análise do Quadro 5 (i.e. utilidade do ciberespaço, foco operacional, uso da violência e objetivo último dos terroristas), essas diferenças se dão conforme explicitado.

Quadro 6 - Visões dos países sobre atual utilização do ciberespaço por terroristas

Variável/ País	**EUA**	**UK**	**Austrália**	**Canadá**	**Nova Zelândia**
Utilidade do ciberespaço	Logística/ Estratégica	Logística/ Estratégica	Logística	Logística	Logística
Foco Operacional	Operações com foco em comunicação+ invasão de dados e sistemas tecnológicos	Operações com foco em comunicação	Operações com foco em comunicação	Operações com foco em comunicação	Operações com foco em comunicação
Uso de violência	Indireta	Indireta	Indireta	Indireta	Indireta
Objetivo último	Auto Fortalecimento	Auto Fortalecimento	Auto Fortalecimento	Auto Fortalecimento	Auto Fortalecimento

relação à interceptação de telecomunicações pelas agências de law enforcement e segurança e inteligência e segurança da Nova Zelândia através da obrigação de provedores de comunicações à fornecer capacidades legais de interceptação para que a Polícia, o NZSIS, e GCSB que poderiam acessar as comunicações uma vez que eles tiivessem um mandado de intercepção. A lei também assegurou que as agências de inteligência pudessem identificar e interceptar telecomunicações nessas redes sem interceptar material que não estava coberto por mandado. Em terceiro lugar, a Lei exigiu que os operadores de rede informassem o GCSB de qualquer decisão, ação ou alteração proposta que criasse um "risco de segurança da rede" relativo à segurança nacional da Nova Zelândia" (GORDON, 2014, p.59-60, tradução nossa).

Variável/ País	EUA	UK	Austrália	Canadá	Nova Zelândia
	+ Enfraquecimento oponente	+ Enfraquecimento oponente			

Fonte: Elaboração própria a partir dos documentos analisados no capítulo.

Dessa forma, é relevante colocar que enquanto Estados Unidos e Reino Unido entendem que o fenômeno do ciberterrorismo já está em curso, sendo ou não sistemático, os outros países salientam a baixa probabilidade do fenômeno ocorrer. Isso gera percepções diferentes em relação ao uso do ciberespaço por terroristas. Com isso, enquanto Reino Unido e Estados Unidos enxerguam uma movimentação estratégica quanto ao que ocorre atualmente, os outros países veem o uso, no momento, apenas do movimento logístico dos terroristas com o ciberespaço.

Essa diferença entre uso estratégico e logístico influenciará o tipo de operação que os países tendem a ressaltar nos documentos oficiais. Assim, embora se entenda que os ataques cibernéticos já estão ocorrendo, de forma não sistemática, o Reino Unido, dentro de seus documentos foca descrições voltadas para o nível das comunicações terroristas, indicando maior peso na tentativa de prevenção da radicalização. Nesse sentido, é gerada uma direção semelhante para a Austrália, Canadá e Nova Zelândia. Um posicionamento diferente é apresentado pelos Estados Unidos que, principalmente nos documentos mais recentes, enfatiza a invasão de sistemas, via *hacking*, e, portanto, acentua determinado caráter para a invasão de dados e sistemas tecnológicos, muito mais forte, se comparada com os outros países.

Quanto à questão da mobilização de massas, os países comentam sobre a radicalização que eleva o fenômeno dos Combatentes Estrangeiros Transnacionais, principalmente depois do uso de dinâmicas desse tipo por grupos terroristas, tal como o caso do Estado Islâmico. O que leva o *Five Eyes* a uma coordenação contraterrorista muito mais enfática, perceptível nas palavras de Teresa May, durante o Summit do grupo em 2016, quando ela mencionou que cabia "a alianças como Cinco Olhos para trazer maior ordem e resolução conjunta do 'trabalho disparatado' que ocorre internacionalmente e desenvolver uma resposta abrangente e coerente à ameaça comum" (MIRANDA, 2016, tradução nossa). De modo semelhante, no encontro em junho de 2017 em Ottawa, onde o comunicado da aliança colocou que os "países concordaram com uma abordagem comum para se engajar com os prestadores de serviços de comunicação e lidar com atividades terroristas e propaganda em linha, enquanto ocorrer a

defesa "da segurança cibernética e os direitos e liberdades individuais" (FIVE, 2017, tradução nossa). De acordo com o documento, em específico na área de segurança cibernética, o comunicado salienta:

> para abordar as ameaças à segurança cibernética, notamos a sólida cooperação em andamento entre os nossos cinco países em questões cibernéticas e notamos nossos esforços coletivos para estudar e avaliar as principais questões e tendências emergentes da segurança cibernética para prevenir, detectar e responder às ameaças cibernéticas (PUBLIC SAFETY CANADÁ, 2017b, tradução nossa).

Quanto ao uso de violência e objetivo último dos grupos terroristas on-line, todos os países ressaltam movimentações gerando algum tipo de perda econômica e psicologia (que denominamos aqui como indireta) com a intenção de multiplicação de força, ou seja, se autofortalecer diante dos oponentes. Isso não significa uma despreocupação com os países em relação a suas infraestruturas críticas, apenas dada a avaliação de baixa probabilidade de invasões complexas de sistemas, coloca essa variável em uma segunda escala de preocupação. Os Estados Unidos e o Reino Unido figuram como exceção, pois percebem invasões cibernéticas como realidade presente, o que gera a ideia de que o objetivo último dos grupos terroristas no ciberespaço é também o enfraquecimento do oponente por meio da possibilidade de ação direta conta infraestruturas críticas.

Diante desse quadro, as movimentações táticas de grupos terroristas on-line, que compreendem o uso de plataformas digitais, invasão de sistemas, narrativa de radicalização e o anonimato estratégico (ver Figura 13) são abordadas por todos os países, variando apenas em grau de ênfase nos documentos, que pode ser esquematizado no Quadro 7, onde "+" significa alta intensidade e "-" baixa intensidade. A intensidade foi atribuída a partir da análise geral dos documentos, sendo atribuído "+" aos países que mencionam a tática de forma atual, preocupante e abrangente e "-" aos países que mencionam a tática como algo pouco desenvolvido na atualidade e de forma mais restrita.

Quadro 7 - Grau de Intensidade sobre abordagens táticas dos terroristas no ciberespaço de acordo com os países

Variável/ País	EUA	UK	Austrália	Canadá	Nova Zelândia
Plataformas Digitais	+	+	+	+	+
Invasão de Sistema	+	+	+/-	-	-

Variável/ País	EUA	UK	Austrália	Canadá	Nova Zelândia
Narrativas de Radicalização	+	+	+	+	+
Anonimato Estratégico	+	+	+	+	+

Fonte: Elaboração própria com base nas análises do capítulo.

A partir do Quadro 7, percebe-se que, em relação aos graus de preocupação, a invasão dos sistemas é a única que varia. Isso se dá exatamente pelo entendimento dos países frente ao que poderia ser classificado como ataque cibernético terrorista. Assim, quanto mais restritiva a legislação, comparando entre os países, menor a intensidade do foco em relação a essa faceta, pois o escopo de possíveis ações defensivas já estaria delimitado. Cabe ressaltar que Austrália ficou com dois sinais por apresentar um meio termo, ou seja, ainda que a ameaça de um ataque cibernético esteja prevista, configurando uma ampla abrangência para o que viria a ser ataque cibernético, ele deverá seguir restrições, como: ser intimidador, causar série interferência aos sistemas, diferenciar motivações de protesto político que servem como forma de demandar *accountability* do governo.

Em específico quanto ao anonimato estratégico, o uso de criptografia é uma grande preocupação dentro da aliança. Segundo o comunicado conjunto dos países de 2017 em Ottawa:

> Ministros e Procuradores-Gerais também observaram que a criptografia pode prejudicar severamente os esforços de segurança pública, impedindo o acesso legal ao conteúdo das comunicações durante as investigações sobre crimes graves, incluindo o terrorismo. Para abordar essas questões, comprometemo-nos a desenvolver o nosso envolvimento com as empresas de comunicação e tecnologia para explorar soluções compartilhadas, mantendo a segurança cibernética e os direitos e liberdades individuais (PUBLIC SAFETY CANADÁ, 2017b, tradução nossa).

Nesse sentido, vale ressaltar que, embora todos os países sejam democráticos, algumas legislações e graus de preocupação que não são equânimes quanto à privacidade dão brecha para pensamentos de hipervigilância da Rede, que, como já comentado, podem ser vistos como um tipo de propagação de terror estatal no ciberespaço.

5 CONCLUSÃO

Vivemos em uma sociedade altamente dependendente das novas tecnologias que ainda não descobriu todo o potencial do ciberespaço, mas já vivencia as ameaças que esse espaço apresenta. O cenário é mais complexo se pensarmos que, para além dessa dependência, os indivíduos tendem a perceber ameaças de uma forma diferente, ou seja, de maneira não geográfica, considerando a percepção de ameaças que determinariam sua forma de pensar e agir. Assim, nesse contexto de Sociedade da Informação e Sociedade de Risco, o uso do ciberespaço ganhou um redimensionamento quanto às antigas ameaças, incluindo o crime, o terroismo e a guerra.

Em tal cenário, entender como os terroristas vêm usando o ciberespaço não apenas abre uma nova área de estudo, mas também se torna fundamental para o mundo do século XXI. Dessa forma, a pesquisa proposta foi dividida em alguns capítulos, para além da Introdução e Conclusão, a fim de entender mais acerca de dois fenômenos que são considerados de modos distintos: o uso terrorista da Internet e o ciberterrorismo.

No capítulo 2 foi desenvolvida a ideia de como o ciberespaço funciona; como os mundos físico e virtual se entrelaçam; bem como as Infraestruturas Críticas se tornam tão vulneráveis e, portanto, figuram como alvos preferidos dos grupos terroristas. De maneira geral, constatou-se que invasões nos Sistemas Industrial de Controle representam uma possibilidade e, por isso, acarretam preocupações, principalmente por parte dos tomadores de decisão, sobre a segurança de infraestruturas críticas. Essa preocupação é exarcebada não apenas porque, em grande parte dos países, essas infraestruturas não estão sob controle estatal, mas sim sob controle privado. Além disso, ainda que as ferramentas cibernéticas utilizadas para perpetrar esse tipo de invasão de sistemas sejam custosas de desenvolver, elas se tornam, de maneira crescente, mais acessíveis aos atores internacionais.

Diante dessa preocupação, tecnicamente embasada e com exemplos concretos já experienciados pelo mundo, tendo como marco o Stuxnet, o Capítulo 3 buscou entrar no debate sobre como a academia percebia a movimentação no ciberespaço por parte dos terroristas. Contudo, para entender o fenômeno do ciberterrorismo, em primeiro lugar, se fez necessário realizar uma retomada acerda da dificuldade de conceituação da base para definição do fenômeno, ou seja, o terrorismo *per se*. Assim, nesse capítulo várias análises e

definições foram colocadas a fim de esclarecer o nível de dificuldade no tocante às definições para descrever fenômenos político-sociais complexos.

Dentro dessa pequena colocação de definições entendeu-se que, para ter qualquer perspectiva de aprofundamento sob tipologias de terrorismo, um conceito raíz teria que ser elencado e o escolhido foi a conceituação dada por Diniz (2002, p. 13) sobre terrorismo:

> (...) emprego do terror contra um determinado público, cuja meta é induzir (e não compelir nem dissuadir) num outro público (que pode, mas não precisa, coincidir com o primeiro) um determinado comportamento cujo resultado esperado é alterar a relação de forças em favor do ator que emprega o terrorismo, permitindo-lhe no futuro alcançar seu objetivo político — qualquer que este seja.

A escolha dessa definição se deu, em grande parte, por aceitar tanto o emprego do terror por atores estatais quanto por atores não estatais, alem de se diferenciar de outros conflitos como a guerra e a guerrilha.

Para além dessa base, o capítulo continua fazendo uma análise sobre as diferentes definições sobre o ciberterrorismo que os autores vêm colocando em debate dentro da academia. Contudo, levando em conta o fato de que as definições de terrorismo são inúmeras, optou-se por destacar três definições, a saber: de Dorothy Denning, Maura Conway e Gabriel Weimann, para depois complementar os elementos semelhantes e diferenciados com definições de outros autores.

Depois dessa análise, então, percebeu-se que a academia faz, sim, uma diferenciação sobre o uso terrorista da Internet e o ciberterrorismo, sendo que, de forma esquemática, algumas diferenciações-chave, com base no conceito de terrorismo de Diniz, poderiam ser elencadas. Tais caracteríticas foram divididas em quatro categorias, isto é, utilidade do ciberespaço; foco operacional; uso de violência e objetivo último, representadas no Quadro 5. Entretanto, apenas a colocação acadêmica dessas características não traria a validade empírica para a análise do fenômeno como um todo, principalmente diante de inúmeros pesquisadores com diferentes bagagens acadêmicas que não concordam sequer com a existência, ou não, do fenômeno do ciberterrorismo.

Com isso em mente, o capítulo 4 tentou desvendar como a documentação legal, especificamente para o setor cibernético e antiterrorista, de um grupo de países escolhidos enquanto amostra: o *Five Eyes* apresentava os fenômenos, se é que haveria alguma distinção sobe o uso terrorista da Internet e o ciberterrorismo dentro dos países. Com base nas análises, percebeu-se que, embora de uma maneira geral os países do F*ive Eyes* tenham uma percepção

parecida sobre a movimentação terrorista do ciberespaço indo de encontro com a academia na diferenciação do uso Terrorista da Internet e ciberterrorismo, graus de diferença um pouco mais sutis foram percebidos (ver Quadro 6 e 7). Esses graus de diferenciação indicaram que, exatamente por não se ter uma definição aclarada sobre o que são os dois fenômenos, separandos consensualmente dentro do escopo do terrorismo, repercute não apenas nas percepções dos países, mas em ações que são tomadas por abrangência a partir da ameaça detectada.

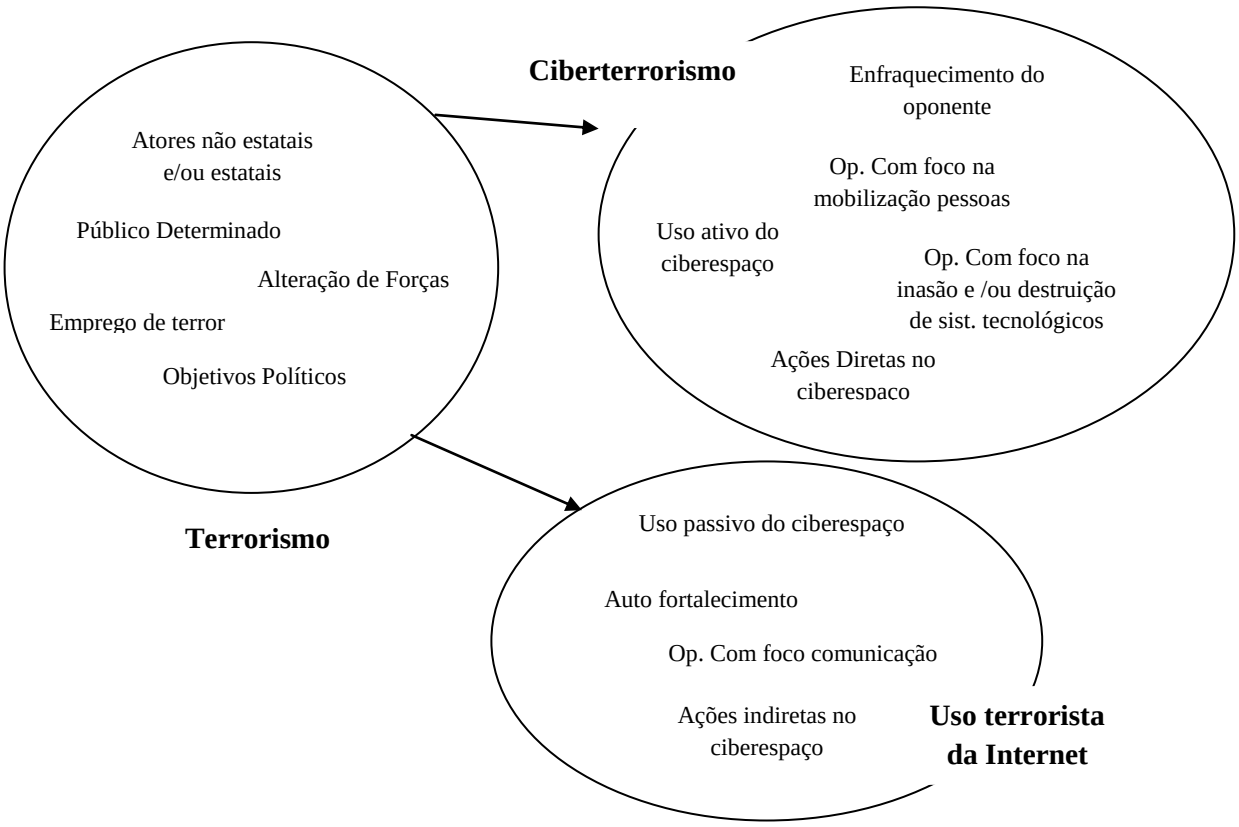
Diante das informações coletadas, percebeu-se que o cenário vivido atualmente, na prática, não é tão preciso quanto às características de um fenômeno ou outro, levando a esse destoamento de percepções dentro dos países analisados, bem como são desenvolvidas ações que, no intuito de englobar todas as variáveis possivies, acabam distorcendo alguns direitos humanos, como a privacidade na Rede.

Nesse sentido, a solução que a pesquisa proposta coloca é, em primeiro lugar, a aceitação generalizada das atividades no ciberespaço como um tipo de terrorismo. Além disso, uma diferenciação entre o ciberterrorismo e o uso terrorista da Internet, como já apregoada por parte da academia mundial. Ademais, ressalta-se que, ao observar uma amostragem de países líderes no combate do terrorismo internacional, outros Estados, da semiperiferia, por exemplo, poderão a partir de tais percepções construir suas estratégias de diálogos sobre a segurança cibernética de forma mais efetiva, contribuindo para a implementação de diversas soluções.

De maneira mais concreta, ao validar que ambos os fenômenos, do ciberterroismo e do uso terrorista, têm como elementos centrais determinada definição de terrorismo convencional, foi proposto que se partisse da definição de Diniz, bem como que eles fossem caracterizados por completo com base em outras características. Tais particularidades adicionais, então, são provenientes das que foram discriminadas pela acadêmia e acabaram tendo uma validação empírica da amostragem dos países, uma vez que, dada a falta de consenso sobre a existência do fenômeno do ciberterrorismo, uma verificação a partir dos casos mencionados passou a ser, no momento, impossível.

Assim, como se percebe, todas as caracteríticas acadêmicas elencadas no Quadro 5 foram descritas pelos documentos dos cinco países analisados, apenas variando em grau de intensidade, principalmente quanto à invasão e destruição de sistemas (ver Quadro 6 e 7). Logo, a proposta distinção pode ser melhor entendida pela Figura 18.

Figura 18 - Proposta de Tipologias de Terrorismo na área cibernética



Fonte: Elaboração própria com base em Diniz (2002) e no Quadro 5

A partir da distinção em voga, podemos afirmar que os dois fenômenos advêm de uma mesma "paleta de cores", mas, mesmo assim, são "cores" diferentes. Ademais, a partir dessa diferenciação não apenas atores não estatais entram em jogo quanto se trata de empregar o terror. Dessa forma, se os governos usarem a questão da hipervigilância para criar um estado de terror, com objetivo político, em determinada audiência, invadindo sistemas tecnológicos para isso, poderíamos pensar no ciberterrorismo ou adaptar a terminologia de Diniz (2002), ito é: "uso político não-terrorista do emprego de terror cibernético". Assim, diferentemente de uma questão bélica, procurará como objetivo último uma alteração de forças, que levem ao enfraquecimento do oponente, e não sua destruição, como o é na guerra.

Com a mesma linha de pensamento, o "uso político terrorista do emprego de terror cibernético" necessitaria que o emprego do terror por terroristas se desse de alguma maneira, mais provavelmente via disrupção ou destruição de sistemas tecnológicos (lembrando que os sistemas em si não podem ser considerados oponentes pelos terroristas, pelo menos até uma Inteligência Artificial ser desenvolvida o suficiente para tal) já que não tem envolvimento

político puramente neles, e sim em seu uso. Sendo assim, as alterações de forças com objetivo último dos terroristas são mantidas como o enfraquecimento do ponente, via a defasagem que esses sistemas costumam proporcionar. Ao mesmo tempo, no âmbito psicológico, a alteração de forças se dará via mobilização de massas, seja a favor da causa ou gerando pavor.

Essa variável psicológica entra igualmente na questão de uso passivo do ciberespaço, uma vez que esse domínio é usado para o emprego do terror, mas com o intuito de ser um multiplicador de força, ou seja, autofortalecer o grupo a partir de uma falsa imagem de grandeza espalhada em narrativas pelo globo. Em realidade, a principal diferença do uso dos terroristas da Internet para o ciberterrorismo se fixa na invasão dos sistemas, porque se ultrapassa a ação logística e se passa para ação estratégica no caso do ciberterrorismo, não sendo, como Diniz (2002) coloca, uma estratégia completa, mas algo parecido com uma parte da estratégia que irá compor um estrategema.

Por fim, salienta-se que essa proposta não buscou ser absoluta e infalível, bem como quaisquer erros comentidos na pesquisa são de responsabilidade da autora. De fato, ao lidar com fenômenos político-sociais complexos oriundos de bases mais indefinidas ainda, o exercício da pesquisa serve, em primeiro lugar, para apontar por caminhos de esclarecimentos, principalmente quanto aos tomadores de decisão, do que propor novas concietuações não palpáveis. Ademais, a questão sobre a ocorrência do ciberterrorismo ficou em aberto diante da falta de definição sobre os fenômenos, mas tomando por referência nossa proposta, percebeu-se que casos de ciberterrorismo não ocorreram até o momento, o que não signifique que tanto do lado dos atores estatais quanto do lado dos atores não estatais capacidades não estejam sendo desenvolvidas.

Diante de todo esse embrólio, nos resta, por enquanto, tentar aprofundar nosso entendimento acerca desses dois fenômenos. Pesquisas que adentrem a espistemologia dos conceitos cibernéticos são de fundamental importância nesse sentido. Estudar características necessárias e suficientes que possam compor os fenômenos conflitivos do ciberespeaço serviria, no mínimo, como forma de padronização das percepções acerca desses fenômenos, bem como ajudariam a aclarar linhas de diferenças existentes entre eles.

De modo semelhante, o desenvolvimento de metodologias mais rigorosas que possam lidar com a alta dinamicidade dos fenômenos virtuais também contribuiriam para estudos no campo social da área cibernética. Afinal, muitas críticas que recaem sobre quem se dedica a uma agenda de pesquisa voltada para o ciberespaço são focadas na falta de rigor científico (i.e. metodológico) das análises. Uma alternattiva interessante que pode ser mais aporfundada

é a proposta da criação do campo próprio das Relações Internacionais Cibernéticas, com proponentes de diversas áreas do mundo, inclusive no Brasil.

Por fim, vale lembrar que, em razão da fluidez do ciberespaço, o sinônimo de avanço dentro das pesquisas é a cooperação. Nesse sentido, a troca de informações entre setor privado e público é essencial para a realização de novas pesquisas, bem como a troca de experiências e descobertas entre países sobre o ciberespaço. Um exemplo disso na América do Sul foi a elaboração do "Guia de Defesa Cibernética da América do Sul" (2017) que fornece um panorama geral dos países da região acerca de conectividade e iniciativas na seara cibernética, tentando, assim, figurar como um esforço pioneiro e detectar a empiria dos acontecimentos virtuais com respaldo no mundo físico. Contudo, como todos os estudos pioneiros, muitas colocações podem ser aprofundadas, principalmente pela troca de informações e agendas de cooperação mútua, uma vez que muitos tomadores dedecisão ainda não veem o ciberespaço como ambiente relevante.

Em resumo, o campo que estuda fenômenos no ciberespaço apresenta uma vasta gama de opotunidades para o aprofundamento e a geração de agendas de pesquisa. Dessa forma, como já comentado, essa pesquisa constitui apenas parte desse esforço, que deve ser coletivo, e precisa ocorrer de forma mundial com debates e iniciativas dentro do Brasil.

REFERÊNCIAS

ABI RESEARCH. **ABI Research Partners with the ITU for a Global Cybersecurity Index**. [S.l.], 15 May 2013. Disponível em: <https://www.abiresearch.com/press/abi-research-partners-with-the-itu-for-a-global-cy/>. Acesso em: 28 jan. 2018.

ABRAM, Marshall; WEISS, Joe. **Malicious Control System Cyber Security Attack Case Study** - Maroochy Water Services, Austrália. Massachusetts: MITRE (technical papers) 7/23/2008. Disponível em: < https://www.mitre.org/publications/technical-papers/malicious-control-system-cyber-security-attack-case-study-maroochy-water-services-australia> Acesso em: 28 jan. 2018.

ACÁCIO, Igor Daniel Palhares. Segurança Internacional no século XXI: O que as teorias de Relações Internacionais têm a dizer sobre o ciberespaço? In: OLIVEIRA, Marcos Aurélio Guedes; GAMA NETO, Ricardo Borges; LOPES, Gills Vilar (Org). **Relações Internacionas Cibernéticas (CiberRI):** Oportunidades e Desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: UFPE, 2016. p. 35-58.

ADAMS, John. **Canada and Cyber.** Canadian. Calgary: Global Affairs Institute, July 2016. (Policy Reviews). Disponível em: <https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/1085/attachments/original/1467750257/Canada_and_Cyber_-_John_Adams.pdf?1467750257> Acesso em: 08 fev. 2018.

ARIELY, Gil. Knowledge Management, Terrorism, and Cyber Terrorism. In: JANCZEWSKI, Lech J.; COLARIK, Andrew M. (Ed.). **Cyber Warfare and Cyber Terrorism**. New York: Information Science Reference, 2008. p.7-16

ARQUILLA, John ; RONFELDT David. The Advent of Netwar (Revisited).In: ARQUILLA, John; RONFELDT David (Ed.). **The Future of Terror, Crime, and Militancy**. Santa Monica, CA: RAND Corporation, 2001. p.1-25

_____. CyberWar is Coming! In: ARQUILLA, John; RONFELDT David (Ed.). **Athena's Camp**: Preparing for Conflict in the Information Age. Santa Monica, RAND: 1997. p.23-60.

ATWAN, Abdel Bari. **Islamic State**: The Digital Caliphate. Oakland: University of California Press, 2015

AUSTRÁLIA. **Australia's Cyber Security Strategy**: Enabling Innovation, growth and prosperity. Camberra, 2016. Disponível em: < https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf> Acesso em: 08 jan. de 2018.

AUSTRÁLIA. **Australia's Counter-Terrorism Strategy**: Streightening our Resilience. Camberra , 2015. Disponível em : < https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/Australias-Counter-Terrorism-Strategy-2015.pdf> Acesso em: 08 jan. 2018.

AUSTRÁLIA. **Criminal Code Amendment (Terrorism) Act 2003**. Camberra, 2003. Disponível em: < https://www.legislation.gov.au/Details/C2004A01125> Acesso em: 31 jan. 2018.

AUSTRÁLIA. **Cyber Security Strategy**. Camberra, 2009. Dispopnível em: < https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf> Acesso em: 08 jan. 2018.

AUSTRÁLIA. **Security Legislation Amendment (Terrorist Act) 2002**. Camberra, 2002 Disponível em : < https://www.legislation.gov.au/Details/C2004C01314> Acesso em: 31 jan. de 2018.

AUSTRALIAN BUREAU OF STATISTICS **. Summary of IT Use and Innovation in Australian Business, 2015-16.** Camberra, 15 June 2017. Disponível em: <http://www.abs.gov.au/ausstats/abs@.nsf/mf/8166.0 > Acesso em: 28 jan. 2018.

AUSTRALIAN BUREAU OF STATISTICS. **Business Use of Information Technology 2015-2016.** Camberra, 20 July 2017a. Disponível em: < http://www.abs.gov.au/ausstats/abs@.nsf/mf/8129.0> Acesso em: 30 de jan. 2018.

AUSTRALIAN CYBER SECURITY CENTER - ACSC. **2015 Threat Report.** Camberra, July 2015. Disponível em: < https://www.acsc.gov.au/publications.html > Acesso em: 31 jan. 2018.

_____. ACSC. **2016 Threat Report**. Camberra, Octobr 2016. Disponível em: < https://www.acsc.gov.au/publications.html > Acesso em: 31 jan. 2018.

_____. ACSC. **2017 Threat Report**. Camberra, October 2017. Disponível em: < https://www.acsc.gov.au/publications.html > Acesso em: 31 jan. 2018.

AUSTRALIAN STRATEGIC POLICY INSTITUTE –ASPI. **Cyber Maturity in the Asia – Pacific Region.** Barton: Australian Strategic Policy Institute, Sptember 2016.

AWAN, Imran. Debating the term cyber-terrorism: Issues and problems. **Internet Journal of Criminology,** [S.L] 2014. Disponível em: <https://docs.wixstatic.com/ugd/b93dd4_d6e57fcde0d44fe6a755dbd315c07093.pdf>. Acesso em: 19 abr. 2015.

AXELROD, Evan M. **Violence Goes to the Internet**: avoiding the Snare of the Net. Springfield: Charles C Thomas Publisher, 2009.

BALLARD, James D; HORNIK, Joseph G; MCKENZIE, Douglas. Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues. **American Behavioral Scientist,** Sedona, v. 45, n. 6, p. 989-1016, Feb. 2002.

BARBAS, João Manual Assis. National Cybersecurity Strategies: Australia and Canada. In: PORTUGAL. Instituto de Defesa Nacional. **Instituto de Defesa Nacional Brief**. Lisboa: IDN, jun. 2015. p.13-14.

BECK, Ulrich. **Risk Society**: Towards a New Modernity. London: SAGE publications, 1992.

BEGGS, Christopher. Cyber-Terrorism: A Threat to Australia? In: KHOSROW-POUR, Mehdi (Ed). **Managing Modern Organizations Through Information Technology, Proceedings of the 2005 Information Resources Management Association International Conference**. Hershey: Idea Group Inc. 2005. Disponível em: < http://www.irma-international.org/viewtitle/32640/> Acesso em: 08 jan. 2018.

BEHR, Ines von et al. **Radicalisation in the Digital Era**. Washington: Research reports RAND Corporation, 2013. Disponível em: < http://www.rand.org/pubs/research_reports/RR453.html> Acesso em: 23 jun. 2017.

BEST, Steve; NOCELLA II, Anthony J. Defining Terrorism. **Animal Liberation Philosophy and Policy Journal**, [S.L], v. 1, n. 2, p. 1-18, 2004. Disponível em : < http://www.drstevebest.org/DefiningTerrorism.pdf> Acesso em: 08 jan. 2018.

BROADBAND COMMISSION FOR DIGITAL DEVELOPMENT. **The State of Bradband 2012**. Geneva, September 2012. Disponível em : < http://www.broadbandcommission.org/Documents/bb-annualreport2012.pdf> Acesso em: 31 jan. 2018.

BROADBAND COMMISSION FOR SUSTAINABLE DEVELOPMENT. **The State of Bradband 2017.** Geneva, September 2017**.** Disponível em : < https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf> Acesso em: 31 jan. 2018**.**

BROOKES, Chris. **Cyber Security:** Time for an integrated whole-of-nation approach in Australia. Weston**:** Australian Defence College (Indo-Pacific Strategic Papers,) March 2015. Disponível em: < http://www.defence.gov.au/ADC/Publications/IndoPac/150327%20Brookes%20IPS%20paper%20-%20cyber%20(PDF%20final).pdf> Acesso em: 08 jan. 2018.

BURKHART, Lori A. Cyber Attack! - Lessons Learned: Aurora Attack. **Fortnightly Magazine** Reston, January 2008. Disponível em: https://www.fortnightly.com/fortnightly/2008/01/cyber-attack-lessons-learned-aurora-attack Acesso em: 28 jan. 2018.

BURNETT, Jonny; WHYTE, Dave. Embedded Expertise and the New Terrorism. **Journal for Crime, Conflict and the Media** [S.L] no 1, vol 4, p.1-18, 2005. Disponível em: < https://www.diplomatie.gouv.fr/IMG/pdf/expertise_terrorisme.pdf> Acesso em: 08 jan. 2018.

BUZAN, Barry **People, States and Fear**: an Agenda for International Security Studies in the Post-Cold War Era. Boulder: Lynne Rienner Publishers, 2. ed, 1991.
BUZAN, Barry; WAEVER, Ole; WILDE, Jaap de. **Security:** A New Framework for Analysis. Boulder: Lynne Rienner, 1998.

CALAFATO, Trevor; CARUANA, Paul. Terrorism in Transition: The Implications of Cyber-Terrorism In: KATSIKIDES, Savvas; KOKTSIDIS, Pavlos I (eds.) **Societies in Transition:** Economic, Political and Security Transformations in Contemporary Europe. New York: Springer, 2015 pp.207-220.

CALVETY, Myrian Dunn. **Information Age Conflicts:** A Study of the Information Revolution and a Changing Operating Environment. Master Thesis. Zurich Contributions to Security Policy and Conflict Analysis, Nr. 64 Zürich, Forschungsstelle für Sicherheitspolitik und Konfliktanalyse, 2002.

_____. Cyber Terror: Looming Threath or Phantom? **Journal of Information Technology & Politics**, v. 4 n. 1, Philadelphia: The Haworth Press, 2007.

CANABARRO, Diego Rafael; BORNE, Thiago. **Reflections on The Fog of (Cyber) War**. Amherst: National Center for Digital Government (Working Paper) no. 13-001. March 1st, 2013. Disponível em : < https://www.umass.edu/digitalcenter/sites/default/files/FogofCyberWar.pdf> Acesso em: 08 jan. 2018.

CANABARRO, Rafael Diego. **Governança Global da Internet**. 2014. Tese (Doutorado em Ciência Política). Universidade Federal do Rio Grande do Sul, Porto Alegre.

CANADÁ. **2013 Public Report on the Terrorist Threat to Canada.** Ottawa, 2013b. Disponível em: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/trrrst-thrt-cnd/trrrst-thrt-cnd-eng.pdf Acessso em: 08 jan. 2018.

CANADÁ. **2014 Public Report on the Terrorist Threat to Canada**. Ottawa, 2014.Disponível em : < https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2014-pblc-rpr-trrrst-thrt/2014-pblc-rpr-trrrst-thrt-eng.pdf> Acesso em: 08 jan. 2018.

CANADÁ. **2017 Public Reporto n the Terrorist Threat to Canada, Ottawa,** 2017. Disponível em : < https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pblc-rprt-trrrst-thrt-cnd-2017/pblc-rprt-trrrst-thrt-cnd-2017-en.pdf > Acesso em: 08 jan. 2018.

CANADÁ. **Anti-Terrorism Act** (S.C. 2001, c. 41) Ottawa, 2001. Disponível em: < http://laws-lois.justice.gc.ca/PDF/A-11.7.pdf > Acesso em: 08 jan. 2018.

CANADÁ. **Building Resilience Against Terrorism:** Canada's Counter-terrorism Strategy, Ottawa**,** 2013a. Disponível em : < https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/rslnc-gnst-trrrsm-eng.pdf> Acesso em: 08 jan. 2018.

CANADÁ**. Canada's Cyber Security Strategy:** For a stronger and more prosperous Canada, Ottawa, 2010. Disponível em : < https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf> Acesso em: 08 de jan. 2018.

CANADÁ. **Criminal Code** (R.S.C., 1985, c. C-46). Ottawa, 1985. Disponível em : < http://laws-lois.justice.gc.ca/PDF/C-46.pdf > Acesso em: 08 jan. 2018.

CANADÁ. **Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection,** Ottawa, November 2004. Disponível em : < http://ccpic.mai.gov.ro/docs/Canada_non_paper.pdf> Acesso em: 08 jan. 2018.

CEPIK, Marco; CANABARRO, Diego Rafael; BORNE, Thiago. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: CEPIK, Marco (Org.). **Do 11 de**

Setembro de 2001 à "Guerra Contra o Terror": reflexões sobre o terrorismo no século XXI. Brasília: IPEA, 2014.

CHALK, Peter. **Encyclopedia of Terrorism**.Santa Barbara: ABC-Clio, 2013.

CHARVAT, Jpiag. Cyber Terrorism: A New Dimension in Battlespace. In: CZOSSECK, Christian; GEERS**,** Kenneth (Ed.) **The Virtual Battle Field:** Perspectives on Cyber Warfare. Amsterdan: IOS, 2009, p.77-87.

CLAUSEWITZ, Carl von. **On War.** 1a. Ed. New York: Alfred A. Knopf, 1993.

CLEMENTE, Dave. **Cyber Security and Global Interdependence**: What Is Critical? London: Chatham House, 2013.

COHEN, Daniel. Cyber Terrorism: Case Studies. In: AKHGAR Babak; STANIFORTH, Andrew; BOSCO, Francesca. **Cyber Crime and Cyber Terrorism Investigator's Handbook,** ELSEVIER: 2014 p.165-175.

COLARIK, Andrew M. **Cyber Terrorism**: Political and Economic Implications.Hershey: Idea Group Publishing, 2006.

COLARIK, Andrew M. Introduction to Cyber Warfare and Cyber Terrorism. In: JANCZEWSKI, Lech J. ; COLARIK, Andrew M. (eds.). **Cyber Warfare and Cyber Terrorism**. New York: Information science reference, 2008, p. xiii-xx

COLLIN, Barry. The future of cyberterrorism. Rockville: **Crime & Justice International** v. 2 n. 13, March 1997, p. 15-18. Disponível em: <https://www.ncjrs.gov/App/publications/abstract.aspx?ID=171868>. Acesso em: 19 abr. 2018.

COMBS, Cindy C.; SLANN, Martin**. Encyclopedia of Terrorism.** New York: Facts on File, Rev. Edition, 2007.

CONNECTSMART. **More about Cyber Security**. [S.L] 2017. Disponível em: < https://www.connectsmart.govt.nz/about/more-about-cyber-security/ > Acesso em: 30 jan. 2018.

CONWAY, Maura. Cyberterrorism: Hype and Reality In: ARMISTEAD, Leigh, (ed.) **Information warfare:** separating hype from reality**.** Washington: Potomac Books, Inc., p. 73-93.

CONWAY, Maura. Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet. Bridgman : **Fisrt Monday** vol 7 no.11, 2002 . Disponível em: < http://doras.dcu.ie/498/1/first_mon_7_11_2002.pdf > Acesso em: 09 jul. 2017.

CONWAY, Maura. Reality Check: Assessing the (Un) Likelihood of Cyberterrorism. In**:** CHEN, Thomas, JARVIS, Lee; MACDONALD, Stuart. (eds) **Cyberterrorism:** Understanding, Assessment and Response. New York: Springer, 2014, p.103-122

COUNCIL COUNTER TERRORISM COMMITTEE EXECUTIVE DIRECTORATE – CTED.**Physical Protection of Critical Insfrastructure Agains Terrorist Attacks**. New York: CTED Trend Reports, 8th March 2017. Disponível em: < https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf> Acesso em: 28 jan. 2018.

CURRAN, Kevin; CONCANNON, Kevin; MCKEEVER, Sean. Cyber Terrorism Attacks In: JANCZEWSKI, Lech J.; COLARIK, Andrew M. (eds.). **Cyber Warfare and Cyber Terrorism**. New York: Information Science Reference, 2008**,** p.1-6

DAILEY, J. The Intelligence Club: A Comparative Look at Five Eyes. [S.L] **Journal of Political Sciences & Public Affairs,** 5:261, June 2017. doi:10.4172/2332-0761.1000261

DENNING, Dorothy E. A View of Cyberterrorism 5 Years Later.In: HIMMA, Kenneth Einar. **Internet Security: hacking Counterhacking and Society**. London: Jones and Bartlett Pubelishers, 2007, p.123-140

DENNING, Dorothy E. Activism, Hactivist, and Cyberterrorism In: Arquilla, John, RONFELT, David (eds) **Networks and Netwars**: The Future of Terror, Crime, and Militancy. Santa Monica: RAND Corporation, 2001, p.239-288.

DENNING, Dorothy E. Terror's web: how the Internet is transforming terrorism. In: JEWKES, Yvonne; YAR, Majid (Ed.) **Handbook of Internet Crime.** Oregon: Willan Publishing, 2010, p.194-213

DENNING, Dorothy. **Cyberterrorism,** Monterry: Calhoun - The NPS Institutional Archive, 2000, Disponível em: <https://calhoun.nps.edu/bitstream/handle/10945/55351/Denning_Dorothy_2000_cyberterrorism.pdf?sequence=1 >. Acesso em: 23 jun. 2017.

DINIZ, Eugenio. **Compreendendo o fenômeno do terrorismo**. In: 3o Encontro Nacional da ABCP – Associação Brasileira de Ciência Política. 2002. Niterói: 28-31 de julho de 2002. Disponível em: < https://ciberativismoeguerra.files.wordpress.com/2016/09/diniz-do-o-fenomeno-do-terrorismo.pdf> Acesso em: 08 fev. 2018.

DREZNER, Daniel W. **All politics is global**: Explaining international regulatory regimes. Princeton: Princeton University Press, 2007.

EDWARDS, Chris. **Who Owns U.S. Infrastructure?** Washington: CATO Institute (TAX AND BUDGET BULLETIN NO. 78). June 1, 2017. Disponível em: < https://www.cato.org/publications/tax-budget-bulletin/who-owns-us-infrastructure#full> Acesso em: 30 jan. 2018.

ERIKSSON, Johan; GIACOMELLO, Giampiero. The Information Revolution, Security, and International Relations: (IR)relevant Theory? Sage Publications, London: **International Political Science Review ,** v. 27, n. 3, 2006, pp.221–244.

FINDLAY, Valarie. **Cyber-Terrorism and Canada's Cyber-Security Strategy.** Ontario: Security Sector Reform Resource Centre, April 9, 2014. Disponível em: < http://secgovcentre.org/2014/04/32575/ > Acesso em: 04 fev. 2018.

FIVE E yes alliance meets in Ottawa, stresses sharing intelligence to detect terrorists. **GlobalNews**, Toronto, June 28, 2017. Disponível em : < https://globalnews.ca/news/3563954/five-eyes-intelligence-alliance-2/> Acesso em: 30 jan. 2018.

FLEMMING, Peter; STOHL. Michael.Myths and Realities of Cyberterrorism, In: SCHMID, Alex P. (Ed.), **Countering Terrorism Through International Cooperation** ISPAC (International Scientific and Professional Advisory Council of the United Nations Crime Prevention andCriminal Justice Program), Vienna, 2001, p: 70-105

G1. **O que se sabe até agora dos irmãos Tsarnaev**. [S.L] 22/04/2013. Disponível em:< http://g1.globo.com/mundo/noticia/2013/04/o-que-se-sabe-ate-agora-dos-irmaos-tsarnaev.html > Acesso em: 04 fev. 2018.

GEARSON, John ; ROSEMONT, Hugo. CONTEST as Strategy: Reassessing Britain's Counterterrorism Approach, Oxfordshire**:** Taylor&Francis. **Studies in Conflict & Terrorism**, v. 38 n. 12, 2015, p.1038-1064 .

GORDON, Richard. **Privacy, Security and the Cyber Dilemma**- An Examination of New Zealand's Response to the Rising Threat of Cyber-attack. Thesis (Master of International Relations). Victoria University of Wellington, Kelburn 2014.

GREENBER, Andy. **Hacker lexicon**: what is the dark web? [S.L] 11/19/2014. Disponível em: < https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/> Acesso em: 04 fev. 2018.

GREENWOOD, Shannon; PERRIN, Andrew; DUGGAN, Maeve**. Social Media Update 2016.** Washington. November 11, 2016. Disponível em: < http://www.pewinternet.org/2016/11/11/social-media-update-2016/> Acesso em: 30 jan. de 2018.

HALOPEAU, Bruno. Terrorist use of the internet. In: AKHGAR Babak; STANIFORTH, Andrew; BOSCO, Francesca. **Cyber Crime and Cyber Terrorism Investigator's Handbook,** Boston: Elsiever, 2014 pp.123-132.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security and the Copenhagen School. Storrs: ISA, **International Studies Quarterly** v. 53, 2009, p.1155-1175. Disponível em < https://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf> Acesso em: 08 fev. 2018.

HARDY, Keiran , WILLIAMS, George. What is 'Cyberterrorism'? Computer and Internet Technology in Legal Defi nitions of Terrorism. In: CHEN, Thomas, JARVIS, Lee; MACDONALD, Stuart. (eds) **Cyberterrorism**: Understanding, Assessment and Response. New York: Springer, 2014, pp. 1-24

HEICKERÖ, Roland. **Terrorism online and the change of modus operandi**. In: UNIDIR Conference: Information & Communication Technologies and International Security, 24-25 April 2008, Geneva. Disponível em: <

http://www.unidir.ch/files/conferences/pdfs/information-warfare-and-cyber-terrorism-en-1-69.pdf> Acesso em: 04 fev. 2018.

HOFFMAN, Bruce. **Inside Terrorism**. Revised and Expanded Edition, New York, Columbia University Press, 2006.

HORRIGAN, John B.; DUGGAN, Maeve. **Home Broadband 2015.** Washington.December 21,2015. Disponível: http://www.pewinternet.org/2015/12/21/home-broadband-2015/ Acesso em: 30 jan. 2018.

HYSLOP, Maitland. **Critical Information Infrastructures:** Resilience and Protection. Middlesbrough: Springer, 2007.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. **Global Cybersecurity Index 2017**. Geneva. 19 July 2017. Disponível em: < https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf>. Acesso em: 28 jan. 2018.

INTERNET WORLD STATS. **World Internet Users and 2017 Population Stats [**S.L] Dec. 31, 2017**.** Disponível em: <http://www.internetworldstats.com/stats.htm> Acesso em: 28 jan. 2018.

JARVIS, Lee; MACDONALD, Stuart; NOURI, Lella. The Cyberterrorism Threat: Findings from a Survey of Researchers. Oxfordshire**:** Taylor&Francis, **Studies in Conflict & Terrorism**, v. 37 p.68–90, 2014.

JINGA, Ion. Terrorism And Critical Infrastructure**. HuffPost** [S.L] 16/02/2017.Disponível em: < http://www.huffingtonpost.co.uk/dr-ion-jinga/terrorism-and-critical-in_b_14781298.html> Acesso em: 28 jan. 2018.

JOHNSON, Le Wayne. **An Analysis of IT Governance Practices in the Federal Government**: Protecting U.S. Critical Infrastructure from Cyber Terrorist Attacks. 2012. Thesis (Doctor Doctor of Philosophy, Public Policy and Administration) Wladen University, Minneapolis, 2012.

JOSHI, Divij. **A comparison of legal and regulatory approaches to cyber security in India and the United Kingdom**. The Internet Center for Society. New Delhi,12 Nov 2017. Disponível em: < https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf> Acesso em: 31 jan. 2018.

JUDY, Michael. *Terrorism's* "Virtual" Safe Haven and the Effects on Terror Operations. Storrs: ISA , **Global Security Studies**, v. 2, Issue 1, winter 2011 p.34-44.

KALLBERG, Jan; THURAISINGHAM, Bhavani. From Cyber Terrorism to State Actors' Covert Cyber Operations In: AKHGAR, Babak; YATEs, Simeon (Ed.) **Strategic Intelligence Management. National Security Imperatives and Information and Communications Technologies**. Oxford: Butterworth-Heinemann, 2013, p.224-233.

KURBALIJA, Jovan. **An Introduction to Internet Governance**. 4th Edition. Malta: DiploFoundation, 2010.

KUROSE, James F.; ROSS, Keith W. **Computer Networking**: A Top-Down Approach. 6th Edition. New York: Pearson, 2012.

KUSHNER, Harvey W. **Encyclopedia of Terrorism.** London: SAGE, 2003.

LANGO, Hans-Inge. Competing Academic Approaches to Cybersecurity. In: FRIIS, Karsten; RINGSMOSE, Jens. **Conflict in Cyber Space Theoretical, Strategic and Legal Pespectives.** New York: Routledge, 2016.

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

_____. Postmodern Terrorism: New Rules for an Old Game. **Foreign Affairs.** New York**,** Sptember/October 1996 p.24-36.

LEVITAS, Ruth. Discourses of Risk and Utopia**.** In: ADAM, Barbara, BECK, Ulrich; VAN LOON, Joost (Ed.) **The Risk Society and Beyond** : Critical Issues for Social Theory. London: SAGE publications, 2000.

LIANG, Christina Schori. Cyber Jihad: **Understanding and Countering Islamic State Propaganda**. Geneva Center for Security Policy (GCSP) Policy Paper 2015/2. Disponível em: < www.gcsp.ch/download/2763/72138>. Acesso em: 25 jun. 2017.

LON (League of Nations). **Convention for the Prevention and Punishment of Terrorism** (Doc. C.546M.383 (1937)). Geneva,1937. Disponível em:< http://legal.un.org/avl/pdf/ls/RM/LoN_Convention_on_Terrorism.pdf> Acesso em. 31 jan. 2018.

LUCERO, Everton. **Governança da Internet**: Aspectos da Formação de um Regime Global e Oportunidades para a Ação Diplomática. Brasília: FUNAG, 2011.

LUIIJF, Eric. Definitions of Cyber Terrorism In: AKHGAR Babak; STANIFORTH, Andrew; BOSCO, Francesca. **Cyber Crime and Cyber Terrorism Investigator's Handbook,** Boston: Elsiever, 2014, p.11-18

MACDONALD, S. et al. **Cyberterrorism**: A Survey of Researchers. Cyberterrorism Project Research Report (No. 1), 2013, Swansea University. Swansea March 2013.Disponível em: < http://www.cyberterrorism-project.org/wp-content/uploads/2013/03/Cyberterrorism-Report-2013.pdf> Acesso em: 17 abr. 2015.

MACKINNON, Lachlan et.al. Cyber Security Countermeasures to Combat Cyber Terrorism. In*:* AKHGAR, Babak, YATES, Simeon (Ed.) **Strategic Intelligence Management.** National Security Imperatives and Information and Communications Technologies. Oxford: Butterworth-Heinemann, 2013 p.234-257.

MANDARINO, Raphael Júnior. **Segurança e Defesa do Espaço Cibernético Brasileiro.** Recife: Cubzac, 2010.

MARSDEN, Sarah V.; SCHMID, Alex P. Typologies of Terrorism and Political Violence.In: SCHMID, Alex P (Ed.) **The Routledge Handbook of Terrorism Research**. New Tork: Routlege, 2011, p.158-200

MAURER, Tim. 'Proxies' and Cyberspace. Oxford: Oxford University Press. **Journal of Conflict & Security Law**, v. 21 n. 3, 2016, p.383–403

MCALLISTER, Bradley; SCHMID, Alex P. Theories of Terrorism.In: SCHMID, Alex P (Ed.) **The Routledge Handbook of Terrorism Research**.New York: Routlege, 2011, p 201-293

MCGUIRE, M. R. Putting the 'Cyber' into Cyberterrorism: Re-reading Technological Risk in a Hyperconnected World. In**:** CHEN, Thomas, JARVIS, Lee; MACDONALD, Stuart. (Ed.) **Cyberterrorism**: Understanding, Assessment and Response. New York: Springer, 2014, p.63-84

MEHAN, Julie E. **CyberWar, CyberTerror, CyberCrime and CyberActivism.** 2nd edition, Cambridgeshire: IT Governance Publishing, 2014.

MENDES, Flávio P. Guerra, Guerrilha e Terrorismo: uma Proposta de Separação Analítica a partir da Teoria da Guerra de Clausewitz. **Carta Internacional**, Belo Horizonte, v. 9, n. 2, jul.-dez. 2014 p.96- 108.

MIRANDA, Charles. **Britain's new plan to tackle terrorism both home and abroad with controversial security alliance**. News Corp Australia Network, London, Feb. 17, 2016. Disponível em: < http://www.news.com.au/world/europe/britains-new-plan-to-tackle-terrorism-both-home-and-abroad-with-controversial-security-alliance/news-story/2ef64da03f39b977834e0214acd0ea05 > Acesso em: 30 jan. 2018.

MUNK, Tine Hojsgaard.Cyber **Security in the European Region**: Antecipatory Governance and Practice. 2015. Thesis (Doctor of Philosophy). University of Manchester, Manchester.

MUNOZ, Grissay**. Cyber Terrorism and the Effects of Advancing Technology**. Dissertation (Master of Science in Cybersecurity) August 2015. Utica College, New York.

NASCIMENTO, Fransllyn Sellynghton Silva. **Multidimensionalidade dos Conflitos Cibernéticos**. 2015. Monografia (Bacharel em Relações Internacionais). Universidade Federal de Roraima, Boa Vista, RR.

NATIONAL RESEARCH COUNCIL – NRC. **Computers at Risk**: Safe Computing in the Information. Washington**,** DC: The National Academies Press. 1991. Disponível em : < https://archive.org/details/computersatrisks00nati> Acesso em: 08 fev. 2018.

NELSON, Rick Ozzie. **The New National Strategy for Counterterrorism**. Washington, Center for Strategic and International Studes - CSIS. June 30, 2011. Disponível em: < https://www.csis.org/analysis/new-national-strategy-counterterrorism> Acesso em: 30 jan. 2018.

NEUMANN, Peter **. Old and New Terrorism.** Cambridge: Polity Press, 2009.

NEW ZEALAND – NZ. **The Thirty Year New Zealand Infrastructure Plan**, Wellington, 2015a. Disponível em: < http://www.infrastructure.govt.nz/plan/2015/nip-aug15.pdf> Acesso em: 09 fev. 2018.

NEW ZEALAND – NZ. **Briefing to Incoming Minister responsible for cyber security policy.** Department of the Prime Minister and Cabinet , Wellington, 30 June 2017 (Tracking Number 3999201). Disponível em: < https://www.dpmc.govt.nz/sites/default/files/2017-12/bim-cyber-security-policy-oct-2017.pdf> Acesso em: 09 fev. 2018.

NEW ZEALAND – NZ. New Zealand **New Zealand's Cyber Security Strategy,** Wellington, 2011. Disponível em: < https://www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-june-2011_0.pdf> Acesso em: 09 fev. 2018.

NEW ZEALAND – NZ. **Terrorism Supression Act 2002**. Wellington, 2002. Disponível em : < http://www.legislation.govt.nz/act/public/2002/0034/43.0/DLM151491.html> Acesso em: 31 jan. 2018.

NEW ZEALEAND –NZ. **New Zealand's Cyber Security Strategy 2015-Action plan,** Wellington, 2015b. Disponível em: < https://www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-action-plan-december-2015.pdf> Acesso em: 08 fev. 2018.

NIEKERK, Brett van; MAHARAJ, Manoj S. Relevance of Information Warfare Models to Critical Infrastructure Protection. Saldanha, **Scientia Militaria, South African Journal of Military Studies,** v. 39, n. 2, 2011, p. 52-75.

NYE JR, Joseph S. **Cyber Power**. Cambridge: Belfer Center for Science and International Affairs, May 2010. Disponível em: <https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>. Acesso em: 28 jan. 2018.

NYST, Carly; CROWE, Anna. Unmasking the Five Eyes' global surveillance practices. In: GLOBAL INFORMATION SOCIETY WATCH. **Global Information Society Watch 2014:** Communications surveillance in the digital age. [S.L] APC/Hivos, 2014 p.51-54. Disponível em < http://giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf> Acesso em: 08 fev. 2018.

OLMSTEAD, Kenneth; SMITH, AARON. **Americans and Cybersecurity**. Washington, Jan 26, 2017. Disponível em: < http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/>Acesso em: 29 jan. 2018**.**

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE -OTAN. **Cyber defence.** [S.L] 14 Dec. 2017. Disponível em: < https://www.nato.int/cps/en/natohq/topics_78170.htm > Acesso em: 28 jan. 2018.

OSULA, Anna-Maria. **National Cyber Security Organisation**: UNITED KINGDOM. Tallinn: CCDCOE, 2015.

PERNIK, Piret; WOJTKOWIAK, Jesse; VERSCHOOR-KIRSS, Alexander. **National Cyber Security Organisation**: UNITED STATES. Tallinn: CCDCOE. 2016.

PETRACIOLI,F. **Sabe o que são sniffing e wardriving***?* [S.L], 27/02/2008. Disponível em :<http://pcworld.com.br/dicas/2008/02/27/sabe-o-que-e-sniffing-e-wardriving/> Acesso em: 31 jul. 2017.

POPE, Lonnie. **Cyber-Terrorism and China.**Research Paper Studies (Master in Military Studies) Marine Corps University, Virginia.2008

PRESCOTT, Cecil. **E-commerce and ICT activity: 2016**. Office for National Statistics, London, 30 November 2017. Disponível em:<https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/ecommerceandictactivity/2016 > Acesso em: 28 jan. 2018.

PUBLIC SAFETY CANADA. **Cyber Security in the Canadian Federal Government.** Ottawa, 2017-09-18a. Disponível em: < https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-en.aspx > Acesso em: 15 dez. 2017.

PUBLIC SAFETY CANADA. **Five Country Ministerial 2017: Joint Communiqué.** Ottawa, June 26, 2017b. Disponível em: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/index-en.aspx > Acesso em: 30 jan. 2018.

PUBLIC SAFETY. **About Public Safety Canada.** Ottawa, 2018- 01-12 Disponível em:< https://www.publicsafety.gc.ca/cnt/bt/index-en.aspx> Acesso em: 31 jan. 2018.

RADU, Roxana, Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace. In: KREMER, Jan-Frederik;· MÜLLER, Benedikt (Ed.). **Cyberspace and International Relations:**Theory, Prospects and Challenges.London: Springer, 2014.

RAPOPORT, David C. The Four Waves of Rebel Terror and September 11**.** Los Angeles, **Anthropoetics VIII**, no. 1 Spring/ Summer 2002**.** Disponível em: < http://anthropoetics.ucla.edu/ap0801/terror/> Acesso em: 28 jan. 2018.

RATTRAY, Gregory J. The Cyberterrorism Threat. In: SMITH, James M., THOMAS, William C. (Ed..) **The Terrorism Threat and U.S. Government Response:** Operational and Organizational Factors. Colorado Springs : US Air Force Institute for National Security Studies, 2001, p.79-118

ROACH, Kent. A Comparison of Australian and Canadian Antiterrorism Laws. Sydney, **UNSW Law Journal** v. 30 (1), 2007, p.53-85.

ROCKWEL, Mark. **How cyber impacts the full spectrum of terror threats**. FCW , McLean,Sep 27,2017. Disponível em: < https://fcw.com/articles/2017/09/27/homeland-threats-hearing-rockwell.aspx> Acesso em: 30 jan. 2018.

ROHR, Altieres. **Vírus que atrasou programa nuclear do Irã foi criado pelos EUA e por Israel.** G1 [S.L] 18/01/2011**.**Disponível em:< http://g1.globo.com/tecnologia/noticia/2011/01/virus-stuxnet-foi-criado-pelos-eua-e-por-israel-diz-jornal.html> Acesso em: 28 jan. 2018.

SALMON, Doug; ZELLER, Mark; Guzmán, Armando; DONOLO, Marcos**. Mitigating the Aurora Vulnerability With Existing Technology**. In: 64th Annual Georgia Tech Protective Relaying Conference, 2010, Atlanta, Georgia. Disponível em : < https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6392_MitigatingAurora_MZ_20090918_Web.pdf?v=20151125-084552 > Acesso em: 28 jan. 2018.

SCHMID, Alex P.; JONGMAN Albert J, **Political Terrorism**: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature. Revised edition prepared under the auspices of the Center for International Affairs, Harvard University. Amsterdam: North-Holland, 1988.

SCHMIDT, Alex P. The Definition of Terrorism.In: SCHMID, Alex P (Ed.) **The Routledge Handbook of Terrorism Research**.New York: Routlege, 2011, p.39-157

SCHMITT, Michael N; WATTS, Sean. Beyond State-Centrism: International Law and Non-state Actors in Cyberspace. Oxford: Oxford University Press **.Journal of Conflict & Security Law** , v. 21 n. 3, 2016, p.595–611

SEAMARK, Michael. **Curse the judge, shout fanatics as the Muslim girl who knifed MP smiles as she gets life.** MailOnline, London, 5 November 2010. Disponível em:< http://www.dailymail.co.uk/news/article-1326208/Roshonara-Choudhry-knifed-MP-StephenTimms-smiles-gets-life.html > Acesso em: 25 jun. 2017.

SEDDON, AYN EMBAR. Cyberterrorism: Are We Under Siege? Washington: Sage Publications. **American Behavioral Scientist**, v. 45 n. 6, February 2002, p. 1033-1043.

SHAKARIAN, Paulo; SHAKARIAN, Jana; RUEF, Andrew. **Introduction to Cyber-Warfare:** A Multidisciplinary Approach**.** Masachuttes: Elsevier, 2013.

SHEA, Dana A. **Critical Infrastructure**: Control Systems and the Terrorist Threat . Congressional Research Service –CRS, Report for Congress. Washington, January 20, 2004. Disponível em: < https://fas.org/irp/crs/RL31534.pdf> Acesso em: 28 jan. 2018.

SINGER, Allan and FRIEDMAN, Paul W **Cybersecurity and Cyberwar**: what everybody needs to know. Oxford: Oxford University Press. 2014.

SISSON, Mary. **Lashkar-e-Taiba**. Encyclopedia Britannica, London: Encyclopædia Britannica, inc. May 30, 2016. Disponível:< https://www.britannica.com/topic/Lashkar-e-Taiba> Acesso em: 04 fev. 2018.

SMITH, Robert. The **Cyber Terrorism Threath to Critical Infraestructure**. 2014. Dissertation (Master of Science in Cybersecurity), Utica College, New York.

START. **Global Terrorism Database** (GDT). [S.L] June 2017. Disponível em: < https://www.start.umd.edu/gtd/search/Results.aspx?charttype=pie&chart=attack&search=infrastructure> Acesso em: 25 nov. 2017.

STATISTICS CANADA. **Infographic**: 2012 Survey of Digital Technology and Internet **Use.** Ottawa, November 19, 2014a**.** Disponível em: <https://www.statcan.gc.ca/pub/11-627-m/11-627-m2014004-eng.htm> Acesso em: 28 jan. 2018.

STATISTICS CANADA. **Infographic**: 2013 Survey of Digital Technology and Internet Use. Ottawa, November 19, 2014b. Disponível em:< https://www.statcan.gc.ca/pub/11-627-m/11-627-m2014001-eng.htm > Acesso em: 28 jan. 2018**.**

STATSNZ. **Business operations survey**: 2016. Wellington, 21 March 2017a. Disponível em: <https://www.stats.govt.nz/information-releases/business-operations-survey-2016 > Acesso em: 30 jan. 2018.

STATSNZ. **Internet service provider survey**: 2017. Wellington, 09 October 2017b Disponível em: < https://www.stats.govt.nz/information-releases/internet-service-provider-survey-2017 > Acesso em: 30 jan. 2018.

STOHL, Michael. Dr. Strangeweb: Or How They Stopped Worrying and Learned to Love Cyber War. In**:** CHEN, Thomas, JARVIS, Lee; MACDONALD, Stuart. (Ed.) **Cyberterrorism**: Understanding, Assessment and Response. New York: Springer, 2014, p.85-102

TALİHÄRM, Anna-Maria. Cyberterrorism: in Theory or in Practice? Ankara, **Defence Against Terrorism Review** ´v.3, n. 2, Fall 2010, p. 59-74

THE GUARDIAN. **Inspire magazine: the self-help manual for al-Qaida terrorists**.London, 2013. Disponível em: < https://www.theguardian.com/world/shortcuts/2013/may/24/inspire-magazine-self-help-manual-al-qaida-terrorists > Acesso em: 25 jun. 2017.

THEOHARY, Catherine A.; ROLLINS, John W. **Cyberwarfare and Cyberterrorism:** In Brief. Washington, March 27, 2015. Disponível em: <https://fas.org/sgp/crs/natsec/R43955.pdf> Acesso em: 25 jun. 2017.

TOFFLER, Alvin. **The Third Wave**. New York: Bantam Books, 1984.

TOMBUL, Faith; AKDOGAN, Huseyin. How Do Terrorist Organizations Use Information Technologies? Understanding Cyber Terrorism. [S.L] **Middle East Review of Public Administration (MERPA**), n. 2 v. 1 2016 p. 1-15.

TSAGOURIAS, Nicholas. Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts. Oxford: Oxford University Press. **Journal of Conflict & Security Law**, v. 21 n. 3, 2016, pp. 455–474.

UNITED KINGDOM – UK. **CONTEST:** The United Kingdom Strategy for Countering Terrorism, London, July 2011b. Disponível em: < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf> Acesso em: 09 fev. 2018.

UNITED KINGDOM-UK **The UK Cyber Security Strategy**: protecting and promoting the UK in a digital world, London, November 2011a Disponível em : < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> Acesso em: 09 fev. 2018.

UNITED KINGDOM-UK .**Cyber Security Strategy of the United Kingdom:** safety, security and resilience in cyber space , London, June 2009. Disponível em : < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf> Acesso em: 09 fev. 2018.

UNITED KINGDOM-UK **.Terrorism Act 2000**. London, 2000. Disponível em : < https://www.legislation.gov.uk/ukpga/2000/11/part/I> Acesso em: 31 jan. 2018.

UNITED KINGDOM-UK **.Terrorism Act 2006** London, 2006. Disponível em : < https://www.legislation.gov.uk/ukpga/2006/11/part/1> Acesso em: 31 jan. 2018.

UNITED KINGDOM-UK. **National Cyber Security Strategy 2016-2021**, London, 2016. Disponível em: < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf> Acesso em: 09 fev. 2018.

UNITED KINGDOM-UK. **Pursue Prevent Protect Prepare:** The United Kingdom's Strategy for Countering International , Terrorism,London, 2009b. Disponível em: < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228907/7833.pdf> Acesso em: 09 fev. 2018.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC).**The use of the Internet for terrorist purposes** New York: United Nations, 2012**.**

UNITED STATES OF AMERICA - USA **.A National Strategy to Win the War Against Islamist Terror.** Washington, September 2016.Disponível em: < https://homeland.house.gov/wp-content/uploads/2016/09/A-National-Strategy-to-Win-the-War.pdf> Acesso em: 09 fev. 2018.

UNITED STATES OF AMERICA - USA. **The National Intelligence Strategy of the United Statesof America**. Washington, 2014. Disponível em : < https://www.dni.gov/files/documents/2014_NIS_Publication.pdf > Acesso em: 09 fev. 2018.

UNITED STATES OF AMERICA - USA. **International Strategy for Cyberspace:** prosperity, security and openness in a Networked World, Washington, May 2011a. Disponível:<https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> Acesso em: 09 fev. 2018.

UNITED STATES OF AMERICA - USA. **National Security Strategy** . Washington May 27, 2010. Disponível em: < http://nssarchive.us/NSSR/2010.pdf > Acesso em: 09 fev. 2018.

UNITED STATES OF AMERICA - USA. **National Security Strategy .**Washington**,** December 18, 2017a. Disponível em: < http://nssarchive.us/wp-content/uploads/2017/12/2017.pdf > Acesso em: 09 fev. 2018.

UNITED STATES OF AMERICA - USA. **National Strategy for Combating Terrorism.** Washington , September 2006. Disponível em : < https://www.hsdl.org/?view&did=466588> Acesso em: 09 fev. 2018.

UNITED STATES OF AMERICA - USA. **National Strategy for Combating Terrorism.** Washington , February 2003b. Disponível em: < https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf> Acesso em: 09 fev. 2018.

UNITED STATES OF AMERICA - USA. **National Strategy for Counterterrorism**. Washington , June 2011b.Disponível em : < https://obamawhitehouse.archives.gov/sites/default/files/counterterrorism_strategy.pdf> Acesso em: 09 fev. 2018.

UNITED STATES OF AMERICA - USA. **Summary of the 2018 National Defense Strategy of the Unites States of America:** sharpening the American Military's Competitive Edge**.**Washington , 2018. Disponível em : < https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf> Acesso em: 09 fev. 2018.

UNITED STATES OF AMERICA - USA. **The DoD Cyber Strategy** . Washington , April 2015.Disponível em : < https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf> Acesso em: 09 fev. 2018.

UNITED STATES OF AMERICA - USA. **The USA PATRIOT Act:** Preserving Life and Liberty. Washington, 2017. Disponível em: < https://www.justice.gov/archive/ll/highlights.htm> Acesso em: 30 jan. 2018**.**

UNITED STATES OF AMERICA - USA.**The National Strategy to Secure Cyberspace**. Washington , February 2003a.. Disponível em : < https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf> Acesso em: 09 fev. 2018.

USA CENSUS BUREAU. **E-Stats 2015: Measuring the Electronic Economy.** E15-ESTATS, Suitland, May 24, 2017. Disponível em: < https://www.census.gov/content/dam/Census/library/publications/2017/econ/e15-estats.pdf>Acesso em: 31 jan. 2018.

VERTON, Dan. Black Ice: **The Invisible threat of Cyberterrorism**. New York: McGrawHill/Osbornne. 2003.

WALTZ, Edward. **Information Warfare Principles and Operations.** London: Artech House, 1998.

WEIMANN, Gabriel, WWW.Al-Qaeda: The Reliance of al-Qaeda on the Internet, In: Centre of Excellence Defense Against Terrorism (The NATO Science for Peace and Security Program) (Ed) **Responses to Cyber Terrorism** Amsterdam: IOS Press, 2008, p.61-69

WEIMANN, Gabriel. **Terror on the Internet**: The New Arena, the New Challenges. Washington: US Institute of Peace Press. 2006.

WEIMANN, Gabriel. **Terrorism in Cyberspace**: the Next Generation. New York: Columbia University Press.2015.

WEIMANN, Gabriel. The sum of all fears? Oxfordshire**:** Taylor e Francis. **Studies in Conflict & Terrorism**, n.28, 2005, p. 129–149

WORLD DIGITAL LIBRARY-WDL. **Convenção para a Prevenção e Punição do Terrorismo**. [S.L]. 2017 . Disponível em:< https://www.wdl.org/pt/item/11579/> Acesso em: 04 de fevereiro de 2018.

WYKES, Maggie; HARCUS, Daniel. Cyber-terror: construction, criminalisation and control. In: JEWKES, Yvonne; YAR, Majid (eds.) **Handbook of Internet Crime.** Oregon: Willan Publishing, 2010, p.214-229

YANNAKOGEORGOS, Panayotis A. Rethinking the Threat of Cyberterrorism In: CHEN, Thomas; JARVIS, Lee; MACDONALD, Stuart. (Ed.) **Cyberterrorism**: Understanding, Assessment and Response. New York: Springer, 2014, p.43-62.

ZITTRAIN, Jonathan L. **The Future of the Internet and How to Stop It**. London: Yale University Press, 2008.