ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

INSTITUTO MEIRA MATTOS

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS MILITARES

ALESSANDRA CORDEIRO CARVALHO

# SECURITIZAÇÃO DO CIBERTERRORISMO E O POSICIONAMENTO ESTRATÉGICO DE DEFESA CIBERNÉTICA DOS ESTADOS UNIDOS DA AMÉRICA

Rio de Janeiro

2019

ALESSANDRA CORDEIRO CARVALHO

# SECURITIZAÇÃO DO CIBERTERRORISMO E O POSICIONAMENTO ESTRATÉGICO DE DEFESA CIBERNÉTICA DOS ESTADOS UNIDOS DA AMÉRICA

ESTUDOS DA PAZ E DA GUERRA

Texto apresentado como Dissertação de Mestrado do Programa de Pós-Graduação em Ciências Militares do Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, como requisito para a obtenção do título de mestre em Ciências Militares.

PROF. DR. LUIZ ROGÉRIO FRANCO GOLDONI

Rio de Janeiro

2019

C331s Carvalho, Alessandra Cordeiro

Securitização do ciberterrorismo e o posicionamento estratégico de defesa cibernética dos Estados Unidos da América. / Alessandra Cordeiro Carvalho. —2019.
101 f. : 3 il. ; 30 cm.

Orientação: Luiz Rogério Franco Goldoni.
Trabalho de Conclusão de Curso (Mestrado em Ciências Militares) —Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2019.
Bibliografia: f. 88-97.

1. SECURITIZAÇÃO 2. CIBERTERRORISMO 3. ESTADOS UNIDOS DA AMÉRICA 4. DEFESA CIBERNÉTICA 5. ESCOLA DE COPENHAGUE.

CDD 001.53

**ALESSANDRA CORDEIRO CARVALHO**

SECURITIZAÇÃO DO CIBERTERRORISMO E O POSICIONAMENTO ESTRATÉGICO DA DEFESA CIBERNÉTICA DOS ESTADOS UNIDOS DA AMÉRICA

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Militares da Escola de Comando e Estado-Maior do Exército, como, pré-requisito para a obtenção do grau de Mestre em Ciências Militares.

Aprovada em 17 de outubro de 2019.

**BANCA EXAMINADORA**

LUIZ ROGÉRIO FRANCO GOLDONI – Prof Dr – Presidente
Escola de Comando e Estado-Maior do Exército

GUILHERME MOREIRA DIAS – Prof Dr – Membro
Escola de Comando e Estado-Maior do Exército

PABLO SATURNINO BRAGA – Prof Dr – Membro
INSTITUTO BRASILEIRO DE MERCADO DE CAPITAIS

Ciente: _____
**ALESSANDRA CORDEIRO CARVALHO** – Postulante
Escola de Comando e Estado-Maior do Exército

# RESUMO

Uma das consequências dos esforços dos EUA para a manutenção de seu status de superpotência no pós-Guerra Fria foi a corrida científico-tecnológica. Esta disputada com as tradicionais potências europeias e os *players* recentes do cenário internacional como Japão, China e os chamados Tigres Asiáticos. O cenário gerado pelo evento terrorista de 11 de setembro de 2001 rompeu com a estrutura política que vinha sendo adotada nos níveis doméstico e internacional. A percepção de que o país era uma nação vulnerável aos ataques assimétricos transformou o posicionamento estratégico de defesa estadunidense. Ao passo que novas tecnologias e sistemas de informações tornavam-se essenciais, o setor cibernético também passou a ser percebido como vulnerável e suscetível a significativos ataques. Dentre as diversas variações de ameaças cibernéticas, o ciberterrorismo é capaz de promover danos letais à sociedade utilizando-se de meios cibernéticos. Compreendendo os riscos, os EUA empenharam-se na reestruturação estratégica da defesa cibernética do país, tanto por meio da criação de agências governamentais quanto de estratégias de defesa. Logo, buscar-se-á responder, na presente dissertação, como se deu a construção estratégica de defesa cibernética dos EUA. Como objetivo geral, visa-se averiguar a existência de um movimento de securitização do ciberterrorismo nos EUA. Para isso, tem-se como objetivos específicos discernir conceitualmente o ciberterrorismo das demais ameaças cibernéticas; analisar discursos securitizadores do ciberterrorismo; examinar as estratégias de defesa e as agências governamentais implementadas no setor cibernético; e, analisar o posicionamento estratégico de defesa cibernética dos EUA. A Teoria da Securitização da Escola de Copenhague servirá para verificar a securitização do ciberterrorismo nos EUA e analisar seu posicionamento sobre a defesa cibernética.

PALAVRAS-CHAVE: Securitização; Ciberterrorismo; Estados Unidos da América; Defesa Cibernética; Escola de Copenhague.

# ABSTRACT

One consequence of United States efforts to maintain its post-Cold War superpower status was the scientific-technological race. This disputed with the traditional European powers and recent players of the international scenario like Japan, China and the so-called Asian Tigers. However, the scenario generated by the terrorist event of September 11, 2001, broke with the political framework that was being adopted at domestic and international levels. The perception that the country was a nation vulnerable to asymmetric attacks transformed the strategic position of US defense. As new technologies and information systems became essential, the cyber sector was also perceived as vulnerable and susceptible to significant attacks. Among the various variations of cyber threats, cyberterrorism is capable of causing lethal damage to society using cyber means. Understanding the risks, the US has engaged in the strategy restructuring of the country's cyber defense, both through the creation of government agencies and defense strategies. Therefore, in the present dissertation, there will be answers to how the strategic of cyber-defense of the USA was built. As a general objective, the main focus is to investigate the existence of a cyberterrorism securitization movement in the US. For this purpose, as specific objectives, this dissertation will discern the concept of cyberterrorism and other cybernetic threats; analyze cyberterrorism securitization speeches; examine defense strategies and government agencies implemented in the cyber sector; and, analyze the strategic positioning of US's cyber defense. The Copenhagen School's securitization theory will serve to verify the securitization of cyberterrorism in the US and to analyze its position on cyber defense.



KEY WORDS: Securitization; Cyberterrorism; USA; Cyber Defense; School of Copenhagen.

## LISTA DE ILUSTRAÇÕES

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| CNCI | *Comprehensive National Cybersecurity Initiative* |
| DoD | *Department of Defense* |
| EUA | Estados Unidos da América |
| ESI | Estudos de Segurança Internacional |
| NSA | *National Security Agency* |
| OTAN | Organização do Tratado do Atlântico Norte |
| TNP | Tratado de Não Proliferação de Armas Nucleares |
| USA | United States of America |
| USCYBERCOM | *U. S. Cyber Command* |

# SUMÁRIO

## INTRODUÇÃO

A conjuntura internacional, posterior à Guerra Fria, pautou-se sobre a não mais existência de uma ameaça potencial que desafiasse a soberania dos Estados. Transformações em diversas escalas da sociedade apontaram para o desenvolvimento de abordagens e ações opostas ao que fora praticado até então. A denominada 'Revolução da Informação' entrou em foco, configurando-se mediante rápida ascensão das tecnologias da informação e comunicações, modificando a percepção de segurança e defesa dos Estados, alterando as relações comerciais e financeiras e possibilitando a intensificação da interação social mundial.

Esse último elemento conferiu características agravantes ao contexto das ameaças. A globalização e a inter-relação das tecnologias nas atividades cotidianas, ao conceder tanto facilidades à sociedade quanto desafios aos Estados, permitiram que novas ameaças surgissem atreladas às antigas. A necessidade de transposição do enfoque das ameaças tradicionais para as ameaças contemporâneas, também impôs atenção para a manifestação de novos atores internacionais. Com isso, criaram-se novos conceitos para corresponder à acelerada transformação tecnológica na sociedade, assim como, para permitir compreensões sobre a dinâmica mundial, possibilitando a inclusão de novos atores e ameaças nas análises das relações internacionais.

Nos Estados Unidos da América (EUA), na década de 1990, as agendas de segurança e defesa voltaram-se principalmente para as políticas contra o narcotráfico, o crime organizado e as ameaças tradicionais interestatais (FERREIRA, 2014). No entanto, a virada do século, acompanhada do gradativo tecnológico, permitiu que novos componentes fossem acoplados às ameaças tradicionais. Mesmo que não relacionadas estritamente com a tecnologia, as novas ameaças oferecem desafios aos Estados que podem ser potencializados ao incluir o elemento em questão. Ainda assim, isto não significa que essa característica ameaça se sobreponha às outras. Porém, indica que, como ela se desenvolve e evolui, o posicionamento estratégico de defesa dos estados deve acompanhar esse processo.

À exemplo, os ataques do 11 de setembro de 2001 demonstraram como determinados eventos podem causar uma ruptura política, econômica e social em detrimento de uma nova ameaça global – que neste caso é o terrorismo[1]. Com a comunidade internacional e a população

[1] Por mais que o terrorismo seja um fenômeno que percorre os séculos, as ondas do terrorismo, propostas por David Rapoport (2002), indicam que, até a terceira onda, as revoluções e os ataques eram direcionados aos representantes políticos e combatentes que oferecessem ameaças à determinada comunidade. Entretanto, o terrorismo atual visa ataques que atinjam a população civil e não-combatente e, por isso, pode ser considerado como um novo tipo de terrorismo.

norte-americana envoltos pelos ataques, os EUA passaram a serem percebidos como nação vulnerável a ameaças externas. Na tentativa de reverter a desestabilização gerada, como reação imediata, instaurou-se um posicionamento político unilateralista, integrado à comoção global e à construção de alianças a favor da chamada "Guerra Global ao Terror"[2] (BARBOSA, 2002). Proposta como uma estratégia emergencial para o combate ao terrorismo, Walter Mead (2006, p. 123) argumenta que, posteriormente, a decisão política assertiva demonstrou que o posicionamento permitiu à "administração prosseguir com seu projeto de reestruturação da política externa norte-americana".

Nos discursos proferidos por George W. Bush após os ataques[3], evidenciou-se o pensamento tradicional da guerra no que se concerne ao combate ao terror. Entretanto, alguns autores argumentam que o emprego do termo 'guerra' ao contexto fez-se inadequado. Tratando-se o terrorismo de um conceito em processo de discussão, caracterizado como um método de ação, o fenômeno foge do escopo no qual estariam os conflitos armados entre Estados, desapropriando a aplicação das leis tradicionais da guerra (SOUZA et al, 2014). Deste modo, pode-se dizer que a recorrência preventiva e as medidas emergenciais tomadas pelo governo norte-americano, além de apresentarem vestígios de securitização, demonstram como os EUA reverteram sua estratégia de defesa nacional para a redução das suas vulnerabilidades em dado momento.

> Embora a Guerra Contra o Terror tenha sido diretamente endereçada a grupos terroristas transnacionais, as ações adotadas pelos Estados para combatê-los expôs profundas tensões, limitações e contradições (pré)existentes na sociedade internacional. [...] Mas o mais importante significado da Guerra Global Contra o Terror reside no fato de que essa política foi elaborada tendo em vista tanto os Estados da Sociedade Internacional quanto os terroristas (VADELL; LASMAR, 2015, p. 3).

Diversos fatores podem estar associados ao direcionamento dos EUA como alvos do terrorismo nesse cenário, dentre eles, a postura política e o protagonismo econômico norte-americano no mundo. Todavia, as facilidades oferecidas por uma nova conjuntura, estabelecida pelo surgimento de um domínio cibernético ainda em processos de adequação político e

[2] Evidenciou-se nos discursos realizados por George W. Bush, logo após os atentados, o combate ao terrorismo como uma "luta entre o bem e o mal". Foi declarado pelo Presidente que os Estados que não estivessem em apoio aos EUA estariam à favor dos terroristas e que, dessa forma, poderiam sofrer retaliações como tal (BARBOSA, 2002).

[3] "Americanos estão se perguntando: Como vamos lutar e vencer essa guerra? Nós vamos direcionar todos os recursos sob nosso controle; todos os meios de diplomacia, todas as ferramentas de inteligência, todos os instrumentos de aplicação da lei, toda influência financeira e toda arma de guerra necessária para a desorganização e derrota da rede global de terror" (FOLHA DE SÃO PAULO, 2001). Ainda: "Não me esquecerei desta ferida causada ao nosso país ou daqueles que a infligiram. Não vou me render; não vou descansar; não vou ceder em travar esta batalha pela liberdade e pela segurança do povo norte-americano" (MEAD, 2006, p. 123).

jurídico, permite que desconhecidas ações ilegais sejam realizadas no ciberespaço. Tendo em vista que os EUA são os maiores detentores de redes de computadores e de sistemas interconectados do mundo, ataques a esta estrutura poderiam gerar danos expansíveis à escala global.

> A crescente dependência das nossas sociedades na tecnologia da informação criou uma nova forma de vulnerabilidade, dando aos terroristas a chance de possuir metas que de outra forma seriam totalmente inacessíveis, como sistemas de defesa nacionais e sistemas de controle de tráfego aéreo. Quanto mais desenvolvido tecnologicamente for um país, mais vulnerável torna-se a ataques cibernéticos contra sua infraestrutura (WEIMANN, 2004, p. 2, tradução nossa).

As ameaças cibernéticas podem distinguir-se entre motivações, atores, objetivos, ações, e danos; porém, algumas caracterizam-se por manterem seus atos apenas no nível cibernético. O ciberterrorismo, no entanto, sendo uma ameaça que tem também por finalidade promover danos letais por intermédio da utilização do espaço cibernético, requer uma atenção aprimorada. Não se tratando de um fenômeno recente, o ciberterrorismo é posto em pauta desde o final da década de 1990 (COLLIN, 1997; POLLITT, 1998) e, assim como ocorre no terrorismo, não há uma definição de ciberterrorismo amplamente aceita (CHEN, 2014).

Levando-se em consideração que o termo pode apresentar atualmente dois vieses de compreensão, Giacomello (2014) os separa em ciberterrorismo 'Hard Rock' e ciberterrorismo 'Lite'. O primeiro diz respeito aos ataques terroristas ocasionados por meios cibernéticos às infraestruturas nacionais essenciais, na intenção de gerar vítimas – como, por exemplo, o bloqueio de água e energia. O segundo compreende as organizações terroristas que utilizam a internet para fins de comunicação, recrutamento e divulgação de ações terroristas[4].

Neste sentido, Giacomello (2014) defende que apenas o tipo 'Hard Rock' deve ser apontado como ciberterrorismo, uma vez que são ações terroristas no ciberespaço que visam causar danos em sistemas e redes de computadores, expandindo-se aos danos virtuais e físicos. Enquanto que, as ações de recrutamento e propagandas terroristas deveriam ser enquadradas como divulgações do terrorismo através da Internet. Para fins desta pesquisa será utilizado o primeiro viés de entendimento.

> Ataques pelo ciberespaço devem ter um componente 'terrorista' para ser rotulado de ciberterrorismo. Os ataques devem instaurar o terror como comumente entendido (ou

[4] Mesmo que as redes de computadores e a Internet façam parte da mesma estrutura, essa possui uma característica especial: além da estrutura física do computador (*hardware*) e dos *softwares* – comum aos dois –, inclui a troca de informações de material humano, ou seja, permite a linguagem humana por intermédio das redes (GIACOMELLO, 2014).

> seja, resultar em morte e/ou em grande escala de destruição), e eles devem ter uma motivação política. No que diz respeito à distinção entre o uso terrorista da tecnologia da informação (ou seja, para fins de comunicação, propaganda, etc.) e terrorismo envolvendo tecnologia de computadores como arma/alvo; somente este último pode ser definido como ciberterrorismo. O terrorista 'usar' computadores como facilitador de suas atividades, seja propaganda, comunicação ou outros fins, é simplesmente: 'usar' (CONWAY, 2003, p. 5, tradução nossa).

O ciberterrorismo é comumente interpretado como uma ameaça politicamente motivada. Sendo composto por atores não estatais e individuais, possui como objetivo a desestabilização de governos por intermédio de intimidação popular. Suas ações têm por finalidade gerar terror e violência contra civis, mediante a realização de ciberataques contra sistemas de informações (POLLITT, 1998; DENNING, 2000; KENNEY, 2015). Todavia, para ser considerado ciberterrorista, os ataques devem resultar em danos físicos. Ataques às infraestruturas críticas, por exemplo, podem prejudicar fisicamente determinada população – até mesmo causar mortes –, além de gerar graves prejuízos ao Estado. No mais, os ciberterroristas vislumbram exibição e publicidade para o alcance de seus objetivos, assim como ocorre com o terrorismo (COLLIN, 1997).

É preciso salientar que a inexistência histórica de ataques ciberterroristas confirmados, até o presente momento, não impede a ocorrência de um dano potencial (CLARKE; KNAKE, 2010). Considerando essa afirmativa, cabe acrescentar que Biazatti (2015) afirma que dois eventos podem ter tido características ciberterroristas. O primeiro relaciona-se com o grupo terrorista *Al Qaeda* – ao serem encontradas informações e instruções para a execução de ações cibernéticas em computadores pertencentes ao grupo, no ano de 2002 – e o segundo refere-se ao controle da rede social do Comando Central das Forças Armadas dos EUA, para a inclusão de conteúdo de divulgação terrorista, em 2015. Contudo, conforme mencionado anteriormente, esses dois eventos não podem ser considerados como ciberterroristas, por conterem o objetivo de utilizar do ciberespaço como uma forma de comunicação e não como uma ferramenta de ataque.

O ciberterrorismo pode apresentar métodos, ferramentas e modelos de ataques similares ao do crime cibernético (MAIMON; TESTA, 2017). Os cibercrimes mais comuns são as invasões de sistemas, deflagração de sites, ataques de DDoS – que negam o acesso dos usuários às redes de computadores – e a distribuição de softwares maliciosos. O que diferencia o ciberterrorismo do crime cibernético é que, o primeiro possui motivações políticas e ideológicas que visam a propagação de suas mensagens, por meio da promoção de danos digitais e físicos

por ataques no ciberespaço. O segundo motiva-se a realizar atos ilícitos para fins privados com o objetivo de ganhos econômicos (ZUCCARO, 2011).

A dificuldade de identificação dos autores dos ataques e suas motivações permeia os mais variados tipos de ciberameaças. De forma geral, os ataques cibernéticos são tratados perante as leis como originalmente criminosos, para facilitar os processos de identificação e atribuição de responsabilidade. Todas as atividades ilícitas realizadas por intermédio do uso da Internet – como chantagens, divulgações de informações privilegiadas, pirataria, recrutamento de pessoas para grupos criminosos e terroristas, entre outros – e/ou do ciberespaço, como ferramenta para ataques contra redes de computadores e sistemas de informações, são considerados crimes praticados por meios cibernéticos. Outro fator é que, pelas ameaças cibernéticas em geral se tratarem de atingir sistemas particulares, facilita-se o reconhecimento como crime, na intenção de ser possível sentenciá-lo (FOLTZ, 2004).

É importante elucidar que mesmo que as atividades ilegais no ciberespaço estejam ambientadas como crimes para a legislação, as ameaças cibernéticas podem ser caracterizadas de forma específica. A partir da concepção de que as investigações sobre os eventos cibernéticos podem conter diversidades que dificultam a identificação, a motivação e, logo, o julgamento dos ataques, determina-se que as redes e sistemas de informações podem ser acessadas por diversas fontes. Logo, a motivação e os atores por trás de um ciberataque podem ser variados. Portanto, tratar todas as ameaças cibernéticas apenas como cibercrime pode tornar as análises generalizadas.

É evidente que o acelerado crescimento tecnológico e o sucessível surgimento de novos atores no Sistema Internacional carecem de regulação e legislação adequada que acompanhem tal processo. Todavia, o avanço das discussões em torno da conceituação e variação das ameaças cibernéticas indica a existência de particularidades que podem contribuir para as análises e para a indexação dos conceitos no âmbito legislativo. Caberá, como parte da dissertação, apresentar as características específicas do ciberterrorismo, da guerra cibernética, do crime cibernético e do ativismo cibernético, com a finalidade de ilustrar elementos exclusivos a eles.

Os apontamentos anteriores assinalam a percepção que as ameaças cibernéticas oferecem aos Estados a necessidade de serem criadas estratégias e políticas de defesa nacionais, assim como, organizações governamentais capazes de regular, proteger e controlar o espaço cibernético. Visto isso, buscar-se-á responder na dissertação a seguinte questão: Como se deu a construção do posicionamento estratégico de defesa cibernética dos EUA?

Para isso, tem-se como objetivo geral da pesquisa averiguar a existência de um movimento de securitização do ciberterrorismo nos EUA. Como objetivos específicos, visa-se discernir conceitualmente o ciberterrorismo das demais ameaças cibernéticas; identificar aspectos teóricos que compreendam o ciberterrorismo na teoria da securitização; identificar discursos securitizadores do ciberterrorismo; examinar as políticas de defesa e as agências governamentais implementadas para o setor cibernético; e analisar o posicionamento estratégico de defesa cibernética dos EUA.

A atual dificuldade dos EUA em reduzir suas vulnerabilidades e o risco de contra-atacar as ameaças está no fato de que as conexões cibernéticas estadunidenses são, em sua grande maioria, de propriedade privada. Isto não ocorre com a China e com a Rússia, por exemplo, pois estes possuem suas redes e sistemas pouco interconectados com outros países e são permeados por um maior controle governamental, oferecendo favoráveis condições defensivas. Pela complexa interdependência tecnológica dos EUA, são desafiadores os processos de desenvolvimento de uma defesa cibernética nacional. Principalmente porque, assim como os Estados, a população conhecedora dos artifícios que podem ser gerados por meio do ciberespaço, de modo geral, também possui acessos e vantagens cibernéticas (DUIC, 2017).

Por essas razões, as ameaças cibernéticas demandam rápidas ações estatais para a proteção da infraestrutura crítica, posto que podem comprometer a segurança nacional. Portanto, é compreendida a necessidade de serem criados novos mecanismos de segurança e defesa contra as ciberameaças mediante o desenvolvimento de políticas e estratégias no setor cibernético para a proteção do Estado. A importância da análise em questão encontra-se em como e em que contexto são executados tais mecanismos, para a verificação da existência de uma securitização do ciberterrorismo em prol da segurança e defesa do setor cibernético norte-americano.

Conceitualmente, entende-se securitização como o processo de medida imediata ao surgimento de uma ameaça existencial ao Estado, sendo necessária uma tomada de ação emergencial que pode tender a burlar as leis e os procedimentos políticos vigentes (BUZAN et al, 1998). Logo, securitização cibernética pode ser interpretada como o processo de ação emergencial contra uma ameaça em potencial, no espaço cibernético. Para constituir a análise deste processo, a Escola de Copenhague mostra-se ideal para a verificação do processo da securitização do ciberterrorismo, por já oferecer o método adequado proposto pela Teoria da Securitização. No mais, tal corrente é também capaz de tratar das questões dos atores não-estatais e atores individuais como ameaça nas relações internacionais – os quais obterão foco no presente estudo.

A teoria será abordada de modo a examinar se há vestígios de securitização do ciberterrorismo nos EUA. A teoria é dividida em três categorias de análise: dos discursos, das unidades de segurança e dos setores de segurança. As unidades de segurança são divididas em objeto referente, atores securitizadores e atores funcionais; e os setores de segurança são separados em militar, político, econômico, societal e ambiental. Esses elementos serão aplicados aos discursos para o reconhecimento de um estado de securitização da ameaça do ciberterrorismo. Para a análise dos discursos e para a identificação daqueles que abordam os temas relacionados a cibernética, será utilizado o *software* NVIVO 11. Logo, a pesquisa terá caráter qualitativo, mediante o método dedutivo de análise e síntese.

Para o ponderamento dos termos que compõem o ciberterrorismo desde sua origem, assim como suas semelhanças e diferenças em relação às demais ameaças cibernéticas, serão utilizadas fontes bibliográficas que dissertem sobre o tema. A fim de verificar a incidência de ataques cibernéticos aos EUA, bem como suas principais características e motivações, serão utilizados os sítios eletrônicos governamentais dos EUA de combate as ameaças cibernéticas.

Para a análise dos discursos, serão apontados aqueles proferidos a respeito do terrorismo, do setor cibernético, do espaço cibernético, das ameaças cibernéticas e, especificamente, do ciberterrorismo. Estas informações encontram-se disponíveis no site da Casa Branca e em órgãos adjacentes ao governo. Serão priorizados na análise dos setores de segurança os níveis político e militar, em busca da identificação das políticas, estratégias e órgãos governamentais criados ou reestruturados para a defesa cibernética. Constituirão como fontes os sítios eletrônicos das agências de segurança e defesa dos EUA, como o *Department of Defense* (DoD), a *National Security Agency* (NSA), a *U.S Cyber Command* (USCYBERCOM), entre outros.

Por fim, a dissertação será dividida em três capítulos. O primeiro abordará a discussão em torno do conceito de ciberterrorismo, sendo destrinchados seus termos componentes. Para isso, será compreendida a evolução do conceito de espaço cibernético em acompanhamento ao crescente tecnológico, assim como, os apontamentos sobre os desafios que o ciberespaço oferece atualmente aos Estados. Serão apresentadas as variações conceituais do terrorismo, além de um breve histórico do fenômeno ao longo dos séculos, para chegar a uma contextualização contemporânea do termo. As demais ciberameaças serão definidas de forma a identificar suas características peculiares que se diferem e se assemelham ao ciberterrorismo, sendo elas a guerra cibernética, o ativismo cibernético e o crime cibernético.

De caráter teórico e metodológico, o segundo capítulo versará sobre a Teoria da Securitização – como metodologia criada pela Escola de Copenhague – com o propósito de se

explicar um estado de securitização. No entanto, antes de adentrar-se às abordagens da Escola, será realizada uma breve apresentação dos debates teóricos do período da Guerra Fria, de forma a contextualizar o leitor sob quais premissas as correntes ampliadoras-aprofundadoras posteriores foram embasadas e contrárias. Serão apresentadas, ainda, as colaborações conceituais da corrente construtivista, tendo em vista o contexto em que surgiu e suas maiores contribuições teóricas para os Estudos de Segurança Internacional.

Por meio disso, visa-se apresentar brevemente as semelhanças e as disparidades do construtivismo com a Escola de Copenhague no que tange à amplificação do caráter da ameaça, assim como se as correntes conseguem explicar o fenômeno do ciberterrorismo em sua totalidade. Posteriormente, será esmiuçada a Teoria da Securitização e os elementos que a compõem, para a compreensão e utilização do método no capítulo seguinte.

No terceiro capítulo, será aplicada a Teoria da Securitização como método de análise e verificação do processo da securitização do ciberterrorismo na agenda de defesa dos EUA. Para isso, serão apresentados e analisados os discursos presidenciais, pós-11 de setembro, sobre as palavras-chave: ciber, cibersegurança, ciberdefesa, ciberameaça, ciberataque, ciberterrorismo, hacker e terrorismo. Após analisados os discursos, serão aplicadas as unidades de análise de segurança para a identificação do objeto referente, do ator securitizador e do ator funcional. Logo, serão apresentados os documentos estratégicos e a agencia militar elaborada pelos atores funcionais, com o objetivo de apontar o posicionamento estratégico de defesa cibernética dos EUA.

# 1. CONTEXTO DAS AMEAÇAS CIBERNÉTICAS

O término da Guerra Fria representou rupturas em diversos setores do globo. Dentre eles, o setor nuclear – predominante no sistema bipolar e que concedeu inúmeras ferramentas de guerra aos Estados nesse período –, afastou-se do imperativo militar, tendo em vista as discussões políticas acerca dos malefícios existenciais de uma guerra nuclear. Neste sentido, a mudança de conjuntura alterou paralelamente as atenções estatais para o desenvolvimento de tecnologias que não fossem exclusivamente nucleares. Assim, ao passo que o cenário internacional se recuperava, o progresso da Tecnologia da Informação e Comunicações (TIC) permitiu que novas abordagens fossem inseridas na sociedade.

O domínio cibernético passou a fazer parte de uma integração tecnológica inserida aos mecanismos que já existiam. Com o processo globalizante, o crescente uso da Internet transformou a lógica convencional conhecida até então. Em contrapartida, a intensificação na transferência de informações e de transações sociais, econômicas e políticas por meio do espaço cibernético, impulsionou o aumento das relações sociais na mesma proporção que criou novos desafios aos Estados.

A estreita aproximação das relações entre o mundo físico e o virtual proporcionou à sociedade um "sentimento de liberdade absoluta, de navegabilidade e mobilidade virtual sem precedentes e sem sujeição hierárquica" (MARTINS, 2012, p. 35). As novas tecnologias não apenas beneficiaram o corpo social, como foram capazes de estimular novos atores no cenário global. Cabe reforçar que, ao tempo em que os Estados evoluíam suas capacidades tecnológicas, quantidades de indivíduos especializavam-se em questões referentes ao novo domínio, tanto para ações positivas quanto negativas.

Esses, ao obterem conhecimentos capazes de criar, direcionar e expandir o alcance de ciberataques, passaram a possuir capacidades anteriormente particulares ao Estado. Por terem a possibilidade de amplificar os danos econômicos, sociais e políticos, os ataques cibernéticos inseriram novas formas de causar danos físicos e virtuais, muitas vezes ligadas às infraestruturas críticas nacionais. Por estas serem controladas por sistemas e redes interconectadas, expandiram-se as probabilidades que eventos de diversas naturezas ocorram, em função do aumento das vulnerabilidades operacionais.

No entanto, quando as ameaças tradicionais se encontram no nível estatal, os poderes militar e político assumem a capacidade de contrabalanceá-las, de forma a combatê-las ou evitá-las. A problemática surge quando atores não-estatais e individuais assumem o caráter de ameaça mediante realização de ataques por meios cibernéticos. A posição assimétrica transfere

particularidades à segurança e à defesa nacional. Isto porque um ataque cibernético de qualquer natureza pode comprometer o Estado ao "interromper os serviços essenciais do governo, ameaçar as operações de negócios, corroer a confiança do público em transações financeiras e interromper as comunicações eletrônicas" (CHERTOFF, 2008, p. 480).

Portanto, serão apresentadas neste capítulo as ameaças cibernéticas e seus aspectos componentes. O ciberterrorismo, como componente elementar da pesquisa, obterá maior atenção estrutural. As demais ciberameaças serão apresentadas de forma a contextualizar o leitor e determinar o que não se enquadra no conceito de ciberterrorismo. Deste modo, serão desenvolvidos também os conceitos de guerra cibernética, de crime cibernético e de ativismo cibernético. Por fim, a construção do aparato conceitual deste capítulo tem o propósito de oferecer embasamento para os níveis de análise necessários aos capítulos posteriores, assim como proporcionar conhecimento sobre as discussões em torno das definições das ameaças cibernéticas.

## 1.1 Arcabouço conceitual do ciberterrorismo

O termo 'terror cibernético' surgiu em meados dos anos 1980 (AKHGAR et al, 2016), juntamente com o crescimento tecnológico e com a discussão a respeito da emergente sociedade da informação (WEIMANN, 2004). Apenas ao final da década de 1990 que a expressão 'ciberterrorismo' foi abordada como um conceito (COLLIN, 1997; POLLITT, 1998). O "medo do desconhecido", apontado por Mark Pollit (1998), ao referir-se ao terrorismo e a tecnologia no final do século XX, fortaleceu o início dos debates contra essa potencial ameaça (POLLIT, 1998; CONWAY, 2011). No entanto, ainda não há uma discussão conceitual finalizada sobre o termo. Em vista disso, para serem compreendidas as mais variadas definições de ciberterrorismo, primeiramente, serão analisados os termos que o compõem. São eles o espaço cibernético e o terrorismo.

### 1.1.1 Desafios do espaço cibernético

Conforme evoluem as interações no mundo real, geram-se simultâneas alterações no domínio cibernético. Ao considerar o progresso dos instrumentos tecnológicos hodiernos, tem-se no espaço cibernético uma ampla área de interconexão que permeia os mais variados tipos de atores, informações e infraestruturas. No mais, agregam-se possibilidades ao ciberespaço

que permitem reconhecê-lo como ferramenta de ataque, transferindo-o à esfera de execução de ações militares.

Daniel Kuehl (2017) afirma que o espaço cibernético representa o quinto domínio de operação militar, juntamente aos já existentes terra, mar, ar e espaço – por mais que este ainda esteja sobre processo de estruturação. Ao definir que "seus usuários variam de estados-nações inteiros e seus elementos organizacionais e comunidades que chegam aos indivíduos solitários e grupos transnacionais amorfos que não podem professar lealdade a qualquer organização tradicional ou entidade nacional" (KUEHL, 2017, p. 28, tradução nossa), o autor entoa uma gama de possibilidades e componentes de ações no espaço cibernético.

A progressão das tecnologias inovadoras e dos meios de comunicações passaram a dispensar a distinção entre o online e o off-line, uma vez que o espaço físico tornou-se cada vez mais interligado com as conexões do ciberespaço (KOOPS, 2016). Além de ser estimado como ferramenta de ação, o ciberespaço é o elemento principal que permeia as informações e as comunicações em diversas atividades do cotidiano. No entanto, a veemente interconexão entre unidades e indivíduos no espaço cibernético – por intermédio das redes e sistemas de computadores –, ao passo que gerou maiores quantidades de fluxos sociais, institucionais e governamentais, em consequência, acarretou no crescimento de ações ilegais no novo domínio (MILICEVIC, 2008; FENZ, 2005).

Neste sentido, a globalização não apenas modificou os processos de interação humana como, também, propiciou o avanço das novas ameaças. Uma vez que as ações cibernéticas podem surgir de qualquer ambiente e entre os mais variados atores, a capacidade de promoção de ataques encontra-se nos maiores possuidores de conhecimento e informações privilegiadas (DUIC et al, 2017). De acordo com Cornish et al (2010), a diversidade permite que vários atores explorem as capacidades e realizem atos ilícitos no ciberespaço. Dessa forma, as mais diferentes motivações e ideologias podem ser encontradas por trás da natureza dos ataques. Logo, é tão necessário o entendimento sobre as características do ciberespaço como a identificação dos seus desafios.

Dentro desse aspecto, o espaço cibernético pode ser definido como uma ferramenta capaz de permear ataques cibernéticos direcionados, além de potencializar os danos promovidos por ameaças já existentes. Este apontamento pode ser verificado sob a égide do elemento da dissertação em questão – o ciberterrorismo – ao se verificar que as peculiaridades inerentes ao ciberespaço potencializam as capacidades e efeitos de ataques terroristas.

Entende-se que, da mesma forma que o espaço cibernético é capaz de promover novas oportunidades tecnológicas que facilitam a interação social, empresarial e governamental;

também incita o surgimento de novas ameaças. A natureza interconectada e transnacional desse domínio favorece a aparição de novos atores interessados em conduzir ataques cibernéticos fortemente motivados que podem gerar danos a sistemas e redes de computadores interconectados (WELLS et al, 2016).

Compreende-se que o ciberespaço é constantemente palco de ataques gerados por espiões, ladrões e sabotadores, capazes de invadir sistemas de computadores, roubar dados pessoais e segredos comerciais, interromper serviços, realizar transações fraudulentas e sabotar dados e sistemas. Por isso, as ciberameaças apresentam desafios consideráveis para a segurança dos Estados (DENNING, 2000). Afinal, os ataques cibernéticos possuem aspectos heterogêneos e complexos pautados pelo anonimato e a não detecção das motivações (WARF; FEKETE, 2015). Além disso, podem gerar graves prejuízos econômicos, políticos, sociais e ambientais, possíveis de serem transmitidos para outros sistemas interconectados e interdependentes (CHERTOFF, 2008).

Pelo caráter multifacetado, o espaço cibernético pode ser utilizado e dividido como: fonte, ferramenta e alvo de conflito. As novas disputas nas esferas dos direitos autorais e propriedade digital, liberdade de expressão, entre outros, são consideradas fontes de conflito. Como ferramenta de conflito, tem-se todos os tipos de confrontos ocorridos no ciberespaço, assim como a transmissão de informações para a coordenação de ações e comunicações. Por fim, como alvo de conflito estão todos aqueles envolvidos em combates cibernéticos nos níveis estatal, não-estatal e individual (BERSON; DENNING, 2011).

Tanto a utilização do ciberespaço como ferramenta e alvo de conflitos faz parte do escopo das ameaças cibernéticas. O primeiro caso enquadra-se na identificação das comunicações e atos que serão estabelecidos. O último, engloba a execução do ataque. Portanto, o ciberespaço permeia interações entre as unidades e os indivíduos capazes de sofrer influência ou interferência de um ao outro e oferece uma gama de possibilidades de ações motivadas que podem ser traduzidas em ameaças cibernéticas.

Além de conceder facilidades aos indivíduos, o espaço cibernético é ainda caracterizado pelo possível anonimato conferido aos seus agentes. Esse fator dificulta a investigação da motivação dos ataques, as características específicas da ameaça e a localização do indivíduo ou grupo responsável (RIBEIRO; RIVEIRA, 2014). Tendo em vista este aspecto, o espaço cibernético se apresenta como ferramenta atrativa também para os terroristas ao propiciar maior alcance dos seus objetivos (BRENNER, 2016). Logo, ataques dessa natureza podem gerar prejuízos humanos e estruturais ao Estado (COLLIN, 1997).

Assim, estratégias que eram anteriormente projetadas para a manutenção da segurança e da defesa estatal tornaram-se defasadas no âmbito cibernético. Isto é, a velocidade de interconexão entre o espaço cibernético e as tecnologias, as redes de computadores e os sistemas operacionais ultrapassam a capacidade de prevenção contra as novas oportunidades de ataques. Os esforços concentrados em solucionar as vulnerabilidades do ciberespaço encontram-se obsoletos em relação ao surgimento constante de novas ameaças no mundo contemporâneo (KILGER, 2015; DUIC et al, 2017).

A problemática encontra-se nos interesses que as ameaças cibernéticas buscam atingir, podendo ser desde ganhos financeiros até a promoção de mortes em grande escala. A utilização generalizada do ciberespaço pode oferecer facilidades aos agentes motivados à determinadas causas, além de gerar capacidades que anteriormente pertenciam unicamente à esfera estatal. Neste sentido, os desafios de redução das vulnerabilidades e proteção do ciberespaço pelo Estado são dificultados pela existência de ataques em diversos níveis estruturais. Pelo déficit de comunicação e informação à população civil envolvida, muitos dos ataques são direcionados aos sistemas hospitalares, às redes educacionais e aos órgãos governamentais. Esse aspecto acarreta no aumento de vítimas ao passo que prejudica o esforço de defesa cibernética.

Outro fator agravante é que os desafios cibernéticos podem permear tanto a esfera pública como a privada. Dessa forma, a consolidação da segurança das redes e sistemas acaba por ser executada de forma particular e diferenciada. Esse fator afeta diretamente a segurança do Estado, principalmente, ao serem conduzidos ataques generalizados às instituições privadas como bancos internacionais e empresas de energia, na qual as políticas de segurança cibernética não são unicamente de responsabilidade estatal. Portanto, a caracterização das ameaças cibernéticas globais se faz necessária na forma de informar e alertar sobre que categoria os ataques poderão ser julgados e legislados. Essa emergência conceitual será analisada no capítulo a partir dos tópicos de ciberterrorismo, guerra cibernética, crime cibernético e ativismo cibernético.

### 1.1.2 Terrorismo: breve histórico e definições

A variedade de perspectivas ideológicas é um dos fatores que dificulta a compreensão do conceito de terrorismo (CHALIAND; BLIN, 2007). Podem ser atribuídos ao conceito o caráter simbólico, a violência contra alvos não combatentes, a promoção do medo, o instrumento de propaganda, a intimidação e coerção de um público-alvo e o nível de combate em caráter assimétrico (SCHMID, 2011). Pelo fato de não existir um consenso amplamente

reconhecido do termo, tem-se a interpretação do terrorismo como uma comunicação política, que se utiliza da violência para transmitir avisos direcionados a alvos pré-estabelecidos (CRENSHAW, 2015).

A disseminação de mensagens visa provocar a intimidação das sociedades e a desestabilização política, na intenção de afetar a segurança nacional, internacional, pública e humana. A busca pela propagação do medo e do terror é gerada por intermédio de atos violentos brutais, os quais podem ter inúmeras possibilidades de objetos de ataque. Não apenas, os atos de terrorismo são reconhecidos por ocorrerem em ambientes civis geralmente populosos que podem gerar danos em ampla magnitude (STEPANOVA, 2008; SCHIMD, 2011).

Com motivações e ideologias complexas, o terrorismo refere-se a uma conduta ilegal ou criminosa que opera por meio da violência indiscriminada (CONTE, 2010). Para Steve Best e Anthony Nocella (2004), os terroristas não visam apenas a intimidação dos seus alvos pela violência. A intenção se concentra em promover ataques que causem danos psicológicos, físicos e letais aos civis, de forma a incitar o terror generalizado e modificar o comportamento da sociedade. É a partir do uso da violência unilateral que o interesse político da ameaça alcança proporções que interferem diretamente na segurança e no funcionamento da infraestrutura civil e, logo, do Estado.

Segundo Ariel Merari (2007), existem três formas de se classificar o terrorismo. A primeira diz respeito a atos violentos de grupos contra Estados. A segunda refere-se à opressão de um Estado contra seus próprios cidadãos. E, por último, atos de guerra terroristas entre Estados. Leva-se em consideração, no entanto, que um Estado não deve ser enquadrado sob o caráter terrorista. As violências estatais induzidas a intimidar governos e populações devem ser situadas no conceito de guerra ou abuso de poder, delimitando a ameaça de terrorismo ao âmbito não estatal (STOHL, 2014).

De forma sintetizada, portanto, o terrorismo é um fenômeno político promovido por atores não-estatais e individuais, na busca de intimidar e desestabilizar governos, por meio da incitação da violência e do terror contra a população civil. Os meios de provocação de ameaças podem variar de acordo com o objetivo almejado e com o propósito de propagação de determinada mensagem. Geralmente, os métodos visam influenciar o comportamento da sociedade com violência deliberada e com alvos aleatórios, porém que traduzam alguma motivação política.

> Na maioria dos casos, o terrorismo representa uma estratégia política. Enquanto a guerra é baseada na coerção física, o terrorismo procura ter um impacto psicológico. [...] o terrorismo é a negação do combate. É sobre atacar um adversário desarmado,

> não sobre ataques surpresa em elementos de um exército regular (CHALIAND; BLIN, 2007, p. 227, tradução nossa).

O conceito de terrorismo fundamenta-se sobre um contexto histórico, ideológico e cultural (CHALIAND; BLIN, 2007). Para a compreensão deste processo, necessita-se de um breve aparato histórico a respeito do terrorismo ao longo dos anos. Para isso, será utilizada a teoria das quatro ondas criada por David Rapoport (2002), com o objetivo de buscar entender, posteriormente, o terrorismo moderno – ou o novo terrorismo. No mais, será demonstrado que, mesmo possuindo um caráter revolucionário como item comum entre as ondas, seus significados se mostram diferenciados entre elas.

A primeira onda, intitulada de "Onda Anarquista", surgiu na década de 1880, marcada pelo período de transformação nas comunicações e no transporte. O terrorismo, verificado principalmente nas revoluções contra o Império Russo, era considerado como uma estratégia para os rebeldes atingirem seus objetivos políticos, mesmo que instaurando o medo por meio de assassinatos e roubos a bancos, com fins de financiar suas próprias atividades (RAPOPORT, 2002).

O final da Primeira Guerra Mundial deu início à "Onda Anti-Colonial". Com a derrota dos impérios – principalmente os europeus –, tornou-se suscetível a dominação territorial entre Estados, o que incitou nos grupos uma necessidade de 'luta pela independência'. Exemplo desse aspecto foi a criação do IRA (Exército Republicano Irlandês) e o surgimento de grupos terroristas que se desenvolveram em domínios imperiais, os quais, ao longo do tempo, foram dissolvidos e se tornaram novos Estados, como os casos da Irlanda, Israel e Argélia (RAPOPORT, 2002).

No final dos anos 1960, surgiu a "Nova Onda de Esquerda", acalorada pela Guerra do Vietnã. O sistema ocidental se encontrava em questionamento, uma vez que sua maior potência dotada de tecnologia moderna estava perdendo a guerra para o País. O fim da guerra, em 1975, transmitiu aos grupos separatistas novamente o caráter revolucionário, desta vez voltado para as dimensões internacionais. No período, a OLP (Organização de Libertação da Palestina) passou a realizar atividades terroristas no exterior, assim como roubo a bancos e ataques às embaixadas. Porém, a inovação principal do período encontrou-se na realização de sequestros de aviões, com a finalidade de captura de reféns para arrecadação de ativos financeiros (RAPOPORT, 2002).

Por fim, na década de 1980, a "Onda Religiosa" ganhou espaço, principalmente no Oriente Médio[5]. A Revolução Iraniana, a resistência muçulmana contra a União Soviética (URSS) no Afeganistão e o início do novo século de acordo com o calendário muçulmano (1979), foram fatores políticos e religiosos condicionantes que incitaram a nova onda. A característica inovadora do período foram os ataques suicidas por bombas, realizados contra instalações militares e governamentais e embaixadas ao redor da região. Ainda assim, pode-se dizer que o ataque mais bem-sucedido de terroristas externos a um Estado foi o atentado ao World Trade Center, nos EUA. Esse fator demonstrou que a organização terrorista Al-Qaeda – responsabilizada pelos ataques – havia desenvolvido padrões de atividades ainda não visto nas ondas anteriores, como sistemas de recrutamento e treinamento restritos não apenas ao Oriente Médio[6] (RAPOPORT, 2002).

Uma possível quinta onda foi proposta por outros acadêmicos. Jeffrey Kaplan (2008) defende a dinamicidade do terrorismo, pois grupos podem evoluir para além do período delimitado pela onda. Dessa forma, na chamada "Onda do Novo Tribalismo", terroristas apropriam-se do poder governamental para reformar a ordem social, muitas vezes, conquistado em forma de genocídio. O autor (2008) utiliza como estudo de caso o Camboja, quando o grupo Khmer Vermelho assumiu o controle do governo no ano de 1975. Compactuando com os ideais anteriores, Anthony Celso (2015) acrescenta que a teoria de Kaplan exclui os grupos terroristas jihadistas que se encontram também alinhados com as características da quinta onda. Exemplos são grupos como o Boko Haram e o ISIS, que buscam adquirir territórios para a construção de uma ordem social por intermédio do califado[7].

Distante do posicionamento das teorias anteriores sobre o escopo do contexto histórico, Jeffrey Simon (2011) apresenta uma concepção acerca dos meios utilizados pelos terroristas. Pautando-se sobre a tecnologia, o autor argumenta que a quinta onda seria na verdade a "Onda Tecnológica" ao se compreender a ligação entre a tecnologia e o terrorismo. A facilidade de acesso à informação permite o desenvolvimento armado, o recrutamento e as comunicações de grupos terroristas. Porém, outro aspecto se faz importante quando é levada em consideração a atuação terrorista no ciberespaço, dificultando-se a compreensão sobre a ideologia ou a

[5] É importante salientar que mesmo o Islã sendo a religião mais representada na quarta onda, é possível observar o terrorismo em outras comunidades religiosas. Ataques de terroristas de religião judaica à santuários Islâmicos em Jerusalém e o ataque de gás tóxico no metrô de Tóquio por religiosos budistas, hindus e cristãos são alguns exemplos (RAPOPORT, 2002).

[6] O recrutamento e o treinamento, visto pela organização terrorista Al-Qaeda, se estendeu por todo o Oriente Médio, África e Ásia, em busca da população sunita, para a criação de um Estado único para os muçulmanos (RAPOPORT, 2002).

[7] Forma de governo de característica muçulmana que visa o renascimento do Estado Nacional Islâmico (NAPOLEONI, 2015).

motivação do ataque. Esse fator pode ter consequências tanto na esfera das ameaças de ataques terroristas por armas químicas, biológicas, radiológicas e nucleares, quanto no campo dos ataques ciberterroristas.

> Se é um operador solitário com habilidades e intenções hostis, ou um grupo terrorista que decide servir ao seu propósito de lançar um "novo" tipo de ataque que ganharia a publicidade mundial, a ameaça do ciberterrorismo provavelmente aumentará nos próximos anos. As inovações táticas terroristas na Quinta Onda também serão impulsionadas pela inovação tecnológica em operações de contra–terrorismo. Isso provavelmente forçará os terroristas a se adaptarem tornando-se mais experientes tecnologicamente (SIMON, 2011, p. 29, tradução nossa).

Portanto, a dinâmica em torno do conceito de terrorismo engloba principalmente a perspectiva histórica. A compreensão sobre as motivações e as mudanças nas execuções dos ataques são fatores que evoluem e se adequam de acordo com o crescimento da ameaça. Isto é, a complexidade de definição do conceito de terrorismo e de proteção e controle da ameaça encontram-se na constante variação do terrorismo em relação as alterações políticas, sociais, tecnológicas, religiosas, entre outros.

Sob a égide do avanço tecnológico, o espaço cibernético configurou-se como um novo meio e ferramenta de ação terrorista para a instauração do terror e desestabilidade política e social. Não apenas, os ciberterroristas propõem disseminar atos de violência contra infraestruturas críticas capazes de atingir um maior número de civis para o alcance dos seus objetivos políticos. Considerando-se a preparação, a conduta e as consequências de um ataque terrorista, é possível prever que toda essa sequência possa acontecer no mundo digital. A preparação de um ataque pode estar vinculada a busca de informações privilegiadas, vigilância de alvos e mapeamento geográfico virtual. A conduta pode envolver ataques cibernéticos específicos que possam desestabilizar sites e programas essenciais, levando a diversas consequências, como danos tecnológicos e físicos (JARVIS et al, 2014).

Logo, terrorismo pode ser encarado como uma ameaça tradicional que possui vertentes conceituais díspares que se transformaram e adquiriram características específicas em cada momento histórico. Mesmo não sendo um fenômeno recente, "o terrorismo se desenvolve sob a influência de vários fatores [...] da sociedade moderna" (IVANOV, 2014). Ao ter a revolução e a identidade política como os pontos comuns entre as ondas propostas por Rapoport (2002), os meios de ação permanecem em constante evolução. Dentre eles, está a recente interação do terrorismo com o aparato tecnológico, permitindo a expansão do caráter da ameaça e a promoção de consequências amplificadas à sociedade.

### 1.1.3 Ciberterrorismo

A natureza do ciberterrorismo pode ser facilmente confundida com diferentes ameaças cibernéticas, devido ao elemento comum em que são executadas: o espaço cibernético (DENNING, 2000). Uma vez que algumas categorias de ameaças promovem as mesmas ações, o que realmente é dissolvido em características específicas são as intenções ou motivações daqueles que a realizam (LYLE, 2016). Pelo fato dos componentes do termo ciberterrorismo não serem bem definidos, tende-se a gerar conceitos vagos, a exemplo do prefixo 'ciber' que é muitas vezes utilizado de forma inconsistente, principalmente pela mídia (CHEN et al, 2014; MCGUIRE, 2014). Neste momento, se faz necessário uma distinção entre atos de ciberterrorismo e atos de preparação para uma ação terrorista.

Atividades terroristas via redes de computadores que envolvam procedimentos de recrutamento, captação de recursos e propaganda que não resultam em graves danos digitais ou físicos por meio de ataques cibernéticos são ações preparatórias para a execução de um ataque tradicional de terrorismo. Os atos de ciberterrorismo são aqueles que utilizam o ciberespaço como ferramenta de ataque – estabelecendo concordância com a presente dissertação (QC; MACDONALD, 2014). Ainda assim, há autores que defendem que, pelo fato de a sociedade estar em constante mudança tecnológica e devido a dinamicidade do terrorismo e da complexidade do espaço cibernético, essa discussão divisória tende a ser ilusória, uma vez que tais atividades podem ser consideradas como fases de uma rápida evolução do terrorismo (ARIELY, 2014).

Segundo Ayn Embar-Seddon (2002), os atos de ciberterrorismo devem ser considerados como táticas empregadas por terroristas para o alcance de determinado fim. Mesmo que as ações por meios cibernéticos sejam diferentes das ameaças tradicionais de terrorismo, a finalidade encontra-se sobre o mesmo objetivo de promover o medo e transmitir mensagens políticas e sociais expressivas. No mais, o autor apresenta o ciberterrorismo como um 'multiplicador de forças' do terrorismo, uma vez que auxilia no desenvolvimento da imagem e das capacidades de ataques às esferas tecnológicas.

Como ocorre com o conceito de terrorismo, existem perspectivas divergentes a respeito do ciberterrorismo (OLESEN, 2016). Primeiramente, sendo definido como a junção da cibernética com o terrorismo (COLLIN, 1997), Mark Pollitt (1998) aprofunda o conceito, utilizando a definição de terrorismo e ciberespaço do Departamento de Estado dos Estados Unidos. Para o autor, terrorismo pode ser entendido como atos de violência promovidos por motivações políticas contra não combatentes, e, ciberespaço, como os computadores, redes e

programas que são utilizados como infraestrutura na coleta e transmissão de informações. Dessa forma, o ciberterrorismo é um "ataque premeditado e politicamente motivado contra os sistemas de informação, programas de computador e dados que resultam em violência contra alvos não combatentes por grupos nacionais ou agentes clandestinos (POLLIT, 1998, p. 3, tradução nossa).

Partindo da mesma concepção, Dorothy Denning (2000) considera que os terroristas utilizam o espaço cibernético para facilitar e expandir os atos de violência. Além de usufruir da Internet para transmitir mensagens, realizar recrutamento e coordenar ações, os realizadores de ataques cibernéticos teriam a vantagem do anonimato, não sendo necessária a presença física para a realização de uma ação violenta. Para ser considerado um ato terrorista, é necessário haver um motivo político e uma ameaça ou ação violenta. Com o ciberterrorismo não é diferente, entretanto, o que o tipifica é o meio de ação violenta por meio do ciberespaço (CONWAY, 2014).

> As forças mais destrutivas que trabalham contra a compreensão da ameaça do ciberterrorismo são o medo do desconhecido e a falta de informação ou, pior ainda, muita desinformação. A palavra ciberterrorismo reúne dois medos modernos significativos: o medo da tecnologia e o medo do terrorismo. Tanto a tecnologia quanto o terrorismo são incógnitas significativas (EMBAR-SEDDON, 2002, p. 1034, tradução nossa).

O não entendimento popular sobre a definição de terrorismo e sobre as novas tecnologias transfere o desconhecimento para o ciberterrorismo, por serem temas que já oferecem alto grau de complexidade e compreensão. Seus aspectos congruentes moldam-se de forma a condicionar um novo fenômeno que reconfigura tanto o conhecimento sobre o terrorismo quanto a noção popular sobre o bom e o mau uso da tecnologia. Deste modo, a percepção que é instaurada do ciberterrorismo pauta-se sobre termos ainda em processo de discussão conceitual. Em específico às tecnologias, tem-se o espaço cibernético como um domínio muitas vezes associado à Internet, transmitindo pouca ou nenhuma informação sobre suas reais características. Esses fatores podem ser responsáveis por manter a diversidade conceitual de ciberterrorismo, assim como enfraquecer as perspectivas sobre a ameaça e os possíveis modos de prevenção.

À vista disto, o ciberterrorismo pode ser considerado como uma ameaça em constante evolução que varia de acordo com o avanço tecnológico e as novas maneiras de propagação do terror. As possibilidades ofertadas pelo ciberespaço aos indivíduos que promovem a incitação

da violência em prol de determinado fim, os dão a condição de poder conflitar diretamente com os Estados.

A problemática encontra-se na forma na qual o ente estatal reagirá frente uma ameaça assimétrica não estatal e/ou individual, sem vínculos com outros Estados. Isso porque as leis, por mais que estejam em processo de adequação ao mundo globalizado e tecnológico, ainda apresentam dificuldades para aplicar responsabilidade à ataques cibernéticos qualificados. Assim, a falta de definição conceitual, o anonimato, as motivações e as ligações criminosas dificultam o processamento de atribuição e penalidade[8].

Portanto, os ataques cibernéticos contra redes de computadores, provenientes de motivações políticas e sociais que possam intimidar ou coagir governos e populações, são caracterizados como ataques ciberterroristas. No entanto, o que o faz realmente distinto das demais ameaças é o fato de ter a intenção de promover atos contra infraestruturas que afetem pessoas, tanto mediante o medo quanto pela promoção de danos letais (DENNING, 2000).

Em outras palavras, "os terroristas cibernéticos buscam conscientemente os não-combatentes para desmoralizar a população civil e trazer pressão sobre um governo para atender suas demandas" (GROSS, 2015, p. 180, tradução nossa). Esses eventos podem ser manifestados por meio de explosões em infraestruturas essenciais à população – como em estações de água e energia –, assim como incitados por acidentes de avião por intermédio, por exemplo, do acesso a controles de tráfego aéreo. Tais situações podem gerar, também, graves perdas econômicas em consequência dos ataques (DENNING 2000; MCGUIRE, 2014).

Em contraste, Maura Conway (2011) argumenta que ataques ciberterroristas são quase improváveis de ocorrer. O fato de grupos terroristas demonstrarem interesse em adquirir habilidades para agir no espaço cibernético não significa que possuem capacidades para tal. A autora sustenta que apenas 2%[9] dos terroristas de caráter jihadistas possuem conhecimento

[8] Exemplo da dificuldade de identificação de atores responsáveis está na ocorrência dos ataques cibernéticos na Estônia, em 2007. Em um período de tensões étnicas entre Rússia e Estônia, ciberataques às infraestruturas do país foram realizados, derrubando sites governamentais e bancários, gerando cerca de $1 milhão em danos e muitos dias para a recuperação total do país. Muitos estudos apontam que as origens dos ataques são provenientes da Rússia, apenas desta afirmar diplomaticamente não ter qualquer tipo de relação com os ataques (CARREIRO, 2012). Outros estudos afirmam que o caso da Estônia pode ser considerado um caso de ciberterrorismo, por haver a utilização do ciberespaço para atacar a infraestrutura crítica nacional e gerar desestabilização política, porém, com o respaldo de um agente estatal (HERZOG, 2011). Entretanto, para um ato ser considerado como ciberterrorista, o ator responsável deve ser não-estatal ou individual. Portanto, apesar da desestabilização política e do terror generalizado criado, a dificuldade de atribuição de responsabilidade dificulta a identificação dos autores dos ataques e, logo, sobre qual ameaça cibernética – ciberguerra ou ciberterrorismo – o caso deve ser tratado.

[9] A autora apresenta um estudo realizado em 2007, no qual verificou que, de 404 membros de grupos islâmicos extremistas, 196 (48,5%) possuíam ensino superior. Destes, 178 possuíam áreas cursadas específicas. Voltados para a área da computação, havia oito (4,5%) membros. Ou seja, de toda a amostra, menos de 2% dos membros avaliados envolviam-se com computação (CONWAY, 2011).

sobre Tecnologia da Informação e Computação; e mais: esses não seriam capazes de obter sucesso em ataques cibernéticos visto a complexidade dos sistemas. Logo, para operar no ciberespaço, os terroristas teriam que "contratar" hackers externos, o que os forçaria a operar fora dos seus grupos, sob o risco de comprometimento da segurança operacional do ataque (CONWAY, 2011).

Entretanto, o argumento da capacitação não influi diretamente a uma relação causal com a ameaça, uma vez que o ciberterrorismo possui complexos mecanismos e fragmentações, a começar pela própria definição do termo. O surgimento de novos agentes em um mundo "onde as relações sociais transcendem tradicionais espaços temporais para se tornarem cada vez mais interligados, fornece uma base mais robusta para teorizar o ciberterrorismo do que suas associações com a TIC" (MCGUIRE, 2014, p. 80, tradução nossa). Considera-se, portanto, que a análise pode ser variável visto que o nível de especialização em computação de um ciberterrorista deriva da sua natureza peculiar, sua formação, sua motivação e do deliberado evento a ser explorado (BRENNER, 2002; SIMON, 2011).

Dessa forma, não apenas o padrão de grupos terroristas de caráter jihadistas deve ser considerado. Ataques podem ser conduzidos por terroristas solitários atraídos por condições que o espaço cibernético proporciona, assim como, pode também ocorrer a anexação de indivíduos com novas características – que possivelmente em outras circunstâncias não seriam ativamente envolvidos – à grupos terroristas (KIRWAN; POWER, 2013). Outro fator proeminente se encontra nas novas gerações de terroristas que crescem em um mundo digital, com acessos facilitados. Novas ferramentas à disposição podem tornar mais atrativas as atividades cibernéticas, de forma a potencializar o risco e a execução de ataques ciberterroristas (DENNING, 2000).

> Um ciberterrorista pode lançar um ataque em qualquer parte do mundo tornando o ato verdadeiramente global. Para realizar um ataque, o terrorista convencional exige inúmeros pré-requisitos, como reconhecimento de alvo, armas e acesso que podem exigir uma rede de apoio considerável, a fim de completar sua missão. O ciberterrorista, em contraste, pode reunir remotamente informações disponíveis gratuitamente na Internet ou usar técnicas padrão de *hacking* para adquirir informações vitais sobre um potencial alvo (AYRES; MAGLARAS, 2016, p. 2, tradução nossa).

Pode-se afirmar que a falta de conhecimento e informação, tanto dos atores quanto das motivações do ciberterrorismo, despertam ainda mais o amedrontamento global. Possíveis consequências de atos terroristas brutais pairam sobre a imaginação de parcela significativa da comunidade internacional, o que não deixa de ser uma das motivações do terrorismo. Tais

preocupações ganham vulto com as possibilidades ofertadas pelo ciberespaço, inclusive para atingir alvos essenciais ao Estado. Agentes estatais, não-estatais e individuais são capazes de ameaçar e interferir diretamente nas esferas política, econômica e social nos níveis nacional e internacional, como será visto no tópico a seguir.

## 1.2 Conceituando as demais ameaças cibernéticas

Considerando o espaço cibernético como um domínio capaz de integrar as relações políticas, econômicas e sociais na esfera digital, compreende-se que a dinâmica e a movimentação dos atores vão, consequentemente, crescendo e sendo modificadas. As operações cibernéticas tornam-se cada vez mais interligadas e os processos comuns à sociedade passam a permear o âmbito virtual em paralelo ao mundo físico.

Tais correlações são fatores que geram aspectos desafiadores para a manutenção e proteção do ciberespaço e dos seus atores, uma vez que dispõem de mecanismos que estão em constante processo de mudança. Tendo em vista este cenário, determinados atores utilizam-se das vulnerabilidades para gerar ganhos, estimular ideologias e realizar operações ilegais no ciberespaço. Assim, serão apresentados, nesta seção, os conceitos de guerra cibernética, crime cibernético e hacktivismo e ativismo cibernético.

### 1.2.1 Guerra cibernética

Independente das categorias de conflito que são traduzidas em hostilidade e violência, a guerra configura-se apenas quando é respaldada por leis que permitem a aplicação concedida das forças armadas (WRIGHT, 1988). Com o aparato tecnológico e a introdução do ciberespaço no conjunto defensivo e ofensivo das forças armadas, os conceitos foram fundidos de forma a ampliar os métodos de guerra. Este fato permite a criação de novas geografias de combate por adicionar combatentes que não necessitam estar no teatro de operações, além de facilitar os mecanismos da guerra convencional (WARF; FEKETE, 2015).

Operações cibernéticas nas quais os Estados e as organizações políticas vislumbram os sistemas militares e de informação dos demais países, caracterizam a guerra cibernética (DIPERT, 2010). Para que um ataque cibernético seja identificado como um ataque de guerra, devem-se manter os conflitos no nível estatal. Isto porque considera-se que existam leis e reguladores de conflito que podem assumir as responsabilidades das ações executadas. Não apenas, subtende-se que os envolvidos possuam certas simetrias de poder como, por exemplo,

forças armadas. Portanto, e independente dos métodos aplicados, os Estados utilizam-se do espaço cibernético para reduzir os poderes de outros Estados, os quais podem, também, estar associados à execução de ataques de guerra físicos (ZUCCARO, 2011).

Ainda assim, pelo anonimato que o ciberespaço concede, existe uma dificuldade em se determinar a origem dos ataques cibernéticos, tornando mais complexa a atribuição da responsabilidade. Isso gera um ambiente de incertezas entre os Estados, uma vez que estes podem tomar ações cibernéticas preventivas (DIPERT, 2010). Por mais que "a guerra cibernética [seja] um meio de incapacitar as instalações de apoio à guerra, não intimidando civis" (GROSS, 2015, p 178, tradução nossa), existe a possibilidade de envolver danos a não combatentes. Em ocasiões de defesa, os esforços podem deslocar-se para medidas emergenciais, as quais podem prejudicar a população, a economia e os sistemas de computadores essenciais (DIPERT, 2010).

A guerra cibernética abrange todas as operações realizadas no ciberespaço que visam obstruir ou lesar sistemas de informações do oponente, à medida que mantém sua própria defesa contra o oponente. As ações cibernéticas dessa natureza geralmente podem ser acompanhadas por conflitos armados (MAURUSHAT, 2013). Não somente, os ataques podem se iniciar a partir da concepção estatal de que a busca de informações sigilosas e a interrupção de sistemas dos outros Estados garantem algum tipo de vantagem competitiva na guerra (LIBICKI, 2009). Em outras palavras, o espaço cibernético pode ser utilizado pelos Estados como ferramenta de ataque em ocasiões de guerra ao promoverem ações cibernéticas diretas ou indiretas de apoio ao fronte armado.

A ciberguerra não difere, em parte, da guerra convencional. Para Cornish et al (2010), o espaço cibernético apenas ampliou o campo de conflito. Isto é, a "guerra cibernética é um componente novo, mas não inteiramente separado de um ambiente de conflito multifacetado" (CORNISH et al, 2010, p. 11, tradução nossa). No entanto, por mais que os Estados possuam recursos e orçamentos capazes de empregar ciberataques de alto desempenho, no espaço cibernético são proporcionadas oportunidades para outros atores desafiarem a vertente tradicionalista do Estado, como principal ator do Sistema Internacional. Conflitos nesta escala podem caracterizar não apenas guerra cibernética entre Estados, como, também, conflitos cibernéticos assimétricos entre Estados e atores não-estatais, caracterizando outros tipos de ameaça.

Entende-se, então, que na ciberguerra o uso da força é empregado por meio do espaço cibernético com a finalidade de promover destruições em diversos níveis fundamentais de um Estado. Os ataques cibernéticos são aplicados de forma a incitar consequências políticas e

intimidação estatal tanto em momentos antecedentes ao conflito como no ambiente de guerra. O conceito parte da concepção de que a "guerra é o uso da força para fins políticos" (LEWIS, 2011, p. 23, tradução nossa). Entretanto, deve-se ponderar que um ciberataque somente pode ser considerado como guerra cibernética se em ambos os lados estiverem forças estatais.

Devido a peculiaridade da ameaça, é visto, no espaço cibernético, a oportunidade de permear sistemas que alcançam alvos essenciais ao Estado na busca de informações relevantes (MARTINS, 2012). As ações podem variar desde a execução de espionagem cibernética, com a finalidade de coleta de informações, até a realização de sabotagens de computadores e máquinas que possam provocar danos ao oponente (VENTRE, 2011).

Ainda assim, os efeitos da guerra cibernética podem variar de acordo com as vulnerabilidades do oponente e da sua capacidade de recuperação (LIBICKI, 2009). Deste modo, pode-se caracterizar a guerra cibernética como a aplicação de atos letais aos sistemas de infraestruturas e comunicações de determinado país que possam inviabilizar ou retardar seu tempo de resposta (WARF; FEKETE, 2015).

Visualiza-se que o Estado tem a capacidade de permear diversos domínios ao tratar-se da guerra. O espaço cibernético, como componente elementar, possui tanto capacidades de promover consequências físicas quanto incitar medidas cibernéticas extraordinárias à guerra convencional. Na intenção de desestabilizar os meios do oponente, um novo campo de conflito é configurado em paralelo ou antecedente ao conflito armado. Portanto, pode-se definir guerra cibernética como o combate entre Estados no ciberespaço, na busca de alcançar a desestabilização do oponente, a partir da realização de ataques cibernéticos que possam promover vantagens competitivas e estratégicas, por intermédio da coleta de informações e geração de danos infraestruturais.

### 1.2.2 Crime cibernético

O crime cibernético pode ser apontado como o uso indevido da tecnologia nas redes e sistemas de computadores na busca de ativos financeiros. A proporção da gravidade do ataque é variada de acordo com a motivação dos atores na promoção de roubos utilizando-se do ciberespaço. Com a abrangência oferecida pelo ciberespaço, os elementos de roubos, fraude e roubo de identidade transferiram-se para um ambiente pouco explorado e legislado.

A complexidade de se instaurar legislação competente parte da dificuldade de controlar acessos indiscriminados de qualquer ator que queira realizar atividades cibernéticas ilícitas. As variadas estipulações motivacionais das ameaças, os obstáculos que o espaço cibernético

proporciona, o anonimato e a falta de consenso nas definições das ciberameaças dificultam a aplicação da lei. Não somente, os recursos humanos qualificados em proteção cibernética, que atuam fora da esfera federal, são restritos no âmbito dos órgãos estaduais e municipais. Tais aspectos oferecem as oportunidades ideais para as organizações criminosas e terroristas promoverem ações ilegais (HUNTON, 2011).

> Instâncias de cibercrime e ciberterrorismo estão aumentando rapidamente e apresentam sérias ameaças tanto para os indivíduos quanto para as sociedades. Elas ameaçam e violam os direitos humanos e causam danos a muitos, desde cidadãos até as infraestruturas críticas. Devido à natureza onipresente do ambiente cibernético em que esses crimes são realizados, detectá-los e investiga-los envolve autoridades policiais que acessam o mesmo ambiente; isso tem o potencial de impactar em muito mais pessoas do que seria o caso com as investigações criminais tradicionais (LYLE, 2016, p. 278, tradução nossa).

Geralmente, os grupos de criminosos cibernéticos especializados possuem recursos computacionais à disposição e são tecnicamente qualificados (EMBAR-SEDDON, 2002). Os cibercriminosos podem ser classificados como hackers individuais ou grupos criminosos que visam encontrar vulnerabilidades nas redes e explorá-las em benefício próprio. No mais, podem ser motivados por ganhos financeiros, ou apenas possuem a intenção de invadir redes desconhecidas em busca de informação como, por exemplo, dados bancários dos usuários da Internet (DAS, 2015). Ainda, são atores provedores de desestabilização econômica que, dependendo da amplitude do ataque, podem gerar danos para além da esfera nacional. Isto pode ser melhor exemplificado ao se considerar ataques cibercriminosos às redes de bancos que possuem abrangência internacional.

Para um ataque cibernético ser considerado crime devem ser utilizadas as redes e sistemas de computadores como ferramenta de ataque (AKHGAR et al, 2016). Tendo em vista sua motivação econômica, os governos, as organizações, as empresas e as corporações, em geral, são os principais alvos do cibercrime. Definindo-o como uma atividade ilícita no ciberespaço gerada por meio de dispositivos eletrônicos – ou seja: fraudes, roubo, vandalismo, violação da propriedades digitais e invasões às redes e sistemas –, tem-se que tais ações podem afetar a segurança nacional e internacional (SPEER, 2000). Em outras palavras, "o Estado, as suas instituições, o setor empresarial e o banco simbolizam um novo alvo a explorar e a abater por representar um motivo de desafio para quebrar os sistemas de segurança" (MARTINS, 2012, p. 41).

Ainda assim, é complexa a compreensão a respeito da natureza dos crimes cibernéticos. Presumindo que os ataques podem ser provenientes desde indivíduos interessados em invadir

computadores por diversão, à criminosos que utilizam o ciberespaço para o roubo de informações, cria-se uma sobreposição de motivações (SPEER, 2000). Com isso, podem-se classificar como principais cibercriminosos os *crakers*[10], os *hackers*[11] e os criminosos de carreira[12]. Em alguns casos, os ciberterroristas também podem ser classificados como criminosos por utilizarem dos mesmos recursos para ataques e pela finalidade da ação alcançada (SAINI et al, 2012).

> Criminosos geralmente visam explorar violações em qualquer sistema a fim de obter lucro, ou usar tecnologias de inovação para aumentar seu impacto, como qualquer negócio. Terroristas, embora diferentes dos criminosos em sua natureza, dispõem das mesmas ferramentas para ameaçar países, organizações, infraestruturas e cidadãos (AKHGAR et al, 2016, p. 297, tradução nossa).

Por mais que a maioria dos ataques criminosos seja realizada por indivíduos, a assimetria de poder e influência, quando comparados aos governos e às grandes instituições, limitam os acessos a determinados sistemas (SPEER, 2000). No entanto, os cibercriminosos que superam as defesas cibernéticas dos seus alvos podem utilizar-se dos dados recolhidos para a obtenção de ganhos econômicos, por meio da venda de segredos empresariais, códigos de programação e, até mesmo, segredos de Estado (MARTINS, 2012).

Contudo, o impacto do ataque cibernético de caráter criminoso, embora quantificável, não é estritamente financeiro (HUNTON, 2011). Outros aspectos, como a imagem e a reputação das instituições perante à sociedade, por exemplo, podem gerar repercussões não favoráveis caso ocorreram vazamentos de dados sigilosos (BYRES; LOWE, 2004). Portanto, define-se o cibercrime como uma ação cibernética realizada por indivíduos e grupos criminosos que visam ganhos econômicos e coleta de informações sigilosas na intenção de obter vantagens financeiras.

Logo, é possível analisar que, por constituir-se de questões criminosas, existem maiores avanços legislativos que visam alcançar a peculiaridade dessa ameaça, em relação às demais ameaças cibernéticas. Entretanto, a constante evolução do cibercrime implica na dificuldade de se acompanhar o processo de reestruturação das leis em uma mesma escala progressiva, uma vez que as leis aplicadas a esses casos são de caráter nacional e, muitas vezes, subjetivas.

---

[10] Atores com intenções de provocar danos e perdas, por alguma motivação específica ou por diversão. Enquadram-se nesse aspecto os criadores e distribuidores de vírus de computador (SAINI et al, 2012).
[11] Indivíduos que exploram sistemas de computadores a fim de alcançar algum objetivo pessoal, de forma a construir uma reputação frente aos outros hackers (SAINI et al, 2012).
[12] Sujeitos que buscam obter renda por intermédio da criminalidade (SAINI et al, 2012).

Outro fator agravante na aplicação da lei encontra-se no aspecto de paridade conceitual entre as ameaças cibernéticas. Como os ataques cibernéticos, em geral, representam ações criminosas no ciberespaço, a identificação das ameaças para o emprego das leis diferencia-se de acordo com as motivações e as finalidades a serem alcançadas. No entanto, percebe-se que a proteção contra o crime cibernético apresenta maiores adiantamentos em termos de legislação e prevenção da ameaça em relação às demais ameaças cibernéticas por, principalmente, já possuir o conceito de crime melhor definido no âmbito do Direito.

### 1.2.3 Ativismo cibernético e Hacktivismo

O ativismo geralmente possui a intenção de levar informação e transparência para a sociedade, em busca da transformação social, econômica, política, ambiental, entre outras (KRAPP, 2013). Ao conectar-se com o ciberespaço, as ações e as motivações possuem a capacidade de alcançar maiores públicos. Neste meio, podem surgir desde indivíduos com habilidades de programação que buscam realizar ataques cibernéticos para explorar plataformas institucionais, como indivíduos em defesa da liberdade de expressão, dos direitos humanos e da ética da informação pela divulgação de dados confidenciais das instituições (KRAPP, 2013).

Conforme Taylor (2004), com a globalização, os *hackers* se tornaram mais conscientes politicamente e os ativistas mais tecnologicamente interconectados no espaço cibernético. Esses, por serem caracterizados por defender diversos tipos de interesses, dentre eles o acesso "transparente" à informações, passaram a se valer de interações tecnológicas para o alcance de seus objetivos. Atividades ativistas baseadas no uso do ciberespaço, que tem como finalidade a realização de protestos contra as grandes instituições e os governos podem, muitas vezes, ser extremas. Por essa razão, é difícil compreender as causas defendidas pelos ciberativistas, uma vez que o anonimato é a caraterística principal dessa ameaça[13], a não ser que esta não seja a intenção (SORELL, 2015).

De acordo com Mark Milone (2003), existem variações entre os ativistas cibernéticos e os hacktivistas. Quando indivíduos pertencem a organismos geralmente formados por pequenos contingentes com o objetivo de organização, coordenação e condução das atividades ativistas nas redes, são denominados de ciberativistas. Quando passam a utilizar o ciberespaço como

[13] Mesmo que o fator do anonimato seja um dos desafios presentes no conceito do espaço cibernético, neste caso, pelo fato dos atores trabalharem com a coleta de informações sigilosas para a divulgação à público, a exposição das suas identidades deve ser ainda mais cautelosa. Isso apenas muda caso a intenção seja a promoção dos ideais de determinado grupo.

ferramenta para manifestar e disseminar informações e ideologias que atinjam um caráter revolucionário, direcionando a atenção para fins políticos e sociais em prol de determinada causa, são designados de hacktivistas (SORELL, 2015).

Os hacktivistas podem se enquadrar entre aqueles grupos e indivíduos que auxiliam o governo com a finalidade de identificar as falhas e as vulnerabilidades das infraestruturas críticas nacionais (MILONE, 2003). Contudo, o não apoio político os levam a uma maior obtenção de poder na sociedade. O conhecimento e a informação podem dar aos atores envolvidos a possibilidade de realizar ataques cibernéticos contra as infraestruturas, roubar segredos comerciais, expor informações secretas do governo e organizações, além de gerar danos diretos contra as redes e computadores institucionais. Mesmo ao possuir o anonimato como característica peculiar, os hacktivistas permitem que seus ataques sejam expostos publicamente, como um ideal em forma de protesto (SORELL, 2015).

Dessa forma, conceitua-se o hacktivismo como ações no ciberespaço que representam inclinações políticas e que tem por finalidade informar a sociedade sobre as instituições que agem em desconformidade com o que declara à população. Sabendo que o ciberterrorismo também possui como característica a motivação política, o hacktivismo se distingue no quesito da não violência. Apesar da subjetividade do que é considerado como um ato de ‘terror’, no hacktivismo, a busca de objetivos políticos é perseguido por intermédio da promoção de debates e não pela incitação da violência como forma de pressionar ou enfraquecer um Estado, como é no ciberterrorismo (HIMMA, 2008).

Logo, tem-se que o hacktivismo opera no espaço cibernético com o objetivo de promover à sociedade o acesso à informação, antes privilegiada. Isto é, denunciar práticas e políticas que vão em desencontro aos Direitos Humanos, ao meio ambiente, aos sistemas financeiros e às outras categorias na intenção de defender determinada causa. Isso pode ser feito mediante acesso à documentação classificada ou por meio de ataques cibernéticos diretos a uma organização específica (MARTINS, 2012).

Portanto, o “hacktivismo denota a capacidade de introduzir ou fazer um uso não convencional das tecnologias da informação para uma variedade de fins políticos” (DESERIIS, 2016, p. 2, tradução nossa). É possível visualizar, ainda que de forma mais generalizada, que os estudos envolvendo o conceito de ciberativismo/hacktivismo estão mais ligados ao debate da ‘legitimidade da ação’, por defender causas com fins pacíficos. Muitos autores apontam que a ação ativista, independentemente de ser por meios cibernéticos ou não, vislumbra a liberdade de expressão da sociedade.

Por fim, para uma melhor compreensão e análise, são apresentadas, no Quadro 1, definições sintetizadas a respeito das ameaças cibernéticas supracitadas. É perceptível que, pelo fato de serem termos já existentes acoplados ao uso do ciberespaço e, tendo em vista suas recentes inclusões nos estudos de segurança internacional, os conceitos conseguem abranger variações ainda pouco delimitadas. A título de conhecimento, mostra-se válido conceituar brevemente outras ameaças e agentes relevantes para a segurança cibernética como um todo, por mais que não façam parte do escopo da presente pesquisa. Com isso, torna-se possível distinguir e classificar as características específicas das atuais ciberameaças como um todo, assim como identificar o que não se enquadra no escopo do ciberterrorismo. Para mais, ver Das (2015) e Olesen (2016).

**QUADRO 1**

Classificação das ameaças cibernéticas e principais atores cibernéticos, segundo Nina Olesen (2016)

| | |
|---|---|
| Ciberterroristas | Utilizam indiscriminadamente a violência para influenciar decisões estatais, em relação aos próprios objetivos. Suas ações são caracterizadas por motivações políticas. Por meio de mecanismos de sabotagem de amplo alcance no ciberespaço, visam lesionar a sociedade e a segurança nacional. |
| Cibercriminosos | Possuem recursos, são altamente qualificados e podem fazer parte de organizações criminosas. Visam obter lucro por meio de atividades ilegais no ciberespaço. Suas principais práticas envolvem fraudes financeiras e desenvolvimento de ferramentas maliciosas. |
| Hacktivistas | São caracterizados por serem dinâmicos e, muitas vezes, sem uma estrutura centralizada. Por meio de ataques ao governo e grandes empresas, visam alcançar a atenção da mídia e influenciar decisões políticas, com a utilização de propagandas. Suas principais motivações derivam das ideologias políticas e sociais, da justiça e da transparência de informações. |

| | |
|---|---|
| Estados-nação | São os principais atores da guerra cibernética. Realizam atividades no ciberespaço em prol da segurança nacional e da inteligência/contra-inteligência. Possuem como objetivo a busca de informações e segredos de Estado, segredos militares e ataques a infraestruturas críticas. |
| Hackers sociais *online* | Exercem atividades de 'pesca', perseguição e violação de privacidade. São caracterizados como qualificados em engenharia social e psicologia social dos alvos. Utilizam-se da informação adquirida para violar dados, criar perfis nas mídias sociais, entre outras atividades. |
| Combatentes cibernéticos | São politicamente motivados. No ciberespaço, utilizam-se da técnica de sabotagem, praticando ações em nome de determinado Estado. Isto é, podem defender regimes totalitários e agir sem denominação. |
| Corporações | Realizam espionagens coorporativas por meio da violação de dados e sabotagem cibernética contra os concorrentes. Possuem o objetivo de coletar informações competitivas. Tal ameaça pode receber recursos e obter estreitas relações dos Estados. |
| Funcionários | Podem ser considerados como as ameaças internas das instituições. Visam violar dados e podem possuir caráter intencional ou não. São motivados por extorsão, vingança, sabotagem e lucro. |
| *Script Kiddies* | Possuem baixos níveis de conhecimento de ferramentas de *hacking*. Geralmente, são jovens motivados pelas habilidades de especialistas em tecnologia. |

Fonte: Elaboração própria baseada em Olesen (2016, p. 272-273).

Com base nas informações conceituais apresentadas, portanto, buscou-se discernir, neste capítulo, as características e os desafios que o fenômeno do ciberterrorismo pode oferecer à segurança e à defesa de um Estado. Tal compreensão se faz importante pela diversidade de atores e ameaças que permeiam o espaço cibernético. Vale acrescentar que, pelos conceitos apresentados se tratarem de temas ainda em processo de discussão, o panorama é debatido em diversas áreas do conhecimento, mas, principalmente, na esfera dos estudos de tecnologia. Por

este motivo, dificultou-se um maior aprofundamento conceitual sobre eles no âmbito das Ciências Sociais.

## 2 TEORIA DA SECURITIZAÇÃO: A ESCOLA DE COPENHAGUE NOS ESTUDOS DE SEGURANÇA INTERNACIONAL

A Escola de Copenhague, como corrente ampliadora dos Estudos de Segurança Internacional (ESI)[14], colaborou com os debates em torno do conceito de segurança e constituiu novos panoramas e objetos de análise no pós-Guerra Fria. Por meio da criação da Teoria da Securitização, os teóricos de Copenhague transferiram a lógica de ameaças anteriormente ligadas ao Estado para outras esferas de análise. Com isso, construíram uma teoria capaz de identificar o nível de segurança no qual determinado objeto de referência se encontra. A partir desses preceitos, buscar-se-á, no presente capítulo, detalhar a Teoria da Securitização para, no capítulo posterior, aplicá-la como lente metodológica para a verificação de um processo de securitização do ciberterrorismo nos EUA.

Com o objetivo de ampliar o conceito de segurança para além de estatal e militar, a Escola de Copenhague ofereceu um novo olhar às concepções e as perspectivas racionalistas nos ESI, presentes durante o sistema bipolar. Considerando que os ESI começaram a tomar forma no final da década de 1940, sob a égide dos Estudos Estratégicos[15] e com uma perspectiva realista – na qual o Estado é tido como o principal objeto de análise –, as questões tratadas pautavam-se, principalmente, sobre os setores militar e político. A emergência na discussão de assuntos correlatos à segurança nacional e à sustentação dos interesses estatais, tendo em vista as ameaças promovidas pelo sistema bipolar, abriu espaço para debates em torno do conceito de segurança. Todavia, os escopos das pesquisas limitavam-se ao progresso da corrida armamentista e às relações entre as superpotências durante a Guerra Fria, e não, necessariamente, na construção de teorias (BUZAN; HANSEN, 2012).

A mudança do Sistema Internacional, o fim da ameaça iminente de uma guerra nuclear e o declínio nas preocupações militares de segurança foram os fatores que permitiram o aprofundamento e a ampliação da agenda de segurança, nos anos 1980 e 1990. Os novos

[14] Vertente das Relações Internacionais que estuda o conceito de segurança em sua totalidade.
[15] Literatura clássica dos Estudos de Segurança Internacional que predominou no período da Guerra Fria, de vertente político-militar e estadocêntrica, que dialoga questões sobre guerras, proliferação nuclear, dissuasão, controle de armamentos, entre outros temas (BUZAN; HANSEN, 2012). Será melhor apresentada na seção a seguir.

questionamentos sobre qual conceito de segurança e epistemologia seriam adotados expuseram os debates presentes na agenda de pesquisa no pós-Guerra Fria (BUZAN; HANSEN, 2012). As discussões foram impulsionadas por esse cenário para além da visão realista de equilíbrio de poder entre os EUA e a URSS. Passaram a surgir uma diversidade teórica e intelectual que buscavam explicar o fenômeno da Guerra Fria e o seu fim. Consequentemente, novos atores foram integrados às análises, inclusive os atores não-estatais.

Sob esse cenário, a Escola de Copenhague se estabeleceu no debate aprofundador-ampliador nos ESI ao integrar em suas análises tanto características racionalistas quanto a epistemologia construtivista. Esses aspectos serão verificados quando a corrente compreende a importância do Estado para as análises de segurança, ao passo que defende que não é possível medir segurança somente de forma objetiva, uma vez que as ameaças são socialmente construídas (BUZAN, 1997). No entanto, o foco teórico da Escola consolidou-se no debate acerca do alargamento da agenda de segurança para outras abordagens conceituais e analíticas. Neste sentido, portanto, além de delinear a Teoria da Securitização, caberá ao capítulo apresentar o debate aprofundador-ampliador da agenda de segurança instaurado no pós-Guerra Fria, a fim de ilustrar o cenário e as discussões teóricas que permearam a criação do conceito de securitização pelo grupo de Copenhague.

## 2.1 Debate sobre a agenda de segurança pós-Guerra Fria

Assim como os grandes eventos históricos, a Guerra Fria transformou o cenário internacional. O problema de segurança gerado entre os EUA e a URSS direcionou as pesquisas para as lógicas estratégico-militares. No entanto, os estudos de segurança decorrentes da conjuntura, além da esfera militar, pairava, também, sobre questões ideológicas e sociais. O alardeado descontrole de armamentos nucleares e os debates em torno da sobrevivência da humanidade geraram pesquisas opostas a Guerra Fria, como abriram discussões acerca de objetos de análise que não fossem apenas o Estado (BUZAN; HANSEN, 2012). Com o fim do sistema bipolar, os ESI demandaram por uma reestruturação da agenda acadêmica que atendesse ao novo cenário internacional. Nesta seção, portanto, será apresentado o debate aprofundador-ampliador em torno da agenda e do conceito de segurança no cenário pós-Guerra Fria.

A principal característica refere-se a adoção de abordagens teóricas que se expandiram para além da perspectiva das disputas de poder estadocêntricas e da concepção de utilização da força. Correntes evoluíram ao passo que novos temas foram acoplados aos estudos de

segurança. Ao integrarem dimensões abrangentes de identidade, cultura, discurso, tempo, entre outros, as análises alcançaram ambientes anteriormente limitados a campos específicos. A expansão concedeu, assim, possibilidades analíticas sobre a lógica dominante do período Guerra Fria e a necessidade de ampliação da segurança para o ambiente não militar, até mesmo para os pensadores das teorias realistas (BARROS, 2017; BUZAN, 1997).

> O poder militar não é a única fonte de segurança nacional, e as ameaças militares não são os únicos perigos que os Estados enfrentam (embora sejam os mais graves). Como resultado, os estudos de segurança também incluem o que as vezes é denominado "ofício de Estado" – controle de armas, diplomacia, gerenciamento de crises, por exemplo. Essas questões são claramente recorrentes ao foco principal do campo, porque elas tem ação direta. Porque os fenômenos não militares também podem ameaçar Estados e indivíduos, alguns escritores sugeriram ampliar o conceito de "segurança" (WALT, 2007, p. 215, tradução nossa).

Nesse quadro, analisa-se que os debates pós-Guerra Fria tornaram-se abrangentes a partir da concepção de que as ameaças não provinham exclusivamente da ação estatal. A necessidade de que os temas emergentes dos anos 1990 e da virada do século fossem introduzidos nos campos teóricos de segurança, proporcionou a inserção de novos objetos de análise e a ampliação do conceito de segurança. Adotar como objeto de referência o indivíduo, por exemplo, impulsionou as correntes ampliadoras a relacionar as análises de segurança militar para com outros setores, firmando novas perspectivas aos ESI. "Se não houvesse uma pequena [...] preocupação com conceitos mais amplos de segurança nos anos 1980, é duvidoso que as abordagens mais amplas dos anos 1990 pudessem ter crescido da maneira como o fizeram" (BUZAN; HANSEN, 2012, p. 168).

Na citação supracitada de Stephen Walt (2007), a percepção de ameaça ultrapassa a esfera militar ao tratar as ameaças como não apenas militar e ao incorporar a visão de que tais ameaças não afetam apenas o Estado, como também o indivíduo. O ciberterrorismo alcança ambas as perspectivas enunciadas por definir-se como uma ameaça não-estatal que busca afetar e desestabilizar o Estado mediante ataques contra a população. Compreende-se, assim, que o esforço teórico ampliador-aprofundador do conceito de segurança, estabelecido no pós-Guerra Fria, viabilizou a anexação de novos tópicos nos ESI.

De acordo com Buzan (1997), os debates nos ESI dividem-se em três vertentes teóricas: tradicionalista, crítica e abrangente. A vertente tradicionalista diz respeito àquelas nas quais o Estado, o uso da força e as capacidades militares são os principais objetos de análise. A vertente crítica engloba os teóricos que defendem que os objetos de segurança são construídos socialmente, incluindo aspectos sobre o indivíduo e as estruturações sociais. Em meio termo às

anteriores, a vertente abrangente refere-se ao alargamento do conceito de segurança e ameaças para além de militares – na qual inclui-se a Escola de Copenhague (DUQUE, 2009).

Buzan et al (1998) argumentam que, na vertente tradicional, a identificação dos problemas de segurança no âmbito militar e estadocêntrico é facilitada por meio da compreensão das capacidades militares e o uso da força. Entretanto, quando foge do escopo tradicional, ao utilizar apenas o Estado como objeto de referência, torna-se mais difícil tratar da segurança. Neste quesito, as correntes não realistas exigiram esforço teórico no que concerne às discussões sobre a ampliação e o aprofundamento do conceito de segurança.

Neste caso, tendo o Estado como o principal objeto de referência analítica e normativa e, pelo fato de a segurança estar diretamente ligada ao Estado, compreende-se o pensamento de que os demais componentes ligados a ele também são assegurados. A segurança do Estado assegura os outros objetos de referência como, por exemplo, o indivíduo. Outra característica da vertente tradicional é o argumento de que, como a segurança é um componente anexo à soberania estatal, as ameaças externas moldam-se de acordo com o movimento interno nacional, mantendo a análise sobre a esfera do Estado (BUZAN; HANSEN, 2012).

No sentido contrário, a vertente crítica dos ESI integra a perspectiva construtivista sobre o objeto de análise de segurança. Isto é, considera que os fatos existem porque a sociedade atribui significado a determinado objeto. Com isso, os atores individuais, para compartilhar de um mesmo significado em relação ao objeto, necessitam da aquisição de um conhecimento de natureza interpretativa dos acontecimentos, podendo ser em um contexto cultural ou social do indivíduo com relação à sociedade. Afirma-se, portanto, que "o conhecimento da realidade é socialmente construído" (GUZZINI, 2013, p. 398).

Alexander Wendt (1992, p. 396) define que "as pessoas agem relativamente aos objetos, incluindo outros atores, com base no significado que os objetos têm para elas". Ao transferir esta lógica para o nível dos atores não-estatais e individuais, pode-se compreender que as identidades são traçadas sob crenças pessoais que, ao compartilharem de um mesmo entendimento sobre um objeto, se tornam crenças comuns. Este fenômeno pode ser visualizado na consolidação de organizações não-governamentais, agremiações religiosas e nos mais variados grupos, dentre eles, os terroristas. Mais precisamente, a respeito do ciberterrorismo, no qual o espaço cibernético é o meio de ação e a Internet oferece facilidades para a disseminação de crenças, tornam-se ainda maiores as possibilidades de conhecimento comum em relação ao objeto, podendo levar ao aumento das ameaças e dos atos de ciberterror.

No mais, é importante acrescentar que o viés construtivista serviu como um importante panorama para as novas análises do sistema internacional. Correntes teóricas adjacentes

aderiram aos seus moldes epistemológicos com o propósito de permear os debates ampliadores e aprofundadores do período. A inclusão da análise de atores não apenas estatais permitiu que o entendimento de construção social fosse aderido no âmbito dos ESI. Ao conferir embasamento para a criação de novas teorias e metodologias de análises – aspecto este que influenciará também a Escola de Copenhague –, os princípios construtivistas instituíram um norte para análises epistemologicamente ampliadas do cenário internacional pós-Guerra Fria.

Por último, a categoria abrangente concentra-se nos estudos voltados para a ampliação do conceito de segurança e do objeto de referência para além de militar e estadocêntrica. Representada pela Escola de Copenhague, a vertente inclinou-se para uma agenda de pesquisa que "desenvolveu um quadro teórico e conceitual inovador, cujo escopo permite a interpretação de continuidades e mudanças no cenário internacional, ao ser aplicável não só ao período atual como também à história recente das relações internacionais" (DUQUE, 2009, p. 475).

Buzan (1997, p. 12, tradução nossa) aponta que "a agenda de segurança irá variar de ator para ator em termos de questões e prioridades". Isto é, a mudança do paradigma realista para o debate ampliador não significou a falta de importância do Estado na agenda de segurança pós-guerra. Para a Escola de Copenhague, o ente estatal ainda continua como ator central, entretanto, não deve ser o único e exclusivo objeto de referência ou agente de ameaça. Outras fontes de ameaças podem ser apresentadas na forma de permear o Estado como, por exemplo, as instituições internacionais, os órgãos não governamentais e os indivíduos, além de sistemas complexos como a economia global e o meio ambiente. Portanto, as variações em questões de fatores e prioridades, em relação causal, depende do cenário internacional.

Este argumento serve de base para a análise proposta na dissertação em tela. Tendo em vista o alcance das ameaças cibernéticas na conjuntura contemporânea, a expansão dos danos e a capacidade de execução de ataques fogem da esfera apenas estatal. A interação tecnológica que permeia os mais variados setores e Estados inferem diretamente na segurança da sociedade. A partir desse aspecto, ter o ciberterrorismo como ameaça a um objeto referente traduz a afirmação de Barry Buzan no tocante à mudança na qual os atores do ambiente internacional deixam de ser apenas os Estados. A Escola de Copenhague sintetiza esta lógica no âmbito da Teoria da Securitização e, por isso, serve adequadamente como metodologia para o estudo apresentado.

Logo, o principal norte da Escola de Copenhague encontra-se na abertura da agenda de segurança para as mais variadas esferas de ameaças. Ao sair do quadro de análise de segurança como inteiramente militar, é permitido explorar objetos de referência díspares, ao mesmo tempo em que se entende o ambiente de ameaças como não exclusivamente estatal. Isso descreve o

ímpeto intelectual na intenção de construir uma embasada conceituação de segurança em seu nível mais específico que é a securitização. Portanto, a Escola de Copenhague alcançou outros objetos de referência ao retirar a lógica de ameaça como apenas estatal e ao introduzir novos conceitos e inovações acadêmicas sob aspectos mais abrangentes dos fenômenos internacionais por meio da Teoria da Securitização, conforme será visualizado a seguir (BUZAN, 1997).

## 2.2 Teoria da Securitização da Escola de Copenhague

Tendo como principais teóricos Barry Buzan e Ole Waever, a Escola de Copenhague apresenta como primeira contribuição a criação do conceito de segurança social, fundamentado sobre as premissas construtivistas, em resposta aos conflitos étnicos que ocorriam no Leste Europeu no início da década de 1990 (BUZAN et al, 1998). Entretanto, estes eventos permitiram demonstrar que as teorias em que o conceito de segurança era vinculado à lógica estatal tornavam-se irrelevantes ao se considerar que os níveis de análise de segurança eram incapazes de alcançar outras entidades ameaçadas (TANNO, 2003). Tal problemática somente será resolvida ao ser modificada a concepção de segurança, a partir da criação do conceito de securitização no campo dos ESI (BUZAN; HANSEN, 2012).

> Enquanto um conceito, a segurança claramente requer um objeto de referência, pois sem uma resposta para a questão "A segurança de que?" a ideia não faz sentido. Responder simplesmente "o Estado" não resolve o problema [...]. Rapidamente se descobre que a segurança tem muitos objetos de referência possíveis. Estes objetos da segurança multiplicam-se não só conforme aumenta o número de membros na Sociedade de Estados, mas também na medida em que olhamos "para baixo e através" dos Estados para o nível dos indivíduos, assim como "para cima e além" [dos mesmos Estados] para o nível do Sistema Internacional como um todo (BUZAN, 1991, p. 26 apud AMARAL, 2008, p. 68).

Os novos focos de análise de segurança permitiram que a Escola de Copenhague desenvolvesse novos instrumentos abrangentes a inclusão de novos atores e objetos de referência nos ESI. Neste sentido, a utilização da Escola de Copenhague, sob os parâmetros da Teoria da Securitização, possibilita que a análise seja levada até o nível individual, ao tornar capaz o entendimento de como as ameaças podem ser formadas socialmente e, ainda, consegue identificar os setores nos quais as ameaças podem causar efeitos.

Este fator é essencial para a dissertação em questão, ao considerar que o ciberespaço é o meio utilizado para a realização de ataques cibernéticos e que a interconexão de infraestruturas críticas não será restrita a apenas um setor. Isto é, a execução de um ataque

ciberterrorista pode gerar graves consequências a diversos setores de um Estado e, por isso, vê-se a necessidade de securitização e de estratégias contra essa ameaça.

Embasada na construção de uma agenda amplificada de segurança, tornou-se necessária, também, a especificação dos setores nos quais podem ocorrer a securitização. Dentre os setores de análise estão o militar, o político, o econômico, o societal e o ambiental[16] (BUZAN et al, 1998). Essa divisão tem por objetivo tornar as análises mais abrangentes visto que, em cada setor, existem objetos específicos de referência que podem ir para além da esfera do Estado e que podem ter sua segurança ameaçada (TANNO, 2003). Além da divisão por setores, são desenvolvidas as unidades de análise de segurança que constituem o processo de securitização. São elas: os objetos referentes, os atores securitizadores e os atores funcionais (BUZAN et al, 1998). Esses componentes serão abordados a seguir de forma a constituir uma base metodológica para a análise de securitização do ciberterrorismo.

Previamente, para sumarizar a Teoria da Securitização, tem-se que os processos de análise seguem um direcionamento para alcançar os resultados de um estado de securitização. Dessa forma, para a teoria ser aplicada à análise de determinada ameaça, deve-se: (i) reunir e analisar os discursos que discorram a respeito do tema em questão; (ii) aplicar e identificar as unidades de análise de segurança nos discursos analisados; (iii) verificar na análise dos discursos para qual setor de segurança a ameaça se destina; (iv) apurar a existência de ações realizadas pelos atores funcionais após os discursos e; (v) determinar se a ameaça encontra-se no nível não politizado, no nível politizado ou no nível securitizado.

Na dissertação, os focos de análises irão se restringir aos setores militar e político. Pelo fato da pesquisa ter como objetivo identificar o posicionamento estratégico de defesa cibernética dos EUA, a análise do setor militar se faz necessária. A lógica transfere-se também para o setor político, uma vez que o ciberterrorismo é uma ameaça politicamente motivada, que procura afetar a esfera governamental. No entanto, tais apontamentos não excluem as apresentações dos demais setores propostos pela teoria.

### 2.2.1 Conceito de securitização

[16] O setor econômico, o setor ambiental e o setor societal são aqueles que representam o alargamento da agenda de segurança desenvolvido pela Escola de Copenhague visto que, ao longo do século XX, os setores militares e políticos eram os objetos de referência utilizados com maior frequência nos tradicionais estudos de segurança (DUQUE, 2008).

A Teoria da Securitização, criada por Buzan, Weaver e De Wilde (1998), no livro *Security: a new framework of analysis*, tem como base a compreensão schimittiana do Estado de exceção, a teoria dos atos de fala e os debates em torno da agenda segurança – este último, já discutido anteriormente. Em primeira instância, os autores compreendem a segurança como um ato de fala. Isso significa que, para se tratar uma questão como prioridade de segurança, necessita-se que um representante estatal declare uma situação de emergência. Entretanto, para tornar legítimas quaisquer ações tomadas em prol do combate ao desenvolvimento da ameaça, deve-se previamente haver a aceitação do discurso por um determinado público (BUZAN; HANSEN, 2012).

> Ameaças e vulnerabilidades podem surgir em muitas áreas diferentes, militares e não-militares, mas para considerá-las como questão de segurança, precisam atender a critérios estritamente definidos que as distinguem do curso normal do meramente político. Elas devem ser encaradas como ameaças existenciais a um objeto de referência por um agente securitizador, que por sua vez gera endosso para medidas de emergência, além das regras que, de outra forma, seriam vinculadas (BUZAN, 1997, p. 13, tradução nossa).

Adicionalmente, o conceito de Estado de exceção define que os Estados liberais, quando se sentem existencialmente ameaçados, tendem a sobrepor-se às normas gerais pré-estabelecidas, alegando legitimidade nas suas justificativas a favor de uma ação imediata. Buzan (1997) sustenta esta argumentação ao inferir que a securitização em si legitima o uso da força por tratar de casos que sairiam da lógica política habitual, evidenciando a circunstância com o termo ‘política de pânico’ em sua análise.

A teoria apresenta um nivelamento em escala que possibilita a identificação da securitização como o extremo da politização. Essa identificação poderá variar de acordo com as circunstâncias que o cenário propor. O caráter não politizado ocorre quando a ameaça está fora das discussões e das decisões políticas, não havendo a necessidade do Estado em levá-la ao debate público. Em contrapartida, o politizado acontece quando o Estado se utiliza da ameaça para tratar das políticas públicas, sendo exigida uma decisão governamental. Já a securitização ocorre quando as ameaças ultrapassam a esfera das decisões políticas na necessidade de medidas e ações excepcionais que podem violar, por exemplo, a própria legislação (BUZAN, 1997; MOTTA, 2014).

De acordo com esse nivelamento, a criação do conceito de securitização parte do propósito de oferecer um termo capaz de distinguir as ameaças existenciais dos normais

problemas de segurança. Buzan et al (1998) afirmam que o critério de securitização está no estabelecimento de uma ameaça existencial que pode gerar ações políticas substanciais. No mais, defendem que, para se identificar um processo de securitização, basta analisar os discursos, a movimentação política e verificar os procedimentos, as normas e as regras que saem do percurso gradual da política que estava sendo adotada.

No entanto, não é suficiente identificar uma ameaça apenas pela concepção anterior. Deve-se, também, incluir a análise dos discursos nesse processo, uma vez que são neles que se apresentam a colocação social de uma ameaça existencial. Isto é, apenas pode ser dada uma movimentação política como securitização ao se verificar ímpetos discursórios que incitem na imposição de uma ameaça a um público que a aceite como tal. Buzan et al (1998, p. 21, tradução nossa) ainda definem que "a inovação da segurança tem sido a chave para legitimar o uso da força, mas de maneira geral abriu o caminho para o Estado mobilizar-se, ou para tomar poderes especiais, para lidar com ameaças existenciais". Ou seja, os discursos proferidos pelos atores securitizadores – que serão vistos adiante – devem ser aceitos socialmente pela audiência que os recebe.

> [...] um tópico somente é securitizado se e quando a audiência o aceitar como tal. Por isso, o caso da securitização é uma negociação entre um agente-securitizador e a audiência – ou seja, dentro de uma unidade (Estado) – e que somente assim o agente-securitizador poderá conseguir a permissão para não levar em consideração as regras vigentes, ou então, mudá-las, pois caso contrário ele as seguiria (RUDZIT, 2005, p. 309).

O ato de securitização ainda pode violar práticas políticas do estado de direto com a finalidade de bloquear potenciais ameaças, assim como, pode se tornar capaz de realizar, também, violações às soberanias de outros Estados (TANNO, 2003). Em outras palavras, "a securitização não é cumprida apenas pela quebra de regras (que pode assumir muitas formas) nem somente pelas ameaças existenciais (que pode levar a nada), mas por casos de ameaças existenciais que legitimam a quebra de regras" (BUZAN et al, p. 25, 1998). Todavia, não significa que todas as ameaças sejam consideradas como questões de segurança. Ao considerar que não são todas as questões políticas que se tornam prioridade de segurança, é preciso, previamente, gerar uma construção discursiva do caráter da ameaça que forneça o consentimento de uma audiência deliberada (BUZAN; HANSEN, 2012).

De acordo com Buzan et al (1998), o processo de securitização é intersubjetivo. Ou seja, a distinção do conceito de segurança para o conceito de securitização está na emergência da questão. Entra-se em um discurso coletivo de sobrevivência estatal ao se ter que lidar com ameaças que necessitam de priorização extrema. Além do mais, percebe-se que a utilização de

termos discursivos expansivos e que conferem gravidade em sua totalidade dizem respeito as ameaças que são capazes de desestabilizar um Estado. Buzan (1997) afirma que para uma execução analítica ser bem-sucedida no âmbito da securitização, no processo, deve-se desviar das ameaças objetivas na intenção de se buscar uma compreensão compartilhada e pública do que deve ser tratado e respondido como ameaça.

> Quando um ator securitizador usa a retórica da ameaça existencial e tira uma questão sob as condições de uma "política normal", temos um caso de securitização. Assim, a definição exata e os critérios de securitização são constituídos pelo estabelecimento intersubjetivo de uma ameaça existencial com uma importância suficiente para ter efeitos políticos substanciais (BUZAN et al, 1998, p. 25, tradução nossa).

No âmbito da teoria da linguagem, securitização pode ser traduzida em atos de fala. De acordo com Pierre Bourdieu (1991), o que fundamenta um ato de fala é, principalmente, a figura de alguma autoridade que impele o discurso. Este fator é imprescindível ao vislumbrar o consenso social e o aceite comum sobre determinada ameaça. Bourdieu ainda descreve que existem condições sociais que facilitam a aprovação do discurso e que, em casos excepcionais, podem ocorrer trocas simbólicas de palavras ou expressões na intenção de convencer o ouvinte. Em outras palavras, "um tópico se torna de segurança não necessariamente por causa da existência de uma ameaça real, mas porque ele é apresentado como uma ameaça" (RUDZIT, 2005, p. 309).

Como exemplo específico desse aspecto, pode-se identificar, na natureza dos discursos de George W. Bush, pós-11 de setembro, palavras do contexto de guerra, além do ideal de que aqueles que não se posicionassem contra o terrorismo, seriam considerados terroristas. Tais características, em sua primeira instância, demonstravam um discurso de securitização e que, logo, o combate ao terrorismo transformar-se-ia em políticas de segurança e defesa nos EUA. No entanto, não necessariamente é preciso haver nos discursos a identificação da expressão da segurança como propriamente dita. A intenção encontra-se em promover a aceitação de um tema a uma audiência pública significativa, mesmo em termos de uma necessidade de segurança extrema ou de utilização da segurança como uma referência para o discurso securitizador (BUZAN, 1997).

Cabe elucidar que, pelo fato das questões de securitização serem tradadas pela urgência, as operações de defesa assumem protagonismo em relação as ações definidas no escopo político. Isso porque, segundo Thierry Balzacq (2011, p. 1, tradução nossa), a securitização pode ser considerada como um processo estratégico embasado na "configuração das circunstâncias, incluindo o contexto, a disposição psico-cultural da audiência, e o poder que

tanto o orador quando o ouvinte trazem para a interação". Por estes termos, a presente dissertação propõe identificar a securitização do ciberterrorismo nos EUA ao mesmo tempo em que constrói uma frente de análise sobre o posicionamento estratégico de defesa cibernética do país em relação a ameaça.

> Se a ação estratégica do discurso opera no nível da persuasão e usa vários artefatos (metáforas, emoções, estereótipos, gestos, silencio, e, até mesmo, mentiras) para alcançar seus objetivos, o ato de fala procura estabelecer os princípios universais da comunicação, valor do qual deve ser funcional, independente do contexto, cultura e de qualquer que seja o poder relativo dos atores (BALZACQ, 2011, p. 2, tradução nossa).

Portanto, Buzan et al (1998) sintetizam que, para que seja evidenciada a securitização, deve-se haver três componentes: uma ameaça existencial declarada por meio do discurso, uma ação emergencial aprovada pela audiência e a legitimação de ações que podem transpassar a política governamental vigente. Enquanto qualquer dessas etapas esteja em processo de aceitação discursiva em prol da segurança, determina-se que o objeto de referência encontra-se em um movimento de securitização, uma vez que "uma ordem sempre depende da coerção e do consentimento. Já que a securitização nunca pode ser imposta, há necessidade de argumentar" (BUZAN et al, p. 25, 1998). Neste sentido, compreende-se securitização como parte de uma ação estratégica que visa a aprovação pública de um discurso em favor da segurança e defesa de determinado objeto ameaçado.

### 2.2.2 Unidades de análise de segurança

Considera-se que um estado de securitização é observado a partir da movimentação de segurança em torno de um alvo ameaçado, desde o discurso até a execução de ações legítimas contra a ameaça. No entanto, para ser feita a análise desse processo, devem-se ser verificadas as dinâmicas das unidades de análise de segurança. Dentro desse escopo, Buzan et al (1998) as segmenta em objeto de referência, atores securitizadores e atores funcionais. O objeto de referência diz respeito aos elementos que podem ser existencialmente ameaçados e que detém a legitimação para manter sua sobrevivência. Os atores securitizadores referem-se àqueles que declaram algo como fator de segurança – por meio dos discursos. Já os atores funcionais são aqueles que afetam a dinâmica dos setores securitizados, ou seja, influenciam as tomadas de decisões no âmbito da segurança. Ambos serão tratados de forma mais abrangente durante a seção (BUZAN et al, 1998; BALZACQ, 2011).

Ao longo dos ESI, o objeto de referência tem sido o Estado. É compreensível entender esse aspecto ao identificar diversos temas de segurança ligados a ele, como soberania, nação e identidade. No entanto, a Escola de Copenhague argumenta que o estreitamento a apenas uma ótica de análise impede que outras fontes sejam consideradas como problemas de segurança. Outro aspecto é que os atores securitizadores possuem a capacidade de construir discursivamente um objeto de referência, assim como, alguns objetos de referência possuem maior probabilidade de serem ameaçados e defendidos discursivamente. A Escola ainda reconhece que o Estado contém os meios necessários para defender-se e, por isso, compreende o motivo das análises serem maior direcionadas a ele (BUZAN et al, 1998).

Segundo Buzan et al (1998, p. 36, tradução nossa), "a ação de segurança é geralmente tomada em nome e com referência a uma coletividade". Isto é, pelo fato do discurso voltar-se a uma limitada audiência, o agente securitizador deve ter conhecimento sobre a coletividade a que se destina, assim como, ser pertencente a ela para que uma securitização seja bem sucedida. Dessa forma, dificilmente grupos minoritários – grupos de indivíduos – ou agentes sistêmicos – organizações internacionais – darão início a um processo de securitização. Aqueles que possuem coletividades limitadas como, por exemplo, o Estado, as nações e as civilizações, apresentam-se mais propensos a estabelecer a securitização e a servirem de objeto de referência (BUZAN et al, 1998).

> Objetos de referência devem estabelecer legitimidade de segurança em termos de uma reinvindicação de sobrevivência. Burocracias, regimes políticos e firmas raramente detêm essa sensação de sobrevivência garantida e, portanto, não costumam ser classificados como objetos de referência. Logicamente, eles poderiam tentar estabelecer uma reinvindicação de sobrevivência e, portanto, legitimidade de segurança, mas, empiricamente, a segurança não é totalmente subjetiva. Existem limites socialmente definidos para o que pode e o que não pode ser securitizado, embora esses limites possam ser alterados. Isso significa que a análise de segurança está interessada principalmente em casos bem-sucedidos de securitização – os casos em que outras pessoas seguem a liderança securitizadora, criando uma constituição social e intersubjetiva de um objeto de referência em grande escala (BUZAN et al, 1998, p. 39, tradução nossa).

Existem casos, ainda, em que o objeto de referência pode se confundir com o agente securitizador. Exemplo disso, é quando se tem o Estado como objeto de referência e determinado agente político representa o governo vigente. De forma mais abrangente, "o Estado (geralmente) tem regras explícitas sobre quem pode falar em segurança nacional, então quando um governante diz 'nós temos que defender a nossa segurança nacional', ele tem o direito de agir em nome do Estado" (BUZAN et al, p. 41, 1998, tradução nossa). No entanto, a nível de

análise, se deve realizar a separação do objeto e do agente para a verificação de um estado de securitização.

> Esses atores geralmente não são objetos de referência para segurança, porque raramente podem falar em segurança por meio da referência à necessidade de defender sua própria sobrevivência. Seu argumento, normalmente, é que é necessário defender a segurança do Estado, nação, civilização ou alguma outra comunidade, princípio ou sistema maior. Apenas ocasionalmente atores como governos ou empresas poderão falar de maneira sucinta da segurança em seu próprio nome (BUZAN et al, 1998, p. 40, tradução nossa).

Assim, os atores securitizadores são os grupos ou indivíduos que reproduzem os discursos na intenção de alcançar a securitização. Nesse caso, podem ser considerados os entes de pressão que incitem o tópico da segurança como, por exemplo, os líderes políticos. Sob essa classificação, verificam-se argumentos de segurança voltados para o ambiente estatal ou das coletividades. Isso vai variar de acordo com a natureza da questão que virá a ser securitizada. Deste modo, tem-se que a identificação de atores pode oferecer maiores desafios do que o reconhecimento dos objetos de referência, uma vez que pode permear diferentes níveis de análises (BUZAN et al, 1998).

No entanto, a distinção entre o objeto de referência e o agente securitizador pauta-se sobre a constituição do discurso. O ator securitizador, a partir da lógica de estabelecer a aprovação e o convencimento de uma audiência sobre determinada questão, percorre a função de demonstrar algum problema emergencial de segurança ao público, com o objetivo de tornar suas ações excepcionais legitimadas. Outro fator distinto, também, é que, quando se tem o Estado como objeto de referência, por exemplo, consequentemente o representante do governo vigente possui genuinamente a legitimidade de expor à público os problemas de segurança e tentar convencê-los sobre a necessidade de segurança. Com base nessas premissas, considera-se que os atores securitizadores são os sujeitos que declaram a ameaça a determinado objeto de referência (AMARAL, 2008).

Por último, os atores funcionais podem ser caracterizados, de maneira geral, como os provedores da segurança. Ou seja, são as unidades de segurança do objeto de referência (BUZAN et al, 1998). Geralmente, são "atores que afetam a dinâmica do setor. Sem ser o objeto de segurança ou o ator que solicita segurança em nome do objeto de referência, esse é um ator que significativamente influencia as decisões no campo de segurança (BUZAN, et al, 1997, p. 36, tradução nossa). Essa característica pode ser vista em diversas áreas como, por exemplo, no setor militar, na indústria de armamentos e nas agências governamentais que regulam as políticas externa e interna de defesa. Pode ser exemplificado, ainda, o setor ambiental, no

qual os atores funcionais podem ser os atores econômicos, agências governamentais, organizações não-governamentais, entre outros (DUQUE, 2008).

Duque (2009) argumenta que, a partir da divisão das unidades de análise de segurança, possibilitou-se à Escola de Copenhague a ampliação dos níveis de análise para além da unidade do Estado. É notável ainda que, pelo fato de os objetos referentes passarem a ser definidos por valores e objetivos amplificados, não há a divisão entre o nível doméstico e o internacional. Essa última característica também diz respeito às análises dos setores de segurança. Mediante a ampliação da agenda de segurança apresentada pela Escola de Copenhague, a extensão do conceito de segurança permitiu a criação de uma nova ferramenta/método de análise, a partir da identificação de componentes pertencentes ao processo de securitização de determinado objeto.

### 2.3.3 Abordagem dos multisetores de segurança

Tendo em vista que os setores são unidades que interagem e são pertencentes ao sistema nacional e internacional, Buzan (1997) afirma que o propósito da análise neste âmbito insere-se em sua distinção – ao mesmo tempo em que em sua interação. O autor reconhece que a análise dos setores em unidades específicas pode alcançar diferentes resultados. Não apenas, argumenta que "a natureza da sobrevivência e ameaças irão diferir em diversos setores e tipos de unidades" (BUZAN, 1997, p. 15, tradução nossa). Neste sentido, o autor aborda os multisetores de segurança em militar, político, econômico, societal e ambiental.

> Uma maneira de olhar para os setores é vê-los identificando tipos específicos de interação. Nesta visão, o setor militar é sobre relações de coerção da força; o setor político é sobre relações de autoridade, status governante e reconhecimento; o setor econômico é sobre relações de comércio, produção e finanças; o setor societal é sobre relações de identidade coletiva; e o setor ambiental é sobre as relações entre a atividade humana e a biosfera planetária (BUZAN et al, 1997, p. 7, tradução nossa).

No setor militar, o Estado é tido como o principal objeto de referência e, conforme já elucidado na seção anterior, o objeto também pode ser estendido para as entidades políticas, em casos específicos. As questões voltadas para esse setor englobam todos os processos internos e externos das comunidades que possuem mecanismos governamentais que envolvam o uso do poder militar para, principalmente, a manutenção da soberania em relação às ameaças. Tendo como principal característica a abordagem de coerção de força (BUZAN et al, 1998), Grace Tanno (2003) apresenta que a utilização recorrente do monopólio da força no setor militar auxilia na legitimidade da ação emergencial para a proteção contra as ameaças nacionais.

> Quando a securitização é focada em ameaças externas, a segurança militar é principalmente sobre a interação de dois níveis entre as reais capacidades ofensivas e defensivas dos Estados, por um lado, e intenções um do outro, por outro. As ameaças externas vão desde o medo da obliteração completa do Estado, da sociedade e das pessoas até a coerção ao estilo da diplomacia e intimidação em questões específicas da política (BUZAN et al, p. 51, 1998, tradução nossa).

Não sendo todos os casos militares considerados como problemas de segurança, Buzan et al (1998) apontam casos em que são realizadas intervenções humanitárias para a manutenção da paz e da ordem mundial. Além da defesa e segurança dos Estados no âmbito militar, o setor também interage com as intimidações não-militares nos casos em que se apresentam ameaças ideológicas contrárias ao país. Esta particularidade pode-se atribuir a esfera dos ataques cibernéticos produzidos por atores não estatais. Tais peculiaridades remetem à ampliação da agenda militar explorada pela Escola de Copenhague. Além disso, quando um objeto de referência torna-se securitizado na esfera militar, evidencia-se o estado de securitização por meio da própria lógica de equiparação de forças e imperativos tecnológicos entre os envolvidos. Logo, é no setor militar que a securitização é melhor vislumbrada (BUZAN et al, 1998).

No setor político, as ameaças encontram-se sobre o Estado, porém, com foco no âmbito constitucional. Ou seja, as ameaças à soberania podem significar contrapontos à legitimidade estatal, ao governo ou à autoridade política. Tanno (2003) traduziu este último pensamento em ameaças intencionais ou estruturais. A primeira refere-se à ameaças políticas identificadas quando um Estado não reconhece a legitimidade de outro Estado ou grupos domésticos não legitimam determinado governo. A segunda surge quando há contradições organizacionais dentro do Estado. Em síntese, o setor político abriga ameaças contra a soberania nacional e a ideologia política adotada.

Fator importante encontra-se na atuação do setor político nos casos de securitização. Por ser o setor mais amplo desenvolvido pelos teóricos de Copenhague, a agenda política pode ser expandida para a segurança individual. Por preocupar-se com a segurança política das unidades, a ampliação estende-se para os níveis sistêmicos da Sociedade Internacional e do Direito Internacional, assim como, para as demandas e condições individuais, mediante os Direitos Humanos. Contudo, Buzan et al (1998) argumentam que, como as características gerais de segurança são também consideradas como segurança política, há pouca possibilidade de que a ameaça voltada para este setor seja puramente política, sem haver relação com os outros setores. As ameaças provenientes do espaço cibernético, neste sentido, adequa-se a colocação acima ao ter a capacidade de permear os multisetores, de acordo com a motivação.

No setor econômico, os objetos de referência são mais difíceis de serem identificados. Tem-se a premissa de que a securitização pode se dar tanto na esfera privada quanto pública. No entanto, é no âmbito estatal que a segurança nacional trata de questões de sobrevivência. Por exemplo, crises econômicas em períodos de guerra podem gerar incapacidades para manutenção da segurança da própria população. No entanto, Tanno (2003) acrescentou que podem ser identificados como objetos de referência as instituições liberais – que defenderão que o Estado é ocupado pelas regras que permitem o bom funcionamento dos mercados –, regimes econômicos específicos e o próprio mercado.

Buzan et al (1998) afirmam que a lógica de segurança econômica para os Estados pode ser exemplificada ao considerar que os Estados possuem a capacidade de formar sistemas econômicos autônomos. Se o Estado não for autossuficiente em termos de indústria e alimentação para sua população, será necessário buscar suprimentos externos. O problema de segurança encontra-se justamente quando determinada ameaça interfere diretamente sobre esse processo, sendo necessária a tomada de decisão sobre os preceitos de securitização, tornando a economia nacional legitimamente securitizada mediante a realização e a aprovação prévia dos discursos.

No setor societal, os objetos de referência estão nas identidades coletivas, na cultura e na religião. Diferentemente do setor político que mantém o foco na segurança humana para a estabilidade e legitimidade do Estado, no societal, a principal reflexão encontra-se sobre uma unidade de segurança social que foge da esfera apenas territorial. Isto é, recorre à segurança das comunidades que se identificam ideologicamente e culturalmente fora de uma dimensão apenas espacial (BUZAN et al, 1998).

Segundo Tanno (2003), os pesquisadores da Escola de Copenhague partem do pressuposto de que a sociedade depende da existência da identidade coletiva para criar um sentimento de pertencimento a determinado grupo, constituindo uma unidade. Assim, podem ser consideradas como ameaças societais, portanto, as sociedades ou as identidades dos grupos que se encontram ameaçadas. Em outras palavras, "ameaças societais encontram-se em Estados fracos, em que a sociedade e Estados não se harmonizam. Nestes, os próprios governos poderão ameaçar identidades que lhe são hostis" (TANNO, 2003, p. 64).

No setor ambiental, por fim, os objetos de referência podem ser os mais variados possíveis. Tendo em vista a diversidade da biosfera, entra-se no contexto as questões de sobrevivência de espécies – incluindo a humana e manutenção dos habitats naturais. Nesse setor, duas agendas principais podem ser apontadas, a científica e a política. A primeira constitui as informações sobre os problemas de segurança ambientais enquanto que, a segunda,

refere-se a adoção de políticas públicas para lidar com tais questões. Outros aspectos são que, a agenda científica preocupa-se com a securitização do setor, ao passo que a agenda política responsabiliza-se por gerar conscientização coletiva, gestão político-ambiental no nível internacional e aceitação do compromisso político para com o meio ambiente (BUZAN et al, 1998). Os objetos de referência podem ser identificados como o próprio meio ambiente e a qualidade de vida alcançada (TANNO, 2003).

Portanto, a abordagem multisetorial desenvolvida pela Escola de Copenhague ampliou o alcance das análises nos ESI. A fragmentação dos setores estratégicos, como ferramenta para a execução de pesquisas para além da lógica estatal, traduz o esforço teórico promovido pela Escola no pós-Guerra Fria, assim como, a propriedade da Teoria da Securitização para análises envolvendo as novas ameaças. Quando tratadas das ameaças cibernéticas, a ferramenta de execução de ataques é o ciberespaço, componente importante para as operações e relações cotidianas.

É importante acrescentar que, por mais que os teóricos de Copenhague não tenham inserido especificamente aos estudos de segurança os temas voltados para a revolução da informação e das novas tecnologias, o método de análise criado permite a identificação particular de um estado de securitização de determinado objeto de referência, assim como, a agenda de segurança proposta (JORGE, 2014). Sob essa perspectiva, ameaças a determinado setor podem gerar consequências aos setores e elementos a eles adjacentes e, por isso, a manutenção da segurança e defesa cibernética de um país torna-se essencial, como será analisado no capítulo seguinte.

# 3. TEORIA DA SECURITIZAÇÃO DA ESCOLA DE COPENHAGUE APLICADA NOS EUA PÓS 11 DE SETEMBRO DE 2001

O arcabouço teórico proposto pela Escola de Copenhague permite que as análises sobre as questões de segurança sejam realizadas com o objetivo de alcançar resultados direcionados sobre o estado de securitização de determinado tema, assim como define para que setor estratégico a securitização se dirige. A aceitação social de um discurso, enfatizado sobre aspectos emergenciais, exerce a capacidade governamental de moldar os processos políticos a partir de ações imediatas que podem, até mesmo, violar a própria legislação (BUZAN et al, 1997). Consequentemente, a construção de objetos legais de segurança e defesa tornam-se necessários para a sucessão da legitimidade das atividades políticas em torno do tema estabelecido.

O discurso político de determinado governo, como instrumento crucial de convencimento da audiência, parte de concepções políticas acerca de um contexto histórico ou, em casos mais extremos, de eventos ocorridos repentinamente. Segundo Barros (2015), a formação discursiva parte da interação do enunciado, do sujeito e da ideologia. Considerando que o desenvolvimento do discurso depende de uma posição espacial-temporal, as palavras ou frases ideológicas podem conter significados distintos de acordo com a diferenciação dos sujeitos e dos contextos. Ou melhor, o discurso é capaz de traduzir as intenções dos governos a respeito do seu posicionamento estratégico ao oferecer elementos peculiares para a análise e interpretação dos acontecimentos, sob uma conjuntura específica.

Balzacq (2011) exemplifica tal fundamento ao adotar o termo denominado de "competência linguística". De acordo com o autor, a esfera política depende de autoridades capazes de articular argumentos para o alcance dos seus objetivos políticos. Todavia, em relação às questões de segurança, as informações privilegiadas são concentradas nas autoridades com posições influentes. Presumivelmente, os discursos provenientes desses agentes transmitem confiabilidade para a audiência. Essa característica, ao ser elencada a um discurso voltado para uma ação emergencial, contra uma ameaça à sobrevivência do Estado, possui a capacidade de obter o consentimento imediato do seu público-alvo. Dessa forma, o agente securitizador alcança o objetivo de tornar legítimas as ações do Estado ao tornar os interesses comuns.

Baseado nessas premissas, este capítulo tem por finalidade analisar os discursos presidenciais norte-americanos proferidos nos governos Barack Obama (2009-2016) e Donald Trump (2017-2019), sobre os temas voltados para segurança, defesa e ameaça cibernética. Por

mais que a pesquisa propõe-se a analisar os discursos realizados pós-11 de setembro, a palavra '*cyber*' surge apenas nos discursos do presidente Barack Obama a partir de 2009, conforme será visto a seguir.

A concepção ideológica de terrorismo nos discursos do presidente George W. Bush se faz necessária para a compreensão da ameaça do ciberterrorismo. Além disso, a modificação política imediata realizada para o combate do terrorismo, após os atentados, corresponde a um exemplo recente de securitização nos EUA. A partir dessa concepção, propõe-se verificar um possível processo de securitização sobre a ameaça do ciberterrorismo mediante a análise dos discursos e a compreensão sobre a estruturação do posicionamento de defesa cibernética dos EUA. Portanto, este capítulo visa aplicar a teoria da securitização sobre o cenário dos EUA pós-11 de setembro.

Para isso, foi utilizado o software de análise de dados qualitativos NVIVO 11, como ferramenta para a análise dos discursos presidenciais. Em primeira instância, para identificar os discursos com os assuntos correlatos anteriormente citados, foram aplicadas as palavras-chave: *cyber*, *cyber security*, *cyber defense*, *cyber threat*, *cyber attack*, *cyberterrorism*, *hacker* e *terrorism*. De um total de 106 discursos, apurados nos três governos, verifica-se no Quadro 2 a frequência com que as palavras-chave anteriormente indicadas surgem[17]. Em seguida foram individualmente examinadas as frases, os termos e o contexto histórico dos discursos sobre as questões referentes a pesquisa.

**QUADRO 2**

Frequência das palavras-chave nos discursos presidenciais pós 11 de setembro

| Palavras-chave | Fontes | Referências |
|---|---|---|
| *Cyber* | 6 | 9 |
| *Cyber security* | 0 | 0 |
| *Cyber defense* | 1 | 1 |
| *Cyber threat* | 3 | 3 |
| *Cyber attack* | 3 | 3 |
| *Cyberterrorism* | 0 | 0 |
| *Hacker* | 7 | 2 |
| *Terrorism* | 33 | 56 |

Fonte: Elaboração própria baseada nos dados do NVIVO 11, 2019.

[17] A reunião e captação dos discursos presidenciais encontram-se no site do Miller Center (<https://www.millercenter.org/the-presidency/presidential-speeches>), centro de pesquisa educacional vinculado à Universidade da Virgínia, EUA.

De antemão, cabe acrescentar que a não aparição da palavra ‘ciberterrorismo’ nos discursos analisados, não indica a falta de referência a ameaça ao vê-la sobre um contexto discursivo. Mesmo que em quantidade nula, verifica-se a inserção do conceito durante o discurso e a pauta sobre necessidade de atenção sobre as ameaças cibernéticas nos EUA. O mesmo acontece com o termo cibersegurança. Outro aspecto complementar importante de ser evidenciado é que, dentre os discursos proferidos que envolveram a temática da cibernética, a maior incidência ocorreu na governança do presidente Barack Obama, com exceção de um único discurso promovido pelo presidente Donald Trump.

Dessa forma, serão apresentadas, a seguir, as análises dos discursos presidenciais, já inseridos no contexto da teoria da securitização e das unidades de análise de segurança. No mais, buscar-se-á identificar sobre quais setores de segurança os discursos se destinam, considerando o momento histórico do enunciado. Com isso, poderá ser verificada a existência de um movimento de securitização em torno do ciberterrorismo e, em conjunto, evidenciar uma maior incorporação do tópico de cibernética nos discursos estadunidenses.

### 3.1. Análise de discursos: unidades e setores de segurança

De acordo com Fernandes (2008), os discursos surgem como um meio de materializar uma ideologia por intermédio da linguagem. Na esfera militar e política, a afirmativa se traduz em pleitear um posicionamento nacional frente aos desafios internos e externos enfrentados pelo Estado. Sob esta lógica, a teoria da securitização sugere que, para examinar a disposição dos discursos nos níveis não politizados, politizados e securitizados de um ente em relação a determinada ameaça, deve-se aplicar o procedimento das unidades de análise de segurança (objeto de referência, ator securitizador e ator funcional), sobre o setor que se apresenta em risco (BUZAN et al, 1998).

Em vista disso – e com base nos dados anteriormente mencionados no Quadro 2 –, serão analisados cronologicamente, nesta seção, os sete discursos presidenciais estadunidenses que possuem termos que envolvem a cibernética. São eles o *Address before a joint session of Congress* (2009), o *Address to the British Parliament* (2011), o *State of the Union Address* (2012), o *State of the Union Address* (2013), o *State of the Union Address* (2014), o *State of the Union Address* (2015)[18] e o *Remarks on National Security Strategy* (2017) – este último, um

[18] É importante elucidar que os discursos nomeados ‘*State of the Union Address*’ são considerados como significativos relatórios anuais, tradicionalmente proferidos pelo Presidente em exercício dos EUA. Com a finalidade de apresentar discursivamente os projetos do Poder Executivo e as prioridades governamentais para o

dos mais importantes dentro desse escopo. Ainda, será possível identificar a integração e correlação das palavras-chave propostas nos discursos estabelecidos.

### 3.1.1. *Address before a joint session of Congress* (2009)

A primeira vez que a palavra '*cyber*' esteve presente em um discurso presidencial foi em 24 de fevereiro de 2009, antes da tradicional sessão conjunta do Congresso norte-americano. Com o objetivo de apresentar as ciberameaças como um dos desafios do século XXI, o termo é referenciado apenas uma vez durante todo o discurso, ao lado de outras questões de segurança como o terrorismo, a proliferação nuclear, as pandemias e a pobreza extrema. Neste sentido, o presidente Barack Obama aponta como solução para tais desafios o fortalecimento das antigas alianças, a formação de novas alianças e o uso de todos os elementos do poder nacional.

Contudo, a principal menção do discurso destina-se à recuperação norte-americana contra a crise financeira instaurada em 2008. Tendo como público alvo os congressistas republicanos e democratas, o discurso visa promover a união política e popular para a resolução da recessão econômica. Para o alcance desta finalidade, o Presidente apresenta ao Congresso os objetivos fundamentais de investir em energia, saúde e educação e defende: "eu quero que todos os americanos saibam disso: nós vamos reconstruir, nós vamos recuperar e os Estados Unidos da América irão emergir mais fortes do que nunca" (USA, 2009, tradução nossa).

Logo, ao se tratar das questões de segurança, elucidam-se os desafios norte-americanos quanto as ameaças internas e externas, mesmo que apenas por citação. Ao aplicar as unidades de análise de segurança no contexto do termo '*cyber threats'*, neste caso, apresenta-se como objeto de referência os EUA, como ator securitizador o presidente Obama e como ator funcional os elementos de força nacional, ou seja, as Forças Armadas. Portanto, nota-se que a ameaça cibernética é um desafio para o setor militar.

Mesmo com a singela utilização do termo 'ciberameaça', o discurso tinha por finalidade promover diretrizes para a segurança econômica dos EUA no cenário de crise e não a de expor profundamente todas as ameaças que o país enfrentava. No discurso, analisa-se que a temática cibernética encontra-se no nível não politizado da ameaça, isto é, a ameaça ainda não é levada ao debate público geral e às decisões políticas. Todavia, é possível verificar, nesse momento, a

Congresso Nacional, esses são realizados, geralmente, no mês de janeiro, com o propósito de informar e orientar os congressistas sobre o planejamento nacional para o ano que se inicia (FELINI, 2017).

articulação inicial do governo para chamar a atenção da audiência congressista para as ameaças cibernéticas como questões emergentes de segurança nacional.

Sob esta concepção, agrega-se ainda que, em 2009, os eventos cibernéticos já faziam parte das pautas nacionais e internacionais. O uso do espaço cibernético como ferramenta de ataque na Operação *Iraqi Freedom*, em 2003 (ZUCARRO, 2011) e sua utilização no embate estratégico militar entre Israel e Síria na operação denominada *Orchard*, em 2007 (BIAZATTI, 2015), foram episódios que ilustraram a ação estatal por meio do uso do ciberespaço para fins políticos e militares. Ademais, a ocorrência dos ataques cibernéticos na Estônia que afetaram os sistemas de comunicação governamentais, bancários e de saúde, no ano de 2007 (MARQUES, 2011), e os ciberataques aos sites oficiais do governo realizados em conjunto com o conflito militar físico, na Geórgia, em 2008 (CARREIRO, 2012), podem ter sido fatores que desencadearam uma maior atenção política dos EUA para os desafios que o espaço cibernético impõem ao Estado.

### 3.1.2. *Address to the British Parliament* (2011)

No dia 25 de maio de 2011, o presidente Barack Obama realizou um discurso no Parlamento britânico referente ao papel dos EUA e do Reino Unido no mundo contemporâneo. Nele, demonstrou de forma histórica os resultados positivos gerados por meio dessa aliança estratégica e exaltou as atribuições de segurança bem executadas pela Organização do Tratado do Atlântico Norte (OTAN). Sob este mesmo direcionamento, discursou a respeito do estreitamento político dos dois países para atender aos objetivos comuns de democratização de determinados países do Norte da África, como Líbia e Tunísia, de controle sobre o armamento nuclear em países do Oriente Médio, como o Irã, e a erradicação do grupo terrorista Al-Qaeda, após a morte do seu líder Osama Bin Laden – que ocorreu no dia 02 de maio daquele ano.

> [...] por isso que construímos uma aliança que era forte o suficiente para defender este continente, enquanto dissuadimos nossos inimigos. Na sua essência, a OTAN está enraizada no conceito simples do Artigo Cinco: que nenhuma nação da OTAN terá de se defender sozinha; que os aliados ficarão um pelo outro sempre. E por seis décadas, a OTAN tem sido a aliança de maior sucesso na história da humanidade (USA, 2011, tradução nossa).

Sendo um discurso que incentiva a cooperação militar norte-americana e britânica para atuarem em conjunto contra os desafios de segurança internacional, o termo '*cyber attacks*' surge como referência às capacidades da OTAN para o combate às novas ameaças, juntamente

com os termos terrorismo, pirataria e mísseis balísticos. Contudo, assim como verificado no discurso de 2009, não houve o desenvolvimento da questão cibernética como tema emergencial de segurança. O foco manteve-se sobre o impedimento da proliferação de armas nucleares em países no Oriente Médio.

Esse aspecto possui características que refletem no ataque cibernético denominado "*Stuxnet"* no Irã, ocorrido no ano anterior a este discurso. É sabido que o país utiliza-se das atividades nucleares para a obtenção de fontes de energia. No entanto, a não adoção ao Tratado de Não Proliferação de Armas Nucleares (TNP) e a falta de informação sobre as funções realizadas no programa nuclear iraniano, geraram desconfiança aos demais países. Investigações sobre produções de armas nucleares foram conduzidas, principalmente, pelos EUA e Israel (LOPES; OLIVEIRA, 2014).

Neste contexto, e com o objetivo de serem exploradas as vulnerabilidades de uma usina nuclear iraniana, a ocorrência do ciberataque *Stuxnet* desencadeou alterações nas informações de funcionamento das centrífugas utilizadas para o enriquecimento de urânio, paralisando e inviabilizando a funcionalidade das máquinas por um período de tempo (LOPES; OLIVEIRA, 2014). Por mais que o cenário indique que o ataque fora realizado pelos EUA e Israel, oficialmente, os países nunca se responsabilizaram pela autoria do ataque. Vale especificar que, neste caso, a disseminação do vírus foi realizada por meio de *pendrives* introduzidos diretamente na usina de enriquecimento iraniana (CARREIRO, 2012).

> [...] compartilhamos um interesse comum em impedir a disseminação de armas nucleares. Em todo o mundo, as nações estão bloqueando materiais nucleares para que nunca caiam nas mãos erradas – por causa da nossa liderança. Da Coréia do Norte ao Irã, enviamos uma mensagem de que aqueles que ostentam suas obrigações irão enfrentar as consequências e é por isso que a América e a União Europeia recentemente reforçaram nossas sanções ao Irã, em grande parte por causa da liderança do Reino Unido e dos Estados Unidos. E, enquanto responsabilizamos outros, nós cumpriremos nossas próprias obrigações sob o Tratado de Não-Proliferação por um mundo sem armas nucleares (USA, 2011, tradução nossa).

Portanto, ao serem aplicadas as unidades de análise de segurança, neste escopo, tem-se como objetos de referências os EUA e o Reino Unido, o presidente Obama como o ator securitizador, a OTAN como o ator funcional, o parlamento britânico como a audiência e o setor militar a ser securitizado. Por se tratar novamente de apenas indicar o termo ciberataque, sem haver um maior aprofundamento sobre ele, denota-se que a concepção ideológica e política sobre as ameaças cibernéticas estadunidenses, no contexto, ainda permeavam o nível não politizado. Em outras palavras, o discurso não surtiu o esforço de promover uma aceitação pública comum sobre o tópico de segurança cibernética.

### 3.1.3. *State of the Union Address* (2012)

O tradicional discurso presidencial que inicia e direciona as atividades congressistas a serem cumpridas ao longo do ano se deu no dia 24 de janeiro, juntamente com o anúncio de que os EUA não iriam mais enviar tropas ao Oriente Médio e que os soldados norte-americanos seriam retirados do Iraque e do Afeganistão. Neste período, os EUA apresentaram melhoras econômicas – pós-crise de 2008 – mediante aumento da produtividade empresarial que, logo, gerou aumento na oferta de empregos. De acordo com o discurso, "uma economia construída na manufatura americana, energia americana, trabalhadores americanos habilitados e uma renovação dos valores americanos" (USA, 2012, tradução nossa).

Além de serem abordados assuntos relacionados à esfera econômica, questões sobre o complexo conflito ideológico dentro do Congresso norte-americano foram postas em pauta, com o objetivo de estimular o consenso entre os partidos democrata e republicano para a execução das políticas públicas. Outras características que estiveram presentes no discurso dizem respeito à liderança estadunidense no mundo, as fortes e antigas alianças com os países europeus e asiáticos, a proximidade política e a cooperação militar com Israel, além de outras coalizões que mantém a influência dos EUA no cenário internacional.

Neste sentido, o presidente Barack Obama utilizou este discurso para propor uma nova defesa estratégica em parceria com as lideranças militares com a finalidade de estabelecer a segurança de temas em destaque na agenda de segurança norte-americana como, por exemplo, o uso de materiais nucleares, a erradicação da fome e de doenças por meio de missões estratégicas, a estipulação de novas formas de lidar com os inimigos nacionais e os perigos promovidos por ataques cibernéticos.

> [...] trabalhando com nossos líderes militares, eu propus uma nova estratégia de defesa que assegura a manutenção dos melhores militares no mundo, ao mesmo tempo em que salvaguarda aproximadamente quase trilhões de dólares em nossos bolsos. Para ficar um passo à frente de nossos adversários, eu já enviei esta legislação para o congresso que irá proteger nosso país dos perigos crescentes das ameaças cibernéticas (USA, 2012, tradução nossa).

Entretanto, elucida-se que, quando o termo '*cyber threats'* surge no discurso, não são apresentados complementos discursivos acerca do tema. O argumento em torno de uma nova estratégia de defesa, que possui o poder de legislar ações defensivas contra as ciberameaças, mostra-se indefinido perante a audiência congressista. Logo, inserindo esta lógica às unidades

de análise de segurança, tem-se os EUA como o objeto de referência, o presidente Barack Obama como o ator securitizador e as Forças Armadas e as instituições políticas como os atores funcionais.

Conforme os princípios expostos denotam a característica de defesa nacional e a construção de uma estratégia nacional, é possível dizer que o discurso dirige-se ao setor militar e político. Ainda assim, nota-se que o fator mais importante para ser verificado, neste momento, é a passagem da temática cibernética do nível não politizado – que era presente até então – para o nível politizado de ameaça. Em outras palavras, exigiu-se do Congresso Nacional um posicionamento político sobre a estratégia de defesa sugerida pelo presidente Obama para, por fim, serem executadas novas políticas públicas que envolvessem o tópico proposto.

### 3.1.4. *State of the Union Address* (2013)

O desenvolvimento discursivo de assuntos relacionados à segurança e à defesa cibernética iniciou-se em 13 de fevereiro de 2013. Após o Congresso não aceitar as reduções orçamentárias recomendadas pelo presidente Obama – para a incorporação de uma nova estratégia de defesa que combatesse as ameaças cibernéticas, em 2012 –, o discurso expõe a necessidade de resposta imediata dos EUA contra o crescimento das ciberameaças e, logo, dos ataques cibernéticos. Sob esta perspectiva, são melhor esclarecidas, neste discurso, as palavras-chave '*cyber attack*', '*cyber defense*' e '*hacker*'.

> Agora, nós sabemos que os *hackers* roubam as identidades das pessoas e infiltram-se em e-mails privados. Nós sabemos que países e companhias estrangeiras trocam nossos segredos corporativos. Agora nossos inimigos também estão buscando a habilidade de sabotar nossas redes de poder, nossas instituições financeiras, nossos sistemas de controle do espaço aéreo. Nós não podemos daqui a alguns anos olhar para este momento e questionar por que não fizemos nada em relação às reais ameaças à nossa segurança e à nossa economia (USA, 2013, tradução nossa).

A tentativa presidencial de introduzir elementos para a defesa cibernética estadunidense corresponde aos desafios impostos pelo cenário internacional. Ao considerar o aumento da incidência de ataques cibernéticos no âmbito global, é inerente que mais setores se tornem ameaçados e carentes de assistência e proteção imediata das autoridades responsáveis. Isto é, na medida em que as deficiências nas infraestruturas críticas promovem a possibilidade de acesso ilegal aos sistemas informacionais – extensíveis ao aumento do número de ciberataques –, a atenção governamental tende a direcionar-se para a segurança e defesa dos setores estratégicos ameaçados.

No caso dos EUA, a preocupação emergente presente no discurso se dá pela construção de mecanismos capazes de tornar o país protegido ciberneticamente. Até dado momento, as pautas ligadas à segurança nacional enfatizavam a evolução do planejamento estadunidense contra o terrorismo e a não proliferação de armas nucleares. A citação de termos vinculados à ciberdefesa indicaram o direcionamento político de que, no futuro próximo, o Congresso deveria acelerar os processos para criar novas leis e mecanismos capazes de salvaguardar o país da ameaça cibernética. A declaração de fevereiro de 2013 demonstrou que as ameaças cibernéticas mereciam a atenção do governo e do Congresso ao considerar a habilidade de promoverem novos desafios para a segurança norte-americana. Com isso, o Presidente apresentou à audiência congressista uma ordem executiva com o objetivo de fortalecer as defesas cibernéticas do país.

> [...] eu assinei uma nova ordem executiva que irá fortalecer nossas defesas cibernéticas aumentando o compartilhamento de informações e desenvolvendo padrões para a proteção da nossa segurança nacional, nossos empregos e nossa privacidade. Mas agora o congresso deve agir também aprovando legislações para dar ao nosso governo uma maior capacidade de proteger nossas redes e deter ataques. Isso é algo que nós devemos ser capazes de fazer em uma base bipartidária (USA, 2013, tradução nossa).

A partir disso, ao serem aplicadas as unidades de análise de segurança, tem-se os EUA como objeto de referência, o presidente Barack Obama como ator securitizador e as Forças Armadas e as instituições políticas como os atores funcionais – para o estabelecimento da defesa cibernética estadunidense. Dessa forma, o discurso destina-se ao setor militar – por oferecer ameaças à segurança nacional – e ao setor político – por ameaçar a estabilidade política –. Compreende-se, portanto, que a discussão política permanece no nível politizado, porém, o discurso expõe com mais detalhes os desafios para a cibersegurança norte-americana, assim como incentiva a constituição de meios de proteção contra os crescentes perigos e ameaças.

### 3.1.5. *State of the Union Address* (2014)

Em 28 de janeiro de 2014, a declaração presidencial focou-se em tratar das questões de segurança voltadas para as operações de contraterrorismo e a responsabilidade governamental para com o Afeganistão. Sobre este tema, o Presidente proferiu as seguintes palavras: “se o governo afegão assinar um acordo de segurança, uma pequena força americana poderá permanecer no Afeganistão com aliados da OTAN para o [...] treinamento e assistência das forças afegãs” (USA, 2014, tradução nossa). Tal posicionamento pautou-se no objetivo norte-

americano de averiguar a existência de resquícios do grupo *Al Qaeda* no país mediante realização de operações de contraterrorismo.

A elucidação discursiva de que a ameaça do terrorismo ainda permanece constante para os EUA – mesmo anos após a ocorrência dos ataques do 11 de setembro – propõe a contínua liderança estadunidense em relação ao combate ao terrorismo no país e no mundo. Nos países do Oriente Médio, o argumento a favor de medidas contra a ameaça mantém-se sobre o desenvolvimento de parcerias para desabilitar as redes terroristas. No entanto, "enquanto colocamos a liderança central da *Al Qaeda* em um caminho para a derrota, a ameaça evoluiu, à medida que afiliados da *Al Qaeda* e outros extremistas se enraízam em diferentes partes do mundo" (USA, 2014, tradução nossa).

A partir desses preceitos, o discurso presidencial pondera a influência norte-americana no mundo na medida em que expõe o fortalecimento de suas próprias defesas. É mencionado o combate contra as novas ameaças, como os ataques cibernéticos. Entretanto, assim como nos primeiros discursos analisados, este discurso volta a demonstrar pouco incremento sobre as questões de segurança cibernética, evidenciando novamente as ameaças de terrorismo e de proliferação de armas nucleares. Tal característica pode ser expressada pela mudança de contexto nos conflitos do Oriente Médio – mais precisamente, na Síria.

Outro fator importante, que pode ter impactado na redução da temática cibernética no tradicional discurso anual, trata-se da revelação pública de dados secretos do governo, em 2013[19]. Nela, havia informações de que os EUA realizavam ações de espionagem cibernética nos níveis nacional e internacional. Esta operação era denominada de PRISM e possuía como objetivo estabelecer uma vigilância global acerca da ameaça do terrorismo. Contudo, os documentos manifestaram que a *National Security Agency* (NSA) monitorava a população norte-americana sem permissão, assim como espionavam dados, conteúdos de *e-mails* e transferências de arquivos de diversos países (PILATI; OLIVO, 2014).

Esse argumento pode ser melhor interpretado a partir do seguinte recorte da fala do presidente Obama: "trabalhando com este congresso, vou reformular nossos programas de vigilância, porque o trabalho vital de nossa comunidade de inteligência depende da confiança pública, aqui e no exterior, de que a privacidade das pessoas comuns não está sendo violada (USA, 2014, tradução nossa).

[19] Em 2013, Edward Snowen – antigo funcionário da *Central Intelligence Agency* (CIA) e de empresas privadas que prestavam serviços à *National Security Agency* (NSA) – reuniu documentos secretos que admitiam a coleta de dados da população dos EUA e de diversos países do mundo como França, Itália, Rússia, Alemanha e Brasil, com a finalidade de monitorar operações no ciberespaço e comunicações na Internet (PILATI; OLIVO, 2014).

Dessa forma, o termo '*cyber attacks*' compõe a percepção de que os EUA se mantém em atenção defensiva contra as ameaças cibernéticas, todavia, não explora discursivamente os mecanismos para tal defesa. Ainda assim, pelo fato das medidas políticas constituírem-se de um processo evolutivo que acompanha o avanço das ameaças, pode-se dizer que o discurso permanece no nível politizado, porém, neste caso, de forma branda. Portanto, visualiza-se os setores militar e político como os mais ameaçados, os EUA como objeto de referência, o presidente Barack Obama como ator securitizador e as instituições militares e políticas como atores funcionais – no escopo das unidades de análise de segurança.

### 3.1.6. *State of the Union Address* (2015)

O discurso proferido em 20 de janeiro de 2015 pelo presidente Barack Obama teve como principais pontos o fim das missões no Afeganistão e a recuperação completa da economia dos EUA – desde a crise financeira de 2008. Em conjunto, pautou sobre a importância de serem retirados os embargos impostos à Cuba, apresentando à audiência congressista os benefícios desta atitude para o hemisfério norte e para o legado norte-americano. Quanto aos assuntos relacionados ao campo cibernético, os termos '*cyber threats*' e '*cyber attacks*' surgem no discurso para incentivar a decisão política do Congresso para a execução de uma legislação contra os ataques cibernéticos.

> [...] eu peço a este Congresso que finalmente aprove a legislação que precisamos para melhor atender a crescente ameaça de ataques cibernéticos, combater o roubo de identidade e proteger as informações de nossos filhos. Esse deveria ser um esforço bipartidário. Se não agirmos, deixaremos nossa nação e nossa economia vulneráveis. Se o fizermos, podemos continuar a proteger as tecnologias que desencadearam incontáveis oportunidades para as pessoas em todo o mundo (USA, 2015, tradução nossa).

Nesse sentido, a preocupação nacional volta-se para as ações ilegais no espaço cibernético e para a proteção de tecnologias. No entanto, o obstáculo político e de diálogo entre os partidos democrata e republicano no Congresso, dificulta a execução de políticas de segurança e defesa cibernética, nos EUA. Em função disso, o Presidente declara que "nenhuma nação estrangeira, nenhum *hacker*, deveria ser capaz de desligar nossas redes ou invadir a privacidade das famílias americanas, especialmente das nossas crianças" (USA, 2015, tradução nossa). São identificados os atores cibernéticos que agem contra os EUA, assim como as questões de cibersegurança discutidas neste momento.

Verifica-se que, ao longo dos anos, os discursos que assumiram posicionamentos a respeito do tópico de cibernética foram acompanhados pela tentativa de convencimento da audiência congressista sobre as necessidades e os desafios nacionais a serem enfrentados, no presente e no futuro. Geralmente, tem-se, também, a pauta sobre as medidas de contraterrorismo como referência para a execução de projetos de leis na esfera da segurança e defesa cibernética. Esta afirmação é presente no seguinte recorte: "nós temos certeza que nosso governo integra inteligência para combater as ameaças cibernéticas, assim como nós temos feito para combater o terrorismo" (USA, 2015, tradução nossa).

Ao empregar as unidades de análise de segurança, tem-se como objeto de referência os EUA, como ator securitizador o presidente Barack Obama, como atores funcionais as Forças Armadas e as instituições políticas, como audiência o Congresso norte-americano e como setores ameaçados, o militar e o político. A discussão sobre as questões cibernéticas em relação aos discursos anteriores permanece no nível politizado, tendo em vista a constância de estímulo presidencial para o Congresso, com o objetivo de conseguir a aprovação de medidas de segurança e defesa cibernética.

### 3.1.7. *Remarks on National Security Strategy* (2017)

O discurso, datado de 18 de dezembro de 2017, representa o marco de uma nova postura ideológica e política nos EUA. Com o presidente Donald Trump no exercício do poder – e pela nova conjuntura nacional e internacional –, questões além de econômicas foram colocadas em pauta durante seu governo. Ao voltar-se para os assuntos relacionados à segurança e à defesa nacional, o Presidente declara que os governos anteriores inclinaram-se para questões adjacentes às necessidades do país como, por exemplo, a inserção de taxações financeiras que defasaram o poder militar dos EUA. Conforme Trump: "eles negligenciaram a ameaça nuclear na Coréia do Norte; fizeram um desastroso, fraco e incompreensível mau negócio com o Irã; e permitiram que terroristas como o ISIS ganhassem controle de vastas partes do território do Oriente Médio" (USA, 2017, tradução nossa).

A partir da concepção de que os governos anteriores foram negligentes em relação a manutenção de poder do país, Trump incita a prioridade governamental de confrontar os desafios nacionais e de reconstruir a confiança e a posição dos EUA no mundo. A alegação de que o investimento para a área de defesa foi de 700 bilhões de dólares no ano de 2017, demonstra a inovação do posicionamento norte-americano no que tange ao setor militar e ao viés político adotado neste governo. Dessa forma, analisa-se no discurso uma predisposição aos

assuntos relacionados ao tema de segurança e defesa contra o terrorismo, as armas nucleares norte-coreanas, crimes transnacionais, ameaças modernas, entre outros.

Sendo empregada a justificativa de que as medidas de contraterrorismo anteriores não surtiram o efeito esperado, o discurso apresenta novas formas de combate à ameaça, a partir de sanções e alianças com os países do Oriente Médio. Quanto a ameaça nuclear da Coréia do Norte, Trump declara que a utilização de sanções mais duras e o isolamento norte-coreano dos EUA e seus aliados serão fatores que ajudarão a promover a desnuclearização do país. Em relação aos crimes transnacionais, o discurso refere-se a não aceitação política de imigrantes ilegais nos EUA. No tocante às ameaças modernas, infere-se a proteção dos novos domínios como o ciberespaço e os ataques eletromagnéticos.

Sob tais perspectivas, o presidente Trump revela no discurso a consolidação da nova Estratégia Nacional de Segurança norte-americana, "baseada em princípios realistas, guiada por nossos interesses nacionais vitais e enraizada em nossos valores atemporais" (USA, 2017, tradução nossa). Nela, constituem-se quatro pontos principais: a proteção dos cidadãos norte-americanos, a prosperidade dos EUA, a preservação da paz por meio da força e a influência norte-americana no mundo. Neste momento, o termo '*cyber*' surge duas vezes no discurso, apontado como um dos desafios enfrentados pelos EUA.

Em primeira instância, Trump declara que os combates às ameaças modernas percorrem um domínio estratégico que merece a atenção do governo, assim como, afirma que a Estratégia Nacional de Segurança reconhece e delineia as novas formas de conflito. Uma outra frente discursiva remete-se ao fortalecimento de alianças capazes de compartilhar uma responsabilidade de segurança comum contra essas ameaças. Estas afirmações retratam a percepção norte-americana sobre uma conjuntura internacional pautada sobre o desenvolvimento do componente tecnológico e do domínio cibernético como formas de ataques integradas.

O aspecto mais importante referente às ameaças cibernéticas para os EUA – e para a dissertação em questão – encontra-se na seguinte passagem:

> [...] nossa estratégia nos chama para confrontar, desacreditar e derrotar o terrorismo e a ideologia radical islâmica e evitar que ele se espalhe pelos Estados Unidos. Vamos desenvolver novas maneiras de combater aqueles que usam os novos domínios, como o ciberespaço e as mídias sociais, para atacar nossa nação ou ameaçar nossa sociedade (USA, 2017, tradução nossa).

Analisa-se que, por mais que o termo '*cyberterrorism*' não tenha sido mencionado, as características relacionadas acerca desta ciberameaça encontram-se presentes neste discurso.

Em outras palavras, a compreensão e a relação estabelecida entre a ameaça do terrorismo e a utilização do espaço cibernético, como ferramenta de ataque, pode identificar tanto a atenção do governo para o terrorismo e para os atores cibernéticos de forma separada, como a concepção conjunta das ameaças que podem ser ilustradas por meio do conceito de ciberterrorismo. O fato que permite conjecturar o recorte discursivo voltado para o segundo viés de análise corresponde às frequentes e crescentes divulgações de ações terroristas através das redes sociais, assim como, a perspectiva de terem sido declarados os termos 'ciberespaço' e 'mídias sociais' de forma complementar.

Outro aspecto refere-se à comum compreensão sobre a ameaça do terrorismo para os EUA. Por mais que se tenham poucos discursos acerca das questões cibernéticas, tem-se o terrorismo como um tema bastante difundido na sociedade norte-americana. De acordo com os dados analisados pelo NVIVO 11, de 106 discursos apurados, 33 fazem referência ao termo '*terrorism*'. No entanto, quando modificada a configuração de análise do software, para serem identificados os números referentes as variações do termo de terrorismo – como, terror, terroristas etc. –, encontram-se um total de 100 discursos, sendo que, dentro destes, as variações foram utilizadas 1303 vezes.

Neste sentido, a construção discursiva que elenca a estratégia contra o terrorismo e a ideologia radical islâmica em relação ao uso de novos domínios para atacar e ameaçar a sociedade, pode determinar que os terroristas utilizam-se do ciberespaço como forma de ataque e ameaça contra os EUA. Sobretudo, também, reconhece que canais de divulgação terroristas podem ser criados nas mídias sociais, com o objetivo de realizarem operações de recrutamento e financiamento do terrorismo.

Portanto, ao serem aplicadas as unidades de segurança neste contexto, tem-se como objeto de referência os EUA, como ator securitizador o presidente Donald Trump, como ator funcional as forças militares e as instituições políticas e como audiência os membros do Congresso e a população norte-americana. A análise aplica-se ao setor militar e político, uma vez que são ameaças que dizem respeito diretamente à segurança nacional e à desestruturação política. Todavia, o discurso mantém-se no nível politizado de discussão, pois ainda depreende de uma opinião pública a respeito da ameaça.

No mais, é importante elucidar, que nos anos 2016, início de 2017 e 2018, não houve discursos presidenciais que abordassem a temática cibernética. Todavia, a ausência discursiva em torno da segurança e defesa cibernética dos EUA, nesse período, também institui o emprego de análise. O percurso político estadunidense, em 2016, teve como principais feitos o acordo internacional com o Irã sobre a prevenção de aquisições de armas nucleares em troca da redução

de sanções econômicas ao país e a retomada das relações com Cuba com a primeira visita de um presidente norte-americano ao país, desde 1928 (USA, 2016). Apesar dos grandes feitos, no entanto, as atenções mundiais estavam sobre as eleições presidenciais dos EUA, que ocorreram em novembro daquele ano.

Consequentemente, este evento esteve envolvido nos debates do âmbito cibernético ao serem levadas a público informações sobre interferências da Rússia nas eleições norte-americanas, mediante o uso do ciberespaço. A declaração dos EUA é de que o governo russo utilizou informações secretas estadunidenses – obtidas pelo e-mail da candidata Hillary Clinton –, para alterar o percurso político das eleições, principalmente, de forma midiática e mediante o uso do veículo de divulgação WikiLeaks (MANESS, 2016). Com a posse do presidente Trump em 2017, portanto, novas perspectivas de segurança e defesa cibernética tiveram que ser aplicadas.

De acordo com o documento elaborado sobre as ameaças à segurança nacional dos EUA pelo Diretor de Inteligência Nacional, Daniel R. Coats, a interferência cibernética eleitoral e as operações de influência *online* constituem ameaça para a democracia e, logo, também, para as eleições de 2020. Segundo Coats (2019, p. 7, tradução nossa), "adversários e concorrentes estratégicos dos EUA certamente usarão as operações de influência *online* para tentar enfraquecer as instituições democráticas, minar alianças e parcerias dos EUA e moldar resultados das políticas nos Estados Unidos e em outros lugares". Dentre os principais oponentes cibernéticos atuais dos EUA apontados pelo autor estão China, Rússia, Irã, Coréia do Norte e atores não-estatais.

> Adversários e competidores estratégicos também podem procurar usar meios cibernéticos para manipular ou interromper diretamente os sistemas eleitorais – tais como adulterar o registro de eleitores ou interromper o processo de contagem de votos – ou alterar dados ou questionar nosso processo de votação. A Rússia, em 2016, e atores não identificados, em 2018, já realizaram atividades cibernéticas quem têm como alvo a infraestrutura eleitoral dos EUA, mas não temos nenhum relatório de inteligência para indicar qualquer comprometimento da infraestrutura eleitoral da nossa nação que tenham impedido a votação, mudanças na contagem ou interrupção da capacidade de contabilizar votos (COATS, 2019, p. 7, tradução nossa).

Na esfera dos atores não-estatais – importante para a dissertação em questão –, a ênfase é dada aos criminosos e terroristas cibernéticos. Coats (2019) afirma que a preocupação dos EUA gerada pelos cibercriminosos encontra-se na expansão de roubos e extorsões financeiras às redes e infraestruturas críticas estadunidenses de saúde, financeiras e governamentais, para os próximos anos. Sob o mesmo sentido, os terroristas poderiam utilizar-se de informações confidenciais captadas mediante uso do ciberespaço para coagir, extorquir e realizar ataques

físicos contra a população. Ainda assim, essas características não entram dentro do escopo do conceito de ciberterrorismo, uma vez que diz respeito ao uso do ciberespaço para outros fins e não concentra-se na utilização do ciberespaço como ferramenta de ataque.

Ao se considerar a perspectiva apresentada, é possível determinar que por mais que os discursos de 2016 a 2018 – com exceção de apenas um discurso em 2017 – não levassem a temática cibernética para uma audiência, o efeito surtiu-se na movimentação política alimentada pelo cenário pós-eleições. Com o novo posicionamento governamental e pelo indício das eleições terem sofrido influência externa, os documentos de segurança e defesa norte-americanos foram reelaborados em 2017 e 2018, além de ter sido criado um documento específico para a temática cibernética, conforme será visto a seguir.

### 3.2. Posicionamento estratégico de defesa cibernética dos EUA

Tendo em vista a análise dos discursos e sua aplicação nas unidades de análise e nos setores de segurança – determinados pela Teoria da Securitização –, averígua-se que as questões relacionadas à cibernética e, logo, ao ciberterrorismo, encontram-se no nível politizado das discussões. Ou seja, situa-se na fase na qual o ator securitizador necessita que uma audiência faça parte da construção político-ideológica sobre determinada ameaça. Em contrapartida, somente pode-se considerar um estado de securitização quando não há a necessidade de serem levadas as discussões à público, por tratar-se de uma ação de emergência. Característica que contribui para a definição de um estado de securitização é a dinâmica política imediata pós-discurso.

No entanto, os processos no nível politizado podem conter indícios de uma futura securitização. Tais procedimentos correspondem às ações dos atores securitizadores em relação a determinada ameaça. Como as ameaças cibernéticas podem visar diversas fontes e, pelo fato de não terem sido mencionados nos discursos nenhum evento cibernético específico que pudesse justificar a entrada do objeto de referência em um grau de securitização, determina-se que, por se tratar de uma ameaça que abrange o âmbito nacional, os atores securitizadores em sua maioria são as forças políticas e militares. A afirmativa pode ser exemplificada a partir da exposição de mecanismos contra as ciberameaças como, por exemplo, mediante elaboração de estratégias.

Portanto, na seção anterior foram identificados nos discursos os objetos de referência, os agentes securitizadores, os atores funcionais, a audiência a que o discurso se destina e os setores envoltos sobre o processo de securitização. Ao verificar que, dentre os setores propostos

pela Teoria da Securitização, os setores militar e político foram apontados na análise como os principais setores ameaçados, caberá a esta seção ilustrar a movimentação política e militar verificada para o combate das ameaças cibernéticas elucidadas nos discursos presidenciais. É importante averiguar, também, que os atos de fala foram, em sua totalidade, designados aos tomadores de decisões nacionais. Isto é, mesmo que os discursos presidenciais alcancem a audiência nacional e internacional, o fato de ser realizado em um congresso ou parlamento, identifica a prioridade de discussão governamental sobre o tema apresentado.

Uma vez que a pergunta de pesquisa da dissertação propõe-se a verificar como se deu a construção da defesa cibernética dos EUA, necessita-se a divisão da seção em duas partes: (i) apresentação da evolução dos documentos que envolvem a temática de segurança e defesa cibernética nos EUA e (ii) identificação dos mecanismos criados para a construção da defesa cibernética do país. Após tal processo, poderá ser verificado na conclusão se o ciberterrorismo influenciou alguma dessas decisões governamentais. Dessa forma, serão apresentados os documentos de segurança e defesa criados na esfera política e militar norte-americana que dissertam sobre a temática cibernética. No mais, será analisada a *U.S. Cyber Command* (USCYBERCOM), responsável por combater as ameaças cibernéticas estadunidenses.

### 3.2.1 Evolução dos documentos de segurança e defesa cibernética

O evento terrorista de 2001 representou o marco da mudança política pelo contexto das novas ameaças no século XXI. A criação e a aprovação do *Patriot Act*, poucos dias após os atentados, demonstraram um dos maiores exemplos de securitização nos EUA. Sendo uma lei implementada pelo governo norte-americano para combater o terrorismo, caracteriza-se por não ter tido a aprovação total da opinião pública naquela dado momento. Porém, "apesar de toda a contradição da opinião pública em relação aos perigos que a lei representaria às liberdades individuais de seus cidadãos, o Ato Patriótico se configura como uma lei fundamental" (RIBEIRO; RIVERA, 2014, p. 141). A instituição desse mecanismo nos EUA possibilitou a inserção política para os novos temas relacionados à segurança e defesa do país, inclusive o cibernético.

> [...] no artigo 814, o Congresso tratou de ampliar o alcance da proteção oferecida a computadores de propriedade do governo federal. Antes da aprovação do Ato Patriótico, havia quatro categorias de danos possíveis que terminariam por causar a condenação da pessoa envolvida: o artigo 814 cria uma quinta categoria de danos. Esse seria o caso de haver dado em qualquer sistema ou computador usado pelo

> governo ou para o mesmo, em prol da defesa nacional ou da segurança nacional (RIBEIRO; RIVERA, 2014, p. 142).

De acordo com Luiijf et al (2013), uma das características comuns, evidenciadas na compreensão estadunidense sobre a segurança cibernética para o país, paira sobre a segurança da informação. Neste sentido, criou-se a *National Strategy for Homeland Security*, em 2002, com o objetivo de prevenir novos ataques terroristas nos EUA e reformular os serviços de informações nacionais e suas vulnerabilidades. No ano seguinte, para tornar mais específica a estratégia nacional contra o terrorismo, foram divulgadas simultaneamente a *National Strategy for Combating Terrorism*, a *National Strategy for the Physical Protection of Critical Infraestructure and Key Assets* e a *National Strategy to Secure Cyberspace*, reunindo diversos elementos do poder nacional para tornarem efetivos os mecanismos de defesa (BORGES, 2006).

A elaboração e divulgação conjunta dos documentos refletem as prioridades da agenda de segurança norte-americana naquele cenário. A constituição de estratégias específicas para a segurança da infraestrutura crítica e do espaço cibernético demonstra que a ameaça do terrorismo despertou os EUA para ambientes anteriormente pouco ou não explorados pela defesa nacional. Evidentemente, mesmo tratando-se de temas que podem abranger diversos elementos da sociedade, o foco de ambos estava na proteção das infraestruturas contra ataques terroristas ou contra qualquer potencial ator capaz de utilizar-se do ciberespaço para ameaçar as infraestruturas nacionais. É importante demonstrar que, apesar de envolver a temática cibernética e o terrorismo, a discussão estratégica pautava-se sobre a reunião de informações confidenciais nas mãos dos terroristas. Em outras palavras, as estratégias preocupavam-se com o acesso de terroristas ao banco de dados dos EUA e os meios que poderiam ser utilizados para o alcance desse objetivo. Neste contexto, também, a cibernética ganhou a característica de domínio e instrumento de poder nacional.

Em 2005, no âmbito militar, foi criada a *National Defense Strategy of the United States of* America, sob a responsabilidade do Departamento de Defesa dos EUA. Com o objetivo de proteger os EUA de ataques externos, o documento visa, também, manter a capacidade de intervir globalmente e realizar alianças estratégicas para dissuadir os potenciais inimigos. Além disso, a estratégia de defesa instrumentou a mudança das Forças Armadas estadunidense para a adequação dos seus mecanismos para lidarem com as ameaças assimétricas (BORGES, 2006). Ademais, a *National Security Strategy*, no ano seguinte, estipulou os interesses nacionais e as políticas que seriam adotadas até o final do governo George W. Bush, ainda com o foco voltado para a ameaça do terrorismo (BORGES, 2006).

No entanto, o instrumento que formalizou a segurança e a defesa cibernética dos EUA no período, foi o *Comprehensive National Cybersecurity Initiative* (CNCI), criado em resposta ao aumento de 31% das atividades ilegais no ciberespaço dos anos 2000 a 2007 (RIBEIRO; RIVERA, 2013). Sob o âmbito do DoD e do mandato Bush:

> [...] o CNCI estabelece a política, estratégia e diretrizes de defesa para proteger os sistemas de rede e servidores federais. Além disso, o CNCI possui como diretriz uma abordagem que antecipa as ameaças cibernéticas e tecnologias que estariam por vir. O mesmo exige que o governo federal utilize de forma otimizada suas capacidades técnicas e organizacionais para identificar tanto ameaças quanto vulnerabilidades que possam vir a apresentar algum risco (RIBEIRO; RIVERA, 2013, p. 143).

Considerando os desafios para defender ciberneticamente os sistemas de informações e as infraestruturas de comunicações norte-americanos, permitiu-se a adequação do CNCI para o governo Barack Obama. A partir de novas recomendações destinadas ao documento, sendo estas denominadas de *Cyberspace Police Review*, foram identificadas três principais estratégias de defesa: estabilizar a linha de frente de defesa contra ameaças imediatas, defender todos os aspectos de ameaça e fortalecer o desenvolvimento da cibersegurança. Essas prerrogativas serviram de base para a constituição dos mecanismos de defesa cibernética em diversas escalas da sociedade, assim como, ficou reconhecido como o componente chave para o estabelecimento de uma segurança cibernética efetiva, nos EUA (USA, 2009).

Dentro desse escopo, uma das principais preocupações elencadas pelo governo Obama, foi o caráter transnacional do ciberespaço. De acordo com Ribeiro e Rivera (2013), esse aspecto incentivou o desenvolvimento de uma cooperação internacional sobre o âmbito da cibernética, uma vez que despertou a necessidade de se terem mecanismos capazes de regular e proteger as atividades no ciberespaço na esfera global. Com isso, criou-se a *International Cyberspace Strategy*, em 2011, com o objetivo de tornar transparentes as prioridades da política externa norte-americanas no espaço cibernético (AMARAL, 2014).

Em 2015, o Departamento de Defesa dos EUA publicou o *The DoD Cyber Strategy* com a finalidade de direcionar o desenvolvimento da defesa cibernética estadunidense e sua postura de dissuasão. O foco do documento encontra-se na construção e organização das capacidades militares para proteger as infraestruturas do DoD, manter a segurança nacional e oferecer suporte operacional para a manutenção dos interesses nacionais contra os ataques cibernéticos. O documento, ainda, estabelece que tanto os atores estatais quanto não estatais oferecem perigo aos EUA, principalmente, pela possibilidade de ataques cibernéticos à infraestrutura crítica

nacional e roubos de propriedade intelectual para o ganho de vantagens competitivas (USA, 2015).

Com a mudança de governo para o Presidente Donald Trump e as especulações sobre as interferências cibernéticas nas eleições de 2016, os documentos de segurança e defesa nacional foram reelaborados. A cibernética passou a fazer parte de diversos documentos de segurança e prospecções de defesa nas agências governamentais dos EUA. No entanto, três principais documentos oferecem as diretrizes para os demais, são eles o *National Security Strategy*, o *Summary of the National Defense Strategy* e o *National Cyber Strategy of the United States of America*. Ambos serão melhor apresentados, a seguir, por representarem a postura política norte-americana atual.

A *National Security Strategy* foi inaugurada no discurso presidencial de 18 de dezembro de 2017, com o objetivo de fortalecer a liderança do país no mundo, a partir da manutenção dos interesses nacionais. Ao apresentar que as responsabilidades nacionais se destinam à proteção da população, da pátria e do modo de vida estadunidense, determina como estratégia nacional a defesa das infraestruturas críticas, o posicionamento contra os atores cibernéticos ilegais e o fortalecimento do ciberespaço como um dos domínios norte-americanos (USA, 2017a).

> A responsabilidade americana em relação aos desafios e oportunidades na era cibernética determinará o nosso próspero e seguro futuro. Ao longo da nossa história, os Estados Unidos tem sido capazes de proteger a pátria controlando os domínios terrestres, aéreos, espaciais e marítimos. Hoje, o ciberespaço oferece aos atores estatais e não estatais a habilidade de promover campanhas contra a política americana, a economia, e os interesses de segurança sem atravessar fisicamente as nossas fronteiras (USA, 2017a, p. 12, tradução nossa).

De acordo com a estratégia, os ciberataques oferecem sérios danos à infraestrutura crítica, assim como para os negócios e as redes econômicas dos EUA. Neste sentido, o crime cibernético é colocado em pauta, sendo determinado pelo país que seriam utilizadas sofisticadas formas de investigação cibernética nacional, com a finalidade de impedir que os cibercriminosos se utilizem dos mercados *online*, das moedas criptografadas e de outras atividades ilícitas. Outro fator corresponde à identificação de que, as vulnerabilidades em infraestruturas críticas, são palcos para os atores cibernéticos que buscam desestabilizar os comandos militares, as operações financeiras, os meios de comunicações, entre outros. Com isso, incita-se a necessidade de se proteger as infraestruturas e as operações no espaço cibernético (USA, 2017a).

A prevenção de ataques cibernéticos em seis pilares nacionais essenciais – segurança nacional; energia e poder; bancos e finanças; saúde e segurança; comunicações; e, transportes

–, é determinante para a estabilidade norte-americana. Considerando que os ciberataques podem gerar graves impactos à sociedade, a estratégia estipula o desenvolvimento das capacidades militares, assim como, a modernização dos sistemas de informação do país. Especifica, ainda, que os atores cibernéticos, os governos estrangeiros e os criminosos que realizarem ações maliciosas contra os EUA, terão que arcar com as consequências (USA, 2017a).

A estratégia designa uma seção somente para o ciberespaço. Nela, são constituídas alegações acerca dos atores estatais e não estatais que dispõem das habilidades cibernéticas e das vulnerabilidades infraestruturais para realizar atividades de extorsão e de desinformação. Neste sentido, o documento informa que os investimentos em capacidades militares devem ser tomados como ações prioritárias do governo para promover respostas imediatas contra os ciberataques (USA, 2017a).

No mais, são retratados os propósitos de aperfeiçoar a integração entre as autoridades e os procedimentos norte-americanos para a realização de operações cibernéticas contra os adversários quando necessário. Conforme o discurso de Donald Trump na ocasião de lançamento do documento: "nós vamos trabalhar com o Congresso para enfrentar os desafios que continuam a dificultar a inteligência oportuna e o compartilhamento de informações, planejamento e operações, e o desenvolvimento necessário de ferramentas cibernéticas" (USA, 2017, p. 32, tradução nossa).

O *Summary of the National Defense* Strategy, criado em 2018, é um documento público anexo ao documento classificado de defesa nacional dos EUA. Seu conteúdo discorre sobre as missões das forças militares no tocante à proteção da segurança nacional e apresenta como objetivo impossibilitar o surgimento de uma guerra. Atuando em conjunto com a Estratégia de Defesa Nacional, o documento tem como propósito proporcionar o direcionamento das Forças Armadas nos domínios aéreo, terrestre, marítimo, espacial e cibernético. Dessa forma, acentua que o desenvolvimento e a manutenção da segurança dependem da adaptação dos componentes militares com o avanço tecnológico, uma vez que este altera o caráter da guerra. Dentre os desafios decorrentes das novas tecnologias, são apresentados a computação avançada, as análises de *big data*, a inteligência artificial, a robótica, a energia direcionada, os hipersônicos e a biotecnologia (USA, 2018e).

Os principais atores do palco internacional que apresentam ameaça à segurança dos EUA pela constituição das suas capacidades, são Estados e os atores não-estatais: terroristas, organizações transnacionais, *hackers* cibernéticos e outros atores maliciosos que possuem capacidade de promover o desequilíbrio da sociedade. Assim, a Estratégia de Defesa Nacional apresenta como objetivos defender a pátria de ataques; deter adversários de agressões contra os

interesses norte-americanos; dissuadir, prever e deter os Estados adversários e os atores não estatais de adquirir, proliferar ou usar armas de destruição em massa; prever a ação terrorista contra o Estado e seus aliados; assegurar os domínios comuns, entre outros (USA, 2018e).

Outro aspecto atinente a atuação das Forças Armadas contra as ameaças refere-se à modernização das capacidades militares. As adoções de equipamentos e armas, que correspondam a um nível de combate superior ao dos adversários, são elementos essenciais para a eficiência militar norte-americana. Reconhecida a necessidade de uma vantagem competitiva, o documento apresenta um planejamento fiscal, para até o ano de 2023, com a designação de orçamentos para a aceleração dos programas de modernização. Com isso, serão disponibilizados investimentos para a defesa cibernética, para a integração das capacidades cibernéticas e para a reconstituição das operações militares no domínio cibernético (USA, 2018e).

Portanto, o investimento em capacidades militares percorre a preservação dos propósitos nacionais e internacionais norte-americanos. Ao priorizar o desenvolvimento de instrumentos de defesa, tanto na área cibernética como no campo militar como um todo, são gerados ganhos de competitividade e vantagens estratégicas nas operações de defesa. No entanto, tem-se que "a modernização não é definida apenas por *hardware*; requer mudanças nas formas como organizamos e empregamos forças" (USA, 2018e, p, 7, tradução nossa). Assim, a adoção de novos conceitos e tecnologias são fatores que aprimoram as vantagens militares competitivas dos EUA (USA, 2018e).

Dentre os três documentos apontados, o de maior importância para a segurança e a defesa cibernética dos EUA é a *National Cyber Strategy of the United States of America*, que corresponde ao instrumento de legitimação dos processos executados no ciberespaço. A percepção de que o domínio evoluiu para diversas esferas de sociedade, incitou a prioridade de serem criados mecanismos capazes de permear e proteger as operações militares, econômicas e sociais no espaço cibernético, assim como, prevenir ataques aos sistemas de informação e às infraestruturas críticas (USA, 2018d).

> Novas ameaças e uma nova era de estratégia competitiva demandam uma nova estratégia cibernética que responda às novas realidades, reduza as vulnerabilidades, detenha adversários e salvaguarde as oportunidades. A segurança do ciberespaço é fundamental para nossa estratégia e requer técnicas avançadas e eficiência administrativa por meio do Governo Federal e do setor privado. [...] Os Estados Unidos devem ter escolhas políticas para impor custos se quiserem dissuadir os atores cibernéticos mal intencionados (USA, 2018d, p, 2, tradução nossa).

Fato importante, para esta dissertação, encontra-se na exposição dos atores cibernéticos pela Estratégia. Ao considerar os principais atores cibernéticos estatais, o documento cita Rússia, China e Coréia do Norte, como os países que utilizam o ciberespaço para realizar operações de espionagem política e econômica. O texto apresenta como principais atores cibernéticos não estatais, os criminosos e os terroristas. Segundo o documento, estes são responsáveis por explorar o ciberespaço com a finalidade de obtenção de lucro, realização de operações de recrutamento e propaganda, mas, sobretudo, atacar os EUA e seus aliados por meio de ações cibernéticas hostis.

Tendo em vista os perigos que o espaço cibernético oferece aos EUA, o documento é dividido em quatro pilares estratégicos principais. Com o objetivo de proteger as instituições públicas e privadas dos EUA, delineia: (i) a proteção da população americana, a pátria e o modo de vida americano; (ii) a promoção da prosperidade americana; (iii) a preservação da paz por meio do uso da força e; (iv) o estabelecimento de avanços da influência americana no mundo (USA, 2018d).

O primeiro ponto diz respeito às defesas dos interesses norte-americanos e das redes de informações privadas. Tendo como objetivo o gerenciamento de riscos de segurança cibernética, os EUA visam aumentar a segurança e a resiliência dos sistemas de informações e das informações privadas da população. A partir disso, constituem-se como prioridades supervisionar a segurança cibernética civil no nível federal, alinhar as atividades de gerenciamento de riscos e tecnologia da informação, melhorar a gestão de riscos da cadeia de suprimentos, incentivar investimentos em cibersegurança, refinar os papéis e as responsabilidades das agências, melhorar a segurança do ciberespaço, entre outros (USA, 2018d).

O segundo pilar corresponde aos benefícios gerados pela Internet que colaboraram para a manutenção dos valores de liberdade, segurança e prosperidade norte-americanos no âmbito nacional e internacional. Possui como objetivos a preservação da influência dos EUA no ecossistema tecnológico e o desenvolvimento do espaço cibernético como um mecanismo de crescimento econômico, inovação e eficiência. Suas principais prioridades constituem-se em promover uma economia digital resiliente, promover e proteger a inovação tecnológica dos EUA e desenvolver uma superior força de trabalho em segurança cibernética (USA, 2018d).

O terceiro ponto do documento apresenta os desafios quanto à segurança nacional e econômica dos interesses norte-americanos no ciberespaço, como uma estratégia de poder. Consistem como objetivos: "identificar, combater, interromper, degradar e deter o comportamento no ciberespaço que está desestabilizando e contrariando os interesses nacionais,

ao mesmo tempo em que preserva a sobreposição dos EUA no e através do ciberespaço" (USA, 2018d, p, 20, tradução nossa). Possui como prioridade, dessa forma, a estabilização cibernética por intermédio de normas de comportamento para o Estado responsável pela ação ilegal e atribuir e deter os comportamentos inaceitáveis no ciberespaço.

Por fim, o quarto pilar do documento refere-se à manutenção da liderança norte-americana no nível internacional. No entanto, os desafios e as ameaças provenientes do ciberespaço são fatores que podem prejudicar a influência do país no globo. Em vista disso, o documento objetiva preservar a abertura das operações integradas, da segurança e da confiabilidade na Internet para, assim, reforçar os interesses nos EUA. Neste sentido, propõe-se a promover uma Internet aberta, interoperável, confiável e segura para o país, a indústria e a sociedade civil, além de construir uma eficiência cibernética por meio de esforços para a capacitação nacional (USA, 2018d).

Visto isso, analisa-se que os documentos publicados durante o governo Trump apresentam diretrizes mais assertivas a respeito da segurança e da defesa cibernética, em relação aos governos anteriores. Evidentemente, o cenário atual e o desenvolvimento das tecnologias requerem a adequação frequente dos documentos nacionais para que estejam em conformidade com a realidade e com as necessidades apresentadas. A evolução constante dos documentos e das prioridades governamentais contribuem para que os instrumentos de defesa desenvolvam-se e atuem em conformidade com as prioridades do país.

### 3.2.2 Defesa cibernética dos EUA

De acordo com a Teoria da Securitização, para identificar se determinado tema está no estágio de securitização, deve-se observar a movimentação gerada em torno do setor ameaçado (BUZAN et al, 1998). No caso dos EUA, os principais setores apontados pelos discursos, que poderiam sofrer gravemente em casos de elaborados ataques cibernéticos à eles, são o político e o militar. No espectro político, a elaboração de documentos que direcionam o posicionamento estratégico adotado, demonstra que o domínio cibernético está no nível politizado dos debates nacionais. Isto é, a discussão gerada em torno das ciberameaças passam pelo processo de aprovação dos congressistas para a publicação dos documentos nacionais. Esse processo gera efeitos nos demais setores dos EUA, como no militar. No entanto, em casos de securitização, a tomada de decisão é realizada no nível do Departamento de Defesa norte-americano e da Casa Branca, pela urgência da situação. Enquanto a securitização não é necessária, as operações e documentos publicados seguem as diretrizes da estratégia de segurança nacional.

No setor militar, a *U.S. Cyber Command* (USCYBERCOM) é a agência encarregada de promover a segurança e a defesa cibernética dos EUA. Criada em 2009, sobre o espectro do Departamento de Defesa, possui o objetivo de planejar e realizar operações militares no ciberespaço. Além disso, é responsável por dirigir, sincronizar e coordenar os interesses dos EUA com a defesa do ciberespaço. Sendo a principal estrutura de defesa cibernética do país, a agência propõe-se a executar missões que protejam os sistemas vitais de informação dos EUA, assim como, projetar as capacidades militares por meio do comando e controle das Forças Armadas estadunidenses. Atuando em conjunto a ela, estão a *U.S Army Cyber Command*, a *Fleet Cyber Command*, a *Air Forces Cyber* e a *Marine Corps Forces Cyberspace Command*. Ambas serão apresentadas ao longo da seção.

Mas, primeiramente, necessita-se analisar a importante função da USCYBERCOM para os EUA. Pautada sobre a manutenção da superioridade militar sobre os domínios físicos e cibernético, a organização compreende que a velocidade e o volume de eventos no ciberespaço, geram obstáculos para a estratégia de defesa norte-americana. Em razão disso, em 2018, criou-se um documento denominado de *Achieve and Maintain Cyberspace Superiority*, para orientar a USCYBERCOM e as Forças Armadas na realização dos procedimentos cibernéticos e no avanço dos interesses nacionais. Nele, é declarado que:

> políticas, doutrinas e processos devem acompanhar a velocidade dos eventos no ciberespaço para manter uma vantagem competitiva. Os efeitos estratégicos superiores dependem do alinhamento das operações, capacidades e processos, e da integração perfeita da inteligência com as operações. Agora devemos aplicar essa experiência dimensionando a magnitude da ameaça, removendo restrições à nossa velocidade e agilidade, e manobrando para conter adversários e melhorar nossa segurança nacional (USA, 2018c, p. 2, tradução nossa).

Quanto aos atores cibernéticos enfrentados pelos EUA, tem-se os atores estatais – que possuem capacidades de promover ataques sofisticados como, por exemplo, a Rússia, a China, o Irã e a Coréia do Norte – e os atores não estatais como os terroristas, os criminosos e os hacktivistas. No que diz respeito aos atores estatais, a relação de combate encontra-se no nível militarizado e, por isso, exige que as capacidades de defesa nacional sejam competitivas. Ao sofrer ciberataques sob essa esfera, a organização opera em defesa de atividades ofensivas de exploração de vulnerabilidades, roubo de propriedade intelectual, manipulação de informações, softwares maliciosos capazes de derrubar sistemas, entre outros. Em relação aos ataques promovidos por atores não estatais, compreende-se que o nível de ameaça é menor, quando comparado com os atores estatais, por pressupor uma redução das capacidades e de instrumentos de ataques. Ainda assim, esses ataques são capazes de gerar danos às capacidades

militares norte-americanas e à infraestrutura crítica que, consequentemente, geraria danos à população (USA, 2018c).

Tendo em vista as ameaças enfrentadas pelo EUA, a agência militar integra-se à percepção de que a implementação conjunta dos instrumentos de poder nacional favorece a atuação da organização na competição estratégica do ciberespaço. Não apenas, determina que as operações realizadas no âmbito da USCYBERCOM podem gerar benefícios tanto ao poder diplomático – por meio de sanções rápidas, comunicações discretas ao adversário e identificação de operações no domínio cibernético como fator capaz de estimular a tomada de decisão –, quanto ao poder econômico – por intermédio de informações que podem tornar a defesa dos mecanismos econômicos mais assertivos (USA, 2018c).

Neste sentido, as Forças Armadas operam em conjunto no ciberespaço para a manutenção da segurança nacional. No âmbito do Exército, a *U.S. Army Cyber Command* defende as redes norte-americanas, as plataformas do Exército e a infraestrutura crítica dos EUA. Vigiando as operações globais no espaço cibernético ininterruptamente e contando com cerca de 16.500 funcionários – entre soldados e civis –, o comando caracteriza-se por realizar ações defensivas e ofensivas contra os adversários cibernéticos. A missão principal dessa agência é defender agressivamente a rede de informação do Departamento de Defesa, além de desenvolver capacidades para a proteção contra oponentes futuros (USA, 2019b).

A *U.S. Fleet Cyber Command*, também conhecida como *U.S. Tenth Fleet*, é responsável por planejar e coordenar operações no ciberespaço e no espaço eletromagnético, com a finalidade de garantir que a atuação da Marinha funcione sem a interferência adversária. A frota contém o objetivo, também, de tornar habilitadas as operações de comando e controle e definir as condições das operações. Em outras palavras, o comando é capaz de "direcionar e entregar os efeitos táticos e operacionais desejados no ciberespaço, no espaço e no espectro eletromagnético para comandantes da Marinha em todo o mundo e garantir a execução bem-sucedida das áreas de missões atribuídas ao *U.S. Fleet Cyber Command*" (USA, 2017b, tradução nossa). De forma equivalente, a *Marine Corps Forces Cyberspace Command* realiza operações de defesa no ciberespaço, porém, no âmbito da Rede Corporativa dos Fuzileiros Navais. Apenas nos casos de operações ofensivas no espaço cibernético, a agência atua em apoio às Forças Conjuntas e de Coalisão (USA, 2019a).

Por último, a *Air Forces Cyber* responsabiliza-se por defender as redes da força aérea e garantir que as operações militares norte-americanas ao redor do mundo sejam eficazes ao proteger a informação no ciberespaço. Ou seja, a organização é caracterizada por atuar nas operações de combate à guerra e por abranger suas capacidades à esfera global. Para o alcance

desses objetivos, a agência recorre a seis funções principais: "construir, operar, proteger, defender a rede de informação da *Air Forces Cyber*, direcionar o terreno cibernético de missão crítica ao estender as capacidades cibernéticas à borda tática do moderno campo de batalha e envolver o adversário em apoio aos comandos de combate e componentes aéreos" (USA, 2018a, tradução nossa).

Ainda assim, ao considerar os obstáculos para a execução de planos operacionais no espaço cibernético, cinco questões são levantas pela USCYBERCOM, que apresentam necessidades de resoluções urgentes para as missões tornarem-se mais eficazes. A primeira, diz respeito à capacidade de tornar as tecnologias e os mecanismos operacionais mais eficientes do que os do adversário para que se obtenham vantagens no ciberespaço. A segunda refere-se a criar, desenvolver e integrar operações capazes de operar em conjunto com os demais domínios e, logo, incorporar em ambientes de conflito (USA, 2018c).

O terceiro aspecto corresponde a conquistar vantagens de informações para o alcance do objetivo estratégico, por meio da integração de operações conjuntas. A quarta questão estabelece a prioridade de operacionalizar batalhas cibernéticas de forma ágil e responsável, assegurando os processos desde a análises de sistemas alvo até as atividades de gerenciamento de força. Por último, o quinto ponto determina a expansão e o aprofundamento do conhecimento dos atores e dos processos cibernéticos por meio da identificação dos produtos e do avanço do ciberespaço de parceiros no setor privado, em outras agências, na academia, entre outros (USA, 2018c).

Dessa forma, a USCYBERCOM é responsável pelos processos e as operações no âmbito cibernético estadunidense. A superioridade militar e a manutenção dos interesses norte-americanos na esfera física são fatores que atualmente estão ligados a vantagem competitiva que o espaço cibernético oferece. Para isso, a agência opera como a força cibernética dos EUA e compreende que "devemos parar os ataques antes que eles penetrem nas nossas defesas cibernéticas ou prejudiquem nossas forças militares; e mediante operações persistentes e integradas, podemos influenciar o comportamento adversário e introduzir incerteza em seus cálculos" (USA, 2018c, p. 2, tradução nossa). Portanto, a organização condiciona a percepção de que as operações no domínio cibernético estadunidense exercem influência sobre as frentes de defesa dos outros domínios, além de estabelecer uma integração capaz de tornar fortalecidos os mecanismos de defesa nacional.

Além de gerar influência aos demais domínios, a atuação da agência permite que os outros setores nacionais operem seguramente. Verificando o documento da análise fiscal anual dos EUA – *A budget for a better America: analytical perspectives* (2018) –, identifica-se a

cibersegurança como um importante componente da agenda norte-americana, ao constatar os fundos financeiros designados a ela. Embasado na Estratégia Nacional de Cibersegurança, os EUA reconhecem que um espaço cibernético seguro oferece também segurança para o governo, as instituições privadas e os indivíduos. Porém, na mesma instância, o Governo Federal compreende que atividades cibernéticas maliciosas, com alto grau de sofisticação sobre entidades públicas ou privadas, são de responsabilidade dual para a manutenção da segurança nacional (USA, 2018b).

> Cibersegurança é um importante componente dos esforços de modernização de TI da Administração e o Presidente continua dedicado a proteger a empresa Federal contra ameaças relacionadas a cibernética. A avaliação do risco geral de cibersegurança do Governo Federal continua a achar que a empresa Federal está em risco. As prioridades orçamentárias de cibersegurança continuarão buscando reduzir esse risco com base na avaliação baseada em risco e em dados do ambiente de ameaças e da atual postura Federal de segurança cibernética (USA, 2018b, p. 305, tradução nossa).

Considerando essas premissas, o orçamento designado para a cibersegurança dos EUA foi de US$ 14,9 bilhões, no ano de 2018, com estimativa de serem gastos US$ 17,4 bilhões, em 2020. Com as maiores partes do financiamento destinadas, historicamente, ao Departamento de Defesa e ao Departamento de Segurança Nacional, no ano de 2018, estas agências obtiveram 53,7% e 12,4% do valor total determinado, respectivamente. No entanto, o governo norte-americano constatou a necessidade de promover incentivos, também, às demais agências federais que sofrem interferência cibernética, abrangem diversos setores nacionais e esforçam-se no combate aos ciberataques. Dessa forma, o governo estipulou fundos de segurança cibernética para os departamentos nacionais, assim como, realizou uma prospecção sobre as futuras despesas fiscais anuais com cibersegurança, conforme é vislumbrado no Quadro 3.

**QUADRO 3**

Totais de financiamento de cibersegurança para agências (em milhões de dólares)

| | 2018 | 2019 | 2020 |
|---|---|---|---|
| Departamento de Agricultura | 262 | 480 | 311 |
| Departamento de Comércio | 350 | 403 | 392 |
| Departamento de Defesa | 8,048 | 8,734 | 9,643 |
| Departamento de Educação | 104 | 139 | 143 |
| Departamento de Energia | 448 | 520 | 557 |
| Departamento de Saúde e Serviços Humanos | 359 | 474 | 460 |

| | | | |
|---|---|---|---|
| Departamento de Segurança Nacional | 1,859 | 1,921 | 1,919 |
| Departamento de Habitação e Desenvolvimento Urbano | 15 | 35 | 25 |
| Departamento de Justiça | 821 | 824 | 881 |
| Departamento de Trabalho | 93 | 93 | 94 |
| Departamento de Estado | 362 | 363 | 400 |
| Departamento do Interior | 88 | 103 | 111 |
| Departamento do Tesouro | 445 | 505 | 522 |
| Departamento de Transportes | 185 | 224 | 232 |
| Departamento de Assuntos Veteranos | 386 | 530 | 513 |
| Agência de Proteção ao Meio Ambiente | 21 | 44 | 45 |
| Administração de Serviços Gerais | 72 | 79 | 80 |
| Administração Nacional Aeronáutica e Espacial | 171 | 169 | 171 |
| Fundação de Ciência Nacional | 247 | 239 | 224 |
| Comissão de Regulamentação Nuclear | 25 | 32 | 29 |
| Escritório de Gestão Pessoal | 38 | 45 | 47 |
| Administração de Pequenos Negócios | 9 | 16 | 16 |
| Administração de Segurança Social | 167 | 225 | 205 |
| Agência para o Desenvolvimento Internacional | 44 | 68 | 44 |
| Agências de Ação não-CFO | 362 | 382 | 372 |
| **Total** | **14.978** | **16.645** | **17.435** |

Fonte: USA, 2018b, tradução nossa.

Sob essa perspectiva, analisa-se que os EUA compreende que a proteção do espaço cibernético e, logo, da segurança nacional, precisa ser integrada, para ser eficiente. A designação financeira do governo, para o desenvolvimento de capacidades cibernéticas dos departamentos e agências norte-americanas, institui a percepção de que tais organizações possuem responsabilidades que vão além da proteção das suas próprias redes e sistemas de informação. Fator interessante, identificado no quadro anterior, é que, logo após o Departamento de Defesa e o Departamento de Segurança Nacional, as maiores destinações financeiras encaminham-se para o Departamento de Justiça, o Departamento de Energia e o Departamento do Tesouro. Esse aspecto pode indicar que esses são os departamentos/setores que sofrem mais ataques cibernéticos nos EUA e que o governo está tomando medidas preventivas de cibersegurança por se tratarem de departamentos/setores sensíveis.

Com base nos dados apresentados verifica-se, portanto, que o domínio cibernético confere oportunidades de ações maliciosas, tanto para os atores estatais quanto para os não-estatais. A adoção de medidas de proteção políticas e militares na esfera cibernética, assinala a preocupação governamental de que informações classificadas podem ser adquiridas e utilizadas contra o próprio Estado. A evolução dos documentos de segurança e defesa cibernética e a criação de agências de defesa e o financiamento do governo para os demais departamento e setores, demonstram o imperativo norte-americano no tocante a segurança da informação e das infraestruturas críticas do país. Sobre esses pilares, no governo Trump, a construção do posicionamento de defesa cibernética dos EUA permeou a estratégia de acelerar, adequar e enxugar os documentos e processos políticos e militares, para uma melhor atuação dos EUA contra as ameaças cibernéticas e para a manutenção da influência estadunidense no mundo.

## CONCLUSÃO

O espaço cibernético, sendo um componente essencial que permeia as escalas financeira, social, governamental e política no cotidiano global, eleva a interconexão entre as tecnologias de informação, que acabam por gerar espaços vulneráveis ao surgimento de novas ameaças. Considerando que os atores cibernéticos possuem motivações variadas, as aberturas tecnológicas oferecem palcos para ações ilegais com o benefício do anonimato pela autoria dos ataques. Desse modo, a percepção de que os EUA possuem vulnerabilidades cibernéticas, capazes de promover danos extensíveis às diversas escalas da sociedade, preconiza a prioridade norte-americana de manter protegidos os sistemas de informações dos setores estratégicos nacionais. Esse processo é realizado nos momentos em que a ameaça encontra-se no nível politizado das discussões, no qual são utilizadas resoluções mediante a pré-existência ou necessidade de reparação de uma fragilidade.

A Escola de Copenhague oferece esforços para a ampliação do conceito de segurança, mediante a criação do conceito de securitização. O aprofundamento em questões anteriormente pouco discutidas no campo teórico conferiu originalidade mediante o tratamento de unidades e setores de análises. Esse fator permitiu que novos assuntos fossem acoplados aos Estudos de Segurança Internacional, assim como novas frentes de pesquisa. Por esses motivos, o escopo exibido teve o propósito de apresentar a Escola de Copenhague como uma corrente capaz de abranger o fenômeno do ciberterrorismo. A dissertação teve a intenção de apresentar o embasamento teórico e metodológico da Teoria da Securitização, com a finalidade de aplicar a teoria no contexto das ameaças cibernéticas e identificar um posicionamento de defesa cibernética dos EUA. Sob tal contexto, a dissertação propôs-se a identificar o posicionamento de defesa cibernética dos EUA por meio da aplicação da Teoria da Securitização.

A Teoria da Securitização compreende que os discursos proferidos por agentes políticos do alto escalão possuem a capacidade de transformar determinado elemento em uma ameaça contra a existência de um Estado. Tal característica remete ao conceito de securitização que determina que, quando é identificada uma ameaça contra a sobrevivência de um objeto de referência e, a partir desta, são tomadas ações imediatas de segurança que podem se sobrepor às leis vigentes, pois existe um estado de securitização. Somente quando a audiência, a qual o discurso se destina, aprova os argumentos com entonações emergenciais oferecidos pelo agente securitizador, legitima-se a ação do objeto de segurança.

> A essência de uma ação discursiva é seu poder irresistível de fazer com que um receptor ou um público realize uma ação. Assim, discurso e ação estão ligados de duas maneiras distintas. Primeiro, o discurso é parte da agência, [...] e o lado constitutivo da ação discursiva é outra maneira de dizer que, mediante o conhecimento mútuo, o discurso molda as relações sociais e constrói sua forma e conteúdo. Em segundo lugar, no lado casual, como veículo de ideias, o discurso alveja e cria a solicitação de uma ação comunicativa particular (BALZACQ, p. 23, 2011, tradução nossa).

Ao se aplicar a Teoria da Securitização aos discursos presidenciais dos EUA que propuseram a temática cibernética, verificou-se que a crescente preocupação estadunidense pautou-se, principalmente, sobre a saída de informação privilegiada para seus adversários estatais e não-estatais. Tendo em vista os processos sobre quais os EUA passaram, desde o primeiro discurso envolvendo os aspectos cibernéticos até a execução de um documento estratégico para a proteção do ciberespaço e das operações permeadas por ele, atesta-se que as ameaças cibernéticas estão presentes nas discussões políticas dos EUA, assim como, nos mecanismos de defesa e segurança nacionais.

A elaboração de uma estratégia nacional voltada especialmente para as questões cibernéticas determinou o posicionamento dos EUA para a regulamentação e a legitimação dos procedimentos a serem executados nesse domínio. Por mais que tenham havido esforços constantes para a construção de instrumentos de segurança e defesa cibernética durante o governo do presidente Barack Obama, foi no mandato de Donald Trump que os processos foram acelerados. Considerando esse aspecto, podem ser estabelecidas conexões com a divulgação da *National Cyber Strategy* com o anúncio de que a eleição presidencial norte-americana, de 2016, havia sofrido interferência do governo russo.

A partir dessa concepção, compreende-se que a limitada existência de órgãos reguladores no ciberespaço estimula a competitividade estatal e econômica no tocante à informações privilegiadas, ganhos financeiros e roubos de identidades promovidos por cibercriminosos e as possibilidades de serem exploradas as vulnerabilidades por atores com intenções maliciosas. É possível dizer, portanto, que a USCYBERCOM, como a agência norte-americana responsável pela defesa do ciberespaço, estabelece atribuições de defesa ao passo que incentiva uma vantagem competitiva dos EUA, em relação aos outros Estados.

> O ciberespaço é um espaço operacional ativo e contestado, no qual a superioridade está sempre em risco. Nós sustentamos a vantagem estratégica aumentando a resiliência, avançando as defesas e continuamente engajando nossos adversários. O aumento da resiliência reduz nossa superfície de ataque em casa, antecipa ações adversárias e aumenta a flexibilidade em nossa responsabilidade. [...] O envolvimento contínuo impõe fricção tática e custos estratégicos aos nossos adversários, obrigando-os a mudar os recursos de defesa e reduzir os ataques (USA, 2018b, tradução nossa).

De acordo com Richard Clarke e Robert Knake (2010), a guerra cibernética demonstra como as armas podem ser operadas por meio do ciberespaço, sem necessariamente, os atacantes ou os adversários apresentarem suas capacidades físicas militares. Esse aspecto favorece a execução de ataques assertivamente direcionados e capazes de promover alterações na tomada de decisões dos inimigos. Não apenas, é capaz de gerar antecipação de hostilidades mediante a realização de operações contra redes, sistemas e infraestruturas adversárias, as quais podem ser utilizadas tanto durante a natureza do conflito quanto em momentos de paz, para o ganho de vantagens competitivas.

A título de exemplo, os atores empregados na guerra cibernética sobre a esfera do Estado, para a manutenção da posição e da influência estadunidense no mundo, são denominados guerreiros cibernéticos. Estes são responsáveis por entrar nas redes de controle, bloquear tais redes, destruir dados, promover colapsos ao sistema financeiro, parar transações da cadeia de suprimentos, entre outras funcionalidades cibernéticas que tenham como objetivo afetar o inimigo estatal. Sob esta concepção, os guerreiros cibernéticos são os únicos reconhecidos como os atores que são habilitados a proporcionar oportunidades e vantagens competitivas para os EUA no ciberespaço (CLARKE; KNAKE, 2010).

Com o objetivo de se alcançar o conteúdo proposto pela *National Cyber Strategy*, de proteger as estruturas nacionais na medida em que expande a influência norte-americana no ambiente internacional, outros aspectos também podem ser mencionados como, por exemplo, cooperações no âmbito das organizações internacionais, realizações de espionagem estatal, ciberataques sofisticados direcionados às infraestruturas nacionais, entre outros. Porém, fugiu do escopo da presente pesquisa maiores análises dentro desses aspectos, podendo ser estendido para estudos posteriores.

> O fato de nossos sistemas vitais serem tão vulneráveis à guerra cibernética também aumenta a crise. Enquanto nossos sistemas econômico e militar forem tão obviamente vulneráveis à guerra cibernética, os oponentes tentarão atacar em um período de tensões. Opositores podem pensar que têm uma oportunidade de reformular o equilíbrio político, econômico e militar, demonstrando ao mundo o que podem fazer para os EUA. Eles podem acreditar que a ameaça de um dano ainda maior parecerá crível e impedirá uma resposta dos EUA. Uma vez que eles lançam um ataque cibernético, no entanto, a liderança dos EUA pode se sentir compelida a responder. Essa resposta pode não se limitar ao ciberespaço, e o conflito pode subir rapidamente e sair do controle (CLARKE; KNAKE, 2010, p. 77, tradução nossa).

Na esfera dos atores cibernéticos não-estatais, a atenção governamental permeia os diversos níveis de segurança e defesa, uma vez que as motivações podem ser variadas. No caso dos EUA, as precauções voltam-se para a detenção de invasores às redes e aos sistemas norte-

americanos por considerar que os ciberataques concedem poderes aos seus executores, assim como, produzem ações generalizadas capazes de desestabilizar governos e economias sensíveis. Segundo Wells et al (2016, p. 44, tradução nossa), a natureza transnacional e ilimitada do ciberespaço viabiliza a atuação de criminosos, além de ser uma condutora de "ataques que buscam interromper, destruir ou roubar sistemas interligados digitalmente". Portanto, o ciberespaço oferece facilidades aos indivíduos para o acesso de informações sigilosas e para o controle de sistemas e redes de computadores essenciais aos setores privados ou públicos.

É sabido que o ciberterrorismo caracteriza-se por estender os danos dos ataques à esfera física a partir da utilização do ciberespaço como ferramenta. Esse aspecto peculiar difere-se das demais ameaças ao gerar atenção sobre a necessidade de serem criados elementos de segurança e defesa nacional que estejam conectados ao desenvolvimento de estratégias para a proteção cibernética do Estado em casos de emergência. Mediante a análise dos discursos, verificou-se que a crescente ameaça de ataques cibernéticos aos EUA intensificaram os processos a partir da adoção de discursos que incentivaram a construção de medidas políticas e militares contra as ciberameaças.

Por mais que o termo ciberterrorismo não apareça nos discursos presidenciais norte-americanos, a transversalidade discursiva dada à esfera de segurança dos EUA integra a percepção de que o terrorismo encontra-se difundido em diversas escalas da sociedade e que as ciberameaças são questões ainda recentes e em processo de discussão política na agenda de segurança nacional do país. Por essa razão, e pela complexa interdependência tecnológica dos EUA, são desafiadores os processos de criação, desenvolvimento e fortalecimento de uma defesa cibernética nacional (DUIC, 2017). Contudo, o discernimento correspondente à necessidade de capacitação dos meios militares para a atuação no espaço cibernético fez com que os processos se tornassem acelerados.

> O sucesso da Estratégia [Cibernética de Defesa] será dado quando as vulnerabilidades da segurança cibernética forem efetivamente gerenciadas por meio da identificação e proteção de redes, sistemas, funções e dados assim como detecção, resiliência, resposta e recuperação de incidentes; atividades cibernéticas maliciosas, destrutivas, perturbadoras ou de alguma forma desestabilizadoras, direcionadas contra os interesses dos Estados Unidos são reduzidas ou evitadas; atividade contrária ao comportamento responsável no ciberespaço é dissuadida por meio da imposição de custos através de meios cibernéticos e não cibernéticos; e os Estados Unidos estão posicionados para usar recursos cibernéticos para alcançar objetivos e segurança nacional (USA, 2018d, p. 3, tradução nossa).

Dessa forma, objetivou-se verificar se a ameaça do ciberterrorismo gerou alguma influência na formulação da agenda de segurança e defesa dos EUA, em relação ao campo

cibernético. A partir do panorama da análise de discursos, da análise das unidades de segurança e da análise dos setores de segurança, constatou-se o esforço político e militar no tocante a absorção de recursos de Defesa para a esfera nacional e internacional. Cabe acrescentar, nesse momento, que a utilização do *software* NVIVO 11 demonstrou-se eficiente para a análise e discussão dos dados selecionados.

Nas análises dos discursos presidenciais, a ausência analítica dos setores econômico, societal e ambiental se dá pela não identificação desses setores como possivelmente ameaçados pelas questões cibernéticas e, por isso, não fundamentou-se um maior aprofundamento sobre esses setores no terceiro capítulo. Afirma-se, no entanto, que o desempenho dos atores securitizadores políticos na formulação dos documentos estratégicos e das capacidades militares no âmbito da USCYBERCOM, estimularam a concepção da agenda de defesa norte-americana no que concerne às questões cibernéticas. Em razão disso, determina-se que os setores atualmente ameaçados nos EUA são o político e o militar. Como resultado para a pergunta de pesquisa, portanto, alega-se que os EUA apresentam um posicionamento preventivo e ofensivo de defesa cibernética, tendo em vista a evolução dos documentos de segurança cibernética e a criação de agências de defesa cibernética especializadas.

Conclui-se, assim, que os discursos são elementos nacionais essenciais para a transmissão de informações governamentais para a população e, consequentemente, geram transparência política para outros Estados. Obtendo conteúdos esclarecedores sobre os mecanismos políticos adotados, os discursos também oferecem aparatos para a construção de estruturas administrativas e operacionais em diversos setores nacionais. Visualizou-se que, no setor cibernético, as estratégias nacionais auxiliam os processos de defesa e a legitimação das operações no ciberespaço. Conforme a criação dos documentos de defesa relacionavam-se com a aceitação pública da audiência congressista, analisou-se que os níveis de debates passaram do nível não politizado para o politizado, a partir de 2009. Ao considerar a execução de políticas públicas referentes aos temas cibernéticos abordados discursivamente, principalmente quanto à segurança e defesa nacionais, sustenta-se o argumento de que os EUA apresentam-se em um processo de securitização.

No entanto, a constituição de defesa emoldurada pelas ações nacionais, até o presente momento, engloba as ameaças cibernéticas como um todo, sem grandes especificações sobre como as classificações das ameaças oferecem perigos aos EUA. Em outras palavras, existem correlações nos documentos e no comando cibernético estadunidense acerca da proteção dos sistemas de informação contra os terroristas, contudo, a verificação dos EUA estarem passando por um processo de securitização pauta-se de uma forma geral sobre as ameaças cibernéticas e,

não, específica ao ciberterrorismo. Ou seja, quanto ao objetivo geral proposto na presente dissertação, tem-se o resultado de que o ciberterrorismo – juntamente com as demais ameaças cibernéticas – encontra-se ainda no nível politizado, mas possível de ser securitizado.

Pelo fato da discussão política encontrar-se atualmente no nível politizado, a estrutura lógica proposta pela Teoria da Securitização é a sucessão deste nível para o estado de securitização. Entretanto, para transformar o curso político por meio da mudança de níveis, seria necessário haver um evento inesperado de grande magnitude que conduza o Estado para uma ação política emergencial. Portanto, atribui-se a concepção de que para os EUA ultrapassarem a esfera de discussão politizada de determinada ciberameaça seria necessário, primeiramente, existir um ataque cibernético que promova a desestruturação da trajetória política prefixada e incentive a anexação de estratégias de defesa ligeiramente direcionadas. No entanto:

> Tentativas malsucedidas ou parcialmente bem sucedidas de securitização são interessantes principalmente pelos *insights* que oferecem sobre a estabilidade das atitudes sociais em relação à legitimidade de segurança, o processo pelo qual essas atitudes são mantidas ou alteradas, e a possível direção futura de políticas de segurança (BUZAN et al, p. 39, 1998, tradução nossa).

Nos casos de emergência, não securitizar ou não tomar ações preventivas imediatas, significa tornar os mecanismos de defesa incapazes de lidar com a ameaça de forma eficaz. Com isso, as tentativas de securitização, ainda que não completas, podem estimular a criação de novas políticas de segurança e defesa. Neste sentido, o nível politizado dos discursos em torno de determinada ameaça oferece a possibilidade de serem criados elementos políticos eficientes no combate às ameaças cibernéticas. Esse apontamento pôde ser vislumbrado sobre a pesquisa em questão.

Sendo assim, a pesquisa focou-se em estabelecer conexões entre a ameaça do ciberterrorismo e as estratégias políticas e militares de defesa, para a verificação de um estado de securitização no âmbito doméstico dos EUA. No entanto, é de comum conhecimento que o espaço cibernético é caracterizado por ser transnacional ao permear diversas esferas políticas, econômicas e sociais do mundo e, por isso, são dificultados seus processos de segurança e defesa. Em outras palavras, "o ciberespaço compõe todas as redes de computadores no mundo e tudo que está conectado a e controlado por eles" (CLARKE; KNAKE, 2010, p. 38, tradução nossa). Portanto, conclui-se que as operações cibernéticas são direcionadas para o âmbito externo ao mesmo tempo em que para a esfera doméstica dos EUA.

## REFERÊNCIAS BIBLIOGRÁFICAS

AKHNAR, Babak et al. Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism. In: AKHNAR, Babak; BREWSTER, Ben (eds). **Combatting Cybercrime and Cyberterrorism**. Switzerland: Advanced Sciences and Technologies for Security Applications. 2016.

AMARAL, Arthur Bernardes do. **A Guerra ao Terror e a tríplice fronteira na agenda de segurança dos Estados Unidos**. 2008. Dissertação (Mestrado em Relações Internacionais) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro.

ARIELY, Gil Ad. Adaptive Responses to Cyberterrorism. In: CHEN, Thomas M; JARVIS, Lee; MACDONALD, Stuart (ed). **Cyberterrorism: Understanding, Assessment, and Response**. New York: Springer, 2014, p. 175-196.

AYRES, Nicholas; MAGLARAS, Leandros A. **Cyberterrorism Targeting the General Public Through Social Media**. Leicester: Australia: Jonh Wiley & Sons: Security Communication Netwoks, 2016.

BARBOSA, Rubens Antônio. Os Estados Unidos pós 11 de setembro de 2001: implicações para a ordem mundial e para o Brasil. Brasília: **Rev. Bras. Polít. Inter**. v. 45, n. 1, p. 72-91, 2002.

BARROS, Marinana Andrade. O estado pós-positivista: uma análise a partir das perspectivas construtivista e pós-estruturalista das relações internacionais. Belo Horizonte: **Estudos Internacionais**, v. 5, n.1, 2017.

BARROS, Thiago Henrique Bragato. Por uma metodologia do discurso: noções e métodos para uma análise discursiva. In: **Uma trajetória da Arquivística a partir da Análise do Discurso: inflexões histórico-conceituais**. São Paulo: Editora UNESP; São Paulo: Cultura Acadêmica, 2015, p. 73-95.

BAYRES, Eric; LOWE, Justin. The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. Canada and London: **PA Consulting Group**, dez. 2004.

BERSON, Thomas A; DENNING, Dorothy E. **Cyberwarfare**. USA and Canada: The IEEE Computer and Reliability Societies, 2011.

BEST, Steve; NOCELLA, Anthonty J. **Defining Terrorism**. New York and Texas: Animal Liberation Philosophy and Policy Journal, v. 2, n. 1, p. 1-18, 2004.

BRENNER, Susan W. Cyberterrorism: How Real is the Threat? Hong Kong: **Media Asia**, v. 29, n. 3, p. 149-154, 2002.

BIAZATTI, Bruno de Oliveira. Ataques cibernéticos e seus impactos na definição de conflitos armados não internacionais. **Alethes**: Per. Cien. Grad. Dir. UFJF, v. 5, n. 9, p. 257-280, jul./dez, 2015.

BORGES, João Vieira. O terrorismo e a transformação do planejamento estratégico de segurança nacional dos EUA. Portugal: **Nação e Defesa**, n. 14, ed. 3, 2006, p. 193-227.

BOURDIEU, Pierre. **Language and Symbolic Power**. Cambridge: Polity Press, 1991.

BUZAN, Barry. Rethinking Security after the Cold War. London: **Cooperation and Conflict**, v. 32, n. 1, p. 5-28, 1997.

BUZAN, Barry et al. **Security: a new framework for analysis**. Boulder: Lynne Rienner Publishers, 1998.

CARREIRO, Marcelo. A guerra cibernética: *cyberwarfare* e a securitização da *internet*. **Revista Cantareira**, ed. 17, jul./dez, 2012.

CASTRO, Thales. **Teoria das Relações Internacionais**. Brasília: FUNAG, 2012.

CELSO, Anthony N. **The Islamic State and Boco Haram: Fifth Wave Jihadist Terror Groups**. Orbis, v. 59, n. 2, p. 249-268, 2015.

CHALIAND, Gérard; BLIN, Arnaud. From 1968 to Radical Islam. In: CHALIAND, Gérard; BLIN, Arnaud (Ed.). **The History of Terrorism from Antiquity to Al Qaeda**. California and England: University of California Press, 2007, p. 221-254.

CHEN, Thomas M; JARVIS, Lee; MACDONALD, Stuart (eds). **Cyberterrorism: Understanding, Assessment, and Response**. New York: Springer, 2014.

CHERLOFF, Michael. The Cybersecurity Challenge. Australia: **Regulation and Governance**, n. 2, 2008, p. 480-484.

CLARKE, Richard A; KNAKE, Robert K. **Cyberwar: the next threat to National Security and what to do about it**. Ecco, 2010.

COATS, Daniel R. **Worldwide threat assessment of the US intelligence community**. USA, 2019.

COLLIN, Barry. The future of cyberterrorism. Oxford: **International Criminal Justice**, v. 13, n. 2, p. 15–18, 1997.

CONTE, Alex. **Human Rights in the Prevention and Punishment of Terrorism**. Berlin: Springer-Verlag Berlin Heidelberg, 2010.

CONWAY, Maura. Privacy and Security Against Cyberterrorism: Why cyber-based terrorist attacks are unlikely to occur. **View Points**, Communications of the Association for Computing Machinery, v. 54, n. 1, fev. 2011.

CONWAY, Maura. Reality Check: Assessing the (Un) Likelihood of Cyberterrorism. In: CHEN, Thomas M; JARVIS, Lee; MACDONALD, Stuart (eds). **Cyberterrorism: Understanding, Assessment, and Response**. New York: Springer, 2014, p. 103-121.

CONWAY, Maura. **Terrorism and IT: Cyberterrorism and Terrorist Organizations Online**. Portland: International Studies Association, 2003.

CRENSHAW, Martha. **Terrorism Research: The Record**. London: International Interactions, 2014.

CORNISH, Paul et al. **On Cyber Warfare**. London: Chathan House, 2010.

DAS, Saini. The Cyber Security Ecosystem: Post-global Financial Crisis. In: CHATTERJEE, S. et al (eds). **Managing in Recovering Markets**. India: Springer, 2015, p. 453-459.

DESERIIS, Marco. Hacktivism: On the Use of Botnets in Cyberattacks. London: **Theory, Culture and Society**, 2016, p. 1-22.

DIPERT, Randall R. The Ethics of Cyberwarfare. London: **Journal of Military Ethics**, v. 9, n. 4, 2010, p. 384-410.

DUIC, Igor et al. International Cyber Security Challenges. Zagreb: **MIPRO**, 2017, p. 1525-1529.

DUQUE, Marina Guedes. **A teoria de securitização e o processo decisório da estratégia militar dos Estados Unidos na Guerra do Iraque**. 2008. Dissertação (Mestrado em Relações Internacionais) – Instituto de Relações Internacionais, Universidade de Brasília, Brasília.

_____. O Papel de Síntese da Escola de Copenhague nos Estudos de Segurança Internacional. Rio de Janeiro: **Contexto Internacional**, v. 31, n. 3, set/dez 2009, p. 459-501.

EMBAR-SEDDON, Ayn. Cyberterrorism: Are We Under Siege? USA: **American Behavioral Scientist**, v. 45, n. 6, 2002, p. 1033-1043.

FELINI, Carina Rafaela de Godoi. **Discursos interpelativos de George W. Bush (2000-2004): nacionalismo e neoconservadorismo na busca de legitimação doméstica para a guerra ao terrorismo**. 2017. Dissertação (Mestrado em Ciências Sociais) – Pontifícia Universidade Católica do Rio Grande do Sul, Rio Grande do Sul.

FENZ, Stefan. Cyberspace Security: **A definition and a Description of Remaining Problems**. Wien: Institute of Government and European Studies, 2005.

FERNANDES, Claudemar Alves. **Análise do discurso: reflexões introdutórias**. São Carlos: Editora Claraluz, 2008.

FERNANDES, José Pedro Teixeira. Utopia, Liberdade e Soberania no Ciberespaço. In: VIANA, Vitor Rodrigues. **Cibersegurança**. Portugal: Nação e Defesa, 2012, p. 11-31.

FERREIRA, Marcos Alan S.V. Panorama da política de segurança dos Estados Unidos após o 11 de setembro: o espectro neoconservador e a reestruturação organizacional do Estado. 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.

FOLHA DE SÃO PAULO. O discurso de Bush no Congresso dos EUA. **Folha de São Paulo**, 2001. Disponível em: <http://www1.folha.uol.com.br/folha/mundo/ult94u29639.shtml>. Acesso em 30 de janeiro de 2018.

FOLTZ, Bryan C. Cyberterrorism, Computer Crime, and Reality. Bingley: **Information Management & Computer Security**, v. 12, n. 1, 2004, p. 154-166.

GIACOMELLO, Giampiero. **Close to the Edge: Cyberterrorism Today**. Bingley: Emerald Group, Contributions to Conflict Management, Peace Economics and Development, v. 22, 2014, p. 217-236.

GROSS, Michael L. **The Ethics of Insurgency: A Critical Guide to Just Guerrilla Warfare**. New York: Cambridge University Press, 2015.

GUZZINI, Stefano. Uma reconstrução do construtivismo nas Relações Internacionais. Tradução de João Nackle U.R.T. Dourados: **Monções**: Revista de Relações Internacionais da UFGD, v.2, n.3, jul./dez, 2013.

HERZOG, Stephen. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. **Journal of Strategic Security**, v. 4, n. 2, 2011, p. 49-60.

HIMMA, Kenneth E. Ethical Issues Involving Computer Security: Hacking, Hacktivism and Counterhacking. In: HIMMA, Kenneth E; TAVANI, Herman T**.** Australia: **The Handbook of Information and Computer Ethics**. John Wiley & Sons INC, 2008, p. 191-217.

HUNTON, Paul. A rigorous approach to formalizing the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. Cleveland: **Digital Investigation**, Elsevier, jan. 2011.

JARVIS, Lee; NOURI, Lella; WHITING, Andrew. Understanding, Locating and Constructing Cyberterrorism. In: CHEN, Thomas M; JARVIS, Lee; MACDONALD, Stuart (eds). **Cyberterrorism: Understanding, Assessment, and Response**. New York: Springer, 2014, p. 25-41.

KAPLAN, Jeffrey. **Terrorism's Fifth Wave: A Theory, a Conundrum and a Dilemma**. Massachusetts: Perspectives on Terrorism, v. 2, n. 2, fev, 2008.

KENNEY, M. Cyber-terrorism in a post-Stuxnet World. **Orbis**, v. 59, n. 1, p. 111-128, 2015.

KIRWAN, Grainne; POWER, Andrew. **Cybercrime: The Psychology of Online Offenders**. New York: Cambridge University Press, 2013.

KILGER, Max. Integrating Human Behavior into the Development of Future Cyberterrorism Scenarios. **10th Internacional Conference on Availability, Reliability and Security**, San Antonio, 2015.

KOOPS, Bert-Jaap. Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research. In: In: AKHNAR, Babak; BREWSTER, Ben (eds.). **Combatting Cybercrime and Cyberterrorism**. Switzerland: Advanced Sciences and Technologies for Security Applications, 2016.

KRAPP, Peter. **Terror and Play, or What Was Hacktivism?** USA: Grey Room, The MIT Press, n. 21, 2005, p. 70-93.

KUEHL, Daniel T. From Cyberspace to Cyberpower: defining the problem. In: KRAMER et al. **Cyberpower and National Security**. Nebraska: University of Nebraska Press, 2009, p. 24-42.

LEWIS, James A. Cyberwar Thresholds and Effects. USA and Canada: **IEEE Security and Privacy**, 2011, p. 23-29.

LOPES, Gills; OLIVEIRA, Carolina Fernandes Jost de. Stuxnet e defesa cibernética estadunidense à luz da análise de política externa. **Rev. Bras. Est. Def**. v. 1, n. 1, p, 55-69, jul./dez 2014.

LUIIJF, H. A. M et al. Ten national cyber security strategies: a comparison. Netherlands: **Springer-Verlag**, 2013, p. 1-17.

LYLE, Alison. Legal Considerations for Using Open Source Intelligence in the Context of Cybercrime and Cyberterrorism. In: AKHNAR, Babak; BREWSTER, Ben (eds.). **Combatting Cybercrime and Cyberterrorism**. Switzerland: Advanced Sciences and Technologies for Security Applications, 2016.

MACDONALD, Stuart (eds). **Cyberterrorism: Understanding, Assessment, and Response**. New York: Springer, 2014, p. 63-83.

MAIMON, David; TESTA, Alexander. On the Relevance of Cyber Criminological Research in the Design of Policies ad Sophisticated Security Solutions against Cyberterrorism Events. In: LAFREE, Gary; FREILICH, Joshua D. **The Handbook of the Criminology of Terrorism**. Australia: Jonh Wiley & Sons Inc, 2017.

MANESS, Ryan C. Did Russia just hand Donald Trump the presidency? In: LILLEKER, Darren et al. **US Election Analysis 2016: media, voters and the campaign**. Center for Politics & Media Research. Bournemouth University, 2016.

MARQUES, Luiz Antonio. **Segurança cibernética de defesa**. 2011. Monografia (Curso de Altos Estudos de Política e Estratégia) – Departamento de Estudos da Escola Superior de Guerra, Escola Superior de Guerra, Rio de Janeiro.

MARTINS, Marco. Ciberespaço: uma Nova Realidade para a Segurança Internacional. In: VIANA, Vitor Rodrigues. **Cibersegurança**. Portugal: Nação e Defesa, 2012, p. 32-49.

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

MAURUSHAT, Alana. From Cybersecurity to Cyberwar: security through obscurity or security through absurdity? Canada: **Canadian Foreign Policy Journal**, v. 19, n. 2, 2013, p. 119-122.

MERARI, Ariel. Terrorism as a Strategy of Insurgency. In: GÉRARD, Chaliand; BLIN, Arnaud (eds). **The History of Terrorism from Antiquity to Al Qaeda**. California: University of California Press, 2007.

MEAD, Walter Russel. **Poder, terror, paz e guerra: os Estados Unidos e o mundo contemporâneo sob ameaça**. Rio de Janeiro: Jorge Zahar Ed., 2006.

MILICEVIC, Mladen. **Cyberspace and Globalization**. Los Angeles: Loyola Marymount University, 2008.

MILONE, Mark. Hacktivism: Securing the National Infrastructure. Switzerland: **Knowledge, Technology, & Policy**, Spring, v. 16, n. 1, 2003, p. 75-103.

MOTTA, Bárbara Vasconcellos de Carvalho. **Securitização e política de exceção: o excepcionalismo internacionalista norte-americano na segunda Guerra do Iraque**. 2014. Dissertação (Mestrado em Relações Internacionais) – UNESP/ UNICAMP/ PUC-SP, Programa San Tiago Dantas de Pós Graduação em Relações Internacionais, São Paulo.

NAPOLEONI, Loretta. **A Fênix Islamista: o Estado Islâmico e a Reconfiguração do Oriente Médio**. Rio de Janeiro: Betrand Brasil, 2015.

OLESEN, Nina. European Public-Private Partnerships on Cybersecurity – An Instrument to Support the Fight Against Cybercrime and Cyberterrorism. In: AKHNAR, Babak; BREWSTER, Ben (eds.). **Combatting Cybercrime and Cyberterrorism**. Switzerland: Advanced Sciences and Technologies for Security Applications, 2016.

PILATI, José Isaac; OLIVO, Mickail Vieira Cancelier de. Um novo olhar sobre o direito à privacidade: caso Snowden e pós-modernidade jurídica. Florianópolis: **Sequência**, n. 69, p. 281-300, dez. 2014.

POLLITT, Mark M. **Cyberterrorism – Fact ou Fancy?** Washington D.C: FBI Laboratory, 1998.

QC, Lord Carlile; MACDONALD, Stuart. The Criminalisation of Terrorists' Online Preparatory Acts. In: CHEN, Thomas M; JARVIS, Lee; MACDONALD, Stuart (eds). **Cyberterrorism: Understanding, Assessment, and Response**. New York: Springer, 2014, p. 155-173.

RAPOPORT, David C. **The Four Waves of Rebel Terror and September 11**. Los Angeles: Anthropoetics 8, n. 1, 2002.

RIBEIRO, Vinicius G; RIVERA, César G. A Inserção da Segurança Cibernética na Agenda de Segurança dos EUA no século XXI. Porto Alegre: **Século XXI**, v. 5, n. 2, jul-dez 2014.

RUDZIT, Gunther. O debate teórico em segurança internacional: mudanças frente ao terrorismo? **Civitas**, v. 5, n. 2, jul./dez. 2005.

SAINI et al. Cyber-Crimes and their Impacts: A Review. **International Journal of Enginnering Research and Applications (IJERA)**, v. 2, n. 2, mar-abr, 2012, p. 202-209.

SCHIMD, Alex P. The definition of Terrorism. In: SCHMID, Alex P. (Ed). **The Routledge Handbook of Terrorism Research**. USA and Canada: Routledge, 2011.

SIMON, Jeffrey D. Technological and Lone Operator Terrorism: Prospects for a Fifth Wave of Global Terrorism. In: ROSENFELD, Jean E. (Ed.). **Terrorism, Identity and Legitimacy: The Four Waves Theory and Political Violence**. New York: Routlegde, 2011.

SORELL, Tom. Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous. Oxford: **Journal of Human Rights Practice**, Oxford University Press, v. 7, n. 3, 2015, p. 391-410.

SOUZA, André de Mello et al. **Do 11 de setembro de 2001 à Guerra ao Terror: reflexões sobre o terrorismo no século XXI**. Brasília: IPEA, 2014.

SPEER, David L. Redefining Borders: The Challenges of Cybercrime. Nederland: **Crime, Law & Social Change**, n. 34, 2000, p. 259-273.

STEPANOVA, Ekaterina. **Terrorism in Asymmetrical Conflict: Ideological and Structural Aspects**. SIPRI Research, n. 23, Oxford University Press, 2008.

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

TANNO, Grace. A contribuição da Escola de Copenhague aos Estudos de Segurança Internacional. Rio de Janeiro: **Contexto Internacional**, v. 25, n. 1, p. 47-80, jan./jun. 2003.

TAYLOR, Paul A. Hacktivism – Resistance is Fertile? In: SUMNER, Colin (ed). **The Blackwell Companion to Criminology**, Blackwell Publishing Ltd, 2004, p. 486-500.

USA. **24th Air Force (Air Forces Cyber)**. Air Forces Cyber, 2018a. Disponível em: <https://www.afcyber.af.mil/About-Us/Fact-Sheets/Display/Article/458567/24th-air-force-afcyber/>. Acesso em: 10 de agosto de 2019.

_____. **A budget for a better America: analytical perspectives**. Office of Management and Budget, 2018b.

_____. **Achieve and Maintain Cyberspace Superiority**. U.S. Cyber Command, 2018c.

_____. **Marine Corps Forces Cyberspace Command**. Marine Corps Forces Cyberspace Command, 2019a. Disponível em: <https://www.marforcyber.marines.mil/>. Acesso em: 09 de agosto de 2019.

_____. **National Cyber Security of the United States of America**. The White House, 2018d.

_____. **National Security Strategy of the United States of America**. The White House, 2017a.

_____. **Summary of the National Defense Strategy**. Department of Defense, 2018e.

_____. **The Comprehensive National Cybersecurity Initiative**. The White House, 2009.

_____. **The Dod Cyber Strategy**. Department of Defense, 2015.

_____. **U.S. Army Cyber Command: attack, defend, exploit**. U.S. Army Cyber Command, 2019b. Disponível em: < https://www.arcyber.army.mil/>. Acesso em: 09 de agosto de 2019.

_____. **U.S. Fleet Cyber Command/U.S. Tenth Fleet**. U.S. Cyber Command, 2017b. Disponível em: <https://www.public.navy.mil/fcc-c10f/Pages/usfleetcybermission.aspx>. Acesso em: 09 de agosto de 2019.

VADELL, Javier A.; LASMAR, Jorge Mascarenhas. A longa Guerra Global Contra o Terror e seus efeitos na sociedade internacional: conceitos, contradições e estudos de caso. Paraná: **Revista de Sociologia e Política**, v. 23, n. 53, p. 3-7, 2015.

VENTRE, Daniel. Cyberconflict: Stakes of Power. In: VENTRE, Daniel (Ed). **Cyberwar and Information Warfare**, Wiley, 2011, p. 113-243.

WALT, Stephen M. The Renaissance of Security Studies. In: BUZAN, Barry; HANSEN, Lene. **International Security**: the transition to the post-Cold War security agenda. Grã-Bretanha, 2007, v. 2.

WARF, Barney; FEKETE, Emily. Relational geographies of cyberterrorism and cyberwar. **Space and Polity**, 2015.

WEIMANN, Gabriel. **Cyberterrorism: How Real is the Threat?** Washington: Special Report, 2004.

WELLS, Douglas; BREWSTER, Ben; AKHGAR, Babak. Challenges Priorities and Policies: Mapping the Research Requiriments of Cybercrime and Cyberterrorism Stakeholders. In: AKHNAR, Babak; BREWSTER, Ben (eds.). **Combatting Cybercrime and Cyberterrorism**. Switzerland: Advanced Sciences and Technologies for Security Applications, 2016, p. 39-52.

WENDT, Alexander. Anarchy is what States Make of it. The Social Construction of Power Politics. Cambridge: **International Organization**, vol. 46, n. 2, p. 391-425, 1992.

WRIGHT, Quincy. **A guerra**. Biblioteca do Exército, Coleção General Benício, v. 260, 1988.

ZUCCARO, Paulo Martino. **Tendência global em segurança e defesa cibernética – reflexões sobre a proteção dos interesses brasileiros no ciberespaço. In: Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011, p. 49-77.