

UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”
FACULDADE DE FILOSOFIA E CIÊNCIAS – FFC
CAMPUS DE MARÍLIA

RAQUEL TORRECILHA SPIRI

**CIBERSEGURANÇA NO BRASIL: UMA ANÁLISE DE SEUS
DESDOBRAMENTOS À LUZ DA SECURITIZAÇÃO**

MARÍLIA
2020

UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”

RAQUEL TORRECILHA SPIRI

**CIBERSEGURANÇA NO BRASIL: UMA ANÁLISE DE SEUS
DESDOBRAMENTOS À LUZ DA SECURITIZAÇÃO**

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Sociais da Faculdade de Filosofia e Ciências, da Universidade Estadual Paulista – UNESP – Campus de Marília, como requisito parcial para a obtenção do título de mestre em Ciências Sociais.

Área de concentração: Relações Internacionais e Desenvolvimento

Orientador: Prof. Dr. Rodrigo Duarte Fernandes dos Passos

MARÍLIA
2020

S759c Spiri, Raquel Torrecilha
Cibersegurança no Brasil : Uma análise de seus desdobramentos à
luz da Securitização / Raquel Torrecilha Spiri. -- Marília, 2020
202 p. : tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp),
Faculdade de Filosofia e Ciências, Marília
Orientador: Rodrigo Duarte Fernandes dos Passos

1. Cibersegurança. 2. Brasil. 3. Securitização. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de
Filosofia e Ciências, Marília. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

RAQUEL TORRECILHA SPIRI

CIBERSEGURANÇA NO BRASIL: UMA ANÁLISE DE SEUS DESDOBRAMENTOS
À LUZ DA SECURITIZAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Sociais da Faculdade de Filosofia e Ciências – Universidade Estadual Paulista —Júlio de Mesquita Filho – UNESP, Campus de Marília, como requisito parcial para a obtenção do título de Mestre em Ciências Sociais.

Linha de Pesquisa: Relações Internacionais e Desenvolvimento

BANCA EXAMINADORA

Orientador: _____

Prof. Dr. Rodrigo Duarte Fernandes dos Passos (UNESP-FFC/Marília)

2º Examinador: _____

Prof. Dr. Paulo Ribeiro Rodrigues da Cunha (UNESP-FFC/Marília)

3º Examinador: _____

Prof.^a Dr.^a Carla Cristina Wrbieta Ferezin (UFSC)

Marília, 04 de setembro de 2020

AGRADECIMENTOS

Aos meus familiares por todo o apoio e suporte durante este período acadêmico. À minha mãe Silvia, ao meu pai Walter e à minha irmã Bárbara: obrigada por estarem sempre presentes e por sempre valorizarem a educação e criarem oportunidades para que eu conseguisse conquistar meu caminho neste meio. Vocês foram essenciais para que eu me tornasse quem sou hoje. Agradeço toda paciência e preocupação nos momentos mais difíceis do Mestrado. Eu não os teria superado sem vocês. Amo vocês.

À minha segunda família, Felipe, Sandra e William expresso meu imenso agradecimento, pois sua ajuda foi fundamental para que eu permanecesse em Marília e completasse meus estudos. À Nayara por todo companheirismo, paciência, ajuda e pelas risadas e lágrimas que compartilhamos nessa jornada. Levarei isso comigo para sempre.

Aos meus queridos amigos de Bauru Gabriel, Luisa, Renan, Thiago e Victor por me ouvirem falar sobre o tema dessa dissertação incansavelmente, discutirem e se interessarem, valorizando minhas ideias. Agradeço também pelos momentos de descontração e pelo suporte emocional, necessários para que eu não chegasse ao pico do esgotamento no meio do caminho.

Ao meu orientador e colega professor Rodrigo Duarte Fernandes dos Passos por me acolher como orientanda em 2018, por sempre me respeitar, por acreditar em meu potencial, e por me valorizar como acadêmica. Agradeço por toda paciência e suporte, fundamentais para que eu pudesse permanecer no programa de Mestrado.

Aos professores doutores Carla Cristina Wrbieta Ferezin e Paulo Ribeiro Rodrigues da Cunha por estarem presentes como banca e também por acompanharem meu trabalho, oferecendo sempre importantes *insights* para que esta pesquisa se concretizasse.

Ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) por acreditar e financiar pesquisas acadêmicas no âmbito das Ciências Sociais, mesmo em meio a uma grande dificuldade de fomentar a educação e a pesquisa no Brasil atualmente.

“I don’t think we have seen the tip of the iceberg. I think the potential of what the Internet is going to do to society, both good and bad, is unimaginable. I think we are actually on the cusp of something exhilarating and terrifying [...] I am talking about the actual context and the state of content. It's going to be so different to anything we can really envisage at the moment – where the interplay between the user and the provider will be so in simpatico it is going to crash our ideas of what mediums are all about”

David Bowie, 1999

RESUMO

Tema recente na esfera da Segurança Internacional, a segurança cibernética ganhou espaço em discussões em nível governamental a partir da popularização das Novas Tecnologias da Informação e Comunicação. Parte-se do entendimento que a difusão da Internet passou a apresentar ameaças em âmbito do chamado ciberespaço e que podem caracterizar um problema à segurança de um Estado. Ao que se refere à atuação do Brasil no ciberespaço, o Ministério da Defesa, no ano de 2008, elaborou diretrizes para lidar com novas ameaças engendradas pela transição do século XX ao XXI, entre elas, questões envolvendo a área cibernética, através da publicação da Estratégia Nacional de Defesa. A partir de tal documento, tutelou-se às Forças Armadas, especificamente ao Exército Brasileiro, a segurança do espaço cibernético do Brasil. Considerando a teoria de Segurança Internacional desenvolvida pela Escola de Copenhague e seus principais expoentes, Barry Buzan, Ole Wæver e Jaap de Wilde, entende-se que é possível traçar maneiras de compreender o processo de segurança cibernética ocorrido no Brasil. No livro publicado em 1997, *Security: A New Framework for Analysis*, os três autores apresentaram o conceito de Securitização, ideia de que uma questão pode ser tratada como matéria de segurança desde que haja um agente securitizador que, através do discurso, atribui caráter emergencial a ela e toma medidas para protegê-la. Dessa forma, objetiva-se testar, sob a ótica Securitização da Escola de Copenhague, a hipótese de que o Brasil, através da Estratégia Nacional de Defesa, buscou securitizar seu espaço cibernético, outrossim, procurando compreender os desdobramentos de uma política de proteção do setor cibernético, em particular ao que se refere aos recursos dispendidos com a cibersegurança no país desde a criação do Centro de Defesa Cibernético, em 2010. O trabalho faz uso de bibliografia pertinente ao assunto, pautada sobre os trabalhos desenvolvidos pela Escola de Copenhague bem como documentos disponibilizados pelo governo brasileiro. No que se refere aos resultados alcançados, concluímos que o Brasil securitizou seu espaço cibernético em três fases entre 2002 e 2018: na primeira, promoveu-se o discurso de segurança cibernética no governo; na segunda, tomou-se medidas emergenciais; e, na terceira, consolidou e ampliou-se a atuação das Forças Armadas na cibersegurança no Brasil.

Palavras-chave: Cibersegurança. Brasil. Securitização.

ABSTRACT

As a new theme in the sphere of International Security, cyber security has gained space in discussions at the governmental level from the popularization of New Information and Communication Technologies. It is known that the spread of the Internet presented threats in the context of the so-called cyberspace and that process may characterize a problem to the security of a state. Regarding Brazil's role in cyberspace, the Ministry of Defense in 2008 drew up guidelines to deal with new threats engendered by the transition from the twentieth to the twenty-first century, including issues involving the cyber area through the publication of the National Defense Strategy. As from this document, the Armed Forces, specifically the Brazilian Army, were responsible for the security of Brazil's cyber space. Considering the International Security theory developed by the Copenhagen School and its main exponents, Barry Buzan, Ole Wæver and Jaap de Wilde, it is understood that it is possible to outline ways to understand the cyber security process that took place in Brazil. In their 1997 book, *Security: A New Framework for Analysis*, the three authors presented the notion of Securitization, the idea that an issue can be treated as a security matter as long as there is a securitizing agent that, through discourse, attributes an emergency feature to this issue and take steps to protect it. Thus, we aim to test, under the scope of the Securitization of the Copenhagen School, the hypothesis that Brazil, through the National Defense Strategy, sought to securitize its cyber space. We also try to understand the outcomes of this protection policy in cyber space, in particular, regarding the resources spent on cybersecurity in the our country since the foundation of the Cyber Defense Center in 2010. This work makes use of relevant bibliography, based on the works developed by the Copenhagen School as well as documents made available by the Brazilian government. Regarding the achieved results, we educe that Brazil securitized its cyberspace in three phases that occurred between 2002 and 2018: the first one promoting the cybersecurity discourse in government; the second phase taking emergency measures; and the third phase consolidating and expanding the role of the Armed Forces in cybersecurity in Brazil.

Keywords: Cibersecurity. Brazil. Securitization.

LISTA DE TABELAS

Tabela 01	Principais tipos de ataques cibernéticos sofridos no Brasil no século XXI	25
Tabela 02	Espectro de localização de questões de segurança internacional	43
Tabela 03	Os níveis de análise na Securitização	48
Tabela 04	Unidades envolvidas na análise de segurança segundo a Escola de Copenhague	50
Tabela 05	Componentes para o processo de securitização de sucesso segundo a Escola de Copenhague e o caso brasileiro	106
Tabela 06	Unidades da análise de segurança segundo a Escola de Copenhague e o caso brasileiro	106
Tabela 07	O caráter das Ações Cibernéticas pelas Forças Armadas Brasileiras	156
Tabela 08	Processo de securitização do ciberespaço brasileiro	170
Tabela 09	Despesas do Ministério da Defesa entre 2012 e 2019	175

LISTA DE ABREVIATURAS E SIGLAS

ANSA	Associação de Nações do Sudeste Asiático
CDCiber	Centro de Defesa Cibernético
COPRI	<i>Copenhagen Peace Research Institute</i>
CS	Conselho de Segurança das Nações Unidas
EB	Exército Brasileiro
EC	Escola de Copenhague
END	Estratégia Nacional de Defesa
DDOS	<i>Distributed Denial of Service</i>
DOS	<i>Denial of Service</i>
FFAA	Forças Armadas
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
MD	Ministério da Defesa
MCTIC	Ministério da Ciência, Tecnologia, Inovações e Comunicações
MRE	Ministério das Relações Exteriores
NSA	<i>National Security Agency</i>
NTIC	Novas Tecnologias de Informação e Comunicação
NuCDCiber	Núcleo do Centro de Defesa Cibernético
OUA	Organização da Unidade Africana
OEA	Organização dos Estados Americanos
OPEP	Organização dos Países Exportadores de Petróleo
PDN	Política de Defesa Nacional
PND	Política Nacional de Defesa
PNSI	Política Nacional de Segurança da Informação
SIC	Segurança da Informação e da Comunicação
SINDE	Sistema de Inteligência de Defesa
SMDC	Sistema Militar de Defesa Cibernética
TIC	Tecnologias de Informação e Comunicação

SUMÁRIO

1	INTRODUÇÃO	12
1.1	O ciberespaço enquanto objeto de estudo	17
1.2	Procedimentos metodológicos	28
2	CAPÍTULO 1 - SECURITIZAÇÃO	35
2.1	A ampliação e o aprofundamento do conceito de segurança	38
2.2	Securitização e o <i>speech-act</i>	42
2.3	Elementos do processo de securitização	47
2.4	Os limites da Teoria de Securitização segundo seus principais críticos	54
2.4.1	A linguagem e o <i>speech-act</i>	55
2.4.2	A contextualização histórica	57
2.4.3	A teoria, a prática e a experiência europeia	57
2.5	Algumas considerações	60
3	CAPÍTULO 2 - CONTEXTUALIZAÇÃO INTERNACIONAL	62
3.1	O caso Estônia (2007)	65
3.2	O caso Geórgia (2008)	68
3.3	O caso Stuxnet (2010)	72
3.4	O caso <i>WikiLeaks</i> (2010)	75
3.5	O caso Snowden (2013)	82
3.6	O caso <i>Lázarus</i> (2014)	90
3.7	O caso Ucrânia (2015)	95
3.8	O caso <i>WannaCry</i> (2017)	98
3.9	Considerações a respeito do contexto internacional	101
4	CAPÍTULO 3 - SECURITIZAÇÃO DO ESPAÇO CIBERNÉTICO: O CASO BRASILEIRO	104
4.1	Contextualização Nacional	108
4.1.1	Sociedade da Informação no Brasil e Estratégia Brasileira para a Transformação Digital	109
4.1.2	Política de Defesa Nacional (1996)	113
4.2	<i>Speech-act</i>: O desenvolvimento do discurso de cibersegurança	116
4.2.1	Seminário Política de Defesa para o Século XXI (2002)	116
4.2.2	Projeto de Declaração Sobre a Segurança Nas Américas (2003)	121
4.2.3	Política de Defesa Nacional (2005)	123
4.2.3.1	<i>Algumas diferenças entre a Política de Defesa Nacional de 2005 e a Política Nacional de Defesa de 2012</i>	127
4.2.3.2	<i>Algumas considerações a respeito da PDN (2005)</i>	130
4.3	Medidas voltadas à cibersegurança	132
4.3.1	Estratégia Nacional de Defesa (2008)	132
4.3.1.1	<i>A atualização de 2012</i>	136
4.3.1.2	<i>A importância da Sexta Diretriz da Estratégia Nacional de Defesa</i>	138
4.3.1.3	<i>Algumas considerações a respeito da END</i>	141
4.3.2	Boletim nº 31/10 do Exército Brasileiro (2010)	141
4.4	Produtos das políticas de cibersegurança	145

4.4.1	Política Cibernética de Defesa (2012)	146
4.4.2	Doutrina Militar de Defesa Cibernética (2014)	152
4.4.3	Marco Civil da Internet (2014)	160
4.4.4	Guia de Defesa Cibernética na América do Sul (2017)	163
4.4.5	Política Nacional de Segurança da Informação (2018)	165
4.5	A cibersegurança no Brasil	168
5	CAPÍTULO 4 - OS DESDOBRAMENTOS DA SECURITIZAÇÃO NO BRASIL	172
6	CONSIDERAÇÕES FINAIS	184
	REFERÊNCIAS	189
	APÊNDICE A – Linha do Tempo da Contextualização Internacional	201
	APÊNDICE B – Linha do Tempo do Processo de Segurança Cibernética no Brasil	202

1 INTRODUÇÃO

As Tecnologias da Informação e Comunicação que se popularizaram no século XX se consolidaram como elementos fundamentais das relações sociais, políticas e econômicas ainda no início do século XXI. Esta transformação, em conjunto com a presença constante da tecnologia no cotidiano, ocorre principalmente, pelo avanço tecnológico na área da informática que permitiu maior acesso a computadores e sistemas de informação e, posteriormente, à Internet.

Podemos inferir, também, que a incorporação da informatização no sistema de produção capitalista foi responsável pela consolidação do ideário de que a tecnologia é *indispensável*.

A informatização tratou-se de uma verdadeira revolução nas relações sociais. Isso, pois, transformou a forma como nos comunicamos, trabalhamos, nos entretemos e nos comportamos. É possível dizer, inclusive, que diversos segmentos da sociedade dependem especificamente da tecnologia atualmente.

Entretanto, como afirmaram Cepik, Canabarro e Borne (2014):

[...] à medida que cresce a dependência da sociedade em relação a sistemas informáticos e computacionais, bem como se diversificam as possibilidades de aplicação destas tecnologias para fins lícitos e ilícitos, intensifica-se o debate em torno dos desafios que a era digital apresenta à *segurança nacional e internacional* (CEPIK; CANABARRO; BORNE, 2014, p. 161, grifo nosso).

Tendo as Relações Internacionais se tornado objeto de estudo com o fim da Segunda Guerra Mundial e a partir da criação da Organização das Nações Unidas, surgiu a necessidade da condução de estudos a respeito da Segurança Internacional.

A Segurança Internacional, ora entendida subjetivamente como um termo elástico, ora entendida objetivamente como um dado preciso, obteve seu próprio campo de estudo, os Estudos de Segurança (WILLIAMS, 2008, p. 02).

Podemos observar, dessa forma, o desenvolvimento quase que simultâneo dos Estudos de Segurança Internacional e a própria tecnologia desde a segunda metade do século XX em diante.

Apresentam-se aqui, portanto, a relação entre dois elementos: a *tecnologia* e a *segurança*. Tal relação é importante de ser compreendida enquanto a tecnologia se consolida no que aqui chamaremos de “elemento presente nas relações internacionais” e a Segurança

compreende as vulnerabilidades que podem acompanhar tal dependência tecnológica, como já apresentado nos supracitados Cepik, Canabarro e Borne.

Ademais, consideramos que, como afirmou o sociólogo Pierre Lévy, ainda em 1999:

O desenvolvimento das cibertecnologias é encorajado por Estados que perseguem a potência, em geral, e a supremacia militar em particular. É também uma das grandes questões de competição econômica mundial entre as firmas gigantes da eletrônica e do software, entre os grandes conjuntos geopolíticos (LÉVY, 1999, p. 24).

Podemos inferir a partir da afirmação de Lévy que a tecnologia, chamada por ele de cibertecnologia, permeia os diversos segmentos das relações internacionais e, por este motivo, é incentivada e encorajada pelos atores presentes nessas relações na medida em que passa a oferecer alguma vantagem, seja ela econômica ou militar.

Como argumentaremos posteriormente, o incentivo ao desenvolvimento tecnológico bem como à *segurança tecnológica* vem, normalmente, de atores que estão em uma posição privilegiada e têm seu discurso reconhecido.

Justifica-se, portanto, o estudo da relação entre tecnologia e segurança. Em termos mais específicos, delimitamos o *ciberespaço* como a tecnologia a ser investigada. Dessa forma, a cibersegurança se posiciona como tema central em nossa pesquisa.

Williams (2008) no livro *Security Studies: An Introduction*, o qual editou e organizou, afirmou que a maior parte dos estudiosos de Segurança trabalham “[...] com uma definição de segurança que envolve o alívio de ameaças a valores estimados” (WILLIAMS, 2008, p. 01, tradução nossa¹).

Dessa forma, tomando como ponto de partida tal compreensão do *germen* dos Estudos de Segurança, objetivamos inferir o papel que o principal produto das Tecnologias da Informação e Comunicação, o *ciberespaço*, pode ser configurado como elemento de segurança.

Esclarecemos que, como parte de nossa análise, tomamos uma perspectiva essencialmente Construtivista dos Estudos de Segurança Internacional como contexto, ou seja, como estudo de caso, a realidade brasileira a partir do século XXI.

¹ No original: “[...] with a definition of security that involves the alleviation of threats to cherished values” (WILLIAMS, 2008, p. 01).

Cabe o esclarecimento de que, quando afirmamos que nossa perspectiva teórica envolve a Teoria Construtivista dos Estudos de Segurança Internacional, estamos falando da Teoria de *Securitização* desenvolvida pela Escola de Copenhague. Entendemos que os expoentes desta escola de pensamento desenvolveram uma teoria que ofereceu um quadro de análise, um *framework*, capaz de compreender a tecnologia como elemento de segurança, especialmente quando analisado o caso brasileiro em questão.

Isto, pois, o Construtivismo se trata de um referencial teórico das Relações Internacionais – e, por conseguinte, dos Estudos de Segurança – que oferece uma perspectiva de *construção* nas relações entre os atores presentes na análise (MCDONALD, 2008, p. 59).

O Construtivismo não apenas apresenta este caráter de construção social dos comportamentos, mas também valoriza o papel da "[...] *interpretação* da realidade, especialmente ao que se refere às atividades políticas e sociais" (ERIKSSON; GIACOMELLO, 2007, p. 18, tradução nossa², grifo nosso).

Eriksson e Giancomello (2007), no livro *International Relations and the Security in the Digital Age*, afirmaram que:

O estudo da ‘política simbólica’ (o uso e abuso de símbolos para manipular o discurso político e a opinião pública) é altamente relevante para estudar a segurança na era digital [...] [e que] [...] os estudos Construtivistas podem contribuir para a compreensão destes símbolos, [bem como eles] se manifestam [...] (ERIKSSON; GIANCOMELLO, 2007, p. 21, tradução nossa³).

No caso da Escola de Copenhague, como veremos adiante e em maior detalhe, esta perspectiva Construtivista, em termos de segurança, significa que a ameaça pode ser *construída socialmente* através do discurso que é usado como uma ferramenta de legitimação. Ou seja, a construção social ocorre através de um conceito compreendido como *speech-act*, levando a uma *percepção* (ou interpretação) e posterior legitimação da ameaça por uma audiência a quem o discurso se dirige (BUZAN; WÆVER; WILDE, 1998; MCDONALD, 2008).

² No original: “Constructivists emphasize the unavoidability of the interpretation (and thus distortion) of reality, especially with respect to the understanding of social and political activity” (ERIKSSON; GIACOMELLO, 2007, p. 18).

³ No original: “The study of ‘symbolic politics’ (the use and abuse of symbols for manipulating political discourse and public opinion) is highly relevant for studying digital-age security [...] constructivist studies can contribute for understanding these symbols, how they manifest [...]” (ERIKSSON; GIANCOMELLO, 2007, p. 21).

Na medida em que questões envolvendo a presença da *informação* e o desenvolvimento de Tecnologias da Informação e Comunicação e suas vulnerabilidades passaram a estar cada vez mais latentes – apesar de recentes – nos debates internacionais, justifica-se tanto classificá-las enquanto problemas de Segurança Internacional quanto investigá-las sob uma perspectiva que seja capaz de dialogar com tais transformações – como é o caso da abordagem construtivista.

Dessa forma, dentre as teorias existentes, entendemos que a Securitização se trata de uma escolha adequada na análise para o caso qual escolhemos compreender: o processo de segurança do ciberespaço brasileiro no século XXI.

Dentre as motivações que nos incentivaram a desenvolver este trabalho, destacamos uma percepção crescente de trabalhos envolvendo as Relações Internacionais e a tecnologia sendo publicados internacionalmente. Entendemos que a tecnologia enquanto elemento de pesquisa nas Relações Internacionais e, sobretudo, na Segurança Internacional, pode se apresentar de diversas formas: as chamadas Guerras Híbridas; as transformações das práticas terroristas com o recrutamento *online*; o uso de DRONES e outros equipamentos eletrônicos como instrumentos de vigilância, monitoramento e coleta de informações; e, entre outros, a ciberspionagem e o poder cibernético.

Observamos que o ciberespaço, em específico, se tornou tema latente nas pesquisas acadêmicas mesmo com a complexidade dos fenômenos que o envolve e as diferentes formas de interpretá-lo: seja politicamente, militarmente ou culturalmente. Chamou nossa atenção o fato de um país como o Brasil, situado na periferia mundial, com poucos investimentos em tecnologia e inovação técnica, especialmente quando comparados aos gigantes China e Estados Unidos, estabelecer o setor cibernético como sendo estratégico para a defesa nacional, tal-qualmente os setores espacial e nuclear.

A partir do estabelecimento do ciberespaço enquanto setor estratégico pela Estratégia Nacional de Defesa de 2008, passamos a tentar compreender os motivos pelos quais o governo brasileiro apreendeu o espaço cibernético dessa forma e *por que* houve o envolvimento das Forças Armadas neste processo. Dessa forma, buscamos estabelecer um recorte temporal que compreendesse os principais acontecimentos antes e depois de 2008 no Brasil. Chegamos, assim sendo, ao período compreendido entre 2002 e 2018.

Partindo do princípio de que a análise a respeito do tratamento do ciberespaço no Brasil seria feita através de uma perspectiva da Segurança Internacional, compreendemos

que a teoria de Securitização desenvolvida pela Escola de Copenhague seria uma escolha adequada enquanto quadro de análise de um fenômeno recente – e multifacetado – como a cibersegurança.

Objetivamos, portanto, testar a hipótese de que o governo brasileiro, especialmente entre 2002 e 2018, passou por um processo de securitização de seu espaço cibernético, através da construção social de uma ameaça a partir do uso do discurso.

Justifica-se este recorte temporal na medida em que 2002 representa o início de um novo governo e 2018 o fim de outro, completando um ciclo. Ademais, o engendrar do século XXI teve um acontecimento muito importante para a segurança internacional em 2001: o ataque às Torres Gêmeas, em Nova Iorque. Dessa forma, se justifica o início de nossa análise no ano de 2002.

A partir de 2002, o Ministério da Defesa sinalizou a respeito de potenciais problemas envolvendo a tecnologia, reformulando sua Política de Defesa Nacional em 2005 e publicando a Estratégia Nacional de Defesa, em 2008, esta última qual menciona pela primeira vez o termo ciberespaço em um documento oficial de Defesa no Brasil (BRASIL, 2003; BRASIL, 2005; BRASIL, 2008).

Estes foram os principais pontos de partida para um levantamento de outros significativos documentos publicados promovendo a defesa cibernética no Brasil, como Decretos, Leis, Doutrinas e Políticas específicas para o setor – considerado como *estratégico*.

O ano 2018 marca o fim do governo Temer antes de se iniciar outro ciclo presidencial. Ademais, em dezembro de 2018 foi publicado o Decreto 9.637 que previu ações voltadas à Segurança da Informação no Brasil. Dessa forma, escolhemos o ano de 2018 como ano final de análise do processo de securitização.

Considerando tais motivações, apresentaram-se as seguintes indagações de pesquisa: o governo brasileiro securitizou seu espaço cibernético? Em caso positivo, quais os principais desdobramentos neste processo? Qual o papel das Forças Armadas na garantia da cibersegurança?

Tendo em vista o objetivo de responder tais perguntas, faz-se pertinente, ainda nesta Introdução, o esclarecimento de elementos que giram em torno do nosso objeto de estudo, a cibersegurança, além de alguns procedimentos metodológicos que tomamos ao longo de nossa investigação.

1.1 A cibersegurança enquanto objetos de estudo

O termo “ciberespaço” foi cunhado, originalmente, pelo escritor William Gibson em seu livro de ficção científica, *Neuromancer*, de 1984. Em sua obra, o ciberespaço se trata de um espaço no qual os personagens podem acessar através de seu sistema nervoso e desfrutar dos serviços por ele oferecidos. Durante a trama, aquilo que é feito no ciberespaço tem implicações no “mundo real”. Gibson descreveu:

Ciberespaço. Uma alucinação consensual vivenciada diariamente por bilhões de operadores autorizados, em todas as nações, por crianças que estão aprendendo conceitos matemáticos... uma *representação* gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano [...] (GIBSON, 2016, p. 77, grifo nosso).

Neuromancer se tornou uma obra popular que continuou ganhando novas edições, mesmo trinta anos após a sua publicação (GIBSON, 2016). Neste livro, a informação e os dados são os elementos centrais das relações sociais no contexto futuro qual Gibson descreve. A presença de *hackers* (denominados de *cowboys* pelo autor) e de vulnerabilidades do ciberespaço desenrolam a trama.

Apesar de sua obra ter sido escrita antes da popularização das Novas Tecnologias da Informação e Comunicação, muitos elementos da ficção encontraram seus correspondentes na realidade dos anos que seguiram a publicação de *Neuromancer*. Para além da esfera literária, o ciberespaço tornou-se um termo cotidiano, mas também acadêmico.

À vista disso, como o ciberespaço e sua segurança podem ser compreendidos enquanto objeto de estudo em nosso caso específico?

O desenvolvimento das Tecnologias de Informação e Comunicação – e das Novas Tecnologias de Informação e Comunicação⁴ – fomentou, como compreendemos, o que pode ser entendido como Revolução Informacional⁵. Investimentos no setor fizeram com que estas tecnologias se popularizassem exponencialmente, passando a fazer parte do cotidiano em regiões urbanizadas a partir da década de 1990 e início século XXI.

⁴ Entendemos que as Tecnologias de Informação e Comunicação e as Novas Tecnologias de Informação e Comunicação emergem de um mesmo processo de desenvolvimento tecnológico que se iniciou na década de 1970 e são apenas separadas metodologicamente. As NTICs descrevem uma tecnologia atualizada e presente no século XXI, tais como os Smartphones, a Internet e a conexão presente entre aparelhos eletrônicos diversos.

⁵ Crítica desenvolvida pelo sociólogo francês Jean Lojkin a despeito do processo de transformações tecnológicas as quais colocaram a *informação* como elemento central cotidiano, presente desde às relações sociais às econômicas (LOJKINE, 2002).

Dessarte, o ciberespaço tornou-se produto da relação entre estas tecnologias, outrossim da relação destas próprias tecnologias para com a sociedade. Ressaltamos, contudo, a novidade de tal conceito em meio acadêmico. Apesar de ter suscitado debates e estudos, uma definição acadêmica consensual e universal do ciberespaço enquanto objeto ainda não existe (GUDES DE OLIVEIRA; PORTERLA, 2017).

Entendemos que a dificuldade de definir o que é o ciberespaço reflete sua própria característica subjetiva, muitas vezes na condição de um “espaço abstrato”, como afirmou Maier (2019, p. 11). Conforme leitura adotada, diferentes compreensões de ciberespaço podem ser desenvolvidas.

Guedes de Oliveira e Portela (2017, p. 79) também apontaram que “[...] a contínua evolução e mudanças de estruturas e dinâmicas do próprio espaço cibernético, assim como a intangibilidade de algumas das suas fronteiras [...] dificulta o apontamento da dimensão do espaço cibernético [...]”, fazendo com que o debate se torne ainda mais complexo em torno do conceito de ciberespaço.

Dessa forma, na falta de uma definição consensual, o ciberespaço pode ser compreendido diferentemente dependendo da perspectiva que se adota, seja ela *cultural*, *política* ou *militar* (MAIER, 2019).

Tendo em vista nosso objeto de estudo – a cibersegurança – e nosso contexto de investigação – o Brasil – apresentemos aqui a forma pela qual o ciberespaço é definido pelo Ministério da Defesa brasileiro: “[...] espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas” (BRASIL, 2014b, p. 18). Podemos inferir que o caráter conciso desta compreensão de ciberespaço vai ao encontro do contexto *militar* qual foi publicada.

Tal definição de ciberespaço foi postulada, em 2014, no documento oficial Doutrina Militar de Defesa Cibernética do Ministério da Defesa (BRASIL, 2014b). Apesar de considerarmos que tem sua validade no contexto de sua publicação, gostaríamos de acrescentar alguns pontos em nossa própria definição de ciberespaço.

Apesar de ser um elemento que se tornou importante para a Defesa Nacional no Século XXI, ganhando atenção especial das Forças Armadas brasileiras, como discutiremos

nesta investigação, a compreensão carece de alguns elementos que consideramos importantes para o debate esclarecedor a respeito do ciberespaço e suas nuances.

Primeiramente, como já apresentamos, entendemos o ciberespaço como um produto da interação entre as Tecnologias de Informação e Comunicação (TICs), bem como da reciprocidade da tecnologia com a ação humana. As TICs, por sua vez, são produto do desenvolvimento tecnológico gerado a partir da segunda metade do século XX e promovido pelos países ricos que, por conseguinte, gerou a Revolução Informacional. Esta última pode ser compreendida como o processo, que vem se tornando cada vez mais amplo, do sistema capitalista de empregar as ferramentas de Tecnologia da Informação na *produção*, nas relações sociais e também na economia (LOJKINE, 2002).

Em uma definição mais recente – e também mais recorrente – de 2010, a respeito do espaço cibernético, Oliveira e Portela compreenderam, através da leitura de Clarke e Knake⁶, que: “O espaço cibernético consiste em todas as redes de computadores do mundo e todas as coisas conectadas a esses aparelhos ou submetidas aos seus controles” (CLARKE; KNAKE, 2012 apud⁷ GUEDES DE OLIVEIRA; PORTELA, 2017, p. 80).

Guedes de Oliveira e Portela ainda complementaram:

Para esses autores, a internet está dentro do espaço cibernético, mas esse não pode ser resumido somente a ela. O espaço cibernético é mais abrangente, pois também se refere às estruturas que não estão conectadas à internet e todos os aparelhos submetidos a ela (GUEDES DE OLIVEIRA; PORTELA, 2017, p. 80).

Mesmo com a complementariedade de Guedes de Oliveira e Portela (2017), podemos observar que este trecho compreende, ainda, uma definição bastante objetiva de um ambiente complexo tal como se apresenta o ciberespaço.

Inferidos tais elementos – papel da informação e lugares pelo qual transita – do espaço cibernético, cabe-nos considerar, também, a contrapartida da *interação humana* com este

⁶ Clarke e Knake são autores norte-americanos que se dedicaram ao estudo recente a respeito do papel do ciberespaço e da digitalização da Guerra. Seu trabalho se tornou bastante popular ao que se refere à junção de questões militares e tecnológicas. Por este motivo são bastante retomadas em trabalhos na área. Salientamos, entretanto, que os retomamos a fim de ilustrar tal conceito, mas que buscamos privilegiar visões mais aprofundadas do conceito de ciberespaço de maneira que vá ao encontro de nossa perspectiva teórica construtivista. Ademais, tratando-se contexto brasileiro, autores brasileiros serão retomados para que melhor dialoguem com o trabalho.

⁷ CLARKE, Richard A; KNAKE, Robert A. **Cyber War: The Next Threat to National Security and What to do About It**. New York: HarperCollins Publishers, 2012.

ambiente, uma vez que os acessos são promovidos por estes agentes sociais, como já evidenciou Maier (2019).

Para além de todas estas questões, conferimos carácter de *internacionalidade* do ciberespaço. Apesar da dificuldade de compreender ou definir as “fronteiras do ciberespaço” – este nem é o objetivo desta investigação – podemos afirmar que o ciberespaço está presente em todo o Mundo (CEPIK; CANABARRO; BORNE, 2014). Portanto, nos resta considerar a dimensão internacional do espaço cibernético que permeia a relação entre diferentes figuras do sistema internacional e que também permeia as esferas econômica, política e social.

Isto posto, compreendemos que, como argumentamos nesta investigação, o espaço cibernético passou a ser elemento presente nas Relações Internacionais, exigindo maior atenção de todos os atores presentes no sistema internacional. Na medida em que o ciberespaço pode apresentar vulnerabilidades e desvantagens econômicas, políticas, militares, entre outras, é possível justificar a atenção empregada à cibersegurança por estes atores.

Em suma, se considerarmos nossas ressalvas a respeito da definição oficial do governo brasileiro – mas não a desqualificarmos -, e tomarmos como base a perspectiva Construtivista descrita neste trabalho e as leituras mais recorrentes do assunto tais como as aqui apresentadas, construímos nossa própria compreensão do espaço cibernético. Este é um elemento da Revolução Informacional, sendo um meio pelo qual a informação digitalizada transita local ou globalmente, através ou não da Internet, interagindo reciprocamente com a ação humana através de aparelhos eletrônicos. Tal espaço pode ter carácter caótico pelo seu crescimento incontido e por sua popularização mundial. Agentes internacionais, por sua vez, podem *perceber* neste espaço cibernético, o surgimento de possíveis ameaças, dignas de serem compreendidas e – possivelmente – neutralizadas.

Apesar de expoentes da Escola de Copenhague mencionarem a questão da tecnologia e considerarem, ainda que brevemente, o papel do espaço cibernético na Segurança Internacional e, sobretudo, no “encurtamento de distâncias” promovido pelas novas tecnologias, estes não se debruçaram sobre o assunto a ponto de produzir sua própria definição ou desenvolver um argumento mais elaborado (BUZAN; WÆVER; WILDE, 1998, p. 163).

Dessa forma, nosso intuito com a nossa própria definição de ciberespaço foi apresentar uma tentativa de aproximação do conceito com a perspectiva Construtivista das

Relações Internacionais, sobretudo, do ponto de vista da Segurança Internacional. Ou seja, nossa definição visa criar a relação entre ciberespaço e segurança de um ponto de vista específico.

Compreendidas ambas definições – a nossa e aquela publicada em documento oficial do governo brasileiro de 2014 – cabe a pergunta: De que forma a cibersegurança se torna objeto de estudo em nossa investigação?

Tomando como ponto de partida o espaço cibernético, objetivamos compreendê-lo sob uma perspectiva Construtivista da Segurança Internacional, segundo as bases teóricas desenvolvidas pela Escola de Copenhague (BUZAN; WÆVER, WILDE, 1998). Não obstante, o intuito do presente trabalho é compreender os aspectos *militares* que circundam o ciberespaço no contexto do governo brasileiro.

Optamos por desenvolver nossa própria definição de ciberespaço que pudesse contemplar uma perspectiva Construtivista enquanto matriz teórica presente em nossa investigação. Ressaltamos, contudo, que a compreensão oficial de ciberespaço pelo governo brasileiro é aquela que aparece na Doutrina Militar de Defesa Cibernética e que permanece válida na discussão que aqui propusemos.

A nossa definição de ciberespaço, ainda, objetiva demonstrar a complexidade do objeto, comparando-o com definições majoritariamente militares que desconsideram alguns elementos relevantes do caráter do ciberespaço.

Tendo em vista a novidade de pesquisas acadêmicas voltadas ao estudo do ciberespaço com rigor metodológico e também teórico, justifica-se a nossa tentativa de fazer uma abordagem mais esclarecedora possível do objeto que aqui trataremos extensivamente.

Já inferida a ideia de ciberespaço, nossa tentativa agora é apresentar a forma pela qual é assegurado pelo Estado brasileiro. Ou seja, a forma pela qual se dá a *cibersegurança* no Brasil. Para tal, faz-se necessário compreender todos os elementos presentes quando tratamos de cibersegurança.

De acordo a Política Nacional de Defesa, em sua versão atualizada de 2012, a Segurança, conforme o entendimento do Ministério da Defesa Brasileiro, pode ser definida como “[...] a condição em que o Estado, a sociedade ou os indivíduos se sentem livres de riscos, pressões ou ameaças, inclusive de necessidades extremas” (BRASIL, 2012, p. 15).

O documento ainda propõe uma diferenciação entre Defesa e Segurança no Brasil, adotando os seguintes conceitos:

I. Segurança é a condição que permite ao País preservar sua soberania e integridade territorial, promover seus interesses nacionais, livre de pressões e ameaças, e garantir aos cidadãos o exercício de seus direitos e deveres constitucionais; e **II.** Defesa Nacional é o conjunto de medidas e ações do Estado, com ênfase no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas (BRASIL, 2008, p. 15).

Tomando como base estas definições, entendemos a cibersegurança como a condição do ciberespaço de se manter seguro, protegido de vulnerabilidades que podem ameaçar a *soberania* e os *interesses nacionais*. A defesa cibernética, por sua vez, trata-se do conjunto de medidas que são tomadas objetivando a cibersegurança.

Considerando que fizemos um levantamento das principais medidas tomadas pelo governo brasileiro voltadas ao ciberespaço, tratamos, também, de defesa cibernética e não somente a segurança cibernética.

Entretanto, o debate que propomos gira em torno da cibersegurança, pois nosso objetivo é analisar o ciberespaço brasileiro nos termos da Segurança Internacional, em específico, a Teoria de Securitização, como já mencionado. Ademais, o projeto de cibersegurança no Brasil dialoga com uma tendência internacional de investimentos no setor cibernético (MORGAN, 2019).

O Ministério da Defesa Brasileiro e as Forças Armadas têm uma definição de cibersegurança (ou segurança cibernética), postulada pela Doutrina Militar de Defesa Cibernética, a saber: “arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas *infraestruturas críticas*” (BRASIL, 2014b, p. 19, grifo nosso).

Destacamos o termo “infraestrutura crítica” pois este é bastante recorrente quando estudamos e pesquisamos a respeito de cibersegurança. O principal objetivo que justifica as medidas tomadas no âmbito da segurança cibernética - não apenas no Brasil, mas também no mundo é justamente a proteção das infraestruturas críticas.

As infraestruturas críticas, de forma geral, podem ser entendidas como tudo aquilo que um Estado considera como estratégico e de que o país não pode abrir mão.

O governo brasileiro definiu as infraestruturas críticas como sendo as: “instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade” (BRASIL, 2014b, p. 19).

Uma definição tão geral como essa não é por acaso. Considerar como infraestrutura crítica tudo aquilo que pode ser de caráter militar, político, econômico, social e até “internacional”, como compreendido pela Doutrina Militar de Segurança Cibernética, justifica quaisquer meios e medidas de promoção da cibersegurança.

Retornaremos a este argumento posteriormente, especialmente quando apresentarmos casos notórios de ataques cibernéticos que danificaram as infraestruturas críticas de outros países.

Considerar a cibersegurança no Brasil como objeto de estudo faz com que seja necessário, também, considerar que existem ameaças e vulnerabilidades que se apresentam e justificam as medidas tomadas na proteção do ciberespaço e das chamadas infraestruturas críticas.

Dessa forma, tentaremos responder nas próximas páginas, dentro de nossas possibilidades, a seguinte pergunta: Sob quais vulnerabilidades ou ameaças o espaço cibernético brasileiro está submetido quando falamos sobre cibersegurança?

De acordo com o Guia de Defesa Cibernética na América do Sul, publicado e disponibilizado em 2017, o Brasil é “o país que mais sofreu ataques cibernéticos na América Latina nos últimos anos” (GUDES DE OLIVEIRA et al., 2017, p. 65). Um estudo desenvolvido pela Kaspersky Lab⁸ e noticiada em português pelo G1 alertou que o Brasil ocupava, em 2016, a nona posição mundial entre os países que mais sofriam ataques cibernéticos (G1, 2016, s/p).

Apesar de uma crescente tentativa de tornar os servidores brasileiros cada vez mais seguros, os principais ataques sofridos no país referem-se àqueles do tipo *scan* (54%) e *phishing* (34%), de acordo com dados de 2015 (GUEDES DE OLIVEIRA et al., 2017, p. 67).

⁸ Empresa russa de segurança da informação. É produtora de um dos principais antivírus comercializados mundialmente e conduz pesquisas na área da segurança da informação periodicamente.

Ataques que ganharam notoriedade na década de 2010 foram relacionados a *malwares*⁹ tais como o *web skimming*, que afetou o Ministério das Relações Exteriores em 2015, e o *WannaCry*, em 2017, que afetou diversos computadores no Brasil, especialmente aqueles em repartições públicas que usavam o sistema operacional Windows (CAPELAS, 2017). Este último, o caso *WannaCry*, será discutido em maior detalhe posteriormente em uma apresentação do panorama internacional geral.

Seria inevitável, em um trabalho sobre cibersegurança e tecnologia, não esbarrarmos com alguns termos que não são familiares às Relações Internacionais tais como *malware*, *software* e *hackers*. Não cabe ao escopo da presente investigação se aprofundar em termos específicos da Computação, mas buscamos esclarecer da melhor forma possível alguns dos ataques cibernéticos mais comuns com o objetivo de apresentar um panorama mais genérico da situação brasileira.

⁹ *Malware (malicious software)* é como a informática oficialmente trata o que é chamado informalmente de “vírus de computador”.

Tabela 01: Principais tipos de ataques cibernéticos sofridos no Brasil no século XXI

Tipo de Ataque	Definição
<i>Scan (Port scanning)</i>	Varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Este ataque serve para identificar alvos, pois permite visualizar falhas em servidores e permitir a “entrada” de <i>hackers</i> que terão acesso àquele servidor e suas informações.
<i>Phishing</i>	Usuários mal-intencionados se utilizam de mensagens ou formulários que parecem legítimos para roubar informações pessoais tais como CPF, números de contas bancárias e senhas. Tais mensagens podem chegar via e-mail, por exemplo, e a vítima, voluntariamente, preenche com suas informações pessoais.
<i>Web Skimming</i>	Trata-se de quando uma página legítima que contém o preenchimento de informações pessoais está infectada por um <i>malware</i> e o usuário legítimo não tem conhecimento. Suas informações são repassadas ao usuário mal-intencionado que fez uso do <i>malware</i> .
<i>WannaCry</i>	Tipo de software nocivo disseminado para explorar falhas do sistema operacional Windows. Ele é capaz de criptografar as máquinas infectadas e pede um resgate para que a máquina seja “liberada” para uso.
Negação de Serviço (<i>DoS Attack</i>)	Está entre os principais ataques que ocorrem mundialmente pela dificuldade de evitá-lo. O usuário mal-intencionado (ou <i>hacker</i>) infecta, através de um <i>malware</i> , outros computadores que atuam sob seu comando na tentativa de acessar algum site ou servidor. Com a quantidade de acessos simultâneos, o servidor para de oferecer seu serviço a usuários legítimos. Dessa forma, o site fica “fora do ar”.

Fonte: Elaborado pela autora com base em CERT.BR, 2016; CAPELAS, 2017.

Além dos ataques cibernéticos mais “tradicionais” presentes no espaço cibernético do Brasil, destacamos aqueles relacionados aos atos de espionagem articulados pelo governo

norte-americano e expostos pelo “ciberativista” Edward Snowden, em 2013 (HARDING, 2014), além de diversos documentos divulgados pelo grupo *WikiLeaks* (WIKILEAKS, 2015), que se organizou a partir da crença de que toda a informação deve ser acessível a todos e todas. Pretendemos trazer estes episódios para a discussão posterior a respeito da cibersegurança em uma perspectiva mais geral, pois tanto o caso Snowden quanto os *WikiLeaks* obtiveram grande notoriedade internacionalmente.

Cabe aqui ressaltar que a prática de ataques cibernéticos no Brasil é ilegal, ainda que muito seja necessário evoluir no campo jurídico para o enquadramento dos responsáveis (BORTOT, 2017). Ainda sob a perspectiva jurídica, a legislação brasileira vem avançando em alguns aspectos que envolvem tecnologia e o direito nos últimos anos.

Brevemente, destacamos as Lei 12.735/2012, Lei 12.737/2012 e Lei 12.965/2014, conhecidas como “Lei Azevedo”, “Lei Carolina Dieckmann” e “Marco Civil da Internet”, respectivamente. Conforme Bortot esclareceu em seu trabalho, tais leis representaram um significativo avanço no combate à criminalidade na Internet no Brasil. De forma geral, tais leis objetivam *proteger os usuários* e garantir seus direitos na esfera do espaço cibernético.

Destas três Leis mencionadas, o Marco Civil da Internet é o documento que trataremos com maior abundância nesta pesquisa, pois é responsável por tratar de pontos relevantes ao que se refere à construção da segurança na Internet e ao direito do usuário de forma mais extensiva. Ademais, o Decreto 9.637 de 2018, responsável por instituir uma Política Nacional de Segurança da Informação também terá destaque aqui, no terceiro capítulo, na medida em que se tratou de uma tentativa de reforçar a proteção a informações sensíveis no País (BRASIL, 2018).

Apesar da questão jurídica não ser o foco de nossa investigação, é inevitável que elementos jurídicos apareçam ao se pesquisar cibersegurança no Brasil. Por se tratar de um elemento constantemente presente no cotidiano da sociedade brasileira, ainda é muito recente, e questões de legislatura tentam evoluir no mesmo ritmo da evolução tecnológica – mesmo que com dificuldades. Nosso intuito é apresentar apenas alguns dados jurídicos com o objetivo de enriquecer a discussão deste trabalho, mas não nos aprofundarmos nestes termos.

Além da questão estratégica que permeia a aquisição de informações oficiais do Estado, a questão econômica também é latente ao se tratar de ataques e crimes cibernéticos

no Brasil. Conforme evidenciou-se no Guia de Defesa Cibernética na América do Sul, de 2017:

Os crimes cibernéticos, de forma geral, afetam cerca de 20 milhões de brasileiros por ano e geram um custo médio de US\$ 831 por vítima, valor superior à média global em 2013, de US\$ 298. Tal realidade resulta em um custo líquido total de US\$ 8 bilhões ao Estado brasileiro (GUEDES DE OLIVEIRA et al., 2017, p. 67).

Dessa forma, entendemos que os incentivos à cibersegurança no Brasil estão relacionados não somente à infraestrutura crítica, mas também às questões de proteção de informação sensível e de proteção de roubos ou problemas que acarretem indenizações. A própria Lei Carolina Dieckmann (Lei 12.737/2012) prevê um agravante da pena no caso de invasões a dispositivos informáticos resultarem em prejuízos eletrônicos (BRASIL, 2012, s/p).

Uma outra questão passível de argumentação quando tratamos da *justificativa* para a cibersegurança no Brasil e que aqui também levantamos, trata-se da vontade do governo brasileiro em se equiparar a potências tais como os Estados Unidos e China em matéria de Segurança da Informação. Ora, podemos argumentar que na medida em que há investimento em tecnologia e em segurança cibernética em um determinado local, melhor a sua imagem e confiança externamente. Isto, por conseguinte, pode ser responsável por atrair prestígio internacional e, mais importante, investimentos estrangeiros.

Ademais, podemos observar uma tendência crescente desde o início do século XXI a respeito da relação entre *tecnologia* e *segurança* na medida em que a informatização foi se consolidando cada vez mais nas relações econômicas, políticas, sociais e militares – como já apontaram Cepik, Canabarro e Borne (2014) – e este também é um ponto que pretendemos desenvolver na presente investigação. Entendemos que o Brasil, em sua condição de país em desenvolvimento deu – e continua dando – atenção a investimentos na área tecnológica, ainda que com diferentes focos nos últimos governos, entre 2002 e 2018.

Portanto, tendo em vista a ampliação da agenda de Segurança Internacional, a tecnologia e o próprio ciberespaço puderam ser enquadrados como elemento de segurança e, em particular, da *securitização* (BUZAN; WÆVER, WILDE, 1998, p. 163; p. 195). Isto é capaz de gerar um novo significado não somente ao papel da tecnologia, mas ao próprio aparato militar, responsável por assegurar o ciberespaço. Nosso objetivo é analisar esta relação entre securitização, cibersegurança e Forças Armadas no Brasil.

1.2 Procedimentos metodológicos

Tendo em vista nosso objetivo de compreender se – e de que forma – o Brasil passou por um processo de Securitização do seu espaço cibernético, cabe esclarecer a forma pela qual optamos por fazê-lo.

A respeito de nossa abordagem metodológica, esta pesquisa tem caráter qualitativo, pois coletamos os dados e fazemos uma interpretação subjetiva destes tendo em vista o suporte teórico qual utilizamos que, em nosso caso, é a Teoria da Securitização da Escola de Copenhague, como já apontado.

Enquanto aos objetivos da presente investigação, esta trata-se de uma pesquisa predominantemente exploratória, visto que o ciberespaço e as questões relacionadas às medidas tomadas no campo internacional na garantia de sua segurança têm trabalhos até então incipientes ou até mesmo introdutórios, e o assunto ainda não se esgotou na comunidade acadêmica.

Dentre os nossos procedimentos de coleta de informações para o trabalho destacamos dois: o método bibliográfico e o documental. Isto, pois, a bibliografia conta com trabalhos relevantes na área da tecnologia e do Estudo da Segurança Internacional das Relações Internacionais, bem como a própria Teoria da Securitização desenvolvida por Barry Buzan, Ole Wæver e Jaap De Wilde, responsável por oferecer o aporte teórico que sustenta nossa hipótese.

A pesquisa também é documental enquanto nos utilizamos dos documentos oficiais publicados pelo governo brasileiro, especialmente aqueles expedidos entre 2002 e 2018. São eles, principalmente, Decretos, Leis, Estratégias e Políticas. Dessa forma, acreditamos que seja possível criar um vínculo entre o discurso teórico e a realidade apresentada nos documentos trazidos à análise.

Inicialmente, observamos a relevância da Estratégia Nacional de Defesa publicada em 2008, por se tratar de um documento voltado à Defesa no século XXI que apresenta o caráter estratégico do setor cibernético para o Brasil pela primeira vez e de forma explícita. A partir dele, fizemos um levantamento dos principais documentos publicados considerando a Defesa no Brasil e as chamadas “novas ameaças”, antes e após o ano de 2008, chegando ao recorte temporal dos anos de 2002 a 2018.

Os principais documentos levantados foram: o Seminário Política de Defesa para o Século XXI, de 2002; a Política de Defesa Nacional, de 2005; a Estratégia Nacional de Defesa, de 2008; o Boletim nº 31 do Exército, de 2010; o Livro Verde de Segurança Cibernética no Brasil, de 2010; a atualização da Política de Defesa Nacional e da Estratégia Nacional de Defesa, de 2012; a Política Cibernética de Defesa, de 2012; a Doutrina Militar de Defesa Cibernética, de 2014; o Marco Civil da Internet, de 2014; o Guia de Defesa Cibernética na América do Sul, de 2017; e o Decreto 9.637, de 2018.

Entendemos que questões referentes à Segurança e Defesa no Brasil têm seu sigilo conferido pela Constituição e diversos Decretos Presidenciais que regem sobre elas. Dessa forma, ressaltamos que os dados que trabalhamos são oficiais do governo brasileiro e que eram públicos no momento da coleta dos documentos como propriamente referenciado.

Levamos em consideração em nossa análise, ainda, acontecimentos internacionais relevantes recentes que se relacionam com o tema da segurança cibernética, a saber: o ataque cibernético à Estônia, em 2007; o ataque cibernético à Geórgia, em 2008; o ataque do vírus *Stuxnet*, no Irã, em 2010; o papel do *WikiLeaks*, em 2010; o caso Snowden, em 2013; a atuação do grupo *Lázarus* mundialmente, em 2014; o ataque cibernético à Ucrânia, em 2015; e o ataque do *ransomware WannaCry* mundialmente, de 2017.

Todos os casos acima mencionados tiveram repercussão no Brasil. Entendemos que a contextualização internacional destes eventos mencionados pode contribuir para o debate a respeito da cibersegurança internacionalmente, mas também nacionalmente – dentro do recorte temporal aqui proposto. Dessa forma, compreendemos a importância de mencioná-los.

Ainda a respeito dos casos internacionais – aqui desenvolvido no capítulo denominado “Contextualização Internacional” – compreendemos que têm sua relevância na contribuição para o discurso, cada vez mais latente, de uma necessidade de investimentos na tecnologia, seja ela tanto na área da segurança da informação, quanto na cibersegurança.

Ademais, um capítulo dedicado à explicação de casos internacionais de ciberataques contribui para o estabelecimento da relação entre *teoria e realidade* e serve como repertório de exemplos do emprego do ciberespaço de forma a atender aos interesses dos Estados.

O suporte teórico utilizado em nossa pesquisa é, também, elemento central em nossa análise e interpretação.

Como já mencionado, optamos por partir de um posicionamento Construtivista de segurança, pois compreendemos ser um quadro de análise adequado para o contexto da cibersegurança no Brasil.

A Escola de Copenhague, a partir da década de 1980, já questionava o estadocentrismo de algumas teorias *mainstream* de Segurança Internacional e já propunha outras formas de olhar para a questão da Segurança considerando outros elementos além do Estado (BUZAN, 1983). O professor Barry Buzan, principalmente, desenvolveu seu trabalho com este foco, mas nunca desconsiderou o Estado como possível referencial de segurança. A Escola de Copenhague, portanto, gostaria que houvesse um referencial teórico mais *abrangente* e mais *profundo* da Segurança Internacional, em que a ideia de “ameaça” seria socialmente construída e legitimada.

Dessa forma, a Escola de Copenhague em que aqui recorremos como suporte teórico fez parte de uma corrente que ficou conhecida como *wideners* (ampliadores), pois acreditavam em uma tendência internacional de que novos elementos passaram a ser tratados como questão de Segurança (BUZAN; HANSEN, 2012; VILLA; REIS, 2006).

É nesse sentido que a Escola de Copenhague dialoga com nosso objeto de estudo. O desenvolvimento tecnológico chegou a um nível de aperfeiçoamento que pôde ser usado para servir aos interesses de Estados e de grupos específicos capazes de cometerem crimes e ataques virtualmente, especialmente a partir do século XXI. Dessa forma, o ciberespaço virou um elemento estratégico de segurança e defesa. Investimentos oficiais passaram a ser cada vez mais comuns no setor da *cibersegurança*.

A Teoria de Securitização, portanto, tem o papel de nos auxiliar na compreensão dessa tendência da cibersegurança no Brasil.

O conceito de Securitização – bem como a construção da Teoria pela Escola de Copenhague – será abordado em um capítulo exclusivo que dedicamos ao nosso suporte teórico. O já mencionado livro de 1998 *Security: A Framework for Analysis* (BUZAN; WÆVER; DE WILDE, 1998) é a principal obra dos autores que se debruça sobre uma proposta teórica e a construção da ideia de Securitização, mas os principais expoentes da Escola de Copenhague já haviam desenvolvido outros trabalhos relevantes no âmbito da Segurança Internacional e Construtivismo em anos anteriores. Estes também serão levados em consideração em nossa tentativa de compreensão do quadro de análise proposto pela Teoria da Securitização.

Ainda a respeito do aporte teórico, consideramos a contribuição de Lene Hansen, a respeito do papel do discurso na Segurança Internacional, a partir de *insights* sobre a sua obra *Security as Practice: Discourse Analysis and the Bosnian War* (HANSEN, 2006). Destacamos a professora Lene Hansen e seus trabalhos, pois ela também é creditada como sendo parte da chamada “Escola de Copenhague”. Entendemos que ela contribuiu – e contribui – com os principais autores que se dedicam à Securitização, mas que ela é atribuída à Escola de Copenhague apenas por lecionar, assim como Barry Buzan, Jaap De Wilde, e Ole Waever, na Universidade de Copenhague, sendo todos estes professores colegas de departamento.

Finalmente, consideramos também os *insights* dos principais críticos da Teoria de Securitização para melhor compreensão dos limites teóricos da Securitização (HUYSMANS, 1998; SKIDMORE, 1998; MCDONALD, 2008a; HANSEN, 2000; HANSEN; NISSENBAUM, 2009; BALZACQ; LÉONARD; RUZICKA, 2016).

Efetivamente, buscamos utilizar nosso suporte teórico assim como as principais críticas à Teoria da Securitização de maneira bem específica. Nosso principal ponto de partida é o livro *Security: A New Framework For Analysis*, pois este livro é a principal compilação e construção do pensamento da Escola de Copenhague no que se refere a Securitização.

O referido livro trouxe conceitos dos quais nos utilizaremos durante todo o trabalho tais como: *speech-act*, discurso, audiência, objeto referencial, ator securitizador, atores funcionais, condições facilitadoras, movimento securitizador, ameaça existencial, ação emergencial, relação entre unidades e medidas extraordinárias.

Optamos por analisar o contexto brasileiro de cibersegurança levando em consideração os critérios e conceitos da Escola de Copenhague de maneira a apresentar a correspondência entre os conceitos da Teoria de Securitização e a realidade brasileira a partir dos documentos analisados, dentro do recorte temporal de 2002 a 2018.

No capítulo dedicado à Teoria, apontaremos os limites da proposta da Escola de Copenhague e também indicaremos estas ressalvas quando fizermos a relação com o contexto brasileiro.

Sendo assim, o trabalho ficou dividido da seguinte maneira: o primeiro capítulo, denominado SECURITIZAÇÃO, foi responsável por apresentar um panorama geral da

Teoria de Securitização da Escola de Copenhague que utilizamos para o desenvolvimento do trabalho. Compreendemos que um capítulo dedicado a elucidar, mesmo que brevemente, a abordagem Construtivista da Securitização pode contribuir para o rigor metodológico do trabalho, bem como pode esclarecer os termos quais nos balizamos para o desenvolvimento argumentativo.

O segundo capítulo, denominado CONTEXTUALIZAÇÃO INTERNACIONAL, como já tratamos previamente, foi incumbido de apresentar um panorama geral dos principais ciberataques que ganharam notoriedade internacionalmente e foram responsáveis, conforme interpretamos, pelo desenvolvimento do discurso de segurança do ciberespaço mundialmente.

O terceiro capítulo do presente trabalho, SECURITIZAÇÃO DO ESPAÇO CIBERNÉTICO: O CASO BRASILEIRO, foi responsável por apresentar o desenvolvimento da investigação em si. Nele, apresentamos os documentos oficiais do governo brasileiro voltados às fases da securitização do ciberespaço no período de 2002 a 2018, assim como optamos por fazer uma breve contextualização a respeito da Defesa no Brasil na década de 1990 na medida em que apresentou condições para que o processo de securitização fosse desenvolvido.

Não apenas apresentamos tais documentos, mas fizemos uma análise, dentro dos moldes da Teoria desenvolvida pela Escola de Copenhague, dos principais aspectos das Defesa e Segurança brasileiras ao que se refere ao reconhecimento e tratamento do ciberespaço como setor estratégico.

É neste capítulo, também, que observamos e apontamos a frequente presença das Forças Armadas, em específico o Exército Brasileiro, como tutor oficial da cibersegurança no Brasil. Tentamos resgatar elementos da Teoria da Securitização para corroborar com algumas críticas que fazemos à militarização do nosso objeto de estudo.

O quarto e último capítulo, denominado OS DESDOBRAMENTOS DA SECURITIZAÇÃO NO BRASIL, objetivou apresentar algumas das implicações do processo de securitização do ciberespaço brasileiro em termos de dispêndio de recursos financeiros. Também neste capítulo, analisamos tais desdobramentos de forma crítica e comparamos com outros países da América do Sul que entendemos como relevantes para uma compreensão mais profunda dos resultados da cibersegurança.

Neste capítulo fizemos uma análise superficial da Estratégia Nacional de Segurança Cibernética, aprovada em fevereiro de 2020, apontando algumas semelhanças para com o documento norte-americano que tem o mesmo propósito.

Por fim, traçamos as nossas CONSIDERAÇÕES FINAIS, trazendo um panorama geral da cibersegurança no Brasil e aquilo inferido com nossa investigação. Em termos metodológicos, separamos nossos resultados alcançados com a pesquisa a respeito da securitização do ciberespaço brasileiro em três fases. Já adiantamos: a primeira fase, correspondente ao período de construção do discurso de segurança, foi de 2002 a 2007. É nesta primeira fase que se tem a construção social do setor cibernético como existencialmente ameaçado. O Ministério da Defesa do Brasil foi o órgão responsável por expressar tal necessidade de segurança (REBELO; FERNANDES, 2003).

A segunda fase corresponde ao período de 2008 a 2011. Marco importante para a cibersegurança no Brasil, foi no ano de 2008 que a Estratégia Nacional de Defesa foi promulgada e o ciberespaço tomado como setor estratégico de defesa para o Brasil. Foi neste documento, ainda, que se atribuiu o Exército Brasileiro como responsável pela cibersegurança no Brasil. Entendemos que esta segunda fase corresponde à “ação emergencial” postulada pela Escola de Copenhague como um dos elementos para a Securitização ter sucesso (BUZAN; WÆVER; DE WILDE, 1998; BRASIL, 2008). Ou seja, é nesta fase que, após reconhecida a necessidade de proteção do ciberespaço, medidas foram tomadas visando efeitos práticos.

A terceira e última fase, conforme entendemos, do processo de securitização do espaço cibernético brasileiro corresponde ao período entre 2012 e 2018. Este período foi importante para a conclusão do processo a partir da criação de órgãos responsáveis pela cibersegurança, especificamente e do emprego e treinamento de pessoal no setor. Os investimentos crescentes na área cibernética brasileira também foram observados neste período. Dessa forma, entre os anos de 2012 e 2018, obtivemos a relação entre ciberespaço, segurança, Ministério da Defesa e Forças Armadas. O período se “encerra” em 2018 com o fim do nosso recorte temporal que corresponde ao fim do governo Temer e também à publicação do Decreto 9.637/18 (Política Nacional de Segurança da Informação) no mês de dezembro.

Ressaltamos que a divisão por fases foi um método de apresentar os resultados da investigação. Deve-se ter em mente que a securitização é um processo que contém diversos

elementos que se sobrepõem uns aos outros em alguns aspectos. Nosso objetivo final é interpretar o processo como um *todo*.

Por fim, justificamos que a decisão de estruturar o trabalho dessa maneira correspondeu a uma tentativa de apresentar, inicialmente, os elementos a serem trabalhados em nossa discussão principal: os conceitos teóricos e a contextualização internacional. Os capítulos de número três e quatro, por sua vez, tiveram como objetivo apresentar o desenvolvimento do trabalho em si a partir da compreensão da construção da cibersegurança no Brasil e dos desdobramentos das principais políticas voltadas ao setor cibernético.

CAPÍTULO 1

2 SECURITIZAÇÃO

As Relações Internacionais, enquanto estudo, desde seu surgimento no fim da Segunda Guerra Mundial, têm como tradição o privilégio de uma perspectiva política-militar. Ao que se refere à Segurança Internacional em específico, os estudos *mainstream* também foram aqueles em que os conflitos eram tomados política e militarmente, priorizando o papel do Estado nas relações internacionais.

Apesar de outros debates e contrapontos terem surgido nesta mesma época, esta visão que privilegiava a ação estatal nas relações internacionais foi predominante – especialmente quando consideramos os Estudos de Segurança Internacional (ESI), um dos temas das Relações Internacionais, durante todo o período da Guerra Fria até o fim da bipolaridade na década de 1990 (BUZAN; HANSEN, 2012).

Com a perda do referencial de Estado tal como se obteve a partir do fim da Guerra Fria, outras perspectivas ganharam visibilidade, tais como os chamados Estudos Críticos das Relações Internacionais, que propuseram uma *ampliação e aprofundamento* da compreensão da Segurança (VILLA; REIS, 2006, p. 29, grifo nosso). Esta ideia de ampliação, combinada ao aprofundamento, pode ser observada com frequência quando considerados os estudos conduzidos a partir das décadas de 1980 e 1990 pelos críticos dos estudos tradicionais.

O objetivo de ampliação e aprofundamento da compreensão da Segurança foi justamente tentar explicar novas dinâmicas que passaram a ocorrer dentro dos Estados em que as teorias *mainstream* não eram capazes de contemplar.

Entende-se, ainda, que com o final da Guerra Fria, estudos “híbridos” surgiram na tentativa de melhor explicar os fenômenos internacionais e suas dinâmicas. Villa e Reis (2006) argumentaram que estes estudos híbridos foram fomentados pela Escola de Copenhague, uma vez que incorporaram “elementos da agenda *construtivista* ao enfoque sistêmico e estrutural-realista” (VILLA; REIS, 2006, p. 30, grifo nosso).

Ressaltamos que uma abordagem Construtivista, como argumenta McDonald (2008, p. 64, tradução nossa¹⁰), compreende a segurança como “uma construção social em um

¹⁰ No original: “For constructivists, then, security is a context-specific social construction” (MCDONALD, 2008, p. 64).

contexto específico”. Ou seja, o *significado* da segurança em seu contexto é elemento central para entender suas implicações.

Dessa forma, é possível afirmar que a Escola de Copenhague desenvolveu uma abordagem híbrida, ampliadora e aprofundada da Segurança Internacional, partindo de um ideal Construtivista. Isto, pois, além de considerar o Estado como objeto referencial de segurança, sugeriu que outras questões e contextos fossem levados em consideração, tais como a identidade, a economia e o Meio Ambiente.

Em sua publicação mais completa a respeito de sua principal teoria, a Securitização, a Escola de Copenhague propôs a setorização para a análise de segurança, sendo elas: seguranças militar, política, econômica, societal¹¹ e ambiental (BUZAN; WÆVER; DE WILDE, 1998). Cada setor, por sua vez, tem suas características próprias, ou *condições facilitadoras*, responsáveis na promoção do processo de securitização.

A setorização postula que diferentes objetos referentes podem ser objetos de segurança, assim como diferentes atores podem produzir um discurso securitizador, dependendo do contexto que estão inseridos (BUZAN; WÆVER; DE WILDE, 1998). Chamamos atenção para o fato de que os setores, em uma perspectiva mais ampla, também podem se sobrepor (BUZAN; WÆVER; DE WILDE, 1998, p. 167).

Um importante elemento na compreensão da Securitização, além dos setores, como argumentam, é o papel do discurso-ação, o *speech-act*, pois através dele e de uma audiência que absorve aquilo que é discursado, ocorre a construção de uma questão como existencialmente ameaçada (BUZAN; WÆVER; DE WILDE, 1998).

Mesmo alguns pensadores das Relações Internacionais observando a existência certos problemas e *gaps* teóricos neste novo *framework* de análise, a teoria da Securitização se popularizou na academia, até mesmo fora da Europa, dentre aqueles buscando compreender questões de segurança com elementos diferentes daqueles tradicionais (BALZACQ; LÉONARD; RUZICKA, 2016).

Tendo em vista este caráter Construtivista da Teoria desenvolvida pela Escola de Copenhague, compreendemos que se adequa em uma análise mais ampla do processo de segurança cibernética no Brasil. Elementos tais como o *speech-act*, objetos referenciais e

¹¹ O termo, no original em inglês, *societal* é diferente – e vai além – de uma tradução simples daquilo que é entendido como “social”. O societal postulado pelos autores relaciona-se a também questões psicossociais e, principalmente, de identidade e o contexto qual estão inseridos (BUZAN; WÆVER; DE WILDE, 1998).

ações emergenciais, presentes na Teoria de Securitização, podem ser observados quando analisamos o caso brasileiro enquanto decisões tomadas visando a cibersegurança.

Para a construção de nosso argumento, entretanto, entendemos como fundamental o esclarecimento de alguns conceitos presentes na análise do processo de securitização tal qual elucidado pela Escola de Copenhague em sua obra, bem como as ressalvas e questões problemáticas observadas pelos principais críticos da Securitização.

Nosso objetivo não é esgotar o debate a respeito da Securitização, dado ao seu caráter amplo e a nossa falta de espaço nesta investigação, mas sim apresentar os elementos gerais do Construtivismo e da Securitização enquanto quadros de análise de um caso específico: a cibersegurança no Brasil¹².

¹² Para mais informações a respeito do Construtivismo e sua relação com a Securitização ver: BUZAN; HANSEN, 2012 e BUZAN; WÆVER; DE WILDE, 1998.

2.1 A ampliação e o aprofundamento do conceito de segurança

A escola de pensamento que ficou conhecida como Escola de Copenhague surgiu na Europa durante o fim dos anos 1980 e início dos anos 1990, a partir do Instituto de Pesquisa de Paz de Copenhague (COPRI, em sua sigla em inglês), com o estímulo aos Estudos sobre a Paz – paralelamente aos Estudos Estratégicos que ocorriam, na mesma época, nos Estados Unidos (BUZAN; HANSEN, 2012).

A figura do professor inglês Barry Buzan é recorrente ao tratar da Escola de Copenhague, pois buscou desenvolver um pensamento Construtivista de segurança ainda em 1983 com a publicação do livro *People, States and Fear: The National Security Problem in International Relations*¹³ (1983), qual argumentou que o conceito de segurança não havia sido totalmente desenvolvido quando considerado certos desafios da segurança nacional (BUZAN, 1983). A principal abordagem desta obra, que foi revisitada em 1991, foi a crítica a uma visão demasiadamente limitada a respeito da segurança, focada especialmente em uma perspectiva militar (BUZAN, 1983, p. 13).

Os professores Jaap de Wilde e Ole Wæver também se tornaram figuras proeminentes na Escola de Copenhague ao colaborar com Barry Buzan na tentativa da ampliação e do aprofundamento do conceito de Segurança. Em especial, Wæver e Buzan trabalharam juntos no desenvolvimento do papel da *identidade* enquanto elemento de segurança, levando em consideração o processo migratório que vinha ocorrendo na Europa nos anos 1990 (WÆVER et al., 1991).

Para além de questões envolvendo a identidade, os pensadores de Copenhague também se dedicaram a importância da regionalização nas Relações Internacionais (WÆVER et al., 1991; BUZAN; WÆVER, 2003). Podemos argumentar que isto ocorreu, principalmente, dado o desenvolvimento da União Europeia na década de 1990.

Seu pensamento passou a crescer no contexto europeu, como afirmou Huysmans (1998): “[...] a Escola de Copenhague também começou a trabalhar conceitos e *insights* inovadores, como a ‘securitização’, a ‘segurança societal’ e o ‘complexo regional de

¹³ Traduzido livremente pela autora como: O Povo, o Estado e o Medo: O Problema da Segurança Nacional nas Relações Internacionais.

segurança’, com o objetivo de compreender uma problemática de segurança europeia latente” (HUYSMANS, 1998, p. 480, tradução nossa¹⁴).

A ampliação da agenda de segurança que se formava na Europa à época, principalmente com os esforços da Escola de Copenhague, relaciona-se, como apontou Huysmans (1998, p. 483), aos trabalhos individuais de cada professor a respeito das perspectivas das Relações Internacionais e que foram debatidos coletivamente. Ou seja, “[...] uma abordagem mais ou menos orientada ao neorrealismo de Buzan encontrou a perspectiva social e construtivista de Wæver [...]” (HUYSMANS, 1998, p. 483, tradução nossa¹⁵). O desenvolvimento de uma teoria “híbrida” pela Escola de Copenhague já remonta tais debates, como já foi apresentado.

Com o fim da Guerra Fria e a perda do referencial de Estado tal como se tinha nos estudos tradicionais de Segurança, reforçou-se o pensamento de Copenhague ao considerar novos elementos como matéria de Segurança. A realidade dialogava com a nova ordem estabelecida com o fim da Guerra Fria: conflitos *intraestatais*, que aconteceram na década de 1990, tais como o genocídio em Ruanda e a Guerra da Iugoslávia, foram consequência da perda do Estado como referência.

Em março de 1997, Barry Buzan publicou um artigo intitulado *Rethinking Security after de the Cold War*¹⁶ na Revista *Cooperation and Conflict*, qual apresentou, ainda que de forma incipiente, a ideia de um processo *securitizatório* e a compreensão de diferentes objetos referentes (além do Estado) no estudo da Segurança Internacional (BUZAN, 1997, p. 11). Neste trabalho de 1997, Buzan buscou contra argumentar a crítica tradicionalista de que uma ampliação do conceito de segurança necessariamente o torna incoerente, propondo um método Construtivista de sua abordagem (BUZAN, 1997).

Ainda em *Rethinking Security after de the Cold War*, o autor apresentou alguns limites do conceito tradicional de segurança, quando considerou, por exemplo, questões econômicas – até ambientais – que podem suscitar no engajamento em conflitos armados (BUZAN, 1997, p. 09).

¹⁴ No original: “[...] the Copenhagen School has also set to work innovative concepts and insights such as ‘securitization’, ‘societal security’ and ‘regional security complex’ with the aim of grasping a European security problematic in flux” (HUYSMANS, 1998, p. 480).

¹⁵ No original: “[...] Buzan’s more or less neorealistic oriented approach encounters Wæver’s social constructivist perspective [...]” (HUYSMANS, 1998, p. 483).

¹⁶ Traduzido livremente pela autora como: Repensando a Segurança após a Guerra Fria.

Ademais, ainda sugeriu que fosse considerado o papel do *discurso* na construção daquilo que pode ser percebido como uma ameaça, além de diferentes setores para além do militar na análise de Segurança Internacional (BUZAN, 1997). Buzan (1997) concluiu:

Em um mundo pós-Guerra Fria, portanto, pode ser argumentado que uma agenda de segurança abrangente é uma resposta necessária ao sucesso global do projeto liberal [...] De uma maneira central, o projeto liberal parece ter tido sucesso na marginalização da segurança militar, e junto dela, a abordagem Tradicional de Estudos de Segurança. Mas, ao fazer isso, levantou novos problemas de segurança que apenas podem ser lidados em um quadro de análise que seja multissetorial (BUZAN, 1997, p. 25, tradução nossa¹⁷).

Entendemos que este *paper* publicado na revista *Cooperation and Conflict* foi relevante para a formulação do pensamento da Escola de Copenhague na medida em que apresentou diversos elementos que seriam trabalhados mais extensivamente posteriormente por Buzan, Wæver e de Wilde.

Em 1998, portanto, o livro *Security: A New Framework for Analysis*¹⁸, foi marco definitivo da EC publicado pelos três autores: Buzan, Wæver e de Wilde. Nele, propõem um quadro analítico mais amplo para o estudo da Segurança Internacional, considerando as transformações das relações internacionais e das relações sociais pós-Guerra Fria: a Securitização (BUZAN; WÆVER; DE WILDE, 1998).

Na tentativa de contemplar tanto elementos tradicionais presentes nos Estudos de Segurança Internacional (território, poder, Estado e exército) quanto de uma abordagem crítica (sociedade, identidade, Meio Ambiente, etc.), a Securitização foi elaborada como uma alternativa àquela compreensão da segurança típica, sendo entendida como uma teoria *híbrida* (VILLA; REIS, 2006).

Finalmente, podemos afirmar, baseado em Matt McDonald (2008), que “o trabalho Escola de Copenhague constituiu na maior tentativa combinada a desenvolver uma teoria ou quadro de análise para o estudo da segurança em uma tradição Construtivista”

¹⁷ No original: “In the post-Cold War world, therefore, it can be argued that a wider security agenda is a necessary response to the global success of the liberal project [...] In some central ways, the liberal project does seem to have succeed in marginalizing military security, and, along with it, the approach of Traditional Security Studies. But in so doing it has raised new security problems that can only handled in a multi-sectorial framework” (BUZAN, 1997, p. 25).

¹⁸ Traduzido livremente pela autora como: Segurança: Um Novo Quadro Para Análise.

(MCDONALD, 2008, p. 68, tradução nossa¹⁹). Isto conferiu relevância para esta Escola de pensamento a partir da década de 1990.

Acreditando que a inclusão do ciberespaço enquanto pauta de segurança no Brasil a partir dos primeiros anos do século XXI constitui-se em um processo de securitização, tendo em vista, principalmente, a ampliação e o aprofundamento do conceito de segurança que também ocorreu em âmbito brasileiro, buscamos, portanto, traçar um paralelo entre esta teoria e a realidade.

¹⁹ No original: “[...] the work of the so-called Copenhagen School constitutes the most concerted attempt to develop a theory or framework for the study of security in the constructivist tradition” (MCDONALD, 2008, p. 68).

2.2 Securitização e o *speech-act*

Para o desenvolvimento da teoria de Securitização, os autores partiram da seguinte definição de Segurança Internacional: “Segurança é o movimento que leva a política para além das regras do jogo estabelecidas e enquadra uma questão ou como um tipo especial de política ou como algo acima dela” (BUZAN; WÆVER; DE WILDE, 1998, p. 23, tradução nossa²⁰).

Os autores afirmaram que:

Na teoria, qualquer questão pública pode ser localizada no espectro que vai de não-politizado (o que significa que o Estado não lida com isso de nenhuma forma e isso não é uma questão de debate público ou tomada de decisão) passando por politizado (o que significa que a questão faz parte de políticas públicas e requer decisões governamentais [...]) até securitizado (o que significa que a questão é apresentada como existencialmente ameaçada, requerendo ações emergenciais e justificando ações além dos limites normais dos processos políticos (BUZAN; WÆVER; DE WILDE, 1998, p. 23-24, tradução nossa²¹).

Dessa forma, o ponto de partida para compreender o processo de securitização e se uma questão está sendo, efetivamente, securitizada, é observar se o procedimento segue um *critério específico*, que leva a questão ao extremo do espectro, saindo das esferas normais de tratamento político (BUZAN; WÆVER; DE WILDE, 1998, p. 05, grifo nosso).

²⁰ No original: “‘Security’ is the move that takes politics beyond the established rules of the game and frames the issue either as special kind of politics or as above politics” (BUZAN; WÆVER; DE WILDE, 1998, p. 23).

²¹ No original “In theory, any public issue can be located on the spectrum ranging from nonpoliticized (meaning the state does not deal with it and it is not in any other way made an issue of public debate and decision) through politicized (meaning the issue is part of public policy, requiring government decision and resource allocations or, more rarely, some other form of communal governance) to securitized (meaning the issue is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure)” (BUZAN; WÆVER; DE WILDE, 1998, p. 23-24).

Tabela 02: Espectro de localização de questões de segurança internacional

Não politizado	Politizado	Securitizado
O Estado não lida de nenhuma forma com a questão e não a considera como matéria de decisão ou debate.	A questão é parte das políticas públicas, requerendo decisão governamental e remanejamento de recursos, ou, mais raramente, alguma outra forma de governança comum.	A questão é apresentada como existencialmente ameaçada, requerendo ações emergenciais e justificando ações além dos limites normais dos procedimentos políticos.

Fonte: Elaborado pela autora com base em BUZAN; WÆVER; DE WILDE, 1998, p. 23-24.

A *securitização*, como os autores argumentam, está presente em um espectro amplo do processo de segurança. Então, uma matéria pode variar entre não politizada, politizada à securitizada, esta última quando está presente no extremo do espectro (BUZAN; WÆVER; DE WILDE, 1998). Portanto, quando uma questão é “apresentada como *existencialmente ameaçada*, requerendo medidas emergenciais que justificam medidas fora dos limites normais do processo político” (BUZAN; WÆVER; DE WILDE, 1998, p. 24, tradução nossa²², grifo nosso), ela está sendo securitizada por um agente.

Partindo de experiências empíricas europeias, a Escola de Copenhague sugeriu que uma questão só se torna um elemento de segurança quando *apresentada* dessa forma. Sustentaram: “No caso da segurança [...] algo é designado como uma questão de segurança internacional porque pode ser argumentado que este problema é mais importante que os outros problemas e deve ser tomado como prioridade absoluta” (BUZAN; WÆVER; DE WILDE, 1998, p. 24, tradução nossa²³).

Levando em consideração esta afirmação em particular, podemos perceber o caráter Construtivista da abordagem da Escola de Copenhague, uma vez que a importância do processo de segurança está relacionada à uma construção social de ameaça, ou seja, a *forma*

²² No original: “[...] meaning the issue is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure” (BUZAN; WÆVER; DE WILDE, 1998, p. 24).

²³ No original: “In the case of security [...] something is designated as an international security issue because it can be argued that this issue is more important than other issues and should take absolute priority” (BUZAN; WÆVER; DE WILDE, 1998, p. 24).

pela qual uma questão é apresentada a uma audiência. E, no caso da securitização, por conta do caráter emergencial e de prioridade, a questão é apresentada como existencialmente ameaçada.

Dessa forma, o papel do discurso é relevante enquanto plataforma de promoção do processo de securitização. Este elemento discursivo foi denominado *speech-act* pelos autores na elaboração da Teoria da Securitização (BUZAN; WÆVER; DE WILDE, 1998, p. 26).

Apesar de alguns autores brasileiros que trabalham com a Securitização e a Escola de Copenhague traduzirem o elemento *speech-act* apenas como “discurso” ou “ato-fala”, temos dificuldades em aceitar tais traduções. Isto, pois, trata-se de um discurso que tem um *caráter* de ação (geralmente emergencial), como sugerido no próprio termo. Dessa forma, a partir de então, iremos utilizá-lo em seu idioma original, como *speech-act*.

O *speech-act* é um recurso da teoria da linguagem, ao qual os autores recorrem para demonstrar o processo de securitização. Dessa forma, podemos inferir que “[...] é o próprio enunciado que caracteriza o ato. Ao dizer as palavras, algo está feito [...]” (BUZAN; WÆVER; DE WILDE, 1998, p. 26, tradução nossa²⁴).

Ao tratar do *speech-act*, devemos apresentar o primeiro elemento do processo de securitização: os atores securitizadores. De acordo com os autores, são estes atores que vão declarar uma questão como existencialmente ameaçada (BUZAN; WÆVER; DE WILDE, 1998, p. 36). Entretanto, para que o processo de securitização ocorra, o *speech-act* deve ser voltado à uma *audiência*, a qual legitima as declarações e medidas emergenciais que podem ser tomadas (BUZAN; WÆVER; DE WILDE, 1998, p. 41).

Apesar de não buscarem elucidar mais a respeito do *speech-act* e sua relação com a audiência, os autores definem a securitização como um processo “*intersubjetivo e socialmente construído*” (BUZAN; WÆVER; DE WILDE, 1998, p. 31, tradução nossa²⁵, grifo nosso).

O processo é intersubjetivo, pois os autores entendem que não pode ser compreendido objetivamente na medida em que cada nação tem diferentes limites para delimitar uma ameaça (BUZAN; WÆVER; DE WILDE, 1998, p. 30). Assim como também não pode ser

²⁴ No original: “[...] it is the utterance itself that is the act. By saying the words, something is done [...]” (BUZAN; WÆVER; DE WILDE, 1998, p. 26).

²⁵ No original: “Securitization is intersubjective and socially constructed [...]” (BUZAN; WÆVER; DE WILDE, 1998, p. 31).

apenas subjetivo, pois “Se uma questão é matéria de segurança ou não, isso não é algo que indivíduos decidem sozinhos” (BUZAN; WÆVER; DE WILDE, 1998, p. 31, tradução nossa²⁶). Sendo assim, é intersubjetivo e socialmente construído.

Ademais, podemos inferir que o processo de securitização é socialmente construído através do *speech-act* e da sua posterior legitimação, o que coloca os atores securitizadores, muitas vezes, no centro deste processo.

Assim sendo, como argumentou Tanno (2003), a Escola de Copenhague passou a defender que:

[...] questões de segurança são construídas pelas práticas sociais. Processos de construção de questões de segurança ocorrem, primordialmente, por meio de discursos proferidos pelos atores mais interessados em estabelecer as agendas de segurança. Questões políticas podem, portanto, sofrer processos/movimentos de “securitização” ou “dessecuritização” (TANNO, 2003, p. 57).

Ressaltamos ainda, tendo em vista este trecho desenvolvido por Tanno (2003), que no desenvolvimento da Teoria da Securitização os autores esclareceram que o processo de securitização não é o ideal, mas sim a “dessecuritização”. Isto, pois questões de segurança devem ser debatidas e resolvidas dentro das práticas políticas democráticas comuns, como entendem (BUZAN; WÆVER; DE WILDE, 1998, p. 29).

Dessa forma, hiperbolizar uma causa e dar a ela o tratamento de segurança, como se tivesse sua existência ameaçada pode configurar um processo de securitização, de acordo com o *framework* estabelecido pela Escola de Copenhague.

Um dos exemplos possíveis de securitização que os autores apresentaram no livro *Security: A New Framework for Analysis* – e que dialoga inclusive com uma realidade internacional atual – diz respeito à imigração. Estados ou grupos que se organizam com o discurso de que imigrantes estão ameaçando a “verdadeira identidade”, a economia ou a segurança daquele país ou grupo, e chegam a tomar medidas visando dificultar a migração, podem estar configurando um processo de securitização (BUZAN; WÆVER; DE WILDE, 1998).

Uma maneira de se introduzir o conceito de securitização foi elaborada por Balzacq, Léonard e Ruzicka (2016): “Construído sob a literatura do *speech-act*, a Teoria de

²⁶ No original: “Whether an issue is a security issue is not something individuals decide alone” (BUZAN; WÆVER; DE WILDE, 1998, p. 31).

Securitização é baseada na premissa de que a palavra ‘segurança’ tem um caráter performativo – isto é, não apenas descreve o mundo, mas pode também transformá-lo” (BALZACQ; LÉONARD; RUZICKA, 2016, p. 495, tradução nossa²⁷).

Consideradas as generalidades que envolvem o processo de securitização e os critérios para classificá-lo como tal, bem como o papel do discurso e da linguagem, passemos às considerações a respeito dos elementos mais específicos da Teoria de Securitização, conforme desenvolvidos pela Escola de Copenhague.

²⁷ No original: “Building on the speech act literature, securitization theory is based on the premise that word security has a performative character – that is, does not only describe the world but can also transform it” (BALZACQ; LÉONARD; RUZICKA, 2016, p. 495).

2.3 Elementos do processo de securitização

Como já brevemente apresentado, um dos diferenciais da Securitização é o aprofundamento do conceito de segurança para além de uma análise tradicional, não tendo mais o Estado como principal entidade de segurança.

A proposta da Escola de Copenhague foi apresentar *níveis de análise* que, apesar de ser apenas um *framework*, não deveria priorizar o Estado. Dessa forma, não existiria uma hierarquia entre os níveis na qual o Estado estivesse no topo. O objetivo era, justamente, não reforçar o estadocentrismo.

Segundo os autores, os níveis de análises são: *sistemas internacionais, subsistemas internacionais, unidades, subunidades e indivíduos* (BUZAN; WÆVER; DE WILDE, 1998, p. 05-06, grifo nosso). Cada nível compreende seus próprios agentes presentes nas relações internacionais.

Quando analisado um caso específico de Segurança, identificar o nível que o processo ocorre é fundamental para uma compreensão completa. Dessa forma, a securitização pode ocorrer em qualquer um destes níveis.

Tabela 03: Os níveis de análise na Securitização

Nível	Descrição
Sistema Internacional	O maior conglomerado internacional possível. Este nível compreende todo o planeta.
Subsistema Internacional	Grupos de unidades que podem ser separados de todo o Sistema Internacional. Exemplo: grupos regionais (ANSA, OAU ²⁸) ou as próprias organizações internacionais (OPEP), entre outros.
Unidade	Atores compostos de vários subgrupos tais como organizações e comunidades. Exemplo: Estados, nações, firmas transnacionais.
Subunidade	Grupos organizados de indivíduos que funcionam dentro das Unidades que podem (ou tentam) afetar o comportamento de Unidade. Exemplo: burocracia, <i>lobby</i> .
Individual	A última linha em muitas análises das Ciências Sociais. Os indivíduos.

Fonte: Elaborado pela autora com base em BUZAN; WÆVER; DE WILDE, 1998, p. 05-06, tradução nossa²⁹.

Ressaltamos que a divisão por níveis é uma ferramenta metodológica para o analista de Relações Internacionais compreender o caso em questão.

Uma outra proposta da Escola de Copenhague com a Securitização foi que a Segurança nas Relações Internacionais pudesse ser analisada a partir do *setor* qual ocorre, sendo ele militar, político, econômico, societal ou ambiental.

Definiram os setores como “visões de um sistema internacional através de uma lente que destaca um aspecto particular do relacionamento e interação entre todas as unidades que

²⁸ Optamos por manter os exemplos originais dos autores: Associação de Nações do Sudeste Asiático (ANSA) e Organização da Unidade Africana (OUA).

²⁹ No original “1. International systems, meaning the largest conglomerates of interacting or interdependent [...] this level encompasses the entire planet [...]; 2. International subsystems, meaning groups of units within the international system that can be distinguished from the entire system [...]; 3. Units, meaning actors composed of various subgroups, organizations, communities, and many individuals [...]; 4. Subunits, meaning organized groups of individuals within units that are able (or that try) to affect the behavior of the unit (e.g. bureaucracies, lobbies); 5. Individuals, the bottom line of most analysis in the social sciences” (BUZAN; WÆVER; DE WILDE, 1998, p. 05-06).

o constitui” (BUZAN; JONES; LITTLE, 1993, p. 31 *apud*³⁰ BUZAN; WÆVER; DE WILDE, 1998, p. 27, tradução nossa³¹). Os setores promovem, em última instância, uma “ferramenta analítica” do processo de segurança nas Relações Internacionais (BUZAN; WÆVER; DE WILDE, 1998, p. 27).

Isto, pois, argumentam que “Segurança significa sobrevivência em face de ameaças existenciais, mas aquilo que constitui uma ameaça existencial não é sempre o mesmo em diferentes setores” (BUZAN; WÆVER; DE WILDE, 1998, p. 27, tradução nossa³²). Dessa forma, cada setor tem seu próprio *contexto* e suas próprias *condições* que influenciam no discurso de securitização.

À vista disso, partir do princípio de que questões de segurança podem ocorrer em diferentes setores contribui para a ampliação e aprofundamento do conceito de segurança na medida em que não se limita mais ao âmbito militar ou político. Questões de segurança podem emergir do setor econômico, por exemplo.

Assim como os níveis de análise, a setorização é uma das ferramentas presentes no quadro de análise a se configurar quando estudado um caso de Segurança nas Relações Internacionais. Ressaltamos que um processo de securitização pode perpassar mais de um setor, quando analisada a *bigger picture*.

Além dos setores e as diferentes dinâmicas que o compõe, os autores entenderam que também existem diferentes unidades envolvidas na análise de segurança nas Relações Internacionais. O já mencionado ator securitizador é uma destas unidades, mas existem duas outras também presentes no processo de securitização de acordo com os autores da Escola de Copenhague, a saber: os objetos referentes e os atores funcionais.

³⁰ BUZAN, Barry; JONES, Charles; LITTLE, Richard. **The Logic of Anarchy: Neorealism to Structural Realism**. Nova Iorque: Columbia University Press, 1993.

³¹ No original: “Sectors are ‘views of the international system through a lens that highlights one particular aspect of the relationship and interaction among all of its constituent units’ (Buzan, Jones, and Little, 1993: 31)” (BUZAN; WÆVER; DE WILDE, 1998, p. 27).

³² No original: “Security means survival in the face of existential threats, but what constitutes an existential threat is not the same across different sectors” (BUZAN; WÆVER; DE WILDE, 1998, p. 27).

Tabela 04: Unidades envolvidas na análise de segurança segundo a Escola de Copenhague

Tipos de unidades envolvidas na análise de segurança	Descrição
Objetos referentes	Coisas que são vistas como existencialmente ameaçadas e têm uma reivindicação legítima de sobrevivência.
Atores securitizadores	Atores que securitizam questões ao declararem algo – o objeto referencial – como existencialmente ameaçado.
Atores funcionais	Atores que afetam a dinâmica de um setor. Sem ser o objeto referente ou o ator clamando por segurança em nome do objeto referente, este é um ator que influencia significativamente nas decisões no campo da segurança.

Fonte: Elaborado pela autora, com base em Buzan, Wæver e de Wilde, 1998, p. 36, tradução nossa³³.

Na análise do processo de securitização, especialmente durante o *speech-act*, estas unidades podem ser observadas. A título de esclarecimento, ao que se refere aos *atores funcionais*, estes aparecem presentes com sua influência, dependendo do setor qual a análise de segurança está sendo feita. Os autores exemplificam: “Uma corporação poluente, por exemplo, pode ser um ator central no setor ambiental – não é o objeto referencial e não está tentando securitizar questões ambientais (muito pelo contrário)” (BUZAN; WÆVER; DE WILDE, 1998, p. 36, tradução nossa³⁴).

Aprofundar a agenda de segurança e compreender que diferentes setores podem estar presentes na análise abre espaço para uma interpretação igualmente aprofundada e ampla

³³ No original: “1. Referent objects: things that are seen to be existentially threatened and have a legitimate claim to survival. 2. Securitizing actors: actors who securitize issues by declaring something – a referent object – existentially threatened. 3. Functional actors: actors who affect the dynamics of a sector. Without being the referent object, this is an actor who significantly influences decisions in the field of security” (BUZAN; WÆVER; DE WILDE, 1998, p. 36).

³⁴ No original: “A polluting company, for example, can be a central actor in the environmental sector – it is not a referent object and is not trying to securitize environmental issues (quite the contrary)” (BUZAN; WÆVER; DE WILDE, 1998, p. 36).

daquilo que pode ser caracterizado como questão de segurança, como, por exemplo a tecnologia e o ciberespaço.

Em princípio, qualquer ator securitizador pode designar uma questão como uma ameaça existencial (BUZAN; WÆVER; DE WILDE, 1998). São as condições facilitadoras, ou seja, o *contexto*, responsável por determinar o sucesso do processo de securitização (BUZAN; WÆVER; DE WILDE, 1998, p. 36). Entendemos as condições facilitadoras como o quarto elemento presente na análise do processo de securitização.

Retomando a proposta de setorização desenvolvida pela Escola de Copenhague, cabe esclarecer que cada setor possui seus próprios objetos referentes, atores securitizadores e atores funcionais, bem como suas próprias condições facilitadoras. Entretanto, isso não significa que um setor é totalmente isolado de outro: existem questões que perpassam mais de um setor. É função do analista de Relações Internacionais compreender quando isso ocorre para obter todas as informações do processo de securitização.

O setor militar geralmente envolve dinâmicas do Estado, entidades políticas e o próprio Exército e, dependendo do caso, pode funcionar como objeto referente ou ator securitizador (BUZAN; WÆVER; DE WILDE, 1998, p. 22). Ao que se refere ao setor político, este se relaciona com a soberania ou ideologia de um Estado que pode ser configurada como existencialmente ameaçada.

O setor econômico pode compreender firmas como existencialmente ameaçadas pela falência, por exemplo, mas a economia nacional, por mais ampla que seja, também pode ser apresentada como um objeto referente.

O setor societal, por sua vez, está relacionado a questões de identidades coletivas, entendidas pelos autores como nações e religiões, por exemplo. Questões étnicas que envolvem a segurança também podem ser analisadas através do setor societal.

Por fim, o setor ambiental na teoria da Escola de Copenhague relaciona-se a questões de sobrevivência de espécies ou tipos de habitat, assim como questões mais abstratas como o clima (BUZAN; WÆVER; DE WILDE, 1998, p. 23).

Portanto, compreendemos os principais elementos do processo de securitização como sendo: objetos referentes, atores securitizadores, atores funcionais e condições facilitadoras. O *speech-act*, por sua vez, está presente na dinâmica entre estes elementos.

Ademais, tem-se os níveis e os setores como ferramentas analíticas a serem consideradas na compreensão do processo de securitização.

Efetivamente, os autores afirmaram que uma securitização de sucesso deve apresentar “três elementos (ou passos): [postular a] ameaça existencial; [tomar a] ação emergencial; e [observar os] efeitos na relação entre as unidades após se libertarem das regras” (BUZAN; WÆVER; DE WILDE, 1998, p. 26, tradução nossa³⁵).

Estes passos para o processo de securitização ter sucesso vão ao encontro daqueles critérios estabelecidos pela Escola de Copenhague de levar a questão para além dos limites comuns da politização. Como afirmaram os autores:

Assim, a *definição* exata e os *critérios* de securitização são constituídos pelo estabelecimento intersubjetivo de uma ameaça existencial com um destaque suficiente para ter efeitos políticos substanciais. A securização pode ser estudada diretamente; não precisa de indicadores. O modo de estudar a securitização é estudar o discurso e as constelações políticas [...] (BUZAN; WÆVER; DE WILDE, 1998, p. 25, tradução nossa³⁶, grifo dos autores).

O analista de Segurança Internacional, em vista disso, deve compreender as unidades presentes no processo de declarar algo como matéria de segurança, observar o *speech-act* e determinar se os três passos supramencionados ocorreram no contexto analisado.

Na investigação que aqui propomos a respeito da cibersegurança no Brasil, recorreremos aos critérios estabelecidos pela EC e também aos três passos para a securitização ter sucesso: ameaça existencial, ação emergencial e relação entre as unidades. Assim sendo, será comum nos capítulos seguintes que resgatemos estes termos na construção de nossa argumentação.

Finalmente, a Escola de Copenhague buscou, com a formulação deste aporte teórico, contribuir com os debates pós-Guerra Fria de Segurança Internacional, reconhecendo os limites de uma abordagem realista e oferecendo uma alternativa que abrangesse a agenda de segurança que vinha se formando. Reconhecemos a importância deste suporte teórico

³⁵ No original: “A successful securitization thus has three components (or steps): existential threats, emergency action, and effects on interunit relations by breaking free of rules” (BUZAN; WÆVER; DE WILDE, 1998, p. 26).

³⁶ No original: “Thus, the exact *definition* and *criteria* of securization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects. Securitization can be studied directly; it does not need indicators. The way to study securitization is to study discourse and political constellations” (BUZAN; WÆVER; DE WILDE, 1998, p. 25, grifo dos autores).

Construtivista como relevante na área das Relações Internacionais e do Estudo da Segurança Internacional.

Oferecer um quadro de análise tão amplo fez com que outros estudiosos da área de Segurança Internacional fizessem apontamentos a respeito da Teoria, que não podemos deixar de considerar na presente investigação. O próximo tópico se debruça sobre tais ressalvas.

Ressalta-se que os apontamentos aqui apresentados não desmerecem o trabalho da Escola de Copenhague, mas demonstra a visão que os críticos da academia tiveram a respeito do desenvolvimento da teoria.

Dessa forma, estas considerações apresentadas no tópico subsequente têm como objetivo demonstrar que reconhecemos as limitações de alguns dos elementos presentes na Teoria de Securitização, mas elas não interferem, de uma maneira geral, em nossa análise final.

Por fim, entendemos que seja importante para o leitor levar em consideração tais ressalvas que apresentamos para que tenha um panorama completo (ainda que breve) da Teoria da Securitização.

2.4 Os limites da Teoria de Securitização segundo seus principais críticos

A ampliação da agenda de segurança internacional foi um processo que passou a ocorrer quando a Guerra Fria chegava ao seu fim, com o surgimento de novos elementos relevantes no debate das Relações Internacionais. O desenvolvimento da Securitização enquanto teoria aconteceu com a intenção de ir ao encontro desta nova tendência ampliadora. Entretanto, criar uma teoria tão abrangente pode ser metodologicamente desafiador quando considerada a tentativa de contemplar muitos elementos, novos e tradicionais, simultaneamente em um mesmo *framework* de análise.

Por este motivo, autores diversos revisaram os trabalhos publicados pela Escola de Copenhague ao que concerne a Securitização, buscando fazer apontamentos, na tentativa de contribuir com a teoria. Entendemos que as considerações feitas por estes autores, tanto europeus quanto não europeus, a respeito da Teoria de Securitização, têm relevância metodológica quando aplicado o *framework* da Securitização em certas questões de Segurança Internacional.

A seleção dos principais trabalhos que revisaram a Teoria de Securitização seguiu os seguintes critérios: artigos publicados na mesma época que saiu o livro *Security a New Framework for Analysis* e que serviram como uma revisão do trabalho da EC no mesmo contexto temporal (SKIDMORE, 1998; HUYSMANS, 1998); um artigo publicado pelo menos dez anos depois da publicação original e que obteve alcance nos Estudos de Segurança Internacional (MCDONALD, 2008a); um artigo publicado por Lene Hansen, uma das principais críticas da Teoria de Securitização e que também é considerada parte da Escola de Copenhague (HANSEN, 2000; HANSEN; NISSENBAUM, 2009); e um artigo mais recente que trouxe elementos de cibersegurança na crítica feita a respeito da Securitização (BALZAQ; LÉONARD, RUZICKA, 2016).

Todos os autores que aqui citamos como os principais estudiosos que teceram considerações a respeito da Securitização têm seus trabalhos reconhecidos por outros pesquisadores da área. São considerados como sendo os principais críticos da Escola de Copenhague até o momento.

No caso brasileiro, já citamos Grace Tanno como sendo uma das principais pesquisadoras da Escola de Copenhague e sua relação com a Segurança Internacional (TANNO, 2003). Contudo, não abordaremos o artigo de Tanno, pois suas considerações são as mesmas dos principais autores que aqui utilizamos.

Optamos por não apresentar as considerações de cada autor separadamente. Ao invés disso, buscamos sintetizar as críticas em três eixos principais, conforme foram recorrentes nos trabalhos levantados. São eles: *a) A linguagem e o *speech-act*; b) A contextualização; e c) A teoria, a prática e a experiência europeia.*

2.4.1 A linguagem e o *speech-act*

A linguagem, ponto fundamental na argumentação da intersubjetividade da Escola de Copenhague, foi um ponto criticado pelo professor de Ciência Política David Skidmore após o lançamento do livro *Security: A New Framework for Analysis*. A linguagem e o discurso, segundo o autor, têm grande prioridade no desenvolvimento da teoria, superando, inclusive a *ação* e as *bases materiais* (SKIDMORE, 1998, grifo nosso). Ou seja, há um questionamento por parte do autor se a linguagem e o discurso dos atores (políticos) deveriam se sobrepor sobre suas ações, por exemplo.

A respeito da crítica específica de Skidmore, entendemos que houve pouco desenvolvimento da EC a respeito do *speech-act*. Conforme interpretamos, o *speech-act* é, ao mesmo tempo discurso e ação. O próprio *speech-act* se sustentaria como a ação dos atores políticos.

Já Jef Huysmans, a respeito do uso da linguagem, ou do *speech-act*, entendeu que elementos interpretativos devem ser levados em consideração na análise do discurso, isto, pois, Huysmans compreendeu que as experiências *históricas* e *culturais* influenciam na lógica de segurança em diferentes casos (HUYSMANS, 1998, grifo nosso). Dessa forma, afirmou que: “Uma interpretação histórico-cultural da estrutura retórica [o *speech-act*] reduziria a tendência de *universalizar* uma lógica de segurança específica” (HUYSMANS, 1998, p. 501, tradução nossa³⁷, grifo nosso).

O professor da Universidade de Queensland, Austrália, Matt McDonald também fez uma crítica do livro *Security: A New Framework for Analysis*, mas dez anos após sua publicação, visando debater sua relevância nas Relações Internacionais.

O autor entendeu que a Teoria tem algumas limitações, e entre elas, destacamos especificamente em sua *forma* no sentido de considerar apenas *atores dominantes* (potencialmente líderes políticos) como atores securitizantes, excluindo ou marginalizando

³⁷ No original: “A cultural-historical interpretation of the rhetorical structure would reduce a tendency to universalize a specific logic of security” (HUYSMANS, 1998, p. 501).

outros discursos de segurança que provêm de outras áreas minoritárias ou proferido por minorias (MCDONALD, 2008a, p. 569, grifo nosso).

O discurso de mulheres, por exemplo, se torna marginalizado, por não se tratarem de atores dominantes na esfera de segurança e, ao fazer esta afirmação, McDonald corrobora esta ideia que foi inicialmente desenvolvida por Lene Hansen em uma crítica anterior (HANSEN, 2000; HANSEN; NISSENBAUM, 2009; MCDONALD, 2008a, p. 574).

O trabalho da professora da Universidade de Copenhague Lene Hansen ainda gerou uma crítica extensa a respeito do gênero e outros grupos marginalizados no discurso de segurança. A autora argumentou que a Escola de Copenhague não considerou o gênero e o próprio papel do silêncio como elementos presentes na construção da segurança e, por isso, existe dificuldade em postular sua agenda de segurança como verdadeiramente profunda e ampla (HANSEN, 2000).

Ademais, a presença de atores dominantes e elites como agentes securitizadores levanta o seguinte questionamento: de que forma outros discursos são marginalizados ou silenciados por estes atores dominantes/elites? McDonald apontou que esta questão é importante e não se obtém a resposta na teoria desenvolvida por Copenhague (MCDONALD, 2008a, p. 574).

McDonald ressaltou, ainda, que a ideia da presença de atores dominantes, especialmente da esfera política, na securitização “reforça certos padrões tradicionalistas” do Estudo de Segurança Internacional (MCDONALD, 2008a, p. 575). Por exemplo, podemos considerar o papel do Estado que, desde os estudos mais tradicionais, fora considerado como elemento central do discurso de segurança. Na medida em que o discurso é feito pela camada dominante, muitas vezes será reforçado o papel do Estado como agente de segurança.

Além destas limitações, o autor afirmou que conceitos tais como “audiência”, fundamental no *speech-act*, e “condições facilitadoras” (*facilitating conditions*) não são suficientemente desenvolvidos e integrados à teoria e que poderiam contribuir para o entendimento da Securitização se fossem (MCDONALD, 2008a). Entendemos que estas questões também estão relacionadas às críticas dirigidas, especificamente, à falta de importância dada ao *contexto histórico* pelos autores da Escola de Copenhague em sua obra.

Ainda a respeito da linguagem, McDonald argumentou que a Escola de Copenhague focou mais na questão do *speech-act* do que nas práticas – cotidianas – de segurança, além

do papel das imagens e figuras que são desconsideradas quando se abordam a linguagem e o discurso na construção da Teoria (MCDONALD, 2008a). Imagens, figuras e símbolos, segundo o autor, também deveriam ser levadas em consideração enquanto também são formas de comunicação e elementos de construção de segurança.

Outras questões metodológicas foram levantadas ao considerar figuras e imagens além do discurso, o que exigiria maior dedicação de seus teóricos (MCDONALD, 2008a). Conforme interpretou, o *speech-act* não deveria ser ligado apenas à própria fala, mas à forma pela qual figuras e símbolos presentes na sociedade também podem gerar debates a respeito da segurança.

Os pesquisadores europeus Thierry Balzacq, Sarah Léonard e Jan Ruzicka também comentaram a respeito do discurso em seu artigo publicado em 2016, quando revisitaram a Teoria de Securitização. De acordo com eles, apesar da teoria se sustentar no papel do *speech-act* e da relevância da audiência na construção deste processo intersubjetivo, “[...] a audiência é um dos conceitos menos desenvolvidos na formulação inicial da teoria” (BALZACQ; LÉONARD; RUZICKA, 2016, p. 499, tradução nossa³⁸).

2.4.2 A contextualização histórica

O professor e pesquisador Matt McDonald também encontrou limitações no contexto da obra da Escola de Copenhague. McDonald explicitou que a EC considerou apenas o “momento presente” da securitização, ignorando aspectos contextuais que constituem o processo de securitização, ou seja, quais questões levaram até aquele “momento presente” em que o ato de securitização ocorreu (MCDONALD, 2008a). Este autor buscou reforçar a ideia de que elementos históricos deveriam estar presentes na *interpretação* do processo de securitização, mas que nunca se recorre a tais elementos.

2.4.3 A teoria, a prática e a experiência europeia

Tomar como ponto de partida o contexto de segurança na Europa entre a década de 1980 e 1990 para o desenvolvimento da Teoria de Securitização levantou algumas críticas.

³⁸ No original “Surprisingly, however, the audience is one of the least developed concepts in the initial formulation of the theory” (BALZACQ; LÉONARD; RUZICKA, 2016, p. 499).

Este é um dos principais apontamentos do professor Jef Huysmans, da Universidade de Londres.

A preocupação de Huysmans com o trabalho da Escola de Copenhague diz respeito a uma presença de um europeísmo latente. De acordo com o autor, a Escola desenvolveu seus conceitos em um contexto europeu e toma como exemplos casos que ocorreram na Europa (HUYSMANS, 1998). Isto, por sua vez, levou a uma segunda problemática, mas a respeito da teoria e empirismo. Huysmans entende que teoria e empirismo andam separadamente, ou seja, cria-se a teoria, tem-se uma hipótese e, então, é feito o teste da hipótese naquele contexto (HUYSMANS, 1998).

De acordo com Jef Huysmans, a EC ainda mistura teoria e empirismo, fundamentando sua argumentação e construção teórica sobre casos empíricos – que também são casos europeus (HUYSMANS, 1998). Ele afirma que esta posição epistemológica acaba por definir a centralidade da agenda com esta característica europeia latente (HUYSMANS, 1998).

A presença de casos europeus que constituem a teoria de Securitização não é um problema, segundo o autor, mas que é necessário entender até que ponto a perspectiva pode “constituir um *enviesamento*” (HUYSMANS, 1998, p. 484, grifo nosso).

De acordo com Huysmans (1998): “A relevância política dos estudos não é definida por uma perspectiva americana, e isso muda como questões de segurança são levantadas [...]”. (HUYSMANS, 1998, p. 484, tradução nossa³⁹). Esta afirmação diz respeito a questões que foram latentes na Europa durante o desenvolvimento da teoria, tal como a imigração, que teve papel fundamental no desenvolvimento do setor societal que, por sua vez, “tem papel proeminente na agenda de segurança de Copenhague” (HUYSMANS, 1998, p. 484, tradução nossa⁴⁰).

David Skidmore também argumentou veemente em sua revisão a respeito deste método utilizado pelos autores da Escola de Copenhague na construção de seu argumento teórico. Segundo Skidmore: “O melhor ponto de partida para buscar a inovação teórica é com um enigma convincente e concreto: um problema ou anomalia do mundo real que não pode

³⁹ No original: “The policy relevance of the studies is no defined from an American perspective, and this changes how the security questions are raised [...]” (HUYSMANS, 1998, p. 484).

⁴⁰ No original: “It explains, for example, why societal security questions play such a prominent role in the Copenhagen security agenda” (HUYSMANS, 1998, p. 484).

ser adequadamente resolvido com o emprego das ferramentas teóricas existentes” (SKIDMORE, 1998, p. 1011, tradução nossa⁴¹).

Conforme entendeu, a Escola de Copenhague nunca parte de um desafio como esse, construindo sua argumentação pautada somente na ampliação do escopo de análise de segurança. Dessa forma, Skidmore entendeu a tentativa da EC, mas afirmou que a teoria não era complexa o bastante para dialogar com a realidade.

Em um trabalho mais recente, de 2016, Balzacq, Léonard e Ruzicka já não veem um problema a respeito dos exemplos predominantemente europeus do no desenvolvimento. Argumentam que quase 20 anos após a publicação de seus trabalhos, a Teoria de Securitização foi aplicada por pesquisadores de outros continentes, seguindo os critérios estabelecidos pela EC e tomando como base o contexto local onde o trabalho foi produzido (BALZACQ; LÉONARD; RUZICKA, 2016).

Por fim, consideramos também o uso recente (e crescente) da teoria de Securitização no caso específico da cibersegurança, como já haviam explicitado Balzacq, Léonard e Ruzicka (2016). Os autores entenderam que os estudos empíricos a respeito dos processos securitização cresceram em número e relevância (BALZACQ; LÉONARD; RUZICKA, 2016, p. 507).

Desde as questões de identidade, migração e religião até outras questões que a Escola de Copenhague não poderia ter previsto, como é o caso da informatização e a importância dada ao ciberespaço, que os estudos envolvendo o *framework* da securitização crescessem e isso deve ser levado em consideração em nossa análise.

⁴¹ No original: “The best starting place for pursuing theoretical innovation is with a compelling and concrete puzzle: a real world problem or anomaly that cannot be adequately solved through the employment of existing theoretical tools” (SKIDMORE, 1998, p. 1011).

2.5 Algumas considerações

Nosso objetivo com este capítulo foi apresentar, ainda que de forma abrangente, a Securitização teorizada pelos principais expoentes da Escola de Copenhague, expondo também os elementos que levaram a uma ampliação e aprofundamento do conceito de segurança nas Relações Internacionais.

Dentre os limites teóricos e conceituais que apresentamos sucintamente, levamos todos em consideração quando aplicamos em nosso estudo de caso: a cibersegurança no Brasil.

Assim como os pesquisadores Thierry Balzacq, Sarah Léonard e Jan Ruzicka, acreditamos – como já apresentado na Introdução – que a teoria de Securitização é adequada para analisar o nosso caso em questão, pois fornece um quadro de análise que converge com as tendências atuais e vão além de exemplos europeus de segurança e defesa⁴².

A crescente preocupação com o papel da tecnologia nas relações internacionais faz com que discursos a respeito de ameaças no ciberespaço sejam cada vez mais recorrentes – e a Securitização pode fornecer ferramentas para compreender tal tendência. Como afirmaram os autores:

A importância dessa área decorre de duas tendências inter-relacionadas. Primeiro, Estados, sociedades, empresas e indivíduos dependem cada vez mais de dados, sistemas e tecnologias baseados no ciberespaço. Isso oferece um terreno fértil para diversos atores desenvolverem novos movimentos de securitização, identificando uma variedade de ameaças. Segundo, a preocupação com o ciberespaço se encaixa bem na busca de novas ameaças e riscos que vêm ocorrendo entre profissionais de segurança e burocracias desde o final da Guerra Fria (BALZACQ; LÉONARD; RUZICKA, 2016, p. 515, tradução nossa⁴³).

Dessa forma, a Securitização oferece um *framework* para compreender a relação entre Segurança e ciberespaço.

⁴² Cabe ressaltar que a Escola de Copenhague no livro *Security: a New Framework for Analysis* não se utiliza apenas de exemplos europeus, mas também de outras partes do mundo. Ocorre que a maior parte dos exemplos de aplicação da teoria são tomando como base problemas europeus, visto o contexto que os autores têm mais contato por estarem na Europa e pesquisando sobre segurança na Europa.

⁴³ No original: “The significance of this area stems from two inter-related trends. First, states, societies, business and individuals increasingly rely on data, systems and technologies based on cyber-space. This offers a fertile ground for a range of actors to develop new securitizing moves identifying a variety of threats. Second, the preoccupation with cyber-space fits well with the search for new threats and risks that has been on-going among security professionals and bureaucracies since the end of the Cold War” (BALZACQ; LÉONARD; RUZICKA, 2016, p. 515).

A respeito das críticas ao *speech-act*, compreendemos os limites apontado pelos críticos e usaremos sempre que necessário ao elucidar a respeito das entidades que têm o discurso predominante em nossa análise: o Ministério da Defesa, o Congresso Nacional e as Forças Armadas Brasileiras.

Ademais, entendemos como importante a consideração de elementos de contexto histórico e condições que puderam ter levado a construção da securitização do ciberespaço brasileiro. Dessa forma, o capítulo seguinte é dedicado a contextualização de crimes cibernéticos internacionais que podem ter contribuído ao discurso de segurança cibernética no Brasil.

Uma parte do capítulo referente ao Brasil também foi dedicada à contextualização histórica dos elementos que podem ter levado ao processo de securitização do ciberespaço brasileiro.

Deve-se ter em mente que uma “ação de segurança é geralmente tomada em nome e com referência a uma coletividade” (BUZAN; WÆVER; DE WILDE, 1998, p. 36, tradução nossa⁴⁴). Tendo em vista tal afirmação, buscamos compreender de que maneira ocorreram as ações de segurança tomadas no âmbito cibernético no Brasil, sem desconsiderar as razões que levaram às medidas tomadas.

Nos próximos capítulos, buscamos elucidar quais são os atores securitizadores, o objeto referente, os atores funcionais e as condições facilitadoras durante as medidas tomadas voltadas à segurança cibernética no Brasil, entre os anos de 2002 e 2018.

Todos estes elementos são apresentados com o objetivo de somar à nossa argumentação de que o governo brasileiro, na figura do Ministério da Defesa e das Forças Armadas, buscou securitizar o ciberespaço brasileiro no século XXI.

⁴⁴ No original: “Security action is usually taken on behalf of, and with reference to, a collectivity” (BUZAN; WÆVER; DE WILDE, 1998, p. 36).

CAPÍTULO 2

3 CONTEXTUALIZAÇÃO INTERNACIONAL

Conforme já apresentado, a Revolução Informacional e a grande popularização das Novas Tecnologias da Informação e Comunicação tiveram grandes efeitos nas relações sociais e econômicas, mas também nas relações internacionais. As vulnerabilidades que estas tecnologias passaram a apresentar, principalmente no século XXI, tornaram-se uma preocupação que não foi exclusiva de um único país ou continente.

Desde a popularização destas ferramentas combinada com um avanço da tecnologia que vivenciamos a partir século XXI, diversas maneiras de explorar as vulnerabilidades tecnológicas passaram a ser descobertas, desde o usuário comum até aos órgãos Estatais. Evidência disso é a crescente preocupação com tecnologia em setores públicos criados exclusivamente para lidar com o aperfeiçoamento tecnológico e impedir possíveis ameaças ao setor cibernético e à segurança da informação nas últimas décadas.

Entendemos que foram as ameaças e ataques, em sua parte de caráter mal-intencionados, que expuseram tais vulnerabilidades e, por conseguinte, foram responsáveis por promover a segurança cibernética e a segurança da informação como pautas a serem debatidas nas diferentes esferas sociais.

Partindo desta hipótese, selecionamos os casos de ataques cibernéticos com maior repercussão das últimas duas décadas de que sabemos que aconteceram de fato e quais foram as suas vítimas, apesar de nem sempre ser possível apontar os responsáveis.

Optamos por apresentá-los cronologicamente e utilizar tanto material bibliográfico quanto notícias publicadas à época, dado que são eventos recentes e a literatura é escassa. São eles: o caso da Estônia, de 2007; o caso da Geórgia, de 2008; o caso do Stuxnet no Irã, em 2010; o caso *WikiLeaks*, em 2010; o caso Snowden, em 2013; o caso do grupo Lázarus que agiu internacionalmente, em 2014; o caso da Ucrânia, em 2015; e, por último, o caso do *ransomware WannaCry*, com impacto internacional, em 2017⁴⁵.

A seleção destes episódios em específico seguiu os seguintes critérios: o alto volume de cobertura midiática sobre o caso; a produção acadêmica fomentada após tais casos; e a posterior repercussão que estes episódios obtiveram na comunidade internacional. Seguindo

⁴⁵ Recomendamos ao leitor que acompanhe a Linha do Tempo da Contextualização Internacional, presente no Apêndice A, na página 201, para melhor visualização dos acontecimentos em ordem cronológica.

estes critérios e respeitando o recorte temporal que aqui nos propusemos em analisar (o período entre 2002 e 2018), chegamos nestes oito casos supracitados.

Salientamos que os casos *WikiLeaks* e Snowden não se trataram de ataques cibernéticos “tradicionais” como o restante daqueles presentes em nossa lista proposta. Entretanto, são casos que se relacionaram diretamente com a cibersegurança e com o poder da informação, obtendo grande cobertura midiática em 2010 e 2013, respectivamente.

Até o momento, existem debates que envolvem a postura tanto dos *WikiLeaks* e seu fundador Julian Assange quanto a de Edward Snowden, ex-administrador da CIA (*Central Intelligence Agency*) e da NSA (*National Security Agency*). Do ponto de vista jurídico, ambos são considerados, até o momento, criminosos e que ainda precisam passar por julgamentos. Mas é graças a Assange e Snowden que ainda permanecem em voga discussões a respeito da espionagem por parte dos Estados, do sigilo de informações sensíveis e suas implicações, da moralidade que envolve a divulgação e transparência de certas informações e, sobretudo, da *privacidade*.

Dessa forma, optamos por comentar brevemente os casos que envolveram Julian Assange em 2010 e Edward Snowden em 2013, pois reforçam argumentos favoráveis à segurança cibernética e apresentam um panorama da relevância da Internet e da informação no século XXI. Ademais, ambos os episódios envolveram o governo brasileiro de alguma forma, o que dá ensejo à argumentação relacionada ao objetivo de nossa investigação.

Um outro tema pertinente que objetivamos tangenciar durante este capítulo e que se relaciona com a temática da cibersegurança no Brasil, é o papel não só do Exército, mas das forças militares como um todo que estiveram presentes em muitos dos casos envolvendo o ciberespaço e a segurança.

Em tom de provocação, já questionamos: por que a constante presença ou envolvimento das Forças Armadas em questões que envolvem o ciberespaço? Objetivamos compreender se esta não é apenas uma tendência brasileira, mas também internacional em algum aspecto.

Entretanto, pesquisar um tema tão latente levanta algumas limitações que necessitam esclarecimento.

Investigar um tema tão recente quanto à cibersegurança nas Relações Internacionais faz com que pesquisadores necessitem enfrentar algumas barreiras, tais como a precariedade de fontes para a construção de uma argumentação que seja linear e completa.

Dessa forma, para a construção deste capítulo, contamos com a cobertura midiática nacional e internacional a respeito de alguns destes casos na tentativa de elucidá-los da melhor forma possível. Esperamos que futuramente mais trabalhos acadêmicos sejam fomentados na área da cibersegurança internacional.

Ressaltamos que cada caso aqui apresentado, se analisados de forma aprofundada, dariam uma pesquisa completa por si só. Por este motivo, abordamos cada episódio de forma mais superficial, obtendo os principais *insights* que dialogam com o nosso objetivo final – compreender a securitização do ciberespaço no Brasil.

Acreditamos que, com um breve capítulo totalmente dedicado à compreensão dos principais episódios relacionados à cibersegurança do século XXI (que entram no recorte temporal determinado para a análise geral desta investigação), consigamos oferecer maior suporte para uma argumentação a respeito da crescente preocupação com a segurança cibernética internacionalmente.

A preocupação com a cibersegurança internacionalmente, por sua vez, faz com que países como o Brasil deem maior atenção ao espaço cibernético e dá ensejo para que o discurso de securitização do ciberespaço se amplie no âmbito do nosso Ministério da Defesa.

3.1 O Caso da Estônia (2007)

Ao compreender que acontecimentos no âmbito doméstico dos Estados têm relação com o contexto internacional em que o país está inserido – assim como as relações internacionais também são fruto de medidas tomadas internamente pelos Estados –, faz-se necessário mencionar alguns dos acontecimentos relevantes de repercussão mundial à época e que colaboram tanto para a presente discussão quanto para o enriquecimento do presente trabalho.

Tendo em vista o debate a respeito do espaço cibernético e a vulnerabilidade que apresenta, um importante acontecimento de 2007 contribuiu para que líderes mundiais se atentassem cada vez mais para estas questões. Optamos por utilizar notícias publicadas à época, tanto no Brasil quando na mídia internacional, ao fazer a retomada do acontecimento, além de um artigo publicado no ano de 2011, pois entendemos que existe uma relevância na compreensão da forma pela qual o ataque foi noticiado e entendido no momento em que ocorreu.

Um dos primeiros ataques cibernéticos de que se tem registro ocorreu, portanto, no ano de 2007 na Estônia e durou cerca de três semanas (THE GUARDIAN, 2007, s/p; FOLHA DE SÃO PAULO, 2007, s/p). Ataques massivos de Negação de Serviço Distribuído⁴⁶ (DDOS, na sigla em inglês) foram lançados contra infraestruturas cibernéticas da Estônia, deixando fora do ar sites governamentais, tais como da Presidência da República e de seu Parlamento, de partidos políticos do país e de quase todos os ministros do governo (THE GUARDIAN, 2007, s/p; HERZOG, 2011, p. 51).

Além da “derrubada” destes sites, tem-se registro de que estes ataques também foram direcionados a dois importantes bancos do país, a organizações de comunicação e a portais de notícia estonianos (THE GUARDIAN, 2007, s/p; HERZOG, 2011, p. 51). Estes ataques foram noticiados pela mídia brasileira como uma ação praticada por *hackers* (FOLHA DE SÃO PAULO, 2007, s/p; LANDLER; MARKOFF, 2007, s/p).

⁴⁶ Os Ataques de Negação de Serviço Distribuídos são ataques coordenados por indivíduos ou grupos mal-intencionados que contaminam outras máquinas e computadores remotamente, e que, através de um comando da máquina mal-intencionada central, toda a rede de máquinas infectadas (os chamados zumbis), disparam ataques simultâneos a um mesmo alvo – que pode ser um site –, o que acarreta na sobrecarga do servidor e compromete a disponibilização de seus serviços. Dessa forma, quando um usuário legítimo (que não é mal-intencionado) tenta visitar o site, por exemplo, ele aparece indisponível, fora do ar. Para mais informações ver: Laufer *et al.*, 2005.

Entendeu-se que os ataques virtuais tiveram uma motivação política após a ação de retirada de uma estátua de bronze que homenageava um soldado soviético da II Guerra Mundial, antes fixada na capital estoniana de Talín. Isso reacendeu tensões étnicas, políticas e estratégicas entre Rússia e Estônia que vinham ocorrendo desde o desmantelamento da URSS (LANDLER; MARKOFF, 2007, s/p; HERZOG, 2011, p. 51).

A figura da estátua era um memorial que comemorava a liberação soviética da ocupação nazista na Estônia e sua remoção serviu como um estopim para o imbróglio entre os dois países após ações que vinham ocorrendo desde 2004 e que desagradavam a Rússia: a entrada da Estônia na Organização do Tratado do Atlântico Norte (OTAN) e o distanciamento político entre a Rússia e a Estônia (HERZOG, 2011, p. 51).

Tendo em vista estas questões, a autoria dos ataques recaiu sobre “ativistas nacionalistas” russos que discordavam das ações do governo estoniano, gerando declarações oficiais da OTAN e da União Europeia em apoio à Estônia (THE GUARDIAN, 2007, s/p). Ainda segundo o portal The Guardian (2007), um de seus especialistas consultados reconheceu que os ataques podem ter advindo de qualquer parte do mundo – o que torna difícil de atribuir responsabilidade –, mas que alguns dos responsáveis pelos primeiros ataques foram identificados pelos seus “endereço de Internet” e que podia se afirmar que eram, de fato, da Rússia, alguns, até de instituições daquele País.

Parte dos estudiosos de *ciberguerra* e ataques cibernéticos também consideram os russos como autores dos ataques, seja no nível individual ou estatal, como é o caso de Herzog (2011).

A discussão a respeito do ataque cibernético na Estônia em 2007 ainda é muito recente e carece de investigações e informações oficiais. A dificuldade de atribuir responsabilidade pode fazer com que os debates não sejam constantemente estimulados.

Um elemento importante, entretanto, mencionada em todas as fontes consultadas, e que deve também ser mencionado aqui, se refere à *inovação* do ataque. Entende-se que este foi um dos primeiros ataques cibernéticos coordenados de que se tem registro e com alvo determinado: a Estônia.

A primeira questão que surge da análise deste acontecimento é a respeito da vulnerabilidade do ciberespaço. Noticiado internacionalmente, o ataque contra a Estônia, para o bem ou para o mal, expôs a sensibilidade do espaço cibernético a partir do avanço

tecnológico e popularização das Tecnologias de Informação e Comunicação. Medidas de segurança da informação e debates sobre questões cibernéticas podem ter sido elevadas ao nível estatal após o ocorrido.

Uma segunda questão, mais política – e provocativa de nossa parte – diz respeito a questão do poder cibernético e a atuação russa. O *poder* cibernético deve ser levado em consideração na contabilidade do poder estatal? Os investimentos russos na área tecnológica e o ataque a Estônia em 2007 podem ser entendidos como demonstração do poder cibernético da Rússia se houver comprovação de que os ataques são de sua autoria?

Estas questões são apenas provocações para o debate e não cabe ao escopo do trabalho procurar respondê-las extensivamente. Tais reflexões reaparecerão em nossas considerações.

O caso da Estônia em 2007 pode ter sido a primeira, mas não foi a última vez que a Rússia foi atribuída como responsável. A atuação do país foi implicada, novamente, em 2008, como veremos a seguir, em outro imbróglio cibernético, desta vez com a Geórgia, outro país da ex-União Soviética.

3.2 O caso da Geórgia (2008)

Um ano após os ataques à estrutura da Estônia, outra onda de ataques cibernéticos ocorreu, agora na Geórgia. A peculiaridade deste caso, como entendemos, foi a ocupação do território georgiano por tropas militares russas que acompanhou os ciberataques que a Geórgia sofreu à época.

Dentre os precedentes do conflito, destacamos um, de abril de 2004, para compreensão das implicações políticas do imbróglio: uma declaração pública foi feita pela Organização do Tratado do Atlântico Norte no sentido de que o país da Geórgia viria um dia a ser membro da aliança, assim como objetivara o presidente georgiano Mikheil Saak'ashvili à época. Ressaltamos que Geórgia, na figura do presidente Saak'ashvili tinha uma orientação mais pró-Occidental do que pró-Rússia e, por isso, se elegeu (OPPERMANN, 2010; ALMEIDA, 2008; SOARES, 2008).

A resposta do então presidente russo Vladimir Putin foi o estreitamento das relações com as *regiões separatistas* que eram presentes na Geórgia, uma vez que, geopoliticamente, a Rússia buscava manter sua influência no Cáucaso (ALMEIDA, 2008, p. 34).

Uma das regiões separatistas – e única de interesse no presente trabalho – foi a Ossétia do Sul⁴⁷, a qual sempre teve maior afinidade com a região da Ossétia do Norte que, por sua vez, fica em território russo.

A Ossétia do Sul já havia manifestado desejo de se separar da Geórgia ainda na década de 1990 através de um referendo que foi reprimido militarmente pelo governo georgiano (SOARES, 2008, p. 31). Desde então, tropas georgianas vinham contendo movimentações separatistas na Ossétia do Sul, dentre as quais, destacamos aquelas que vinham ocorrendo durante 2008, o ano deste conflito em questão (OPPERMANN, 2010).

Dessa forma, em agosto de 2008, a Rússia enviou tropas à região da Ossétia do Sul, na Geórgia, na tentativa de *apoiar* as movimentações separatistas. Salientamos que, assim como a Estônia, desde o desmantelamento da União Soviética, as relações entre Geórgia e Rússia eram instáveis, havendo tensões étnicas, políticas e estratégicas (OPPERMANN, 2010, p. 18-19).

⁴⁷ Região onde a maior parte da população é, oficialmente, cidadã russa (OPPERMANN, 2010, p. 18).

Antes da ocupação da Ossétia do Sul no mês de agosto de 2008, entretanto, a Geórgia vinha sofrendo, desde de julho daquele ano, ataques cibernéticos do mesmo tipo daqueles sofridos pela Estônia no ano anterior: Ataques de Negação de Serviço Distribuído (G1, 2008, s/p; OPPERMANN, 2010, p. 18). Compõe o rol dos principais alvos dos ataques cibernéticos: as redes governamentais e o escritório presidencial georgiano; as redes financeiras; os serviços de notícias da Geórgia; e a embaixada norte-americana na Geórgia (OPPERMANN, 2010, p. 18). Os inúmeros ataques a estas redes deixaram-nas indisponíveis por diversos dias (OPPERMANN, 2010).

Dessa forma, podemos observar que, durante o ano de 2008, vinha ocorrendo entre Rússia e Geórgia – e também entre a região georgiana da Ossétia do Sul – um imbróglio não somente político, mas também militar e cibernético, com o envolvimento de tropas e ciberataques.

Conforme afirmou Daniel Oppermann (2010): “Antes e durante as agressões virtuais [à Geórgia], os alvos potenciais foram publicados em vários fóruns de discussão online russos para mobilizar *hackers* patrióticos [...]” (OPPERMANN, 2010, p. 18, tradução nossa⁴⁸). Também existem relatos de especialistas que afirmam que havia “[uma] avalanche de dados direcionados aos computadores do governo da Geórgia com a mensagem: ‘win+love +in+Russia [vencer+amor+na+Rússia]’” (MARKOFF, 2008, s/p).

A partir destas informações, inferimos que os Ataques de Negação de Serviço Distribuídos direcionados à estrutura cibernética da Geórgia advieram de usuários na Rússia e foram estimulados para que mais patriotas russos se juntassem a causa dos ataques cibernéticos.

Em um contexto no qual a Geórgia sofria ataques em suas infraestruturas cibernética e de comunicação, também em portais midiáticos, tropas russas ocuparam a região da Ossétia do Sul com o objetivo de anexá-la ao seu território. Os portais de notícia georgianos, por sua vez, tinham poucas ou nenhuma condição de informar sua população – e o restante do mundo – do que vinha ocorrendo em seu território.

A ocupação da Ossétia do Sul, tanto por tropas militares russas quanto por tropas militares georgianas, resultou no que ficou conhecido como Guerra dos Cinco Dias, ou

⁴⁸ No original: “Before and during the virtual aggressions, potential targets were published on several Russian online discussion forums to mobilize patriotic hackers like it had happened in the Estonia attacks the year before” (OPPERMANN, 2010, p. 18).

Guerra Russo-Georgiana. Após o breve conflito que durou cinco dias, como o próprio nome sugere, a Ossétia do Sul teve sua independência da Geórgia reconhecida pela Rússia.

Já a Geórgia, por sua vez, na tentativa de se tornar mais independente da infraestrutura russa de tecnologia, teve apoio norte-americano na construção de redes mais seguras (mais seguras contra a Rússia, enfatiza-se), na tentativa de proteger seus dados, meios de comunicação e infraestrutura crítica (G1, 2008, s/p).

Apesar do governo russo negar seu envolvimento, podemos inferir que esta foi a primeira combinação de ataque cibernético a uma operação militar implantada na defesa de interesses em outro Estado. Especialistas em tecnologia entendem que “cyber-ataques são tão baratos e fáceis de organizar, com poucas impressões digitais, que quase certamente permanecerão como marca dos combates modernos” (G1, 2008, s/p). Ou seja, a facilidade de mobilização on-line, combinada à uma dificuldade de responsabilização, pode fazer com que estes tipos de ataques cibernéticos se façam presentes enquanto elementos, também, da Segurança Internacional.

Os ataques de Negação de Serviço Distribuído serviram como uma ferramenta que potencializou a eficiência da campanha militar. Dessa forma, buscamos apresentar que os Estudos de Segurança Internacional passaram compreender a tecnologia da informação mais veemente como um elemento presente nas dinâmicas política e militar dentro das Relações Internacionais, conforme cresceu a dependência dessas tecnologias em todos os níveis da sociedade.

Entendemos que a Rússia é uma das maiores potências mundiais que investem em seu ciberespaço e segurança cibernética desde o início do século XXI. Poderíamos argumentar que neste conflito ocorrido em 2008 testou a aplicabilidade de ataques cibernéticos e seus efeitos em um contexto armado.

Ademais, uma outra consideração diz respeito a tentativa de mostrar ao Ocidente, por parte da Rússia, sua presença no ciberespaço e sua capacidade de aplicar ataques cibernéticos remotamente além de interromper acessos a serviços específicos, assim como no caso envolvendo a Estônia.

Em síntese, entendemos que o caso da guerra Russo-Georgiana de 2008 pode oferecer *insights* a respeito da vulnerabilidade e da potência do ciberespaço. Por ter ocorrido no ano

seguinte aos ataques sofridos na Estônia, apenas reforça a ideia de que um debate a respeito do ciberespaço deveria ascender.

Consideramos, inclusive, que estes novos debates emergentes destes ataques cibernéticos contra a Estônia (em 2007) e contra a Geórgia (em 2008) puderam ter influenciado nas decisões brasileiras de incluir o espaço cibernético como pauta de defesa nacional, na medida em que o debate a respeito do ciberespaço enquanto setor estratégico vinha ocorrendo na mesma época em que os ciberataques, como já afirmamos.

3.3 O Caso do Stuxnet (2010)

Ainda considerando a contextualização internacional de explorações de vulnerabilidades cibernéticas, um importante acontecimento ocorreu no ano de 2010 com grande repercussão internacional. Um *malware*, um vírus de computador, teria sido o responsável pela danificação material de usinas nucleares iranianas. O vírus – e este episódio, de forma geral – ficou conhecido como Stuxnet.

Equipes de empresas concorrentes de segurança da informação, tais como a russa Kaspersky Lab e a norte-americana Symantec, cooperaram na compreensão da infecção pelo *malware*, tamanha sua complexidade. Kim Zetter, jornalista estadunidense, acompanhou o caso à época em que ocorreu, chegando a escrever um livro a respeito do Stuxnet em 2014 (ZETTER, 2017).

Zetter relatou em seu livro que há décadas o Irã vinha dedicando parte de seu orçamento na construção de instalações nucleares com a presença de reatores responsáveis pelo enriquecimento de Urânio, que o “Ocidente” desconfiava que não seriam usados para fins pacíficos e, sim, como armas nucleares (ZETTER, 2017, p. 34-35).

As instalações em questão ficavam na cidade de Natanz, localizada a cerca de 320 quilômetros ao sul de Teerã, no Irã, e seus reatores foram alvos de um ataque cibernético, executado por um vírus de computador. Mas, diferentemente do que se estava acostumado a observar pelos ataques “tradicionais”, teve-se implicações físicas, causando prejuízo material nas máquinas infectadas (ZETTER, 2017, p. 32-35).

Especialistas afirmam que se tratou de um ataque sofisticado que explorava falhas nos sistemas operacionais das máquinas, e seus principais alvos eram sistemas de controle de automação e monitoramento industrial, conhecido como SCADA (*Supervisory Control and Data Aquisition*⁴⁹), ou seja, tratou-se de um ataque com o propósito de atingir *infraestruturas críticas* (ROHR, 2010, s/p; ZETTER, 2017, p. 129, grifo nosso).

Apesar de este *malware*, o Stuxnet, ter se espalhado regionalmente, sendo identificado em outros países tais como Índia, Indonésia, Rússia, entre outros, estudos aprofundados afirmaram que o alvo principal era mesmo o Irã e suas instalações nucleares

⁴⁹ Controle de Supervisão e Aquisição de Dados.

(ROHR, 2010, s/p; ZETTER, 2017, p. 65-67; FALLIERE; O’MURCHU; CHIEN, 2015, p. 06).

Faz-se importante mencionar que, como constado no livro da jornalista Zetter: “Em 16 de julho de 2009 [...] o fundador do *WikiLeaks*, Julian Assange, postou uma nota misteriosa em seu website sobre um possível acidente em Natanz” (ZETTER, 2017, p. 175). Esta colocação, entre outras investigações, corrobora na formulação da argumentação de que o alvo do Stuxnet sempre foi as instalações nucleares de Natanz, no Irã.⁵⁰

Em pesquisas desenvolvidas por especialistas em informática e engenharia da computação da Symantec⁵¹, notou-se que, de forma geral, o vírus do Stuxnet infectava máquinas específicas com sistemas que controlavam reatores nucleares e suas turbinas, aumentando sua rotação a ponto de danificá-las (ZETTER, 2017, p. 122). O *malware* também era responsável por ocultar possíveis mensagens de alertas aos operadores das máquinas e, dessa forma, a máquina poderia continuar operando sem interferências até atingir seu objetivo de causar dano físico às turbinas infectadas⁵² (ZETTER, 2017, p. 122).

Em um relatório completo de 68 páginas desenvolvido pelos Diretor Técnico, Gerente de Desenvolvimento e Engenheiro de Software da Symantec, evidenciam-se a densidade, a complexidade e a sofisticação do vírus, pois sua carga útil foi elaborada para agir em etapas que explorariam diversas falhas – algumas, inclusive, desconhecidas publicamente – dos sistemas operacionais das máquinas e garantiriam o sucesso da operação a partir de sua “infecção” (FALLIERE; O’MURCHU; CHIEN, 2015, p. 16-19).

Entende-se que o Stuxnet representou uma “revolução” na forma como os vírus eram empregados (ZETTER, 2017, p. 123). Ao contrário do que especialistas estavam acostumados a estudar e combater, o *malware* não foi desenvolvido e usado para alterar ou roubar dados sensíveis, mas para “alterar fisicamente ou destruir algo na outra ponta” (ZETTER, 2017, p. 122). Por este motivo, apresentava uma inovação na relação com ataques cibernéticos, podendo, inclusive, ser considerado como um novo recurso bélico com alvo pré-definido e certa precisão.

⁵⁰ Posteriormente, ainda enquanto contextualização, abordaremos mais extensivamente o episódio do *WikiLeaks* e o papel de seu fundador Julian Assange.

⁵¹ Empresa norte-americana focada na segurança da Internet e de redes, tanto para usuários domésticos como corporações. Um dos seus principais produtos é o antivírus Norton.

⁵² O ataque do Stuxnet foi muito complexo e envolve conceitos da informática que não cabem serem abordados no presente trabalho. Para mais informações ver: FALLIERE; O’MURCHU; CHIEN, 2015 e ZETTER, 2017.

Tendo em vista estas características supracitadas do vírus do Stuxnet, passou-se a acreditar que havia o envolvimento de governos na elaboração e dispersão do *malware*. Isto, pois, o enriquecimento de Urânio por parte do Irã poderia ser compreendido como uma ameaça à segurança de países da região – ou, também, do restante do sistema internacional. À época, a mídia noticiou a probabilidade do envolvimento de poderosos grupos e governos na criação e desenvolvimento do vírus (ROHR, 2010, s/p).

Uma vez constatado que o ataque se tratou de uma sabotagem intencional, buscou-se os responsáveis por ela. Embora exista, até o presente momento, certa nebulosidade a respeito dos criadores do *malware*, muito se responsabilizou os Estados Unidos e Israel, na medida em que existem relatos a respeito do planejamento de um ataque ao Irã pelas potências desde 2006 (ZETTER, 2017, p. 190). Ademais, o fato de Israel “concorrer” com o Irã regionalmente, em termos geopolíticos, agrava as suspeitas.

Nosso objetivo nesta presente seção não é, entretanto, discutir a responsabilidade pelo ciberataque, mas contextualizá-lo na linha do tempo aqui proposta, compreendendo suas implicações enquanto um possível recurso de poder dos Estados, o que pode ter gerado uma maior atenção de alguns países – especialmente aqueles com condições para tal – para com o espaço cibernético e a sensibilidade das tecnologias e *infraestruturas críticas*.

Dessa forma, é possível afirmarmos que o ano de 2010 foi importante para-o avanço da discussão a respeito da importância de instalações ligadas ao ciberespaço e a sensibilidade de certos equipamentos, principalmente aqueles ligados às *infraestruturas* dos países. Compreendemos que o episódio de Stuxnet pode ter contribuído para que outros países – até mesmo o Brasil – sofisticassem os meios de garantir a segurança cibernética.

A exemplo disso, como trataremos no capítulo seguinte, foi a autorização da criação de um Centro de Defesa Cibernética exclusivamente militar no Brasil também no ano de 2010.

3.4 O caso *WikiLeaks* (2010)

No ano de 2020 completou-se dez anos de um dos maiores vazamentos de documentos oficiais na Internet através de um portal chamado *WikiLeaks*. Fundado em 2006 pelo jornalista Julian Assange, o *WikiLeaks* é descrito como sendo uma “organização de mídia multinacional e biblioteca associada” (WIKILEAKS, 2015, s/p, tradução nossa⁵³).

A partir do estabelecimento da informatização em diferentes segmentos da sociedade, houve uma produção de diversos tipos informação em larga escala e uma consequente utilização destas informações por Estados e organizações. O portal *WikiLeaks*, como os próprios contribuintes mesmo afirmam, se especializou na “análise e publicação de um grande conjunto de dados de materiais oficiais censurados e/ou restritos que envolvem guerra, espionagem e corrupção” (WIKILEAKS, 2015, s/p, tradução nossa⁵⁴).

Ou seja, o portal *WikiLeaks* funciona como um meio de concentração e divulgação de informações entre as quais podem consideradas sigilosas, classificadas ou sensíveis por conterem dados a respeito de crimes de guerra, espionagem e corrupção envolvendo Estados e companhias de grande notoriedade internacional. O próprio nome “*WikiLeaks*” revela o caráter de vazamento de informações sensíveis como o sufixo “*Leaks*” (vazamento) sugere.

Como afirmou a pesquisadora Liliana Pacheco: “Desde a sua fundação, em 2006, a Wikileaks já libertou informação prejudicial ao governo do Quênia, informação relativa às guerras do Iraque e Afeganistão, reportou vários abusos ambientais, entre muitos outros casos polêmicos” (PACHECO, 2011, p. 31). Mas o portal *WikiLeaks* e seu fundador Julian Assange ganharam a dimensão e reconhecimento internacionais que possuem até os dias atuais após os episódios de 2010 e início de 2011, focos deste tópico que se apresenta.

Em 2010, portanto, houve a publicação de diversos arquivos diplomáticos dos Estados Unidos desde a década de 1990, além de arquivos que continham informações classificadas a respeito das campanhas militares no Iraque e no Afeganistão pelo site *WikiLeaks*. Estes vazamentos focados em informações sobre campanhas militares, no site oficial do *WikiLeaks*, são classificados como *WarDiaries*⁵⁵ (Diários de Guerra) (WIKILEAKS, 2015).

⁵³ No original: “WikiLeaks is a multi-national media organization and associated library [...]” (WIKILEAKS, 2015, s/p).

⁵⁴ No original: “WikiLeaks specializes in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption” (WIKILEAKS, 2015, s/p).

⁵⁵ O *WarDiaries* está disponível em: <https://wardiaries.wikileaks.org/>.

O portal possui o contato do que são chamados de *insiders*⁵⁶, pessoas que trabalham em posições no governo ou organizações oficiais e que possuem informações, além da colaboração de *crackers*, que podemos entender, de modo geral, como um tipo de “*hackers*”, que quebram códigos de sites e plataformas online com o objetivo final de obter informações que consideram importantes para a divulgação (PACHECO, 2011; WIKILEAKS, 2015).

O site *WikiLeaks*, ainda, é parceiro de diversos portais midiáticos no mundo todo na divulgação das informações e, é por este motivo, que se consideram “multinacional”. Dentre os parceiros, tem-se os jornais *Der Spiegel*, *El País*, *Le Monde*, *The Guardian*, *The Intercept*, *The New York Times*, *The Telegraph*, *The Washington Post* e os brasileiros *Carta Capital* e *O Globo* (WIKILEAKS, 2015).

A parceria entre o *WikiLeaks* e estes grandes portais de notícia se formou com o tempo através de apresentações que Julian Assange promoveu para elucidar o papel do portal (MAGALHÃES, 2017). De acordo com o exposto por Magalhães (2017), podemos entender que ter o apoio de grandes veículos de imprensa significava três coisas, principalmente: *a*) a ajuda em analisar a grande quantidade de informações mais relevantes coletadas pela equipe do *WikiLeaks*; *b*) dar credibilidade às informações divulgadas, o que gera a confiança da plataforma entre os leitores; e *c*) divulgar para a maior quantidade de pessoas possível estas informações consideradas sensíveis.

O que houve de fato em 2010 que colocou o *WikiLeaks* no radar de diversos Estados? Um caso muito famoso tomou conta da mídia no final do ano de 2010.

O Jornal *The New York Times*, seguido de outros veículos midiáticos internacionais, divulgaram um vídeo no qual oficiais do exército norte-americano abriram fogo contra locais, acertando repórteres do site *Reuters* que estavam cobrindo a campanha militar do país em Bagdá, Iraque (BUMILLER, 2010; ENGELKE, 2020). O vídeo⁵⁷ remontava ao ano de 2007 e tinha 39 minutos de duração, evidenciando a ação dos oficiais e a conversa entre eles. O vídeo apresentou, inclusive, crianças que ficaram feridas durante a ação militar e os oficiais norte-americanos culpando as pessoas injuriadas pela ofensiva, pois levaram “crianças à batalha” (BUMILLER, 2010, s/p).

⁵⁶ Pode ser melhor entendido como “infiltrados”.

⁵⁷ O vídeo está disponível na íntegra em: <https://collateralmurder.wikileaks.org/>. Acesso em: 03 maio 2020.

O episódio foi denominado como *Collateral Murder* (Assassinato Colateral) pelos agentes do *WikiLeaks* que obtiveram acesso ao vídeo através de um *whistleblower*⁵⁸ que trabalhava para as Forças Armadas norte-americanas (BUMILLER, 2010; ENGELKE, 2020).

O jornal The New York Times, que divulgou as informações a respeito do vídeo e da campanha militar no Iraque, apresentou o *WikiLeaks* como a organização que obteve o acesso ao vídeo e ainda a outros documentos, o que colaborou para que a atenção se voltasse ao portal.

Além do episódio do *Collateral Murder* que ganhou grande notoriedade, documentos referentes à guerra, corrupção e espionagem envolvendo outros países além dos Estados Unidos foram divulgados pelo portal. O Brasil, inclusive, esteve entre os países mencionados em informações oficiais “vazadas” e divulgadas na imprensa após a coleta feita pelo *WikiLeaks* (G1, 2020).

Dentre os documentos a respeito do Brasil divulgados pelo *WikiLeaks* e seus parceiros, os que ganharam maior atenção foram aquelas que o ex-embaixador dos Estados Unidos no Brasil, Clifford Sobel, assinou.

Clifford Sobel foi embaixador no Brasil entre 2006 e 2009, nomeado pelo então presidente dos Estados Unidos, George W. Bush. De acordo com os documentos vazados pelo *WikiLeaks*, Sobel fazia relatórios sobre aquilo que considerava importante e estratégico para os Estados Unidos, levando em consideração o comportamento dos líderes do Brasil.

Ainda em 2008, Clifford Sobel enviou um telegrama⁵⁹ classificado aos Estados Unidos que teceu seus comentários a respeito da visita do então Ministro da Defesa Nelson Jobim a Washington. De acordo com o ex-embaixador, o ex-Ministro tinha a intenção de melhorar o relacionamento entre Brasil e EUA em questões referentes a modernização do aparato militar, mas que foi muito cauteloso ao fazê-lo (SOBEL, 2008). Isto, pois, segundo ele existia uma “obstrução por parte do Ministério das Relações Exteriores” (SOBEL, 2008b, s/p).

De acordo com o telegrama vazado pelo *WikiLeaks*, Clifford Sobel afirmou:

⁵⁸ Denunciante ou delator que expõe uma má conduta, seja desonesta ou até mesmo ilegal, geralmente dentro de seu ambiente de trabalho.

⁵⁹ O telegrama está disponível na íntegra em inglês em: https://search.wikileaks.org/plusd/cables/08BRASILIA429_a.html. Acesso em: 03 maio 2020.

[...] Jobim permaneceu cauteloso em melhorar as relações bilaterais de cooperação em defesa, refletindo a abordagem mais negativa dos Ministério das Relações Exteriores (MRE), que procurou restringir a viagem de Jobim e inibir o diálogo EUA-Brasil em questões de defesa. Embora haja boas perspectivas de melhoria nosso relacionamento de defesa com o Brasil, a obstrução do MRE continua sendo um problema (SOBEL, 2008b, s/p, tradução nossa⁶⁰).

Podemos inferir que o então embaixador dos Estados Unidos no Brasil observava uma dificuldade no diálogo com o Ministério das Relações Exteriores (MRE), considerando que mantinham um posicionamento de “não permitir” que o Brasil tivesse um bom relacionamento com os EUA na medida em que, à época, o Brasil estreitava relações com países da América Latina e outros países também em desenvolvimento, tais como os BRICS (SOBEL, 2008b).

Essa “restrição” imposta pelo Ministério das Relações Exteriores e a dificuldade da aproximação entre EUA e Brasil, especialmente em termos de Defesa e Segurança, descrita por Clifford Sobel já havia sido tratada em outro telegrama⁶¹ enviado pelo ex-embaixador em março de 2008. Foi neste telegrama que Sobel afirmou que o então Secretário-Geral do Ministério das Relações Exteriores Samuel Pinheiro Guimarães era “fervorosamente *antiamericano*” (SOBEL, 2008, s/p, tradução nossa⁶², grifo nosso).

Quando este telegrama foi divulgado no final de 2010, Clifford Sobel não era mais embaixador, mas Lula ainda era o presidente, com seu segundo mandato chegando ao fim, assim como Samuel Pinheiro Guimarães se despedia do cargo de Secretário-Geral do MRE. Dessa forma, os vazamentos e divulgações repercutiram internacionalmente e, também, nacionalmente, gerando comentários do então presidente Luiz Inácio Lula da Silva (PASSARINHO; BONIN, 2010).

De acordo com o noticiado pelo jornal G1 da Globo à época, o então presidente Lula demonstrou solidariedade ao grupo *WikiLeaks* pelo vazamento, reforçando valores de liberdade de imprensa. Segundo ele “o culpado não é quem divulgou, é quem escreveu” (PASSARINHO; BONIN, 2010, s/p).

⁶⁰ No original: “[...] Jobim remained cautious on enhancing bilateral defense cooperation, reflecting the more negative approach of the Ministry for External Relations (MRE) which had sought to curtail Jobim's trip and to inhibit the U.S.-Brazil dialogue on defense issues. While there are good prospects to improve our defense relationship with Brazil, MRE obstruction will continue to be a problem” (SOBEL, 2008, s/p).

⁶¹ O telegrama pode ser acessado na íntegra em inglês através do link: https://search.wikileaks.org/plusd/cables/08BRASILIA343_a.html. Acesso em: 03 maio 2020.

⁶² No original: “[...] Pinta Gama, who is chief of staff to the fervently anti-American MRE Secretary General (Deputy Minister) Samuel Pinheiro Guimaraes, [...]” (SOBEL, 2008, s/p).

Clifford Sobel também comentou a respeito da Estratégia Nacional de Defesa Brasileira (END), publicada em 2008, em um telegrama sigiloso enviado aos EUA também vazado pelo *WikiLeaks*. O embaixador fez uma análise geral do documento, reforçando a ideia de que o Brasil gostaria de ser “independente”⁶³ (SOBEL, 2009).

O Brasil realmente postulou a necessidade de uma independência ao se tratar da questão de segurança e defesa na END (BRASIL, 2008) que Sobel recorrentemente retoma. Entretanto, em seus comentários finais, o ex-embaixador viu no objetivo de modernizar o aparato militar brasileiro uma oportunidade de aproximar os EUA das Forças Armadas Brasileiras através da cooperação militar entre os países, especialmente ao que se refere a equipamentos de Defesa, mesmo que de forma lenta e gradual já que, em sua opinião, havia dificuldades da aproximação entre Brasil e EUA por conta de uma postura ideológica do Ministério das Relações Exteriores (SOBEL, 2009; SOBEL, 2008).

Ademais, também apresentamos brevemente outros dois telegramas sigilosos entre Clifford Sobel e governo dos Estados Unidos vazados pelo *WikiLeaks*: o primeiro⁶⁴ demonstrou uma certa preocupação da aproximação do Brasil com países do Oriente Médio, em específico, o ex-embaixador revelou uma preocupação do Brasil entrar para a “órbita do Irã” (SOBEL, 2008a, s/p).

O segundo⁶⁵ tratava a respeito de caças a serem adquiridos pelas Forças Armadas Brasileiras. O documento revelou a preocupação do embaixador em garantir que o Brasil comprasse caças norte-americanos, apesar de o governo francês ter apresentado uma boa proposta ao Ministério da Defesa (SOBEL, 2009a).

Ainda de acordo com este telegrama vazado, Clifford Sobel afirmou que estreitaria suas relações com o Ministro Jobim para que ele atuasse no nível político como um aliado dos Estados Unidos neste quesito, na medida em que as decisões finais seriam tomadas em níveis mais altos do governo e a decisão final seria do então presidente Lula – que, por sua vez, já havia postulado uma necessidade de se tornar mais *independente* em questões referentes à Defesa e Segurança no Brasil (SOBEL, 2009, grifo nosso).

⁶³ Em todos os momentos durante o telegrama enviado aos EUA, o termo independência foi colocado entre aspas pelo ex-embaixador. O telegrama está disponível na íntegra e em inglês em: https://search.wikileaks.org/plusd/cables/09BRASILIA34_a.html. Acesso em: 03 maio 2020.

⁶⁴ O telegrama está disponível na íntegra e em inglês em: https://search.wikileaks.org/plusd/cables/08BRASILIA896_a.html. Acesso em: 03 maio 2020.

⁶⁵ O telegrama está disponível na íntegra e em inglês em: https://search.wikileaks.org/plusd/cables/09BRASILIA41_a.html. Acesso em: 03 maio 2020.

Dessa forma, podemos compreender a atuação do portal *WikiLeaks* e o crescimento que obteve a partir da década de 2010. Liliana Pacheco (2011, p. 32) afirmou que “um sentido de justiça ou uma forma de retaliação contra os seus empregadores” são os dois principais fatores que movem as fontes do *WikiLeaks*. Mas acreditamos que não seja apenas isso e gostaríamos de acrescentar *mais um fator* ao movimento de vazamento de informações e exposição de crimes de guerra e espionagem na Internet.

A partir da informatização e da constante presença da tecnologia no cotidiano das sociedades, tornou-se natural que redes de computadores tomassem conta de todas as esferas dos governos, incluindo os principais tomadores de decisão. A Internet e o ciberespaço, como já argumentamos, estão sujeitos a ter vulnerabilidades exploradas na medida em que a tecnologia se aperfeiçoa cada vez mais em um curto espaço de tempo.

A combinação desta informatização de documentos sensíveis (ou sigilosos, classificados) e das “brechas” que o ciberespaço pode apresentar, fez com que cada vez mais especialistas em informática que acreditam que a informação e a transparência sejam direitos fundamentais se organizassem como *ciberativistas*. Isto, pois, nunca estivemos tão próximos, ainda que pela Internet, de nossos governos e das informações que circulam entre as autoridades.

O debate que se coloca ao tratar deste assunto é: o que deve ser protegido e o que deve ser divulgado ao público? Não faz parte do escopo da presente investigação entrar no cerne deste debate, mas sim apresentar os papel e legado do *WikiLeaks* em meio aos vazamentos e exposições que se tornaram comuns em nosso século.

Dentre as consequências do trabalho do *WikiLeaks* em garimpar informações, podemos inferir que o portal “acabou popularizando a noção da existência de preciosíssimos bancos de dados escondidos na internet, despertando o interesse de ciberativistas e órgãos de inteligência de todo planeta” (MAGALHÃES, 2017, p. 150).

Além de ciberativistas passarem a se organizar para a coleta e divulgação de informações, entendemos que o *WikiLeaks* também foi responsável por criar uma cultura de *whistleblowers*, o que pode ter inspirado, inclusive, Edward Snowden a divulgar informações sigilosas da CIA que revelavam um processo sistemático de espionagem e invasão de privacidade por parte do governo dos EUA (HARDING, 2014). Trataremos mais a respeito do caso Snowden no tópico subsequente.

Quando nos referimos a uma “cultura de *whistleblowers*”, queremos afirmar que uma espécie de comunidade foi criada para que as pessoas pudessem fazer denúncias de forma anônima de condutas inadequadas e até criminosas que observam dentro de seu ambiente de trabalho. A denúncia de tais condutas foi naturalizada não só em órgãos oficiais e governamentais, mas também no setor privado.

Ao que se refere ao Brasil, compreendemos que a exposição feita pelo *WikiLeaks* suscitou debates, principalmente, a respeito da liberdade de imprensa, da importância da informação e, até mesmo, o dever moral do jornalismo (PACHECO, 2011; MAGALHÃES, 2017).

Ademais, o caso *WikiLeaks*, ou seja, o vazamento sistemático de arquivos referentes à diplomacia norte-americana, ocorreu em um contexto de formação do Centro de Defesa Cibernética no Brasil, em 2010. Dessarte, podemos fazer um paralelo entre o investimento em ações de cibersegurança no Brasil e a divulgação indiscriminada de informações que ocorria.

Apesar de discutirmos a criação do Centro de Defesa Cibernética no próximo capítulo, já adiantamos que pode ser que o Brasil, ao compreender o papel de sites como o *WikiLeaks* e a importância da segurança no ciberespaço, pode ter entendido que estava “no caminho certo” ao tomar medidas que aumentassem a segurança no ambiente digital de forma geral.

Finalmente, também podemos tentar compreender, a partir do caso *WikiLeaks*, o objetivo de proteção de infraestruturas críticas e o que elas significam efetivamente. Na medida em que a infraestrutura crítica também está relacionada a questões que envolvem a política, a economia e as relações internacionais, o *WikiLeaks* pode ser entendido como uma ameaça aos países? Buscaremos responder tal questionamento após considerar também o caso Snowden no próximo tópico.

3.5 O caso Snowden (2013)

Outro caso de exposição de atividades irregulares por parte dos Estados Unidos ocorreu três anos após o episódio de maior repercussão dos *WikiLeaks*: o tratamos aqui como caso Snowden. Antes de elucidarmos mais a respeito do episódio e suas consequências, faremos uma breve apresentação de quem é Edward Snowden, responsável pela exposição das ilegalidades da Agência de Segurança Nacional norte-americana.

Edward Snowden é um jovem que trabalhou como analista de sistemas na NSA, a Agência de Segurança Nacional dos Estados Unidos. Apesar de não possuir um diploma formal de Ensino Superior na área, Snowden, desde sua adolescência, teve contato com computadores e com tecnologia da informação em pleno contexto de popularização da Internet e dos *personal computers* (PCs), se tornando um *expert* na área (HARDING, 2014).

Harding (2014) descreveu Snowden como um autodidata que passava muitas horas *online* em fóruns de informática, aprendendo e compartilhando conhecimento sobre o desenvolvimento das novas tecnologias que estavam em ascensão entre o fim dos anos 1990 e início dos anos 2000.

Após um breve período servindo como soldado em Fort Benning, na Geórgia, Edward Snowden foi dispensado e voltou a sua cidade, Maryland, onde ficava a sede da NSA nos Estados Unidos (HARDING, 2014). Em 2005 conseguiu um emprego na Universidade de Maryland, em princípio como guarda de segurança, mas logo chegou ao setor de Tecnologia da Informação.

No ano seguinte já havia demonstrado suas habilidades com a informática e a tecnologia da informação, avançando em sua carreira. Como apresentou o jornalista do jornal The Guardian, Luke Harding:

Snowden podia não ter um diploma. Mas, em meados de 2006, conseguiu um emprego no setor de tecnologia de informação da CIA. Rapidamente descobriu que suas habilidades excepcionais em T.I. abriam todos os tipos de portas interessantes do governo (HARDING, 2014, s/p).

Aos 24 anos, Snowden foi enviado à Suíça como segurança da rede de computadores da CIA, cuidando também da segurança dos diplomatas americanos baseados na missão de Genebra (HARDING, 2014). Este é um momento importante na história de Edward Snowden, pois foi durante este tempo na Suíça que passou a notar o funcionamento da espionagem e de que forma atuava para garantir sempre as melhores informações para o governo qual servia. A partir de então, começou a questionar a moralidade da espionagem

internacional, chegando a declarar que se sentiu “desiludido” com a forma pela qual o governo norte-americano funcionava e com seu papel em meio a tudo aquilo (HARDING, 2014, s/p).

Em 2009, Edward Snowden pediu demissão da CIA e foi trabalhar como terceirizado pela NSA no Japão, onde teve acesso à diversos mecanismos de coleta de informação e espionagem (HARDING, 2014). O jornalista Luke Harding, que ficou responsável pelo relato da história de Snowden no livro “Os arquivos Snowden: A história secreta do homem mais procurado do mundo”, afirmou que o ano de 2009 foi decisivo para o jovem analista de sistemas. Sustentou: “Entre 2009 e 2012, Snowden diz que descobriu o quão desgastante eram as atividades da NSA ‘a intenção deles é tomar conhecimento de todas as conversas e tipos de comportamento do mundo’” (HARDING, 2014, s/p).

Em seu trabalho, que exigia a maior discrição e sigilo, Snowden percebeu a constante vigilância que era feita por parte do governo norte-americano, não só no exterior daqueles considerados “rivais políticos” ou “aliados que deveriam acompanhar de perto”, mas a vigilância ocorria também em meio a própria população norte-americana, com o envolvimento de grandes empresas do setor de telecomunicações tais como Facebook, Microsoft, Google e até mesmo a Apple (HARDING, 2014). A Agência Nacional de Segurança (NSA), dessa forma, tinha acesso aos servidores de grandes e bem posicionadas empresas tecnológicas, e Edward Snowden tinha acesso a todas essas informações.

A partir do livre acesso que tinha aos programas de vigilância promovidos pela NSA e do desgaste que observava em seu ambiente de trabalho, Snowden, depois de refletir sobre suas ações – e as decepções com seu governo –, resolveu fazer uma denúncia pública revelando provas a respeito do funcionamento de programas de vigilância norte-americanos, tais como o *PRISM*, *Boundless Informant*, *X-Keyscore* e o *Stateroom*⁶⁶. Além destes últimos que ficaram conhecidos após o caso Snowden, também destacamos os programas *Muscular* e *Tempora*, programas utilizados em cooperação com o Reino Unido na promoção de uma vigilância sistemática (OLIVEIRA FRAZÃO, 2016).

Snowden deixou o Japão em 2012 para começar a trabalhar no Havaí no *US Cryptological System Group* (Grupo de Sistema Criptográfico dos EUA), onde começou, em

⁶⁶ Todos estes programas citados se utilizavam do ciberespaço para: monitorar o comportamento, a troca de mensagens, e a principal rede de amigos de usuários na Internet; interceptar ligações e chamadas de vídeo; compreender, inclusive, por quais lugares as pessoas se deslocavam, onde passavam a maior parte do tempo, etc. (OLIVEIRA FRAZÃO, 2016).

segredo, a compilar informações ultrassecretas e se organizar a respeito da denúncia que faria no ano seguinte (HARDING, 2014).

Quando no Havaí, Snowden trabalhava com questões sensíveis de criptografia para a NSA e, segundo Harding (2012), mesmo sabendo das consequências que isso traria, se organizou da forma mais discreta possível para entrar em contato com jornalistas que expusessem os abusos dos programas de vigilância norte-americanos. O jornalista esclareceu: “O plano era fazer contato de forma anônima com jornalistas interessados nas liberdades civis. Jornalistas cujas credenciais e integridade não pudessem ser postas em dúvida. E vazar para eles documentos ultrassecretos roubados [...]” (HARDING, 2014, s/p).

O objetivo da exposição planejada por Edward Snowden era provar que ocorriam atividades ilegais que se intensificavam cada vez mais e ameaçavam a privacidade de pessoas em todo o mundo (HARDING, 2014; OLIVEIRA FRAZÃO, 2016). Distintamente dos *WikiLeaks*, Snowden não planejava revelar todos os arquivos de forma indiscriminada, pois acreditava que isso colocava em risco pessoas envolvidas nos casos de espionagem.

O contato com profissionais do jornalismo interessados nas liberdades civis contribuiu no processo de exposição. Conforme avaliou Luke Harding: “[...] [Snowden] queria entregar uma seleção do material a repórteres e deixá-los exercer seu próprio julgamento editorial” (HARDING, 2014, s/p).

Foi então que Edward Snowden contatou os jornalistas do portal The Guardian Laura Poitras⁶⁷ e Glenn Greenwald⁶⁸ solicitando um encontro em Hong Kong, onde ele apresentaria algumas das provas de cooperação em vigilância entre os EUA e o Reino Unido, assim como o envolvimento de grandes empresas do setor tecnológico no fornecimento de informações particulares (HARDING, 2014; GREENWALD; POITRAS, 2013).

Em junho de 2013 começaram as publicações dos arquivos compilados por Snowden com ajuda dos jornalistas do The Guardian. Uma equipe de redação ficou responsável pela análise dos documentos e da elaboração das matérias para o portal The Guardian, respeitando

⁶⁷ Jornalista investigativa e cineasta. Fundou, em 2013 o site de notícias independente The Guardian.

⁶⁸ Greenwald é advogado especialista em liberdade de expressão e jornalista. Em 2005 iniciou um blog para denunciar abusos cometidos por instituições do governo norte-americanos, tais como a CIA. Ganhou notoriedade após o caso Snowden, em 2015, ao contribuir para a exposição da NSA. No Brasil, é conhecido pela exposição de documentos da participação de partes interessadas na Operação Lava-Jato (conhecida popularmente como “Vaza-Jato”), revelando conflito de interesses entre os envolvidos.

a proteção de alguns nomes envolvidos que poderiam correr risco de vida, de acordo com Snowden (HARDING, 2014).

Duas matérias ganharam grande notoriedade naquele mês: a primeira revelava a conspiração entre Reino Unido e Estados Unidos na prática de quebra de criptografias que protegiam a privacidade de usuários na Internet, seja através de e-mails, sites ou aplicativos no roubo de suas informações (BALL; BORGER; GREENWALD, 2013).

A segunda reportagem exclusiva do The Guardian expôs a relação da Agência Nacional de Segurança norte-americana com grandes empresas de tecnologia, tais como Google, Facebook e Apple, na coleta das informações geradas por usuários que estavam sendo vigiados através do programa PRISM (GREENWALD; MACASKILL, 2013).

Até a empresa de telecomunicações norte-americana Verizon Communications foi forçada a gravar e entregar os dados de telefonemas de milhares de norte-americanos à NSA, como registrado em um documento “*top secret*” revelado pelo jornal The Guardian (GREENWALD, 2013).

Ao que se refere ainda ao programa PRISM de vigilância revelado nos documentos de Snowden, os jornalistas afirmaram, em matéria ao The Guardian:

O acesso da NSA faz parte de um programa não divulgado chamado PRISM, que permite às autoridades coletar material, incluindo histórico *de pesquisas, conteúdo de e-mails, transferência de arquivos* e bate-papos ao vivo, de acordo com o documento (GREENWALD; MACASKILL, 2013, s/p, tradução nossa⁶⁹, grifo nosso).

Foi então que mais informações foram vazadas e publicadas pela mídia. Os casos de invasão de privacidade e vigilância eram internacionais, mas também ocorriam em larga escala no próprio território dos Estados Unidos (HARDING, 2014).

As exposições não revoltaram somente os cidadãos norte-americanos. Os documentos de Edward Snowden também revelaram um esquema de espionagem por parte dos Estados Unidos em diversos países da América Latina e Europa (HARDING, 2014). Houve, inclusive, monitoramento e registro de conversas da chanceler alemã Angela Merkel e da presidente do Brasil à época Dilma Rousseff.

⁶⁹ No original: “The NSA access is part of a previously undisclosed program called Prism, which allows officials to collect material including search history, the content of emails, file transfers and live chats, the document says” (GREENWALD; MACASKILL, 2013, s/p).

Na medida em quem Glenn Greenwald tinha residência no Brasil à época dos vazamentos e obteve informações sobre o país através dos documentos, ele colaborou com jornalistas brasileiros na exposição do esquema de espionagem da NSA na América Latina.

O jornal O Globo chegou a fazer uma reportagem exclusiva a respeito dos documentos expostos por Edward Snowden:

O Brasil, com extensas redes públicas e privadas digitalizadas, operadas por grandes companhias de telecomunicações e de internet, aparece destacado em mapas da agência americana como alvo prioritário no tráfego de telefonia e dados (origem e destino), ao lado de nações como China, Rússia, Irã e Paquistão. É incerto o número de pessoas e empresas espionadas no Brasil. Mas há evidências de que o volume de dados capturados pelo sistema de filtragem nas redes locais de telefonia e internet é constante e em grande escala (GREENWALD; KAZ; CASADO, 2013, s/p).

Os jornalistas do O Globo José Casado e Roberto Kaz ainda revelaram, a partir dos documentos ultrassecretos vazados, que existiu no Brasil, pelo menos até o ano de 2002, uma base em conjunto da NSA e da CIA, responsável por monitorar e coletar informações de interesse ao governo norte-americano. Os jornalistas denominaram tal base como uma “estação de espionagem” (KAZ; CASADO, 2013).

Em julho de 2013 continuaram as revelações dos documentos da Agência Nacional de Segurança norte-americana: a inteligência do governo Obama estava monitorando ligações, inclusive, da presidente à época Dilma Rousseff.

Em reportagem exclusiva da Rede Globo, jornalistas expuseram Dilma Rousseff e o presidente do México em 2013 Enrique Peña Nieto como alvos de espionagem norte-americana (G1, 2013). Tais acontecimentos obtiveram grande repercussão na mídia brasileira, gerando, inclusive, um desconforto diplomático na relação Brasil-Estados Unidos.

Edward Snowden não se manteve no anonimato e se apresentou como o *whistleblower* oficial da NSA. O jornal The Guardian foi o responsável por revelar a identidade de Snowden a pedido dele: “Desde o momento em que decidiu divulgar numerosos documentos ultrassecretos ao público, ele estava determinado a não optar pela proteção do anonimato. ‘Não tenho a intenção de esconder quem sou, pois sei que não fiz

nada de errado’ diz ele” (GREENWALD; MACASKILL; POITRAS, 2013, s/p, tradução nossa⁷⁰).

Desde então, Snowden se mantém asilado na Rússia, pois é considerado um criminoso pelas autoridades norte-americanas (HARDING, 2014). Mas as consequências de seus atos que ficaram conhecidos como “O Caso Snowden” ou “Os Arquivos Snowden” internacionalmente, vão além do debate “Edward Snowden cometeu um crime ou não? ”.

Estudiosos do caso Snowden, assim como parte da comunidade internacional, entendem que os programas de vigilância promovidos extensivamente pela NSA “ultrapassam qualquer fronteira de direito, moral ou ética que se possa apregoar” (OLIVEIRA FRAZÃO, 2016, p. 72).

Apesar de muitas respostas internacionais condenarem as condutas tanto de Snowden quanto da Agência Nacional de Segurança norte-americana, a NSA, houve uma declaração aberta de apoio à vigilância dos EUA por parte do presidente russo Vladimir Putin que, inclusive, alegou que “gostaria de possuir um programa semelhante” (OLIVEIRA FRAZÃO, 2016, 95). Mas, desde então, observa-se uma tendência de utilizar os meios de comunicação de maneira mais responsável e uma tentativa, por parte das grandes empresas e marcas, em garantir a proteção e sigilo dos dados de seus consumidores.

O caso Snowden repercutiu no debate a respeito da segurança no ciberespaço e, por este motivo, foi apresentado em nossa presente investigação. Não é o foco deste trabalho se debruçar em todos os pormenores que envolveram o vazamento de arquivos ultrassecretos pelo ex-analista de sistemas da NSA, mas sim desejamos compreender algumas das principais consequências de seus atos e suas implicações no contexto brasileiro de promoção da cibersegurança.

Gostaríamos de destacar dois pontos que podemos interpretar a partir das informações apresentadas a respeito do caso Snowden.

O primeiro deles é a presença do Estado no ciberespaço. O caso Snowden deixou clara a atuação do governo dos EUA no ciberespaço com o objetivo final de manutenção da segurança e integridade do país. Podemos inferir, inclusive, que leis americanas tais como o

⁷⁰ No original “From the moment he decided to disclose numerous top-secret documents to the public, he was determined not to opt for the protection of anonymity. ‘I have no intention of hiding who I am because I know I have done nothing wrong’, he said” (GREENWALD; MACASKILL; POITRAS, 2013, s/p).

*Patriot Act*⁷¹ dão ensejo para que ações de vigilância, monitoramento e espionagem sejam promovidas de forma “ultrassecreta” e constante.

Ou seja, o ciberespaço passou a estar cada vez mais presente na pauta de segurança dos Estados Unidos e houve, conforme entendemos, uma militarização do ciberespaço por parte deste governo, na medida em que a NSA, a Agência Nacional de Segurança norte-americana, é parte do Departamento de Defesa dos Estados Unidos.

O segundo ponto que podemos elucidar diz respeito a uma comparação entre as abordagens de Julian Assange, do *WikiLeaks*, e de Edward Snowden e sua parceria com o *The Guardian*. Ao que se refere ao *WikiLeaks*, todos os arquivos de que tiveram acesso estão disponíveis em seu portal e na íntegra, ao contrário da abordagem de Snowden de tentar preservar alguns dos nomes presentes nos arquivos, focando em expor, principalmente, a Agência qual trabalhava e os governos dos Estados Unidos e Reino Unido.

Dentre os documentos que foram – e ainda são – divulgados pelo *WikiLeaks*, alguns revelam locais vitais para a segurança norte-americana o que, pode ser argumentado, coloca em risco algumas das bases militares dos EUA e as pessoas que lá trabalham (G1, 2010a).

Harding (2014) afirmou em seu livro que Snowden no passado chegou a condenar as atividades do *WikiLeaks* de exposição de arquivos de Segurança Nacional e anos depois esteve envolvido em um caso parecido. A diferença foi o tratamento que Snowden deu às informações das quais tinha acesso (HARDING, 2014, s/p).

Outra diferença que entendemos entre os casos *WikiLeaks* e Snowden é que Julian Assange, apesar de ter seu nome divulgado na mídia e considerado culpado pelos vazamentos do site pois foi o fundador do portal, quem ganhou notoriedade foi o site *WikiLeaks*, enquanto Edward Snowden, desde o início, se assumiu como o *whistleblower* oficial da NSA e foi seu nome que ficou conhecido e estampado quando se apresentavam os “Arquivos Snowden”.

Entretanto, podemos perceber semelhanças em ambos os casos. Edward Snowden e Julian Assange expuseram os Estados Unidos e o envolvimento de outros países em esquemas inadequados por acreditarem que a população tinha o direito de saber a verdade de que tinham acesso. Apesar de haver, como se debate, um dilema moral na exposição de

⁷¹ Nome pelo qual ficou conhecido a Lei Pública 107-56 de 2001 assinada pelo ex-presidente norte-americano George W. Bush após os eventos do 11 de setembro de 2001. Esta lei permitiu que houvesse a interceptação de informações (contidas em ligações ou e-mails, por exemplo) pelo governo dos Estados Unidos sem autorização de nenhum órgão de Justiça desde que houvesse a suspeita de atos de terrorismo.

documentos sigilosos, é inegável que os acontecimentos de 2010 e 2013 estimularam que discussões a respeito da presença do Estado no ciberespaço se intensificassem por parte da sociedade civil.

É possível, inclusive, traçar um paralelo com a realidade brasileira ao analisar este caso. Isto, pois, após as exposições de 2013 obtivemos, em 2014, o Marco Civil da Internet⁷², elaborado a partir da colaboração da sociedade civil e que garantia alguns direitos aos usuários da Internet, bem como foi o Marco Civil que estabeleceu as diretrizes e os limites da ação do Estado na Internet (BRASIL, 2014a).

⁷² O projeto do Marco Civil da Internet surgiu, inicialmente em 2009, mas foi promulgado como lei somente em março de 2014, já no governo Dilma.

3.6 o caso Lázarus (2014)

O caso que buscamos elucidar a seguir não se trata de um episódio de ciberataque como os que previamente apresentamos neste capítulo. Lázarus é um grupo organizado por *hackers* mal-intencionados que agem no ciberespaço e criam *malwares*. Apesar de não se saber muito a respeito de quem são as pessoas envolvidas no grupo Lázarus, especula-se que são uma organização que age da Coreia do Norte e que existe, ao menos, desde 2009, quando houve um ataque direcionado ao ciberespaço sul-coreano.

Grupos que trabalham na área da Segurança da Informação identificaram que certos ataques de Negação de Serviço Distribuído (DDOS) advindos da Coreia do Norte tiveram como alvo *websites* da Coreia do Sul para tirá-los do ar (SANG-HUN; MARKOFF, 2009). Apesar de ser um ataque considerado pouco sofisticado, foi o primeiro registro de atuação do grupo Lázarus.

Em 2013, novos ataques dirigidos à Coreia do Sul foram efetuados. Nesta ação, agora mais sofisticada, as manobras de DDOS derrubaram diversos sites oficiais do governo sul-coreano e outras mídias do país. O incidente ocorreu no aniversário de 63 anos do início da Guerra da Coreia, responsável por dividir o país entre Norte e Sul (BBC, 2013). Novamente, atribuiu-se ao grupo Lázarus a autoria destes ataques que também chegaram a afetar cerca de 32 mil computadores sul-coreanos.

Os ataques não se limitaram ao uso do Negação de Serviço Distribuído para comprometer máquinas, mas também se utilizaram de um vírus de computador. De acordo com o que foi noticiado pelo The New York Times:

O *malware* é chamado “DarkSeoul” no mundo da informática e foi identificado pela primeira vez há cerca de um ano. O objetivo é evitar alguns dos produtos antivírus mais populares da Coreia do Sul e tornar os computadores inutilizáveis (SANG-HUN, 2013, s/p, tradução nossa⁷³).

Este ataque de 2013 chegou a comprometer o funcionamento dos Caixas 24 horas (os chamados ATM) na Coreia do Sul, assim como alguns canais de notícias (SANG-HUN, 2013).

Apesar de atualmente o ataque de 2013 ser atribuído ao grupo Lázarus, o que observamos lendo as notícias a respeito dele é que se coloca a “Coreia do Norte” como

⁷³ No original “The malware is called ‘DarkSeoul’ in the computer world and was first identified about a year ago. It is intended to evade some of South Korea’s most popular antivirus products and to render computers unusable” (SANG-HUN, 2013, s/p).

responsável pelo ataque, pressupondo que as autoridades do país (e seu próprio líder Kim Jong-un) como os autores e não um grupo independente (TALLEY; VOLZ, 2019; SANG-HUN, 2013). Por conta do anonimato e da dificuldade de encontrar responsáveis por ataques cibernéticos, especialmente em um país mais fechado como a Coreia do Norte, torna-se complexo descrever com exatidão o que os ataques significaram de fato.

O que se pode inferir pelo contexto em que o ataque ocorreu é que tais investidas cibernéticas podem ter sido uma resposta aos exercícios de forças sul-coreanas que ocorreram no ciberespaço naquela mesma semana (SANG-HUN, 2013). Como afirmou a jornalista Sang-Hun para o jornal *The New York Times*: “Os ataques na quarta-feira ocorreram alguns dias após a Coreia do Norte culpar a Coreia do Sul e os Estados Unidos por ataques a alguns de seus *websites*” (SANG-HUN, 2013, s/p, tradução nossa⁷⁴).

O caso de ciberataque que ganhou maior atenção, no entanto, ocorreu no ano seguinte, em 2014. Novamente associado ao grupo norte-coreano Lázarus, o ataque ao sistema da Sony Pictures⁷⁵ ficou conhecido internacionalmente. É por este motivo que discriminamos o ano de 2014 em nossa linha do tempo como principal episódio atribuído o grupo Lázarus⁷⁶.

O ataque à Sony Pictures em 2014 ocorreu na tentativa, por parte da organização, de evitar que o filme “A Entrevista” (*The Interview*) fosse distribuído. O filme foi uma comédia gravada nos Estados Unidos e trazia um personagem que satirizava o líder norte-coreano Kim Jong-un que, segundo a estória, deveria dar uma entrevista à dois jornalistas norte-americanos. O enredo do filme se caracterizou pelo recrutamento, por parte da CIA, dos dois jornalistas que, ao invés de fazer a entrevista, foram na realidade incumbidos de assassinar o líder norte-coreano.

O ciberataque ao sistema da Sony Pictures não só falhou em evitar que o filme fosse distribuído em 2014 como ainda atraiu mais atenção à produção. Não obstante, o ataque provocou resposta dos Estados Unidos. Como afirmaram Haggard e Lindsay: “[...] a reação do governo dos Estados Unidos foi sem precedentes, resultando na primeira atribuição de um

⁷⁴ No original: “The cyberattacks on Wednesday came just days after North Korea blamed South Korea and the United States for attacks on some of its Web sites” (SANG-HUN, 2013, s/p).

⁷⁵ Nota-se que a Sony Pictures Entertainment fica na Califórnia, nos Estados Unidos, enquanto a Sony Corp. tem sua base no Japão. O ciberataque que aqui descrevemos ocorreu no sistema da Sony Pictures Entertainment.

⁷⁶ Atualmente o ataque é atribuído ao Lázarus, mas, à época, quem assinava os ataques e as ameaças à Sony Pictures eram os “*Guardians of the Peace*” (Guardiões da Paz). Foi recorrente nos trabalhos lidos que se encontrasse menção a sua sigla (GOP) e, por isso, destacamos este detalhe aqui também.

ciberataque a um Estado feita por um presidente norte-americano, bem como em medidas modestas de retaliação” (HAGGARD; LINDSAY, 2015, p. 02, tradução nossa⁷⁷).

A menos de um mês antes da data prevista para a exibição de “A Entrevista” nos cinemas, a Sony Pictures, portanto, sofreu um ataque cibernético que expôs uma grande quantidade de dados confidenciais da empresa e ainda foi capaz de causar danos aos computadores (DESIMONE; HORTON, 2017). Ademais, ameaças anônimas foram feitas à Sony Pictures pelos agressores.

Ressaltamos que ainda na época do lançamento do trailer do referido filme, em junho de 2014, a produção causava desconfortos internacionais. O embaixador norte-coreano das Nações Unidas Ja Song-nam enviou uma carta ao então Secretário-Geral Ban Ki-moon (que, por sua vez, é sul-coreano) apresentando suas queixas a respeito do tratamento da Coreia do Norte e de Kim Jong-un na produção norte-americana (DESIMONE; HORTON, 2017).

Além dessa queixa à nível das Nações Unidas, o chefe executivo da Sony Corp., sede japonesa, também apresentou certo descontentamento com a controvérsia que a exibição do filme poderia gerar (como, inclusive, foi revelado pelos documentos vazados durante o ciberataque), mas nenhuma medida foi tomada visando à censura do filme (DESIMONE; HORTON, 2017).

A sofisticação do grupo que promoveu o ataque provavelmente contou com semanas de planejamento e organização dos usuários envolvidos. DeSimone e Horton (2017) expuseram em seu estudo de caso:

A URL que conectou aos servidores da Sony – a URL no domínio spe.sony.com – indicou que os envolvidos no ataque comprometeram a rede em nível que os permitiu usar o nome da Sony na Internet de forma pública. Os agressores reivindicaram ter pego um grande volume – 100 terabytes – de dados. O que se observou em uma última análise foi a distribuição de cerca de 200 gigabytes (DESIMONE; HORTON, 2017, p. 05, tradução nossa⁷⁸).

Para que o grupo obtivesse acesso a essa quantidade de dados a serem expostos da Sony Pictures, semanas antes eles se utilizaram de uma manobra muito comum em crimes

⁷⁷ No original: “[...] the reaction of the US government was unprecedented, resulting in the first-ever attribution of a cyber attack to a nation state by a US president as well as modest retaliatory measures” (HAGGARD; LINDSAY, 2015, p. 02).

⁷⁸ No original “The URL that linked to Sony’s servers—the URL in the spe.sony.com domain—indicated that the attackers compromised the network to a degree that allowed them to use Sony’s namespace on the public internet. The attackers claimed to have taken a huge volume—100 terabytes—of data; ultimately, roughly 200 gigabytes was released” (DESIMONE; HORTON, 2017).

cibernéticos que é o *phishing*⁷⁹. Como afirmaram DeSimone e Horton: “Os agressores acessaram a rede da Sony através do envio de e-mails *phishing* aos empregados da Sony com *websites* falsos criados para colher as credenciais destes servidores e ganhar acesso aos sistemas da Sony” (DESIMONE; HORTON, 2017, p. 06, tradução nossa⁸⁰).

Foi a partir da prática de *phishing* que o grupo malicioso se infiltrou no sistema da Sony e ali permaneceu, roubando informações, continuando com pequenos ataques e comprometendo cada vez mais o sistema (DESIMONE; HORTON, 2017). Comprometer e danificar as máquinas, conforme entende-se, eram os principais objetivos do grupo com o ciberataque: “Uma vez que os dados da Sony foram exfiltrados, os agressores modificaram os computadores e servidores da Sony de uma forma que maximizou sua ruptura. O ataque incluiu um comprometimento ao disco rígido do sistema [...]” (DESIMONE; HORTON, 2017, p. 06, tradução nossa⁸¹).

O grupo fazia ameaças à Sony Pictures, exigindo que o filme “A Entrevista” não fosse lançado, mas a Sony seguiu com a decisão de exibir a produção (HAGGARD; LINDSAY, 2015). A data prevista para a estreia do filme era 16 de dezembro de 2014 e, na semana anterior, chegaram ameaças inclusive aos cinemas que exibiriam o filme, como afirmaram Haggard e Lindsay: “[o grupo] fez ameaças veladas aos cinemas onde ‘A Entrevista’ estava programado para estrear, com um aviso ‘Lembrem-se de 11 de setembro de 2001’” (HAGGARD; LINDSAY, 2015, p. 02, tradução nossa⁸²).

Estudiosos do caso afirmam que o ataque a Sony não foi tão sofisticado e complexo quanto o caso Stuxnet que ocorreu anteriormente no Irã, mas que foi planejado e bem executado. É possível inferir que o grupo também tinha o objetivo de causar danos financeiro à Sony Pictures com o ciberataque (HAGGARD; LINDSAY, 2015; DESIMONE; HORTON, 2017).

⁷⁹ Usuários mal-intencionados se utilizam de mensagens, sites ou formulários que parecem legítimos para roubar informações pessoais e senhas. Tais mensagens podem chegar via e-mail, por exemplo e a vítima, voluntariamente, preenche com suas informações pessoais.

⁸⁰ No original: “The attackers accessed the Sony network by sending phishing emails to Sony employees and established phony websites to harvest credentials and gain access to Sony systems” (DESIMONE; HORTON, 2017, p. 06).

⁸¹ No Original: “Once Sony’s data had been exfiltrated, the attackers modified Sony’s computers and servers in a way that maximized disruption. The attack included corruption of the systems’ disk drives” (DESIMONE; HORTON, 2017, p. 06).

⁸² No original: “[...] GOP made veiled threats to attack theaters where *The Interview* was scheduled to open, with a warning to “Remember the 11th of September 2001” (HAGGARD; LINDSAY, 2015, p. 02).

O caso provocou uma reação do presidente dos Estados Unidos à época, Barack Obama, que chegou a estabelecer sanções contra a Coreia do Norte e colocou o FBI para investigar o caso (HAGGARD; LINDSAY, 2015; DESIMONE; HORTON, 2017). Obama chegou a afirmar, inclusive, em pronunciamento oficial, que a invasão ao sistema da Sony foi “um ato de cyber-vandalismo” como foi noticiado na BBC à época (BBC, 2014, s/p).

Em termos técnicos, o ataque foi mais complexo do que apresentamos aqui, contudo não cabe detalhar as técnicas do ataque a Sony Pictures, mas, sim compreender suas consequências, bem como levantar questões de cibersegurança que envolvem um grupo organizado e *politizado* como o Lázarus.

Como já afirmamos, essa foi a primeira vez que um chefe de Estado se pronunciou sobre um caso de ciberataque e atribuiu, abertamente, um responsável – no caso a Coreia do Norte –, tomando medidas no nível internacional. Dessa forma, entendemos que o ataque voltado a Sony Pictures em 2014 pode ser importante na compreensão da relevância da cibersegurança para os Estados.

Do ponto de vista da Segurança Internacional, o espaço cibernético foi compreendido como um espaço estrangeiro invadido e, segundo Obama, “vandalizado”, o que justificaria as sanções, ainda que moderadas, feitas àqueles associados ao crime – no caso, a Coreia do Norte.

Tendo em vista a falta de precedentes para nortear a ação do Estado neste ataque, pode-se dizer que um discurso de segurança do espaço cibernético se desenvolveu nos Estados Unidos a partir de então. Isto, pois, atualmente, os Estados Unidos contam com uma Agência de Cibersegurança e Segurança de Infraestrutura (chamada na sigla em inglês de CISA) criada em 2018 e que está subordinada ao Departamento de Segurança Interna dos Estados Unidos (*Department of Homeland Security*).

Quanto ao grupo Lázarus, outros ataques, como por exemplo aquele que ficou conhecido como *WannaCry*, também são a eles atribuídos, mesmo que se tenha dificuldade em provar sua responsabilidade. Discutiremos mais a respeito do caso *WannaCry*, que também afetou o Brasil, posteriormente neste capítulo.

3.7 O caso da Ucrânia (2015)

Outro caso importante de ser analisado do ponto de vista da cibersegurança é o ataque que ocorreu a instalações da Ucrânia no ano de 2015. Os ataques cibernéticos que ocorreram no país são um bom exemplo de infraestrutura crítica ameaçada pelo uso da tecnologia.

No dia 23 de dezembro de 2015, pelo menos 250 mil⁸³ pessoas ficaram sem energia elétrica na Ucrânia. Segundo reportado pelos jornais, os trabalhadores das usinas não conseguiam apontar uma falha específica para o acontecimento, pois os geradores funcionavam normalmente (LIMA, 2019). Após uma análise mais detalhada, entendeu-se que as centrais de energia sofreram um ataque cibernético.

O Centro de Estudos de Segurança (CSS), em Zurique, elaborou um *report* sobre o caso que buscou elucidar a estratégia cibernética e as implicações internacionais do caso do ciberataque às instalações elétricas da Ucrânia em 2015, levando em consideração todo o contexto geopolítico à época (BAEZNER, 2018).

Ao que se refere às ferramentas e técnicas, podemos inferir através do estudo supracitado, que foram três delas usadas na agressão: “ataques de Negação de Serviço Distribuído (DDOS), *Website Dafaement*⁸⁴ e infecção por vírus (*malware*) através de *phishing*” (BAEZNER, 2018, p. 10, tradução nossa⁸⁵). Dessa forma, podemos observar que se tentou derrubar o sistema com os ataques de DDOS e de *Dafaement*, enquanto o *phishing* serviu como uma forma de espionagem e roubo de informações (BAEZNER, 2018; LIMA, 2019).

Este caso de ciberataque na Ucrânia ficou entendido como primeiro ataque de *hackeamento* de uma usina elétrica bem-sucedido de que se tem registro, pois comprometeu a infraestrutura do país.

Os ataques e o *malware* (BlackEnergy3) utilizado na operação são atribuídos à Rússia. Isto, pois, sabe-se que os ataques ocorreram após a crise na Crimeia⁸⁶, em 2014, reforçando o histórico conturbado da relação Ucrânia-Rússia dos últimos 30 anos.

⁸³ Os dados que encontramos divergem neste ponto. Os veículos de imprensa divulgaram o número de 700 mil pessoas que tiveram a energia elétrica comprometida de alguma forma na Ucrânia. O relatório do Centro de Estudos de Segurança da Suíça trabalhou com o número de 250 mil pessoas afetadas pelo ataque.

⁸⁴ Ataques cibernéticos que mudam a aparência de um site na Internet com o objetivo de enganar um usuário legítimo ou passar uma mensagem (geralmente, política).

⁸⁵ No original: “DDoS attacks, website defacement and malware infection by spear phishing” (BAEZNER, 2018, p. 10).

⁸⁶ Para mais informações, ver: XAVIER, 2015.

A Ucrânia, que se tornou mais próxima politicamente dos EUA e da Organização do Tratado do Atlântico Norte (OTAN) após a Revolução Laranja⁸⁷ (2004-2005), contou com apoio do país em equipamentos tecnológicos e no treinamento de tropas militares desde então (BAEZNER, 2018; KORYBKO, 2018). Podemos inferir a participação dos EUA, também, na tentativa de investigar os ataques às usinas de energia Ucrânicas em 2015.

Cabe ressaltar que, durante os protestos e crises geradas na Ucrânia entre 2013 e 2015, a Rússia também sofreu com ataques cibernéticos, principalmente ataques de Negação de Serviço Distribuído (DDOS) (BAEZNER, 2018).

No relatório elaborado pelo Centro de Estudos de Segurança, Baezner (2018) ainda afirmou que o *malware* instalado nas máquinas na Ucrânia tinha o objetivo de se espalhar e coletar informações não somente a respeito do governo do país, mas também informações referentes à OTAN.

O episódio do ataque às usinas ucranianas não pode ser analisado de forma isolada, pois é importante compreender o contexto de crise entre Rússia e Ucrânia que vinha ocorrendo desde 2013 com a deposição do presidente ucraniano Víktor Yanukóvytch. Compreendemos que os Estados Unidos e a própria OTAN têm relação com o caso também.

Entretanto, queremos destacar no presente tópico o ataque cibernético em si e suas implicações para a cibersegurança e às relações internacionais.

Tanto este ataque que a Ucrânia sofreu quanto aquele dirigido à Geórgia em 2008 são atribuídos à Rússia. Existem estudos e reportagens que compreendem que sejam “hacktivistas”, ou hackers patriotas, que não têm, necessariamente, uma ligação direta com Kremlin. Ademais, o governo russo nega sistematicamente o envolvimento em investidas cibernéticas.

Não podemos descartar, contudo, uma possível tentativa de demonstração de poder de atuação no ciberespaço por parte da Rússia. Em 2008, houve uma combinação do aparato militar e tecnológico, sendo que este último, em termos pragmáticos, não era necessário para garantir que a Rússia se sobressaísse em relação a Geórgia no caso de uma escalada no conflito. Aquele momento pode ser inferido como um teste e também demonstração de poder, como já argumentamos, ao Ocidente.

⁸⁷ Para mais informações, ver: KORYBKO, 2018.

O episódio em 2015 também ocorreu em meio a uma crise política envolvendo Ucrânia, Crimeia, a Rússia e, como entendemos, também a opinião pública do Ocidente. Se utilizar de um ataque cibernético é economicamente mais barato do que uma campanha militar, pode ser eficiente quanto aos seus objetivos e mais difícil de se atribuir uma autoria. Por estes motivos, podemos argumentar que países como a Rússia podem ver no investimento em tecnologia (e em cibersegurança) um meio de se fortalecer nos campos da Segurança e Defesa.

Entendemos que existem elementos de geopolítica que envolvem a influência da Rússia em seu entorno e na região do Cáucaso, mas, em termos de Segurança Internacional e tecnologia da informação, podemos entender, do ponto de vista da Securitização, que eventos como os de 2015 facilitaram que discursos de segurança do ciberespaço sejam promovidos e o investimento em cibersegurança cresça cada vez mais, como, inclusive, efetivamente cresceu na última década (MORGAN, 2019).

O caso da Ucrânia, assim como o Stuxnet no Irã, oferece *insights* para compreender a justificativa da cibersegurança, especialmente no Brasil. Quando se pauta a segurança do setor cibernético na proteção de “Infraestruturas Críticas”, pode-se justificar quaisquer medidas tomadas no setor, com uma definição de infraestrutura crítica tão ampla como a do Brasil (que apresentamos em nossa introdução).

Uma última reflexão que podemos perceber é que os ataques cibernéticos a infraestruturas críticas, tais como as usinas elétricas na Ucrânia e os reatores no Irã, têm motivações políticas. É necessário olhar todo o contexto que se inserem, mas é possível inferir, principalmente a partir destes dois casos, o uso eficiente e eficaz da tecnologia em ataques sofisticados e com alvos definidos.

3.8 O caso *WannaCry* (2017)

Um dos últimos casos mais emblemáticos envolvendo a cibersegurança que chegou, inclusive, a afetar a população brasileira, foi a disseminação do *ransomware* *WannaCry*⁸⁸, responsável por explorar uma vulnerabilidade de computadores com o sistema operacional Windows, principalmente em suas versões mais antigas.

Um *ransomware* é uma variação de um *malware* na forma de programa de computador (*software*) nocivo com um objetivo específico: ao explorar as vulnerabilidades da máquina que infecta, restringe o acesso ao sistema, bloqueando-o. Há uma espécie de “sequestro” das máquinas remotamente. Para que haja o desbloqueio do sistema, é exigido que o usuário pague um “resgate” ou cumpra com as exigências do cyberagressor.

Em 12 de maio de 2017, o mundo experimentou um ataque usando um *ransomware* que ficou conhecido como *WannaCry*. À época que o ataque ocorreu, acreditava-se que cerca de 75 países tinham sido afetados pelo *WannaCry*, mas após análises mais detalhadas no ano seguinte, chegou-se ao dado de que pelo menos 150 países obtiveram prejuízos com a infecção do *ransomware* e mais de 300 mil sistemas foram afetados (G1, 2017; RODRIGUES, 2018; AKBANOV; VASSILAKIS; LOGOTHETIS, 2019).

Usuários mal-intencionados que criaram o *WannaCry* se aproveitaram de uma vulnerabilidade do sistema Windows e, sem precisar ter contato com os usuários destes sistemas, conseguiram infectar suas máquinas. O *ransomware* bloqueou milhares de máquinas pedindo resgate em *bitcoins*, moeda criptografada, para que o computador fosse liberado (AKBANOV; VASSILAKIS; LOGOTHETIS, 2019).

Ao que se refere ao valor pedido pelos agressores, inicialmente pediam o equivalente a US\$ 300,00 em *bitcoins* e, mais tarde, o valor dobrou para US\$ 600,00 equivalentes em *bitcoins*. Caso não se cumprisse tal exigência em até três dias, os criadores do *ransomware* ameaçavam apagar todos os arquivos da máquina permanentemente (AKBANOV; VASSILAKIS; LOGOTHETIS, 2019).

No entanto, não havia garantia que de os arquivos seriam recuperados mesmo diante do pagamento.

⁸⁸ O nome *WannaCry*, apesar de remeter a uma tradução como “QueroChorar”, na verdade vem da ideia de “*WannaCrypt*”, algo como “QueroCriptografar”. O objetivo do *ransomware*, como veremos, era criptografar as informações dos computadores infectados e impedir o seu acesso.

O episódio ficou marcado como o maior ataque de *ransomware* da história tendo em vista seu alcance (RODRIGUES, 2018). Sabe-se que o ataque “[...] afetou uma ampla variedade de setores, incluindo saúde, governo, telecomunicações e produção de gás e petróleo” (AKBANOV; VASSILAKIS; LOGOTHETIS, 2019, p. 114, tradução nossa⁸⁹).

Meses antes do ataque ocorrer mundialmente, o Windows tinha conhecimento da vulnerabilidade de seu Sistema Operacional e lançou os chamados *patches*, que são atualizações para prevenir máquinas de ataques maliciosos. Mas muitos não atualizaram seu sistema e foram vítimas do ataque. Ademais, repartições públicas, como no caso do Brasil, por exemplo, ainda usam máquinas e sistemas operacionais antigos que, muitas vezes, já perderam o suporte oficial do sistema operacional do Windows e não recebem mais atualizações de segurança (RODRIGUES, 2018; G1, 2017).

Este caso de 2017 causou prejuízos mundialmente, como afirmou Rodrigues, funcionário da Kaspersky Labs:

A montadora Renault fechou sua maior fábrica na França e os hospitais do Reino Unido tiveram de rejeitar pacientes. Já no Brasil, o ataque causou a interrupção do atendimento do INSS, além de afetar empresas e órgãos públicos de 14 Estados mais o Distrito Federal (RODRIGUES, 2018, s/p).

No caso do Instituto Nacional do Seguro Social (INSS), o órgão parou de funcionar durante todo o dia, inclusive em seu atendimento da Central 135, serviço feito por telefone (G1, 2017).

Entre os setores públicos brasileiro afetados, teve-se, além do INSS, o IBGE, o Itamaraty, o Ministério Público de São Paulo e a Petrobrás. Igualmente, os Tribunais da Justiça do Amapá, Bahia, Mato Grosso do Sul, Minas Gerais, Piauí, Rio Grande do Norte, Roraima, Santa Catarina, São Paulo e Sergipe também foram afetados pelo *WannaCry*, de acordo com o que foi reportado pelo portal de notícias G1 (2017).

Dessa forma, podemos afirmar que, no caso do Brasil, o setor público foi o mais afetado pelo ataque do *ransomware* *WannaCry* por conta do uso de sistemas Windows desatualizados. Ressaltamos que computadores pessoais também podem ter sido afetados durante o ataque, mas que pouco se reportou sobre isso.

⁸⁹ No original: “The attack affected a wide range of sectors, including healthcare, government, telecommunications and gas/oil production” (AKBANOV; VASSILAKIS; LOGOTHETIS, 2019, p. 114).

Os prejuízos causados pelo *WannaCry* foram contabilizados durante todo o mês de maio de 2017. De acordo com Rodrigues: “O país mais afetado foi a Rússia, com 33,64% das empresas afetadas, seguido do Vietnã (12,45%) e Índia (6,95%). O Brasil foi o sexto mais atacado (4,06%)” (RODRIGUES, 2018, s/p).

Por se tratar de um caso recente, a infecção pelo *WannaCry* ainda possui pouca literatura a seu respeito, especialmente no que tange seus efeitos nas relações internacionais. No caso do Brasil, o então presidente interino Michel Temer não fez um pronunciamento oficial sobre o caso, mas tampouco o fizeram outros chefes de Estado.

Na semana do ataque, Neil Walsh, chefe do *Cyber and Emerging Crime* no UNODC, Escritório das Nações Unidas para Drogas e Crimes, fez um pronunciamento sobre o *WannaCry*, afirmando que poderia “ter sido evitado” com investimentos em cibersegurança e máquinas mais atuais, por exemplo (UN NEWS, 2017, s/p). O objetivo de Walsh era alertar os Estados a respeito da seriedade de crimes cibernéticos e o investimento na segurança.

Podemos, ainda, inferir que o caso foi amplamente estudado por especialistas da Tecnologia da Informação sobre seu funcionamento e sua sofisticação, bem como seus efeitos globais.

Os dados destes estudos evidenciam que questões envolvendo a Tecnologia da Informação e a cibersegurança devem receber atenção especial na medida em que cresce a dependência da informatização e a digitalização de dados por empresas privadas e órgãos públicos (AKBANOV; VASSILAKIS; LOGOTHETIS, 2019; RODRIGUES, 2018).

Como até aqui argumentamos, é difícil reconhecer os responsáveis por ciberataques, bem como penalizá-los pelo prejuízo que causam. No caso da disseminação do *WannaCry*, até o presente momento não se tem um país ou um grupo assumidamente responsável. À época dos ataques, o chefe da Microsoft acusou a Coreia do Norte pelo *WannaCry*, o que nos leva a entender que muitos associaram esses eventos ao grupo Lázarus, que supostamente age naquele país (HARLEY, 2017).

Pelo que se sabe até o momento, não tem como garantir que o *ransomware* foi disseminado pelo grupo Lázarus, apesar de se ter investigações neste sentido feitas pelos serviços de inteligência norte-americana.

3.9 Considerações a respeito do contexto internacional

A apresentação dos principais casos de ameaças cibernéticas neste capítulo foi breve, com o objetivo de inferir alguns elementos da cibersegurança e sua relação com as relações internacionais, bem como inferir a construção do discurso de segurança cibernético ao tomar como exemplo tais casos.

Os casos da Estônia e da Geórgia postularam ataques de Negação de Serviço Distribuído (DDOS) como uma das práticas mais comuns e eficientes para “derrubar” sites e passar mensagens que podem ser políticas ou não. Nos anos de 2007 e 2008, conforme entendemos, uma rede de hacktivistas cresceu, especialmente no Leste Europeu e na Rússia.

Foi no ano de 2008 no Brasil que a Estratégia Nacional de Defesa (END) foi publicada e o setor cibernético colocado como estratégico para a Defesa e Segurança do país, dialogando com uma tendência internacional de atenção ao ciberespaço. Conforme observado em documentos vazados pelo portal *WikiLeaks*, o embaixador dos Estados Unidos no Brasil chegou a comentar a respeito da publicação do Decreto que aprovou a END, reportando às autoridades norte-americanas sobre as possibilidades de aproximação e distanciamento do Brasil.

Entendemos que os vazamentos destes documentos em 2010 só reafirmaram a necessidade do preparo do Brasil em questões de inteligência e segurança. Como veremos no próximo capítulo, o ano de 2010, por sua vez, foi importante para o processo de cibersegurança no Brasil na medida em que foi aprovado, por parte do Ministério da Defesa, a criação do Centro de Defesa Cibernético e do Núcleo (CDCiber) do Centro de Defesa Cibernético (NuCDCiber).

Foi no ano de 2010, também, que ocorreu o ataque aos reatores no Irã com o sofisticado vírus Stuxnet, capaz de causar danos materiais às máquinas. Este episódio obteve grande repercussão internacional e continua sendo estudado tanto por especialistas da área da Tecnologia da Informação quanto das Relações Internacionais, dada sua complexidade, inovação e efeitos políticos e estratégicos no Irã e em seu entorno.

Já em 2013, o caso Snowden ganhou notoriedade mundial com o vazamento dos arquivos do principal órgão de Segurança dos EUA. Dentre os arquivos, tinham-se registros de espionagem que ocorriam no Brasil. Em 2013, o Ministério da Defesa brasileiro já havia

implementado o CDCiber e o NuCDCiber que estavam se preparando para a Copa do Mundo FIFA de Futebol que ocorreria em 2014 no Brasil.

Oficialmente, o CDCiber e o NuCDCiber, como veremos no capítulo subsequente, foram projetados e usados como teste na garantia da segurança neste evento e nas Olimpíadas de 2016, que também ocorreram em solo brasileiro. Funcionaram, como entendemos, como agências de monitoramento e vigilância.

Ademais, em 2014, como produto do Centro de Defesa Cibernético, fora publicada a Doutrina Militar de Defesa Cibernética, consolidando a postura militar adotada na cibersegurança no Brasil.

O que os documentos vazados por Edward Snowden em 2013 provaram foi que o Brasil ainda necessitava de investimentos na área da Segurança da Informação. Ou que pelo menos os Estados Unidos estavam investindo consideravelmente em programas de monitoramento e vigilância, tal-qualmente o período da Guerra Fria.

Finalmente, os ataques de 2015 e 2017 na Ucrânia e mundialmente, respectivamente, exemplificam o uso da tecnologia no comprometimento de infraestruturas críticas, que fizeram com que os países dessem mais atenção a questões de cibersegurança. Evidente que se pode argumentar que os outros episódios analisados também estão relacionados ao comprometimento de infraestruturas críticas, mas os casos da Ucrânia e do *WannaCry* causaram danos materiais com objetivos específicos mensuráveis.

O componente humano, como se pode argumentar, também teve papel nos acontecimentos, especialmente ao ataque à Sony Pictures, em 2014 e no ataque do *ransomware* *WannaCry*, em 2017. Isto, pois, não fossem as pessoas serem vítimas dos ataques de *phishing* ou caso houvessem atualizados seus sistemas Windows, ambos episódios seriam evitados.

Todos estes eventos citados e também a atuação internacional de um grupo mal-intencionado como é o caso do Lázarus, dão ensejo para que o discurso de cibersegurança seja engendrado e legitimado pelos atores envolvidos no sistema. Isso, podemos argumentar, faz parte do processo de Securitização.

No capítulo seguinte, elucidaremos sobre o processo de segurança cibernética no Brasil, apresentando de quais formas se construiu o discurso de cibersegurança, de que forma tal discurso se legitimou e como as Forças Armadas brasileiras se tornaram as principais

tutoras da segurança cibernética no Brasil, considerando o *framework* de análise da Securitização da Escola de Copenhague.

Entendemos que os principais casos de ciberataques supracitados podem ter contribuído para o processo de cibersegurança no Brasil que se sucedeu no período em que aqui nos propusemos em analisar.

CAPÍTULO 3

4 SECURITIZAÇÃO DO ESPAÇO CIBERNÉTICO: O CASO BRASILEIRO

Conforme já introduzido, sustentamos a hipótese de que o Brasil passou por um processo de securitização de seu ciberespaço. Até agora dedicamos parte do trabalho ao esclarecimento dos conceitos de ciberespaço e Securitização que são presentes em nosso debate.

No capítulo anterior, apresentamos alguns casos de ataques cibernéticos que ganharam notoriedade internacional e que entendemos que podem ter contribuído com a construção do discurso de segurança cibernética no Brasil a partir de 2002.

Neste capítulo, temos como objetivo apresentar alguns elementos importantes na compreensão da atuação do governo brasileiro em seu espaço cibernético, levando em consideração não somente as políticas implantadas, mas também debates realizados em diversos níveis governamentais – e também da sociedade civil – que moldaram o processo de securitização deste setor.

Há de se perceber que existe um vínculo inevitável entre a cibersegurança no Brasil e a publicação de documentos pelo Ministério da Defesa e pela Presidência da República (Gabinete de Segurança Institucional). Durante nossa pesquisa, tivemos o intuito de apresentar a *construção* da segurança cibernética no Brasil que foi feita, sobretudo, com a expedição de documentos oficiais, desde o Governo Lula ao Governo Temer.

À vista disso, haveria uma dificuldade de manter nossa coerência argumentativa em apresentar a cibersegurança no Brasil sem apresentar também os principais instrumentos que a estabeleceram. De forma similar a outros países que se pautaram na securitização do espaço cibernético, os principais instrumentos de legitimação da cibersegurança são estes documentos oficiais governamentais. Dessa forma, seria impossível falar de segurança cibernética no Brasil sem apresentar os principais objetivos de documentos do Ministério da Defesa e da Presidência da República tais quais as Política de Defesa Nacional, Estratégia Nacional de Defesa, Boletins do Exército, Decretos, entre outros.

O vínculo entre a cibersegurança no Brasil e a necessidade do estudo documental destes instrumentos ficarão mais evidentes durante este capítulo.

Ressaltamos que a maior parte dos dados presentes neste capítulo partiram do estudo de documentos disponibilizados por fontes oficiais do governo brasileiro, mas também de

discussões acadêmicas que foram apresentadas visando enriquecer o debate proposto por este trabalho na medida em que se trata de um assunto com poucas e recentes fontes de consulta.

O desenvolvimento deste capítulo foi pautado na afirmação da Escola de Copenhague de que existem três componentes para que o processo de securitização ocorra com sucesso sobre uma questão, a saber: “a ameaça existencial, a ação emergencial e os efeitos na relação entre as unidades [...]” (BUZAN; WÆVER; DE WILDE, 1998, p. 26, tradução nossa⁹⁰). Lembrando que as unidades, por sua vez, são: a) objetos referentes; b) atores securitizadores; e c) atores funcionais.

Nossa tentativa, portanto, ao resgatar os elementos da Securitização na análise documental é aproximar a teoria da realidade.

Seguindo essa lógica, se considerarmos o ciberespaço como nosso objeto referente, o Ministério da Defesa e o Congresso Nacional como atores securitizadores e, por fim, as Forças Armadas Brasileiras como os atores funcionais do nosso estudo, objetivamos compreender quais foram: a ameaça existencial, a ação emergencial e os efeitos na relação entre as unidades no contexto brasileiro.

Tomando o Brasil entre 2002 e 2018 como recorte temporal para a compreensão do processo de securitização, entendemos também que o contexto histórico dos anos 1990 é relevante de ser apresentado, ainda que superficialmente, na medida em que, neste momento, se inicia o debate a respeito de tecnologias da informação no Brasil, o que leva ao posterior período do “*speech-act*” que se inicia, conforme compreendemos, ainda em 2002.

Apresentada no capítulo anterior, a contextualização internacional de eventos relacionados à cibersegurança também deram ensejo a debates levantados durante este capítulo, uma vez que entendemos que tais acontecimentos levaram não só o Brasil, mas a comunidade internacional como um todo, a dar atenção a questões de cibersegurança.

Dessa forma, combinando a compreensão dos contextos internacional e nacional, podemos traçar uma tentativa de explicação dos motivos que levaram o governo brasileiro ao momento de *speech-act* e, posteriormente, às medidas tomadas voltadas à cibersegurança.

⁹⁰ No original: “A successful securitization thus has three components (or steps): existential threats, emergency action, and effects on interunit relations by breaking free of rules” (BUZAN; WÆVER; DE WILDE, 1998, p. 26).

O *speech-act* e as medidas voltadas à cibersegurança são aqui compreendidos como os momentos de *ameaça existencial* e ação emergencial, respectivamente. Os desdobramentos das políticas, por sua vez, estão ligados aos *efeitos na relação entre as unidades*, como proposto pelos autores como sucesso para a securitização (BUZAN; WÆVER; DE WILDE, 1998).

Propusemos, com a tabela 05, apresentar visualmente os componentes propostos pelos autores da Escola de Copenhague e suas correspondências no contexto brasileiro:

Tabela 05: Componentes para o processo de securitização de sucesso segundo a Escola de Copenhague e o caso brasileiro

Componentes para securitização de sucesso	Componentes no caso brasileiro
Ameaça existencial	Construção social da vulnerabilidade do espaço cibernético brasileiro a partir dos contextos nacional e internacional e promoção do <i>speech-act</i> a partir de 2002
Ação emergencial	Políticas e medidas tomadas a partir de 2008
Efeito na relação entre unidades	Desdobramentos das políticas analisadas a partir de 2010

Fonte: Elaborado pela autora com base em BUZAN; WÆVER; DE WILDE, 1998.

Já com a tabela 06, propusemos apresentar as unidades da análise de segurança de acordo com os autores da Securitização e quais seriam os correspondentes no contexto brasileiro aqui analisado:

Tabela 06: Unidades da análise de segurança segundo a Escola de Copenhague e o caso brasileiro

Unidades da análise de segurança	Unidades no caso brasileiro
Objeto referencial	Espaço cibernético brasileiro
Atores securitizadores	Ministério da Defesa e Congresso Nacional
Atores funcionais	Forças Armadas Brasileiras

Fonte: Elaborado pela autora com base em BUZAN; WÆVER; DE WILDE, 1998.

Dessa forma, nosso objetivo com este capítulo não é apenas apresentar uma retomada histórica dos eventos que levaram à cibersegurança no Brasil, mas também encaixar tais eventos em uma análise Construtivista do *framework* proposto pela teoria da Securitização da Escola de Copenhague.

Metodologicamente, portanto, optamos por dividir o capítulo em quatro seções dado seu tamanho: 1) Contextualização nacional: Os anos 1990; 2) *Speech-act*: O desenvolvimento do discurso de segurança; 3) As medidas voltadas à segurança do ciberespaço brasileiro; e 4) Produtos das políticas de cibersegurança⁹¹.

Cada seção tem o objetivo de apresentar, de forma clara, os elementos que sustentam a argumentação do processo de securitização do espaço cibernético brasileiro individualmente.

⁹¹ Recomendamos ao leitor que acompanhe a Linha do Tempo do Processo de Segurança Cibernética no Brasil, presente no Apêndice B, na página 202, para melhor visualização dos acontecimentos em ordem cronológica.

4.1 Contextualização Nacional: Os anos 1990

Um dos principais apontamentos feitos pelos principais críticos da Teoria de Securitização diz respeito a falta de uma contextualização histórica na análise das medidas que levaram ao processo de securitização. Compreendemos tal crítica como sendo pertinente, pois a contextualização oferece importantes *insights* a respeito das condições dos ambientes político, econômico, militar e social dos casos analisados.

Dessa forma, optamos por resgatar alguns dos principais acontecimentos no âmbito brasileiro relacionados a defesa, segurança e tecnologia na década de 1990.

Durante a década de 1990, debates em âmbito acadêmico e governamental a respeito da crescente presença de Novas Tecnologias da Informação e Comunicação foram fomentados na tentativa de acompanhar estas transformações. Tais debates objetivaram compreender as Novas TICs e a melhor forma de utilizá-las.

Compreendemos este contexto da década de 1990 como um elemento importante que levou ao processo de securitização no Brasil conforme estimularam que medidas fossem tomadas a partir da década que se seguiu.

Ademais, como estamos tratando de questões relacionadas à Defesa no Brasil, também entendemos como relevante a compreensão dos conceitos de Segurança e Defesa naquele contexto pós-Guerra Fria em que novos elementos entraram em jogo.

Entendemos período de redemocratização vivenciado na década de 1990 combinado ao avanço tecnológico é interessante de ser compreendido na medida em que representou transformações econômicas, políticas, militares e sociais.

O papel das Forças Armadas, por exemplo, começou a ser questionado neste período. Com o fim dos conflitos entre Estados, o surgimento de novos elementos de segurança e defesa presentes em conflitos intraestatais causaram uma “crise de identidade” das Forças Armadas e da compreensão de suas funções tradicionais (MARQUES, 2003).

À vista disso, escolhemos apresentar *dois* casos importantes para o Brasil na década de 1990, a saber: a Sociedade da Informação no Brasil e a Política de Defesa Nacional, de 1996. O objetivo foi apresentá-los como elementos que enriquecem o debate e o argumento trabalhado na presente investigação a respeito do processo de securitização do ciberespaço brasileiro.

4.1.1 Sociedade da Informação no Brasil e Estratégia Brasileira para a Transformação Digital

Em meio às transformações tecnológicas da década de 1990 e a popularização dos *personal computers* (PCs), passou-se a discutir o imperativo denominado *inclusão digital*. A América Latina se organizava, mesmo que de forma incipiente, para a inclusão da pauta tecnológica em suas agendas nacionais.

No caso do Brasil, a década de 1990 ainda foi um período de redemocratização após a fase marcada pela ditadura militar. Dessa forma, entendemos que a democratização das novas tecnologias, por conseguinte, se tornou um tema emergente na medida em que digitalização de muitas das funções da sociedade passou a ocorrer e as Tecnologias da Informação e Comunicação se tornavam cada vez mais presentes nos lares brasileiros.

Ao assistir à tecnologia transformara sociedade e, em especial para o governo, transformar a economia do sistema capitalista, objetivou-se compreendê-la e podemos dizer, em uma perspectiva crítica, que também se objetivou *controlá-la*. Diferentemente das Revoluções Industriais experimentadas em séculos anteriores, a chamada Revolução Informacional ocorreu aceleradamente e os adventos dos computadores pessoais e Internet, por exemplo, chegaram a fazer parte do cotidiano do cidadão comum mundialmente (LOJKINE, 2002).

Considerando estas transformações, com os brasileiros das regiões urbanas cada vez mais conectados, o governo brasileiro na figura do então Ministério da Ciência e Tecnologia⁹² desenvolveu um Livro Verde⁹³ da Sociedade da Informação no Brasil em 2000, considerando que a inclusão digital se aceleraria no século que despontava.

Este documento denominado “Sociedade da Informação no Brasil: Livro Verde” tratou-se de um extenso relatório produzido por representantes do Ministério da Ciência e Tecnologia, mas também de pesquisadores de Universidades de todo o país, especialistas do setor privado e consultores internacionais (TAKAHASHI, 2000, p. X).

Seu objetivo foi, além de relatar a situação brasileira frente ao avanço tecnológico com pesquisas desenvolvidas desde 1996, incentivar que a tecnologia alcançasse a totalidade

⁹² Hoje Ministério da Ciência, Tecnologia, Inovações e Comunicações.

⁹³ Utiliza-se “Livro Verde” para denominar livros e documentos que introduzem algum assunto a partir de uma perspectiva específica.

dos brasileiros para que isso contribuísse ao *desenvolvimento* – econômico, destaca-se – do país (TAKAHASHI, 2000).

Como afirmam Oliveira e Shima (2012, p. 81), o incentivo à Sociedade da Informação no Brasil esteve ligado, principalmente, à competitividade econômica: “[...] o MCT [Ministério da Ciência e Tecnologia] chegou à conclusão que o uso das TICs dentro de uma infraestrutura nacional adequada contribui decisivamente para diminuir a atual distância entre países em desenvolvimento e países ricos no campo econômico e sociocultural” (OLIVEIRA; SHIMA, 2012, p. 81).

O documento também previa algumas estratégias que o governo brasileiro deveria seguir no processo de inclusão digital e implementação da Sociedade da Informação (TAKAHASHI, 2000, p. XV). Visto como um paradigma técnico-econômico e fenômeno global pelo Ministério, a Sociedade da Informação foi apresentada como um programa que urgia ser implementado em um país com grande potencial econômico como o Brasil.

Com discussões iniciadas em 1996 e publicação do Livro Verde em 2000, o programa da Sociedade da Informação foi fomentado durante o governo de Fernando Henrique Cardoso e cabe ressaltar que ficou à margem no novo governo de Luiz Inácio Lula da Silva a partir de 2003 (OLIVEIRA; SHIMA, 2012, p. 82).

Não houve, portanto, nos anos seguintes, documentos dedicados e estratégias específicas à Sociedade da Informação no Brasil. Isto não significa, no entanto, que a inclusão digital não tenha sido proposta nos Planos Plurianuais do governo Lula. (BRASIL, 2003). A perspectiva, entretanto, da inclusão digital, foi mais social do que econômica no governo Lula de forma geral, conforme avaliamos e analisamos.

Segundo sustentaram os pesquisadores Oliveira e Shima, o documento governamental Sociedade da Informação: Livro Verde era fragmentado e não apresentava vias concretas de alcançar algumas das “metas” que foram discutidas, além de os indicadores serem frágeis e focados no âmbito internacional, pouco relacionado com a realidade brasileira da época (OLIVEIRA; SHIMA, 2012, p. 82).

Dessa forma, entendemos que o programa da Sociedade da Informação acabou por não ser implementado como previsto no Livro Verde, mas foi um dos primeiros documentos oficiais a discutir a importância das tecnologias, especialmente aqueles de informação e comunicação que se popularizavam em território brasileiro.

Apesar de os focos do Livro Verde terem sido a tecnologia na indústria, o surgimento do *e-commerce* no Brasil e a competitividade econômica que poderia ser impulsionada pelo uso das novas tecnologias, a temática também foi abordada em uma perspectiva social (universalização do acesso) e até de segurança de informações (proteção de dados)⁹⁴, mesmo que brevemente (TAKAHASHI, 2000).

Sendo assim, avaliamos de forma positiva as discussões engendradas durante a década de 1990 a respeito das novas tecnologias e da Sociedade da Informação, ainda que não tenham sido colocadas em prática conforme planejara o Ministério da Ciência e Tecnologia à época.

O relatório Sociedade da Informação no Brasil: Livro Verde também introduziu a questão do que hoje é chamado de *E-Government*, ou Governo Eletrônico, em seu sexto capítulo – Governo ao Alcance de Todos. Nele é possível observar a afirmação de que o governo deve caminhar no mesmo sentido em que as novas tecnologias e prover informações e serviços aos cidadãos via Internet (TAKAHASHI, 2000, p. 70). A criação de portais com informações e serviços disponíveis a todo cidadão brasileiro com acesso à conexão a Internet foi proposto e discutido, tomando como exemplo outros países, objetivando, entre outros fins, a acessibilidade e a transparência.

Apontamos para esta questão, pois, no ano de 2018, o governo brasileiro retomou, com uma visão “repaginada”, a ideia do *E-Government* – e também o conceito de Sociedade da Informação – a partir da publicação da chamada Estratégia Brasileira para a Transformação Digital: E-Digital.

O então Ministério da Ciência, Tecnologia, Inovações e Comunicações por iniciativa do Governo Federal desenvolveu o novo relatório que teve como objetivo “aproveitar todo o potencial das tecnologias digitais para alcançar o aumento da produtividade, da competitividade e dos níveis de renda e emprego por todo o País, visando a construção de uma sociedade livre, justa e próspera para todos” (BRASIL, 2018a, p. 06).

O documento do E-Digital, assim como o Sociedade da Informação no Brasil: Livro Verde, também contou com trabalhos e pesquisas desenvolvidos por diferentes profissionais da iniciativa privada, sociedade civil e Universidades. Pautados nos 17 Objetivos de Desenvolvimento Sustentável da Organização das Nações Unidas, o documento incentivou

⁹⁴ Abordado sucintamente no anexo IV do documento completo, mas sempre mencionado durante o texto a importância do uso consciente das tecnologias da informação e comunicação.

dois pontos principais, a saber: a *Cidadania Digital* e a *Digitalização da Economia*. Entre estes dois pontos, outros, mas que envolvem ambos, também foram abordados, tais como: Ampliação do Acesso e Uso das TICs; Pesquisa, Desenvolvimento e Inovação; Confiança no Ambiente Digital; Educação e Capacitação; e Dimensão Internacional (BRASIL, 2018a, pp. 08-09). Todos estes pontos são chamados *Eixos Temáticos Habilitadores*.

Dentre os Eixos Habilitadores, aquele que se refere à *Confiança no Ambiente Digital* tem o maior número de ações previstas, totalizando quinze (BRASIL, 2018a, p. 08). Ou seja, ao que se refere à segurança no ambiente digital, o Ministério da Ciência, Tecnologia, Inovações e Comunicações postulou pelo menos quinze pontos estratégicos no alcance da transformação digital (BRASIL, 2018a, p. 08). Este dado pode ser considerado importante para o presente trabalho na medida em que revelou a atenção do governo brasileiro para com questões de cibersegurança também no âmbito civil.

Reforçamos que este documento de 2018, o E-Digital, apresentou semelhanças com o Livro Verde da Sociedade da Informação ao tratar de conceitos previamente abordados em 2000, mas com uma perspectiva mais atual. Contudo, chamamos a atenção para o fato de que a ideia de “Confiança no Ambiente Digital” foi inovadora, ao analisá-la comparativamente. Houve, no documento do E-Digital, uma dedicação exclusiva a questões de segurança e proteção no ciberespaço, usando, inclusive o conceito do *crime cibernético* (BRASIL, 2018a).

Observou-se, portanto, uma crescente – e relevante – preocupação de autoridades governamentais pela segurança no uso das novas tecnologias de informação e comunicação, bem como para com os crimes cibernéticos. Podemos dizer que houve uma atualização, ainda que mais concisa, do Livro Verde da Sociedade da Informação no Brasil e com maior dedicação a elementos de *segurança no ciberespaço*, os quais consideramos relevantes.

Apesar deste recente documento se tratar de uma *estratégia*, como o nome sugere, o documento publicado em 2000 também trouxe como proposta traçar estratégias para o programa da Sociedade da Informação no Brasil, mas ambos têm caráter de *relatório* a respeito da situação brasileira em comparação a outros países (geralmente, os considerados desenvolvidos).

Ademais, traçando um último paralelo entre o E-Digital e o Livro Verde, os dois documentos abordaram as questões envolvendo a tecnologia por uma perspectiva predominantemente *econômica*.

Optamos por abordar comparativamente ambos os documentos, pois entendemos que os primeiros debates mais relevantes no Brasil a respeito da tecnologia e do ciberespaço ocorreram na década de 1990, mas tomaram um caráter militar nos anos seguintes – como veremos posteriormente –, sendo retomado por uma perspectiva civil, com foco no desenvolvimento econômico relacionado à digitalização apenas em 2018, com os estudos realizados para a Estratégia Brasileira para a Transformação Digital: E-Digital.

Pontos aqui tratados a respeito do Livro Verde (2000) e o E-Digital (2018) foram discutidos como parte da contextualização a respeito da relação do Brasil com as TICs e serão retomados na argumentação feita no último capítulo e nas Considerações Finais.

Finalmente, afirmamos que a análise aqui feita é superficial e não tem como foco se estender na compreensão dos documentos e seus objetivos, mas sim apresentá-los como ideia que reforça a argumentação principal da presente investigação: a atenção do governo brasileiro para com questões tecnológicas e de cibersegurança.

4.1.2 Política de Defesa Nacional (1996)

A primeira edição da Política de Defesa Nacional brasileira foi publicada no ano de 1996, durante o governo do então presidente Fernando Henrique Cardoso. Compreendemos que, em seu segundo ano de mandato presidencial, FHC julgou necessário a redação de uma Política de Defesa Nacional que contemplasse o posicionamento brasileiro frente à instabilidade do período pós-Guerra-Fria⁹⁵ e os novos desafios que pudessem se apresentar.

É possível observar que essa “necessidade” ficou clara logo no início do documento, no primeiro ponto da Introdução: “1.1 Diante do novo quadro mundial de desafios e oportunidades, é necessário promover no Brasil o desenvolvimento de modalidades próprias, *flexíveis* e criativas de pensamento estratégico, aptas a atender às necessidades de defesa do país” (BRASIL, 1996, p. 03, grifo nosso).

Destacamos o termo “flexíveis” por ser uma ideia que será retomada pelo governo brasileiro mais adiante no debate a respeito da Defesa, como abordaremos.

O documento não descarta a relevância de elementos tradicionais de segurança – inclusive, o foco do documento ocorreu justamente nos termos destes elementos – tais como

⁹⁵ A Guerra Fria foi tratada como “confrontação Leste-Oeste” pelo documento oficial da Política de Defesa Nacional (BRASIL, 1996, p. 04).

defesa do território, manutenção da soberania, autodeterminação e identidade nacional, mas sugere que novas questões⁹⁶ sejam, pelo menos, ponderadas no âmbito governamental no contexto de transição – e até a própria redemocratização – que vinha ocorrendo à época (BRASIL, 1996, p. 05).

Apesar de não ser muito extensa (contém oito páginas de texto), a Política de Defesa Nacional mencionou, mesmo que brevemente, a importância dos setores político, social e econômico e reconheceu a “participação crescente de atores não-governamentais [no País]” (BRASIL, 1996, pp. 04-05).

Inferimos, a partir destas menções, que o governo brasileiro passou a reconhecer uma *ampliação do conceito de Segurança* engendrado pelas reorganizações pós-Guerra Fria. Novos elementos trazidos à agenda brasileira podem gerar – e geraram – o aperfeiçoamento das Forças Armadas, tanto em suas capacidades, quanto em suas funções, uma vez que devem atuar na defesa do país.

Ao que se refere aos seus objetivos e orientações estratégicas, a Política de Defesa Nacional de 1996 enfatizou questões diplomáticas, dissuasivas e defensivas, tomando um posicionamento tradicional pacífico de sua Política Externa (BRASIL, 1996, p. 08). Menções e incentivos ao desenvolvimento tecnológico e aperfeiçoamento científico apareceram no documento de forma mais abrangente, mas podemos inferir que demonstrou um reconhecimento incipiente das transformações internacionais e a necessidade de acompanhamento, em termos de Segurança, destas transformações (BRASIL, 1996, p. 09).

Nota-se que o documento não se prolongou a respeito das “novas questões” de Defesa apesar de sugerir que havia uma transformação de paradigmas ocorrendo. Não foi mencionado problemas referentes à novas *ameaças*, discussão que só foi suscitada mundialmente após o atentado às Torres Gêmeas, em Nova Iorque, em 2001.

Mencionamos a primeira Política de Defesa Nacional brasileira, pois entendemos que representou uma primeira expressão da Presidência da República a respeito das transformações internacionais que são capazes de refletir no âmbito interno, exigindo um aperfeiçoamento da Defesa no Brasil. A ideia, mesmo que embrionária, de ampliação do conceito de Segurança tomada por Fernando Henrique Cardoso ainda em 1996 sustentam

⁹⁶ Entendemos que a consideração de novos elementos no escopo de Defesa Nacional pode ter sido incentivada pela Organização dos Estados Americanos em suas reuniões a respeito de Defesa e Segurança Hemisférica. Discutiremos esta questão brevemente posteriormente no trabalho. Para mais informações ver: SAINT-PIERRE, 2011.

alguns argumentos traçados no presente trabalho e, por este motivo, consideramos relevante sua referência.

Considerar a importância dos setores político, social e econômico e reconhecer a influência de atores não-estatais em questões de Defesa e Segurança Nacionais dialoga com a tendência observada pela Escola de Copenhague no desenvolvimento da teoria de Securitização.

Podemos afirmar que ao englobar elementos sociais, econômicos e políticos além dos militares em uma das principais ferramentas de Defesa Nacional – a PDN – o governo brasileiro, no papel da presidência da república, poderia passar a securitizá-los.

A transformação dos paradigmas citados na Política, ainda, e o interesse no investimento em questões de Segurança e Defesa também acabaram por resultar na criação do Ministério da Defesa no Brasil em 1999.

Dessa forma, observa-se que a Política de Defesa Nacional é anterior ao próprio Ministério da Defesa Brasileiro. Isto, pois, o governo brasileiro contava com um Ministério da Guerra, que foi alterado para Ministério do Exército durante o período da ditadura militar. Só foi extinto ao final do governo Fernando Henrique Cardoso, em 1999, seguindo uma tendência dos países vizinhos sul-americanos que já possuíam seus Ministérios da Defesa há anos.

Essa criação tardia do Ministério da Defesa com participação civil pode demonstrar uma diferença entre os processos históricos do Brasil em comparação aos seus vizinhos e o papel e prestígio das Forças Armadas em nosso país. Retomaremos tais questões em nossas Considerações Finais.

Completados os esclarecimentos a respeito destes dois momentos do contexto da década de 1990 – Sociedade da Informação e Política de Defesa Nacional de 1996 – iniciamos a apresentação de elementos que dão ensejo ao debate aqui proposto a respeito da cibersegurança.

4.2 *Speech-act*: O desenvolvimento do discurso de segurança

Seguindo com a segunda seção deste capítulo, destacamos a importância do discurso para a tomada de ação voltada à segurança. O *discurso* e sua relação com a sua *audiência* é um elemento presente na teoria de securitização da Escola de Copenhague, ainda que pouco desenvolvido enquanto conceito pelos autores (BUZAN; WÆVER; DE WILDE, 1998; MCDONALD, 2008a). Sendo o processo de securitização “intersubjetivo e socialmente construído”, o discurso de segurança é importante enquanto uma audiência legitima ações a serem tomadas (BUZAN; WÆVER; DE WILDE, 1998, p. 31, tradução nossa⁹⁷).

Objetivando compreender de que forma surgiu e se concretizou o discurso de segurança, em específico o discurso da cibersegurança no Brasil e na América, escolhemos analisar três documentos, a saber: o Seminário Política de Defesa para o Século XXI, de 2002, o Projeto de Declaração Sobre a Segurança nas Américas e a Política de Defesa Nacional, de 2005. Optamos por apresentar cronologicamente tais documentos a seguir.

4.2.1 Seminário Política de Defesa para o Século XXI (2002)

O Seminário Política de Defesa para o Século XXI, como o nome sugere, foi um Seminário promovido conjuntamente pela então Comissão de Relações Exteriores e de Defesa Nacional e a Fundação de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ) e realizado na Câmara dos Deputados, em Brasília, entre 20 e 21 de agosto de 2002. Posteriormente, em 2003, o Seminário foi publicado na forma de um livro.

O presidente da Comissão de Relações Exteriores e de Defesa Nacional à época, Aldo Rebelo, incentivou o projeto do Seminário na medida em que entendia o tema de segurança no Brasil como pouco discutido (REBELO; FERNANDES, 2003, p. 13). Rebelo, inclusive, veio a se tornar Ministro da Ciência, Tecnologia e Inovação em 2015 e, posteriormente, ainda no mesmo ano, Ministro da Defesa.

Tendo como finalidade, portanto, a discussão a respeito da promoção de medidas voltadas aos novos elementos de Segurança e Defesa no Brasil, o Seminário Política de Defesa para o Século XXI contou com a presença de representantes das Forças Armadas e também da sociedade civil no espaço da Câmara dos Deputados (REBELO; FERNANDES, 2003).

⁹⁷ No original: “Securitization is intersubjective and socially constructed [...]” (BUZAN; WÆVER; DE WILDE, 1998, p. 31).

Considerando a recente fundação do Ministério da Defesa brasileiro em 1999, podemos inferir que o Seminário também esteve inserido neste contexto, em 2002, de definição das funções do MD e da compreensão do papel das Forças Armadas. Além disso, o atentado às Torres Gêmeas, em 2001, em Nova Iorque, fomentou o debate a respeito de novas ameaças não apenas nos Estados Unidos, mas internacionalmente.

No caso do Brasil, o Seminário objetivou, portanto, compreender o papel do país em meio às transformações do início do século. Como afirmou o então Ministro da Defesa à época, Geraldo Magela Quintão:

[...] vivemos hoje em um mundo menos previsível. Nesta fase de transição, em que se estabelecem novas regras políticas e econômicas de convivência entre as nações, caracterizada pela ausência de padrões claros e pela participação crescente de atores não governamentais, o Brasil procura determinar, livre de matrizes ideológicas, sua inserção estratégica e suas prioridades no campo da Defesa (QUINTÃO, 2003, p. 22).

Tal fala do ex-Ministro da Defesa foi proferida no discurso de abertura do Seminário. Durante todo seu discurso, Quintão reforçou a importância dos conceitos de Segurança e Defesa no Brasil, bem como a posição brasileira internacionalmente, que considera “estratégica” e o país como sendo “indutor natural de da articulação regional” (QUINTÃO, 2003, p. 23). Tal postura do ex-Ministro pode ser entendida como uma tentativa de justificativa para a criação de uma nova Política de Defesa Nacional, como também propôs durante seu discurso de abertura (QUINTÃO, 2003, p. 26).

Ademais, na fala do ex-Ministro, também pudemos observar menções à Organização das Nações Unidas, bem como a conferência da OEA (Organização dos Estados Americanos) que estava prestes a acontecer, em 2003, e que mencionaremos no tópico seguinte. Entendemos que as organizações regionais ganharam mais importância com o fim da Guerra Fria e, entre os interesses brasileiros no engendrar do século XXI, era ser relevante nestes organismos internacionais, aumentando seu prestígio. Isto justifica a preocupação brasileira com tais organismos internacionais.

Entretanto, entre as questões que consideramos mais interessantes de serem observadas a partir do discurso de Geraldo Quintão à época, destacamos o *resgate* da importância das Forças Armadas, bem como uma necessidade de atualização destas, que considera tendo um modelo herdado do período pós-Guerra Fria, como afirma: “O atual sistema militar de defesa brasileiro ainda possui reflexos de sua pouca autonomia estratégica

decorrente de uma ordem internacional já ultrapassada, cujos paradigmas e conceitos não são mais aplicáveis” (QUINTÃO, 2003, p. 26).

De acordo com o que é apresentado na fala de Quintão, a atualização das funções das Forças Armadas é justificável na medida em que novas ameaças passaram a se apresentar naquela nova conjuntura. Destacamos uma afirmação do ex-ministro na qual postulou que:

[...] o surgimento de ameaças não-ortodoxas, como o terrorismo, o crime organizado, o narcotráfico e as instabilidades internas, bem como a presença crescente de novos atores transnacionais, tornam a análise muito mais complexa. Tais aspectos, associados à *revolução da informação*, que permite o fluxo de dados e de capitais sem eficiente controle governamental, expõem países com economias em fase de consolidação, como a nossa, a grandes riscos (QUINTÃO, 2003, p. 27, grifo nosso).

Destacamos a questão da revolução informacional, pois trata-se do elemento de interesse neste trabalho. Mas, de forma geral, podemos inferir que o governo brasileiro passou, ainda que de maneira incipiente, a reconhecer as transformações que ocorriam em nível global e a traçar maneiras de compreendê-las em contexto nacional.

Ressaltamos, ainda, que como Ministro da Defesa, Geraldo Magela Quintão defendeu, à época, a *flexibilidade* como conceito norteador das melhorias que deveriam ser buscadas pelas Forças Armadas e pela Defesa Nacional amplamente. Afirmou:

Como deve, então, o Ministério da Defesa responder a esse quadro estratégico cada vez mais complexo que se conforma? A resposta está em conceito-chave do novo sistema de defesa nacional: *flexibilidade*. Estamos conscientes que conflitos recentes exigem ênfase na capacidade de pronta resposta, na qual estão subjacentes características como versatilidade e interoperabilidade e sustentabilidade (QUINTÃO, 2003, p. 29-30, grifo nosso).

A flexibilidade foi um termo utilizado anteriormente no documento da Política de Defesa Nacional de 1996, como já mencionamos. Entendemos tal termo como a *adaptabilidade* e *preparo* das forças de defesa do Brasil. Este tornou-se um conceito que pautou a redação dos objetivos para a defesa no século XXI, como discutiremos a seguir.

Considerando as transformações necessárias, o ex-Ministro afirmou no Seminário:

Assim, a *revisão* da estrutura militar de defesa brasileira está sendo norteadada pela associação de missões-tipo, baseada nas nossas vulnerabilidades em quadro hipotético de cenários, e na capacitação operacional para cumpri-las, com maior destaque para forças leves, ágeis bem adestradas, aptas a atuar de modo combinado e a cumprir diferentes tipos de missões. A qualidade assume, portanto, importância bem maior que a quantidade (QUINTÃO, 2003, p. 30, grifo nosso).

Dessa forma, o recém-criado Ministério da Defesa compreendeu que uma atualização das Forças Armadas era necessária, se equiparando aos novos elementos considerados como ameaças. Uma crescente importância conferida às Forças Armadas pode ser observada a partir de então.

Além do – novo – papel das Forças Armadas, o Seminário de 2002 sugeriu, também, que a Política de Defesa Nacional, documento oficial que norteia o Ministério de Defesa e as Forças Armadas, fosse atualizado, dada sua importância (QUINTÃO, 2003; REBELO; FERNANDES, 2003). Esta atualização ocorreu em 2005 (BRASIL, 2005).

Compreendemos que o papel do Seminário Política de Defesa para o Século XXI teve sua importância no sentido de promover o debate a respeito das transformações dos conceitos relacionados à Segurança e Defesa e considerar o contexto brasileiro em meio a tais transformações. O principal produto do Seminário foi a nova Política de Defesa Nacional publicada em 2005 como sugerida pelas autoridades à época (BRASIL, 2005; REBELO; FERNANDES, 2003).

Conforme postularam, além de uma Política de Defesa Nacional, uma Estratégia de Defesa que fosse capaz de promover *transformações* no país também foi incentivada neste Seminário (FERREIRA, 2003, p. 44). O cientista social Oliveiros Ferreira, convidado a participar do Seminário de Política de Defesa para o Século XXI, direcionou sua fala a respeito da Estratégia Nacional de Defesa, inclusive, concedendo importância à figura de Golbery de Couto e Silva:

[...] busquemos esboçar – pois o que me pedem são “ideias de uma concepção estratégica” – as linhas gerais da concepção Estratégica Nacional. Permito-me tomar como referência a definição que o então Coronel Golbery do Couto e Silva deu da Concepção Estratégica Nacional: “A Concepção Estratégica Nacional – CEN – é a diretriz fundamental que, em dado período, deve nortear toda a estratégia da Nação, com vistas à consecução salvaguarda dos Objetivos Nacionais a despeito dos antagonismos que manifestem ou possam vir a manifestar-se, tanto no campo internacional, como até mesmo no âmbito interno do País. Ora, em sentido amplo, a Estratégia de uma nação confunde-se conforme vimos, com a própria Política de Segurança Nacional [...] (FERREIRA, 2003, p. 36-37).

Como veremos posteriormente, o governo Brasileiro, em 2008, elaborou sua Estratégia Nacional de Defesa contemplando a maior parte das considerações deste Seminário de Política de Defesa para o século XXI (BRASIL, 2008).

Destacamos, entretanto, a citação de Oliveiros Ferreira à Golbery de Couto e Silva, figura presente na história da defesa no Brasil. O General Golbery de Couto e Silva foi um intelectual que teve forte influência dos métodos internacionais de Defesa, principalmente aqueles advindos das Forças Armadas Norte Americanas, do período quando viveu nos Estados Unidos (FIGUEIREDO, 2005).

Entendemos que a figura de Golbery está amplamente ligada ao rumo que a Escola Superior de Guerra tomou na década de 1950 e à influência norte-americana nas Forças Armadas brasileiras, bem como na formulação de Objetivos Nacionais e, posteriormente, no golpe de 1964 (FIGUEIREDO, 2005; MIYAMOTO, 1995).

Optamos por fazer referência a estas questões, pois entendemos que contribuem para a compreensão do contexto qual o Seminário de Política para a Defesa no Século XXI foi promovido, bem como a visão das autoridades envolvidas neste evento. Ou seja, em 2002 foi resgatado valores das décadas de 1950 e 1960, denotando importância a atuação das Forças Armadas no Brasil.

Novamente nota-se, no caso brasileiro, uma diferença entre ao tratamento dados às Forças Armadas em comparação aos seus vizinhos. Tendo em vista o caráter conservador da sociedade brasileira que se difere dos processos históricos de outros países da América do Sul durante o período de redemocratização, as FFAA são tratadas com prestígio no País.

De forma geral, pudemos observar que o Seminário foi o principal exemplo de discurso governamental a respeito das transformações engendradas no Século XXI, responsável por promover, nos anos seguintes, a nova Política de Defesa Nacional e a Estratégia Nacional de Defesa. A necessidade de atualização do sistema de defesa e das Forças Armadas foram enaltecidas neste evento e, por este motivo, consideramos como momento importante na história recente do Brasil na constituição do discurso – o *speech-act*.

A partir da emergência de ameaças chamadas “não-ortodoxas” pelo então Ministro de Defesa no pós-2001 e a apresentação de justificativas para o desenvolvimento da Defesa e da Segurança no Brasil, consideramos este Seminário como um momento relevante no que se refere ao discurso proferido em âmbito nacional sobre os novos rumos da Defesa.

Regionalmente, entendemos que este papel do discurso de segurança foi feito pela Organização dos Estados Americanos (OEA) através do Projeto de Declaração Sobre a Segurança nas Américas. Este é tema do tópico subsequente.

4.2.2 Projeto de Declaração Sobre a Segurança Nas Américas (2013)

Nota-se que a discussão a respeito de novas ameaças também se intensificou regionalmente a partir do século XXI. Apesar de considerar uma ampliação do conceito de segurança, em especial a Segurança Hemisférica desde 1991 (SAINT-PIERRE, 2011, p. 412), a Organização dos Estados Americanos (OEA) realizou uma Conferência Especial sobre Segurança sediada pelo México no ano de 2003. Desta Conferência Especial, surgiu o Projeto de Declaração Sobre Segurança nas Américas, aprovada pelos Estados Membros da Organização ainda em 2003 (OEA, 2003, p. 01).

Apesar de ter trazido à tona conceitos tais como a própria Segurança Hemisférica e a Multidimensionalidade da Segurança⁹⁸ (OEA, 2003; SAINT-PIERRE, 2011, p. 414), a Declaração Sobre Segurança nas Américas apresentou, de forma clara, preocupação com novas formas de *insegurança* para os Estados americanos. Aliás, o termo usado pela Organização, tal como foi redigida no documento, foi “novas ameaças”.

De forma geral, a Declaração postulou que as chamadas *novas ameaças* passaram a colocar em perigo os países do hemisfério americano e que a cooperação entre os Estados e o compromisso com os valores da OEA seriam necessários na manutenção da paz, além de ter feito algumas recomendações mais abrangentes (OEA, 2003, p. 02; SAINT-PIERRE, 2011, p. 415).

Não apenas faz-se importante notar a ampliação do conceito de Segurança em âmbito da OEA ao compreender a Multidimensionalidade e as novas ameaças engendradas após o 11 de setembro de 2001, mas também a consideração da Organização ao que se refere à vulnerabilidade do setor cibernético em específico (OEA, 2011, p. 04-09).

Enquadrado ao lado de questões tais como terrorismo, narcotráfico, tráfico de armas de fogo, desastres naturais, pobreza extrema, entre outros, os *ataques cibernéticos* fizeram uma de suas primeiras aparições oficiais como questão de segurança regional, mesmo que brevemente. Isto pode ser observado no trecho seguinte da Declaração:

26. *Desenvolveremos* uma cultura de segurança cibernética nas Américas adotando medidas de prevenção eficazes que prevejam e considerem os ataques cibernéticos e a eles respondam, independentemente de sua origem,

⁹⁸ Como o próprio nome sugere, a *multidimensionalidade* considerou que as ameaças pós-Guerra Fria passaram a ter dimensões múltiplas, diferentes das tradicionais daquele período hostil. Também considerou que estes novos desafios podem ter caráter transnacional e, portanto, requerem cooperação internacional adequada na busca de soluções (SAINT-PIERRE, 2011, p. 413).

lutando contra as ameaças cibernéticas e o delito cibernético, tipificando os ataques contra o espaço cibernético, protegendo a infraestrutura crítica e assegurando as redes dos sistemas. Reafirmamos nosso compromisso de desenvolver e implementar uma estratégia integral da OEA sobre segurança cibernética, utilizando as contribuições e recomendações elaboradas conjuntamente [...] (OEA, 2003, p. 09, grifo dos autores).

Destacamos, no trecho supracitado, a atenção dada ao *ciberespaço* e a *infraestrutura crítica*, dois pontos recorrentes, especialmente no caso brasileiro, como abordaremos posteriormente, em sua Estratégia Nacional de Defesa. Adicionado às preocupações da OEA com a cibersegurança, tem-se a precocidade do tratamento destas questões, uma vez que ainda no ano de 2003 já tinham sido mencionadas e tomadas como recomendações pelos Estados Membros da Organização dos Estados Americanos, entre eles, o Brasil.

Apesar de compreender que, como argumenta Saint-Pierre (2011, p. 420), uma agenda de segurança hemisférica como proposta pela Organização apresentou problemas, principalmente ao se considerar que a ameaça é um *fenômeno perceptivo*, ou seja, deve ser percebida pelos Estados singularmente – além de outras questões complexas de cooperação regional –, entendemos que a apresentação destas questões tais como ampliação da ideia do que envolve segurança e vulnerabilidade do ciberespaço no âmbito hemisférico ainda em 2003 são importantes de serem mencionadas no presente trabalho e contribuem para o debate aqui proposto.

Ainda que não haja uma obrigação, de fato, para que os países sigam todas as recomendações, entendemos que no caso brasileiro, a posição tradicional do Ministério das Relações Exteriores é de valorizar o papel de Organizações Internacionais tais como a OEA e a ONU (Organização das Nações Unidas), na medida em que se pode observar que houve uma tentativa do país se sobressair em relação aos outros países membros destas Organizações a partir do novo século (BRASIL, 2005; BRASIL, 2008).

Tendo em vista que a Escola de Copenhague valorizou as relações regionais enquanto elementos importantes na compreensão da segurança (BUZAN, 1997; BUZAN; WÆVER; DE WILDE, 1998; BUZAN; WÆVER, 2003), optamos por mencionar como um dos principais órgãos regionais da América, a OEA, tratou a segurança e a cibersegurança em um Documento oficial regional no início do século XXI.

4.2.3 Política de Defesa Nacional (2005)

Aprovada em 30 de junho de 2005, a nova Política de Defesa Nacional foi publicada oficialmente apenas no dia seguinte, 1º de julho de 2005, no Diário Oficial da União. O documento foi aprovado pelo então presidente Lula e oficializado também por José Alencar Gomes da Silva (Ministro da Defesa à época) e Jorge Armando Felix (Ministro chefe do Gabinete Institucional da Presidência da República à época).

Como disposto no documento, sua finalidade foi: “[...] estabelecer objetivos e diretrizes para o preparo e o emprego da capacitação nacional, com o envolvimento dos setores militar e civil, em todas as esferas do Poder Nacional. O Ministério da Defesa coordena as ações necessárias à Defesa Nacional” (BRASIL, 2005, s/p).

O documento enfatizou a necessidade de uma política atualizada voltada para a Defesa mesmo em um país considerado pacífico como o Brasil e postulou: “Um dos propósitos da Política de Defesa Nacional é conscientizar todos os segmentos da sociedade brasileira de que a defesa da Nação é um dever de todos os brasileiros” (BRASIL, 2005, s/p).

Com o Ministério da Defesa oficializado em 1999, entendemos que a nova Política de Defesa Nacional surgiu como um produto do Seminário Política de Defesa para o Século XXI realizado no ano de 2002. Isto, pois, a PDN promulgada em 1996 pelo então presidente Fernando Henrique Cardoso necessitava atualização frente a novos acontecimentos que foram considerados como ameaças pela comunidade internacional, tais como ataques terroristas, intensificação do narcotráfico e o próprio desenvolvimento tecnológico acentuado.

Dessa forma, a Política de Defesa Nacional de 2005 foi consequência do *alargamento* do conceito de Segurança que já vinha sendo debatido na década de 1990, mesmo com a PDN de 1996, e que foi ainda mais aprofundado após 2001. Urgia, na visão do governo brasileiro, uma política específica que tratasse da defesa no Brasil, considerando as transformações ocorridas entre a década de 1990 a primeira metade da década de 2000.

Este argumento de alargamento do conceito de Segurança pôde, inclusive, ser observado no item 1.3 da Política de Defesa Nacional de 2005: “1.3 Gradualmente, o conceito de segurança foi ampliado, abrangendo os campos *político, militar, econômico, social, ambiental* e outros. Entretanto, a defesa externa permanece como *papel primordial* das Forças Armadas no âmbito interestatal” (BRASIL, 2005, s/p, grifo nosso).

Conforme apresentamos no capítulo anterior, as Relações Internacionais e os Estudos de Segurança Internacional passaram por um processo de aprofundamento e alargamento do conceito de Segurança (VILLA; REIS, 2006; MCDONALD, 2008; WILLIAMS, 2008). Afirmamos que este processo pode ser entendido como uma evolução dos Estudos de Segurança Internacional, pois novos elementos passaram a ser considerados como parte das relações sociais e relações internacionais com o fim da Guerra Fria.

Podemos aqui fazer um paralelo entre este aprofundamento e alargamento do conceito de Segurança e a nova Política de Defesa Nacional do Brasil, especialmente quando consideramos o trabalho desenvolvido pela Escola de Copenhague (BUZAN; WÆVER; DE WILDE, 1998). Isto, pois, esta *abrangência* dos campos político, militar, econômico, social e ambiental observado na PDN de 2005 já havia sido trabalhada pela setorização da segurança proposta pelos autores da Escola de Copenhague (BUZAN; WÆVER; DE WILDE, 1998, p. 27).

Assim sendo, entendemos que a razão pela qual uma nova Política de Defesa para o Brasil foi elaborada em menos de dez anos após a sua antecessora foi, justamente, abarcar os novos desafios entendidos pelo governo brasileiro como questões de defesa nacional. Retomaremos alguns pontos deste argumento e do exposto a respeito do item 1.3 da PDN de 2005 posteriormente.

Tendo como base uma visão Weberiana do papel do Estado⁹⁹, o documento de 2005 iniciou afirmando que este “detém o monopólio legítimo dos meios de coerção para fazer valer a lei e a ordem, estabelecidas democraticamente, provendo-lhes, também, a segurança” (BRASIL, 2005, s/p). Neste trecho citado, podemos inferir a expressão brasileira de defesa centralizada na figura do Estado e, mais em específico, nas Forças Armadas, como veremos a seguir.

Sabe-se que na maior parte dos documentos de defesa no Brasil, os conceitos de Segurança e Defesa são definidos com o objetivo de embasar sua interpretação. Na Política de Defesa Nacional de 2005 não é diferente. Segundo a visão do MD à época:

I - Segurança é a condição que permite ao País a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do

⁹⁹ Em seu ensaio publicado em 1919, “Política como Vocação”, o sociólogo Max Weber definiu o Estado como tendo pretensão da garantia do “*monopólio do uso legítimo da força física dentro de um determinado território*” (WEBER, 1982, p. 98, grifo do autor). Entendemos que esta concepção de Estado pode ser recorrente no pensamento ocidental. Para mais informações, ver: WEBER, 1982.

exercício dos direitos e deveres constitucionais; II - Defesa Nacional é o conjunto de medidas e ações do Estado, *com ênfase na expressão militar*, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas (BRASIL, 2005, s/p, grifo nosso).

Dessa forma, observa-se a centralidade do Estado e a relevância das Forças Armadas na garantia da Segurança.

A Política de Defesa Nacional de 2005 foi importante, como entendemos, na medida em que passou a considerar, *substancialmente*, ameaças não tradicionais à segurança do País. Foram abordadas questões tais como economia, Meio Ambiente, sociedade e tecnologia na garantia da Segurança, para além de ameaças entendidas como políticas e militares (BRASIL, 2005).

Enfatizamos, como prevê o objetivo deste trabalho, as preocupações tomadas com a chamada “revolução tecnológica” (BRASIL, 2005, s/p) e os novos meios de comunicação:

2.5 Os avanços da tecnologia da informação, a utilização de satélites, o sensoriamento eletrônico e inúmeros outros aperfeiçoamentos tecnológicos trouxeram maior eficiência aos sistemas administrativos e militares, sobretudo nos países que dedicam maiores recursos financeiros à Defesa. Em consequência, criaram-se vulnerabilidades que poderão ser exploradas, com o objetivo de inviabilizar o uso dos nossos sistemas ou facilitar a interferência à distância (BRASIL, 2005, s/p).

Podemos inferir que este trecho é relevante na medida em que evidencia a crescente utilização de tecnologias pelo Ministério da Defesa e a necessidade de constante aperfeiçoamento destas como ferramenta de Defesa Nacional.

O documento ainda fez referência, além da tecnologia, a questões relacionadas ao entorno estratégico brasileiro e a atuação geopolítica do País, bem como a importância de compreender a defesa em cada uma das regiões brasileiras, a proteção da Amazônia, o Direito do Mar, questões energéticas, os crimes transnacionais, o repúdio ao terrorismo e a importância do desenvolvimento da indústria de defesa (BRASIL, 2005).

Entendemos que a enumeração destes pontos fez desta Política de Defesa Nacional mais clara e com foco determinado em comparação àquela aprovada em 1996, que era genérica.

Existiu, como observamos, uma introdução de novos elementos como matéria de Segurança, mas aqueles tradicionais também permaneceram, principalmente quando se analisa os objetivos da Defesa Nacional, conforme o documento:

I - a garantia da soberania, do patrimônio nacional e da integridade territorial; II - a defesa dos interesses nacionais e das pessoas, dos bens e dos recursos brasileiros no exterior; III - a contribuição para a preservação da coesão e unidade nacionais; IV - a promoção da estabilidade regional; V - a contribuição para a manutenção da paz e da segurança internacionais; e VI - a projeção do Brasil no concerto das nações e sua maior inserção em processos decisórios internacionais (BRASIL, 2005, s/p).

Podemos observar, principalmente, a partir destes objetivos, a manutenção territorial e a soberania brasileira, bem como uma tentativa de enfatizar a importância da inserção do Brasil internacionalmente. Cada um destes pontos se relaciona mais aproximadamente de elementos tradicionais de Segurança Internacional (BUZAN; HANSEN, 2012).

O documento da Política de Defesa Nacional anexada ao Decreto nº 5.484 de 2005 apresentou 26 diretrizes estratégicas no cumprimento dos objetivos estabelecidos aqui supracitados. Podemos inferir, a partir das diretrizes, a vontade do Ministério de Defesa em cumprir aquilo que estabeleceu como fundamental na garantia da Defesa Nacional.

A partir desta PDN de 2005, a Estratégia Nacional de Defesa foi elaborada poucos anos depois, em 2008, apresentando também diretrizes estratégicas quais deveriam ser seguidas. Em termos numéricos, a Estratégia Nacional de Defesa estabeleceu menos diretrizes, sendo 23 em sua publicação original, em 2008, e 25 na versão atualizada, em 2012. Entretanto, estas diretrizes foram formuladas mais extensamente e de forma mais aprofundada na END, considerando o papel de cada Força na garantia da Defesa Nacional, como será abordado no ponto 3.3 deste trabalho quando apresentarmos a Estratégia Nacional de Defesa integralmente.

A fim de apresentar argumentos referentes à preocupação do governo brasileiro com a tecnologia e a cibersegurança, apresentamos aqui dois pontos estabelecidos pela PDN de 2005.

O primeiro deles diz respeito à uma orientação estratégica específica do documento: o item 6.19. Segundo este ponto: “Para minimizar os danos de possível ataque cibernético, é essencial a busca permanente do aperfeiçoamento dos dispositivos de segurança e a adoção de procedimentos que reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento” (BRASIL, 2005, s/p).

O segundo ponto diz respeito à uma diretriz estratégica, a de número XII: “aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas

relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, permitam seu pronto restabelecimento [...]” (BRASIL, 2005, s/p).

Tanto na orientação quanto na diretriz estratégica é possível observar preocupação do governo brasileiro em relação a emergente questão cibernética, especialmente, como entendemos, ao que se refere a *infraestruturas sensíveis*.

A modernização de certas tecnologias utilizadas foi demandada a fim de reduzir vulnerabilidades e proteger o Brasil de possíveis ataques cibernéticos. Dessa forma, observamos uma incipiente atenção a questões que envolvem a tecnologia e vulnerabilidades cibernéticas no Brasil a partir deste momento.

4.2.3.1 Algumas diferenças entre a Política de Defesa Nacional de 2005 e a Política Nacional de Defesa de 2012

No ano de 2012, a Política de Defesa Nacional foi atualizada, passando a ter como título “Política Nacional de Defesa”, a fim de seguir a mesma semântica da “Estratégia Nacional de Defesa”, que foi publicada, originalmente, em 2008.

A partir da atualização de 2012, as Política Nacional de Defesa e Estratégia Nacional de Defesa se tornaram um único documento de 155 páginas do Ministério da Defesa. Entendemos que juntando a PND e a END o Ministério da Defesa apresentaria um modelo mais acessível de consulta aos principais objetivos e medidas voltadas à segurança e a defesa no século XXI.

Dessa forma, a atualização de 2012 da Política Nacional de Defesa trouxe algumas mudanças, sendo elas em sua apresentação e também em seu conteúdo.

Quando dizemos que sofreu mudanças em sua apresentação, nos referimos especialmente ao *layout* da Política Nacional de Defesa que antes era apenas um texto corrido anexado ao Decreto nº 5.484 de 2005 (BRASIL, 2005).

Uma crítica pode ser feita quando consideramos um aspecto que pode ter se tornado mais complexo no texto atualizado da Política Nacional de Defesa de 2012. Originalmente, no documento da Política de Defesa Nacional de 2005, o ponto 6.16 trouxe a seguinte Orientação Estratégica: “Com base na Constituição Federal e em prol da Defesa Nacional, as Forças Armadas poderão ser empregadas contra ameaças internas, visando à preservação do exercício da soberania do Estado e à indissolubilidade da unidade federativa” (BRASIL, 2005, s/p).

Em sua versão de 2012, esta mesma Orientação foi reformulada no ponto 7.20 com o seguinte texto: “Nos termos da Constituição, as Forças Armadas poderão ser empregadas pela União contra ameaças ao exercício da soberania do Estado e à indissolubilidade da unidade federativa” (BRASIL, 2012a, p. 35).

Entendemos que a reescrita deste ponto abre margem para a interpretação de que as Forças Armadas podem ser empregadas ainda “contra ameaças internas”, ou seja, contra aquilo que podem considerar uma ameaça originária de sua população, mesmo que não esteja tão explícito como na versão anterior.

Já em relação às diferenças no conteúdo, questão mais relevante, as mudanças ocorreram principalmente na redação, que deixou o texto mais claro em alguns pontos (e em outros, menos), e nas orientações estratégicas, que entendemos que são mudanças mais substanciais (BRASIL, 2012a).

Dentre as Orientações Estratégicas, a maior parte manteve-se igual, com apenas com a reescrita do texto visando deixá-lo mais claro. Três pontos, entretanto, foram removidos do texto original, a saber os 6.7, 6.12 e 6.15¹⁰⁰.

Entendemos que tais pontos tinham uma perspectiva demasiada tradicional da defesa no Brasil, chegando a considerar, inclusive, a Amazônia e o Atlântico Sul como as prioridades de Defesa pelas Forças Armadas (BRASIL, 2005). Esta perspectiva se transformou nos anos seguintes com um novo entendimento daquilo que caracterizava estrutura estratégica no País.

Três novas Orientações foram inseridas no lugar daquelas removidas: 7.10, 7.14 e 7.21. Consideramos estas mudanças importantes na compreensão do texto de 2012 e da mudança de perspectiva tomada pelo Ministério da Defesa e, por este motivo, os apresentaremos integralmente:

[...] **7.10.** Os setores espacial, cibernético e nuclear são estratégicos para a Defesa do País; devem, portanto, ser fortalecidos [...] **7.14.** O Brasil deverá dispor de capacidade de projeção de poder, visando a eventual participação em operações estabelecidas ou autorizadas pelo Conselho de Segurança da

¹⁰⁰ São os pontos originais posteriormente removidos: “6.7 As Forças Armadas devem estar ajustadas à estatura político-estratégica do País, considerando-se, dentre outros fatores, a dimensão geográfica, a capacidade econômica e a população existente [...] 6.12 Em virtude da importância estratégica e da riqueza que abrigam, a Amazônia brasileira e o Atlântico Sul são áreas prioritárias para a Defesa Nacional [...] 6.15 O Brasil precisa dispor de meios e capacidade de exercer a vigilância, o controle e a defesa do seu espaço aéreo, aí incluídas as áreas continental e marítima, bem como manter a segurança das linhas de navegação aéreas [...]” (BRASIL, 2005, s/p).

ONU [...] **7.21.** O Brasil deverá buscar a contínua interação da atual PND com as demais políticas governamentais, visando a fortalecer a infraestrutura de valor estratégico para a Defesa Nacional, particularmente a de transporte, a de energia e a de comunicações (BRASIL, 2012a, p. 33; p. 35).

Com a nova Orientação Estratégica 7.10, o governo brasileiro optou, como entendemos, por seguir uma tendência já manifestada na Estratégia Nacional de Defesa de 2008 de considerar os setores espacial, cibernético e nuclear como estratégicos para a Defesa Nacional, reconhecendo sua vulnerabilidade à época. Consideramos esta questão importante para a argumentação no presente trabalho, recorreremos a ela posteriormente.

A segunda nova Orientação diz respeito às Operações de Paz das Nações Unidas em específico, apesar de já ter mencionado a participação das Forças Armadas Brasileiras em missões internacionais em sua versão de 2005 (BRASIL, 2005). Entendemos que esta menção específica à ONU e ao seu Conselho de Segurança (CS) deve-se, em maior parte, à importante participação que o Brasil teve na MINUSTAH (*Mission des Nations Unies pour la Stabilisation en Haïti*), Operação de Paz das Nações Unidas cujas Forças Brasileiras estiveram liderando desde sua implantação em 2004 (HAMMAN; TEIXEIRA, 2017).

Recorrer à ONU e ao CS nesta Orientação está relacionado muito mais a uma questão política do que de Segurança Internacional, na medida em que o governo brasileiro vem buscando, desde o início do século, maior prestígio frente à Organização Internacional (BRASIL, 2005). Treinar e empregar as FFAA em operações internacionais pode passar a sensação de preparo do nosso aparato militar, gerando maior reconhecimento nacional e internacional¹⁰¹.

Ao que se refere ao terceiro e último novo ponto em relação à PDN original de 2005, o ponto 7.21, entendemos que as palavras-chave “transporte”, “energia” e “comunicações” empregadas nesta Orientação são fundamentais em sua compreensão. Sendo uma das últimas Orientações da Política Nacional de Defesa, este ponto estabeleceu que cada vez mais medidas voltadas para a Defesa Nacional fossem estimuladas considerando principalmente a tríade transporte-energia-comunicações, uma vez que, já citado no documento, desenvolvimento e defesa devem caminhar lado a lado.

¹⁰¹ Para mais informações a respeito da participação do Brasil na MINUSTAH, missão no Haiti, ver: HAMANN; TEIXEIRA, 2017. A publicação trata-se de textos elaborados por civis estudiosos da área e também militares que estiveram presentes na missão.

Entendemos, dessa forma, que houve mais um estímulo à modernização brasileira nestes quesitos, uma vez que podem representar vulnerabilidades quando consideradas do ponto de vista da Defesa Nacional.

4.2.3.2 Algumas Considerações a respeito da PDN (2005)

De forma geral, entendemos que a Política de Defesa Nacional de 2005 surgiu como uma forma de atualização daquela sucinta publicada em 1996. Esta nova versão de 2005 foi elaborada em um contexto pós-2001, ou seja, após o ataque terrorista em Nova Iorque, contexto pelo qual novos elementos passaram a ser considerados quando a Segurança e a Defesa eram debatidas.

Uma vez que o Ministério da Defesa no Brasil foi fundado apenas em 1999, a Política de Defesa Nacional de 2005 também apareceu neste contexto como uma responsabilidade do MD, o que pode justificar maior dedicação ao texto e uma maior especificação das prioridades para a Defesa no Brasil.

Como já mencionado, a Política de Defesa Nacional de 2005 foi um produto das reuniões do Seminário para a Política de Defesa no Século XXI realizadas no Congresso Nacional em 2002, reiterando nosso argumento de que estes dois acontecimentos foram importantes para que se estabelecesse o discurso de segurança nacional envolvendo a tecnologia e sua vulnerabilidade. Isto, por sua vez, pautou os primeiros passos na implementação de medidas efetivas no setor.

A atualização feita em 2012 serviu como meio para anexar a Estratégia Nacional de Defesa de 2008 à Política de Defesa Nacional, reestruturando seus objetivos, de forma a complementar um documento ao outro e deixar as funções do Ministério da Defesa e das Forças Armadas Brasileiras mais claras.

Foi na atualização de 2012, também, como vimos, que o setor cibernético passou a ser considerado como estratégico pela Política (seguindo aquilo já estabelecido em 2008 pela END), garantindo que fosse reconhecida sua importância (e possível vulnerabilidade) para que o emprego das Forças Armadas em sua proteção fosse legitimado pelo documento.

Finalmente, entendemos que a Política de Defesa Nacional, em suas versões de 1996, 2005 e, atualmente, de 2012, são importantes enquanto documentos em que podemos *observar* e *analisar* a evolução da ideia de Segurança e Defesa no Brasil, com novas prioridades que foram sendo modernizadas segundo o contexto na qual se inseriam.

A discussão a respeito da tecnologia evoluiu para a discussão a respeito da importância das tecnologias de comunicação que, por sua vez, resultou na discussão a respeito do ciberespaço e suas vulnerabilidades. Estes últimos passarão a aparecer oficialmente com mais frequência nos documentos governamentais, como veremos posteriormente.

Ademais, a Política de Defesa Nacional brasileira determina, ainda que de forma implícita, a importância das Forças Armadas para o País, sugerindo atualizações e ampliações de sua atuação na sociedade.

4.3 Medidas voltadas à segurança do ciberespaço brasileiro

Tendo o discurso a respeito da relação tecnologia e segurança se postulado entre 2002 e 2005 através dos documentos Seminário Para Política do Século XXI (2002), Projeto de Declaração Sobre a Segurança Nas Américas (2003) e Política de Defesa Nacional (2005), medidas voltadas à segurança do ciberespaço brasileiro puderam ser legitimadas nos anos que se seguiram.

Levando em consideração o processo de *ação emergencial* postulado por Buzan, Wæver e De Wilde (1998) durante a securitização, objetivamos construir, nesta seção, o argumento de que as medidas tomadas a partir de 2008 relacionam-se a estas ações emergenciais, tomando como contexto o espaço cibernético brasileiro.

Ressaltamos que, como já afirmado no capítulo anterior, a fase da ação emergencial é o segundo elemento (ou passo), de acordo os autores da Escola de Copenhague, para que o processo de securitização ocorra com sucesso (BUZAN; WÆVER; DE WILDE, 1998, p. 26). Entendemos, a partir da leitura a respeito da Securitização, que é criada uma *demand*a de segurança para um determinado objeto durante o *speech-act* que, por sua vez, resulta na ação emergencial.

Destacamos a importância da Estratégia Nacional de Defesa, publicada em 2008, qual apresentou o ciberespaço enquanto setor estratégico para o Brasil em termos de manutenção de sua Segurança pela primeira vez. A partir de então, houve registros da criação de Centros e Núcleos militarizados especializados voltados para a segurança cibernética.

Compreendemos que estes momentos – a promulgação da Estratégia Nacional de Defesa de 2008, e a posterior criação dos Centro de Defesa Cibernético através do Boletim nº 31 do Exército em 2010 – caracterizam a fase de tomada de ação emergencial, visando a segurança do espaço cibernético brasileiro.

4.3.1 Estratégia Nacional de Defesa (2008)

Como já tratada, a Política de Defesa Nacional – considerada nova em relação àquela publicada em 1996 – foi um marco importante no que se refere à política voltada para a defesa no Brasil na medida em que seguiu a tendência de *alargamento* do conceito de segurança e definiu novas preocupações em matéria de defesa. Este documento (atualizado em 2012) foi o responsável para que, em 2008, ainda no governo Lula, fosse elaborada a Estratégia

Nacional de Defesa, com orientações às Forças Armadas na garantia da defesa nacional, e que apresentou os interesses e motivações do Ministério da Defesa brasileiro no cumprimento com suas obrigações com a Defesa e a Segurança.

A Estratégia Nacional de Defesa foi aprovada em 18 de dezembro de 2008 através do Decreto Presidencial nº 6.703 pelo então presidente Luís Inácio Lula da Silva. Ao próprio Decreto, a Estratégia estava anexa, enumerando todos os elementos considerados fundamentais na garantia da defesa brasileira, como foi visualizado à época.

Entendemos que tanto o Ministro da Defesa, Nelson Jobim, quanto o Ministro-Chefe da Secretaria de Assuntos Estratégicos da Presidência da República, Roberto Mangabeira Unger, à época, foram parte do processo, como aparecem no Decreto originalmente publicado no Diário Oficial da União.

Dentre os principais objetivos da Estratégia de Defesa, como descrito no documento anexo ao Decreto, teve-se:

Orientar de forma sistemática a *reorganização* e *reorientação* das Forças Armadas; a organização da indústria de material de defesa, com a finalidade de assegurar a autonomia operacional para as três Forças: a Marinha, o Exército e a Aeronáutica; e a política de composição dos seus efetivos, sobretudo a reconsideração do Serviço Militar Obrigatório (BRASIL, 2008, s/p, grifo nosso).

Entendemos que a Estratégia Nacional de Defesa foi organizada para que dispusesse sobre estas três questões. A maior parte da Estratégia é dedicada à primeira: a *reorganização* e *reorientação* das Forças Armadas com, originalmente, 23 diretrizes e seções dedicadas a elucidar sobre cada uma das Forças e sua importância no sistema de Defesa brasileiro (BRASIL, 2008, grifo nosso).

As outras duas questões (a organização da indústria de material de defesa e as reconsiderações a respeito do Serviço Militar Obrigatório) não serão aqui mencionadas, pois não contribuem efetivamente para o debate a respeito do fomento ao setor cibernético no Brasil.

Evidenciou-se, neste documento, o intuito do governo à época de reformular o papel das Forças Armadas, empregando maior responsabilidade ao Exército Brasileiro, Marinha e Força Aérea. Entendemos que este movimento se relaciona a uma tendência de ampliação do conceito de Segurança que iniciou na década de 1990, com a promulgação da primeira Política de Defesa Nacional, pelo FHC, seguida da própria nova Política de Defesa Nacional

de 2005 (BRASIL, 1996; BRASIL, 2005). Em ambos documentos se ampliou a agenda de Defesa Nacional com novos elementos que despontaram com o fim da Guerra Fria, mas pouco se desdobrou o assunto (BRASIL, 1996; BRASIL, 2005).

Na Estratégia Nacional de Defesa, de 2008, o alargamento da ideia a respeito daquilo que é considerado “ameaça” ou “estratégico” é ainda maior em um contexto pós 11 de setembro de 2001, que trouxe outros *novos elementos* ao debate de Segurança Internacional e Defesa, assim como a própria (nova) Política de Defesa Nacional, de 2005.

De acordo com o que pôde se observar da Estratégia Nacional de Defesa, a ideia de “Independência Nacional” foi recorrente no texto do documento. Como apontado, a Estratégia Nacional de Defesa é inseparável da Estratégia Nacional de Desenvolvimento (BRASIL, 2008). O objetivo da “Independência Nacional” pôde ser observado nos três princípios que guiam, especialmente, a questão do desenvolvimento:

- a) *Independência nacional*, efetivada pela mobilização de recursos físicos, econômicos e humanos, para o investimento no potencial produtivo do País. Aproveitar a poupança estrangeira, sem dela depender;
- b) *Independência nacional*, alcançada pela capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear. Não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento; e
- c) *Independência nacional*, assegurada pela democratização de oportunidades educativas e econômicas e pelas oportunidades para ampliar a participação popular nos processos decisórios da vida política e econômica do País. O Brasil não será independente enquanto faltar para parcela do seu povo condições para aprender, trabalhar e produzir (BRASIL, 2008, s/p, grifo nosso).

Apenas neste trecho da disposição original da Estratégia Nacional de Defesa de 2008 já é possível fazer algumas considerações. Primeira: a visão de desenvolvimento do governo Lula estava atrelada a uma ideia de independência brasileira em relação aos grandes centros, sendo elas, quando combinada à Defesa Nacional, a independência *econômica, tecnológica e educacional*; segunda consideração: a independência nacional é importante para um país de localização estratégica como o Brasil na medida em que pode ser capaz de ser mais enfático em suas decisões¹⁰²; terceira consideração: o desenvolvimento, conforme exposto,

¹⁰² Tanto em sua redação original, de 2008, quando na sua atualização, em 2012, a Estratégia Nacional de Defesa foi enfática ao que se refere à independência do país. Como afirmado: “Defendido, o Brasil terá como dizer não, quando tiver que dizer não. Terá capacidade para construir seu próprio modelo de desenvolvimento” (BRASIL, 2008, s/p). Esta citação também aparece na versão de 2012 da END, na página 43.

está relacionado à presença do Brasil em setores estratégicos, entre eles, o *cibernético*, matéria de interesse na presente pesquisa e que será tratado posteriormente nesta seção.

Ainda de acordo com o documento, no que se refere às Forças Armadas e sua atuação no século XXI: “Não se trata apenas de financiar e equipar as Forças Armadas. Trata-se de *transformá-las*, para melhor defenderem o Brasil” (BRASIL, 2008, s/p, grifo nosso). Inferimos, a partir desta citação, que era necessária a transformação da atuação das FFAA na garantia da Defesa do Brasil, pois modernizá-las significaria que o Brasil seria mais proeminente na defesa de seus interesses e, conseqüentemente, mais independente de influência externa.

Dessa forma, a reorganização e a reorientação das Forças Armadas foram pautadas sob o trinômio *monitoramento/controle, mobilidade e presença* (BRASIL, 2008, s/p). Estes três pontos pautaram a formulação das diretrizes e eixos estruturantes da Estratégia Nacional de Defesa ao que diz respeito ao papel de cada uma das Forças.

Cabe ressaltar que o conceito de *flexibilidade* foi utilizado no texto da END. Conceito mencionado como de fundamental importância na reorganização do papel das Forças Armadas na garantia da Defesa Nacional pelo então Ministro da Defesa Geraldo Mangela Quintão em seu discurso na Câmara em 2002, como já mencionado anteriormente neste capítulo (QUINTÃO, 2003), a flexibilidade foi recolocada, agora atrelada a outro conceito: a *elasticidade* (BRASIL, 2008). Ambos imperativos têm sua própria definição, segundo o documento:

Flexibilidade é a capacidade de empregar forças militares com o mínimo de rigidez pré-estabelecida e com o máximo de adaptabilidade à circunstância de emprego da força. Na paz, significa a versatilidade com que se substitui a presença - ou a onipresença - pela capacidade de se fazer presente (mobilidade) à luz da informação (monitoramento/controle). Na guerra, exige a capacidade de deixar o inimigo em desequilíbrio permanente, surpreendendo-o por meio da dialética da desconcentração e da concentração de forças e da audácia com que se desfecha o golpe inesperado (BRASIL, 2008, s/p).

Já a elasticidade é definida como:

[...] a capacidade de aumentar rapidamente o dimensionamento das forças militares quando as circunstâncias o exigirem, mobilizando em grande escala os recursos humanos e materiais do País. A elasticidade exige, portanto, a construção de força de reserva, mobilizável de acordo com as circunstâncias [...] (BRASIL, 2008, s/p).

A Estratégia Nacional de Defesa, portanto, estabeleceu estes dois conceitos a fim de guiar o desempenho das Forças Armadas a partir de 2008. Houve uma tentativa, como entendemos, de dar maior suporte a nova doutrina voltada às Forças Armadas, conferindo crescentes importância e responsabilidade em sua atuação no Brasil.

4.3.1.1 A atualização de 2012

Assim como a nova Política de Defesa Nacional, de 2005, foi atualizada, tornando-se Política Nacional de Defesa em 2012, a Estratégia Nacional de Defesa passou por uma atualização no mesmo ano. Como já afirmamos, a partir de 2012 a PND e a END tornaram-se um único documento anexo.

Diferentemente da Política de Defesa Nacional de 2005, não houve muitas mudanças significativas entre o documento de 2008 da Estratégia Nacional de Defesa e o novo, de 2012. Dessa forma, observamos certa manutenção do pensamento a respeito da Defesa e suas diretrizes entre a passagem do Governo Lula e ao Governo Dilma.

Dentre as mudanças destacamos duas: a nova redação da Diretriz Estratégica nº 19 e a adição de outras duas Diretrizes Estratégicas às aquelas 23 já existentes, as de nº 24 e 25.

Comparativamente, a Diretriz nº 19 rege sobre a mesma questão tanto na versão de 2008 da END quanto naquela de 2012: a participação do efetivo militar brasileiro em empreitadas internacionais.

Em 2008, temos a seguinte descrição da Diretriz nº 19:

19. Preparar as Forças Armadas para desempenharem responsabilidades crescentes em *operações de manutenção da paz*. Em tais operações, as Forças agirão sob a orientação das Nações Unidas ou em apoio a iniciativas de órgãos multilaterais da região, pois o fortalecimento do *sistema de segurança coletiva* é benéfico à paz mundial e à defesa nacional (BRASIL, 2008, s/p, grifo nosso).

Já em sua versão atualizada, de 2012, a décima nona diretriz é descrita como observamos:

19. Preparar as Forças Armadas para desempenharem responsabilidades crescentes em *operações internacionais de apoio à política exterior do Brasil*. Em tais operações, as Forças agirão sob a orientação das Nações Unidas ou em apoio a iniciativas de órgãos multilaterais da região, pois o fortalecimento do *sistema de segurança coletiva* é benéfico à paz mundial e à defesa nacional (BRASIL, 2012a, p. 59, grifo nosso).

Apesar de quase não haver diferenças significativas na nova versão da Diretriz nº 19, destacamos duas questões. A primeira é que, em um primeiro momento, o Ministério da

Defesa deu atenção especial a operações de manutenção da paz, tais quais passaram a ser recorrentes no início do século e promovidas, especialmente pelo Conselho de Segurança das Nações Unidas. Já em sua nova versão, a Diretriz foi reescrita enquanto “operações internacionais de apoio à política exterior do Brasil” (BRASIL, 2012a, p. 59).

Isto pode significar uma visão mais ampla a respeito da participação do Brasil internacionalmente em termos de Defesa, buscando maior presença em operações de quaisquer tipos. Entendemos que esta questão se relaciona à crescente visibilidade que as Forças Armadas brasileiras almejavam à época.

Uma segunda questão que destacamos e que permaneceu a mesma em ambas Diretrizes diz respeito ao “sistema de segurança coletiva” (BRASIL, 2008; BRASIL, 2012a, p. 59). Como já observado no início deste capítulo, as discussões a respeito das transformações em segurança ocorridas em âmbito regional, na Organização dos Estados Americanos em 2003, remontaram esta ideia de uma segurança hemisférica, visando uma cooperação regional para a segurança (OEA, 2003). O conceito de segurança coletiva remonta, por sua vez, uma proposta da Organização das Nações Unidas, visando o mesmo objetivo de cooperação e tomadas de medidas no âmbito da Segurança para a manutenção da paz internacionalmente (REZENDE; AZEVEDO, 2011).

A partir disso, podemos observar que a importância dada a conceitos regionais e internacionais de segurança permaneceram na Estratégia Nacional de Defesa.

Além das questões que envolvem a Diretriz nº 19, duas outras novas Diretrizes foram adicionadas no documento de 2012, totalizando 25. São elas:

24. Participar da concepção e do desenvolvimento da infraestrutura estratégica do País, para incluir requisitos necessários à Defesa Nacional. A infraestrutura estratégica do Brasil deverá contemplar estudos para emprego dual, ou seja, atender à sociedade e à economia do País, bem como à Defesa Nacional. **25.** Inserir, nos cursos de altos estudos estratégicos de oficiais das três forças, os princípios e diretrizes da Estratégia Nacional de Defesa, inclusive aqueles que dizem respeito ao Estado-Maior Conjunto (BRASIL, 2012a, p. 63).

Entendemos que a Diretriz nº 24 reforça a necessidade do desenvolvimento daquelas estruturas estratégicas, na medida em que tem relação com a vontade do Ministério da Defesa em desenvolver sua Indústria de Material de Defesa, voltado à uma independência nacional neste quesito.

A última Diretriz, por sua vez, também reforça a importância de que o reconhecimento de todos os objetivos da Estratégia Nacional de Defesa seja de conhecimento de todos envolvidos na Defesa no Brasil.

Entendemos, como argumentaremos nas considerações desta seção, que houve, a partir da Estratégia Nacional de Defesa, uma crescente preocupação com a capacitação das Forças Armadas para com as transformações no âmbito da Defesa no Brasil. A Diretriz nº 25 – e o documento como um todo – apontaram para a necessidade de práticas de treinamento e capacitação do pessoal, levando em consideração os imperativos de flexibilidade e elasticidade (BRASIL, 2008; BRASIL, 2012a).

4.3.1.2 A importância da Sexta Diretriz da Estratégia Nacional de Defesa

Dentre as atuais 25 Diretrizes postuladas no documento da Estratégia Nacional de Defesa, destacamos a de número seis para a discussão. Isto, pois, entendemos que é a partir de tal Diretriz que houve a intensificação da cibersegurança no Brasil.

Objetivando a reorganização e a reorientação das Forças Armadas, bem como o seu papel frente à ampliação do entendimento a respeito de Defesa e Segurança no Brasil, o documento passou a considerar três setores como sendo de valor estratégico: o Cibernético, o Nuclear e o Espacial.

Conforme apresentou o documento em sua sexta Diretriz:

6. Fortalecer três setores de importância estratégica: o espacial, o cibernético e o nuclear. Esse fortalecimento assegurará o atendimento ao conceito de flexibilidade. Como decorrência de sua própria natureza, esses setores transcendem a divisão entre desenvolvimento e defesa, entre o civil e o militar. Os setores espacial e cibernético permitirão, em conjunto, que a capacidade de visualizar o próprio País não dependa de tecnologia estrangeira e que as três Forças, em conjunto, possam atuar em rede, instruídas por monitoramento que se faça também a partir do espaço [...] (BRASIL, 2012a, p. 49).

Sendo as Diretrizes as ações sugeridas pelo Ministério da Defesa na proteção Brasileira, algumas questões emergem da Sexta Diretriz. Primeira, que o Governo Federal e o Ministério da Defesa assumiram a necessidade de formular um documento com o que pôde ser considerado como setores estratégicos para além daqueles tradicionais, enxergando, também, o ciberespaço; segunda, estes três “setores de importância estratégica” são colocados fora de uma hierarquia, em um “mesmo patamar” pelo Ministério da Defesa e a responsabilidade sobre os três são as próprias três Forças; terceiro e finalmente, o conceito

de flexibilidade foi retomado: agora na condição de imperativo capaz de ser alcançado com o fortalecimento dos setores estratégicos.

Incorporar o ciberespaço como elemento estratégico para a Defesa no Brasil pôde, por sua vez, justificar medidas que foram posteriormente tomadas neste sentido.

A versão atualizada da END, de 2012, disponibilizou uma seção exclusiva para a compreensão dos setores estratégicos, os quais são “essenciais para a defesa nacional” (BRASIL, 2012a, p. 93). Ao que se refere ao setor cibernético, “as capacitações se destinarão ao *mais amplo espectro* dos usos industriais, educativos e militares” (BRASIL, 2012a, p. 93, grifo nosso).

Nesta seção, o documento também apresentou quais seriam as prioridades do setor cibernético. Optamos por trazê-las integralmente¹⁰³. São oito:

- (a)** Fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas; **(b)** Aprimorar a Segurança da Informação e Comunicações (SIC), particularmente, no tocante à certificação digital no contexto da Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa), integrando as ICP das três Forças; **(c)** Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Fazenda, da Ciência, Tecnologia e Inovação, da Educação, do Planejamento, Orçamento e Gestão, a Secretaria de Assuntos Estratégicos da Presidência da República e o Gabinete de Segurança Institucional da Presidência da República deverão elaborar estudo com vistas à criação da Escola Nacional de Defesa Cibernética; **(d)** *Desenvolver sistemas computacionais de defesa* baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual; **(e)** Desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como sistema modular de defesa cibernética e sistema de segurança em ambientes computacionais; **(f)** Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da *proteção das infraestruturas estratégicas*; **(g)** Incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e **(h)** Estruturar a produção de conhecimento oriundo da fonte cibernética (BRASIL, 2012a, p. 94-95, grifo nosso).

Dessa forma, a Estratégia Nacional de Defesa em 2008 reconheceu a existência do ciberespaço brasileiro como um aspecto estratégico de defesa, contendo vulnerabilidades e

¹⁰³ Ressaltamos que estas prioridades foram apresentadas no documento de 2012, a atualização da Estratégia Nacional de Defesa, que acompanhou, também, a atualização da Política de Defesa Nacional. Essa atualização com estas prioridades pode ter relação com o já implementado Centro de Defesa Cibernética em 2010.

vantagens. A atualização de 2012, para além da publicação original de 2008, traçou tais prioridades relacionadas à matéria. Destacamos, entre todas, a “proteção das infraestruturas estratégicas”, por se tratar de um objetivo recorrente no tratamento do ciberespaço (BRASIL, 2003; BRASIL, 2005; BRASIL, 2008; BRASIL, 2012a).

Desde a automação da indústria ao funcionamento do mercado financeiro, sistemas operacionais governamentais e meios de comunicação em geral, entendemos que o ciberespaço cumpre papel de permeá-los. Tais setores, entre vários outros, podem ser considerados, portanto, como estratégicos ou como infraestrutura crítica.

A crescente valorização, à vista disso, de uma segurança voltada ao ciberespaço remonta a proteção destes setores e ou infraestruturas estratégicas para o funcionamento do Estado capitalista. Posteriormente, quando apresentarmos o contexto internacional de vulnerabilidades cibernéticas, ficará mais claro como ataques cibernéticos a certos sistemas podem afetar tais estruturas e acarretar danos materiais e financeiros e também, implicações políticas e militares.

Voltando ao tratamento da END, podemos observar, que o Governo Federal e o Ministério da Defesa, por sua vez, legitimaram, a partir desta Estratégia Nacional de Defesa de 2008, medidas a serem tomadas visando a defesa cibernética (BRASIL, 2008). O emprego das Forças Armadas, em especial o Exército na segurança cibernética, também foi estratégico segundo o entendimento do MD à época na proteção de infraestruturas críticas.

Há uma argumentação que aqui podemos fazer a respeito das responsabilidades ligadas às Forças Armadas e cibersegurança. Entendemos que, desde a criação do Ministério da Defesa em 1999 até a publicação da END em 2008, as Forças Armadas ganharam cada vez mais espaço dentre as funções estratégicas. Entendemos que designar “setores de interesse estratégico” tais como o cibernético à responsabilidade do Exército Brasileiro, por exemplo, geraram *notoriedade* às funções desta Força, além da própria ampliação de sua atuação.

Entendemos, também, que a notoriedade das FFAA no Brasil (e internacionalmente) já era estimulada desde a instauração da MINUSTAH, missão das Nações Unidas para a Estabilização do Haiti, quando em 2004 o chefe da missão era o general brasileiro Ajax Porto Pinheiro (HAMANN; TEIXEIRA, 2017).

4.3.1.3 Algumas considerações a respeito da END

Os objetivos do Ministério da Defesa com a publicação da Estratégia Nacional de Defesa eram, primordialmente, reorganizar e reorientar as Forças Armadas no Brasil, e este documento permitiu postular as mudanças que seriam feitas a partir de 2008. Dentre as principais, consideramos apontar os setores estratégicos enquanto sendo o espacial, o cibernético e o nuclear.

Adicionado aos setores estratégicos, as Três Forças ganharam maior responsabilidade de atuação, como pôde ser observado justamente no tratamento dos três setores estratégicos como assuntos sob tutela de cada uma delas respectivamente.

A capacitação e treinamento pessoal das Forças partindo de uma necessidade de flexibilidade e elasticidade também foi destaque que pudemos observar na redação da Estratégia Nacional de Defesa. O papel da tecnologia, por exemplo, foi reforçado em diferentes pontos (BRASIL, 2008; BRASIL, 2012a, p. 43; p. 47; p. 48), mesmo o documento deixando evidente que “A tecnologia, por mais avançada que seja, jamais será alternativa ao combate. Será sempre instrumento do combate” (2008, s/p; BRASIL, 2012a, p. 47).

Dessa forma, a tecnologia e o desenvolvimento tecnológico sempre são tratados como ferramentas *dissuasórias* no âmbito da Defesa, sendo sempre mais importante o preparo das Forças Armadas, de forma geral, para o combate (BRASIL, 2012a, p. 47).

Ao que se refere ao setor estratégico cibernético em específico, observamos que as medidas voltadas ao seu desenvolvimento estão relacionadas ao caráter de defesa e proteção de possíveis vulnerabilidades, na medida em que não existe o objetivo de utilizá-lo enquanto uma ferramenta ativa de combate.

Assim sendo, podemos observar na Estratégia Nacional de Defesa de 2008 e sua posterior atualização de 2012 apontamentos relevantes na construção da ressignificação das Forças Armadas no Brasil a partir de uma necessidade de uma reorientação de sua atuação. Esta ressignificação, combinada à crescente menção da importância de setores estratégicos, como o cibernético, confere certo prestígio a atuação das FFAA a partir de então.

Ademais, cabe mencionar que, no momento em que este trabalho estava sendo desenvolvido, o Governo de Jair Bolsonaro atualizou algumas das disposições tanto da END como da PND e do Livro Branco de Defesa Nacional, em 2020.

Esta nova versão que, até o momento, foi submetida ao Congresso Nacional para a apreciação, segue um protocolo de atualização exigido pelo Ministério da Defesa de tempos em tempos. Tendo em vista o posicionamento mais autoritário do governo Bolsonaro, a nova END centralizou ainda mais o papel das Forças Armadas na defesa da população brasileira.

As “Diretrizes” da END viraram “Fundamentos” e o “Poder Nacional” e a necessidade de criar estratégias para a manutenção do Poder Nacional foi frequentemente invocado (BRASIL, 2020a). Essencialmente, os imperativos de flexibilidade e elasticidade permaneceram na versão de 2020 como norteador da ação das Forças Armadas. Os setores estratégicos também permanecem os mesmos e, entre eles, o setor cibernético. A Estratégia Nacional de 2020 previu que a estrutura do Sistema Militar de Defesa Cibernética fosse desenvolvida, preparada e recebesse os investimentos necessários, para que possa ser empregada, “em todos os níveis”, no futuro (BRASIL, 2020a, p. 61).

Apesar de não haver tempo hábil para detalhar mais elementos da END de 2020, podemos afirmar que ela reflete o posicionamento autoritário do governo Bolsonaro.

4.3.2 O Boletim nº 31/10 do Exército Brasileiro (2010)

A partir da nova agenda de Defesa e Segurança postulada pela Estratégia Nacional de Defesa de 2008, que passou a considerar o ciberespaço como setor estratégico de defesa para o governo brasileiro, medidas passaram a ser consideradas pelo Ministério da Defesa na garantia da segurança deste setor.

A medida imediata que podemos observar foi a criação do Centro de Defesa Cibernético (CDCiber) e o Núcleo do Centro de Defesa Cibernético (NuCDCiber) pelo Exército Brasileiro em 2010.

No dia quatro de agosto de 2010 foi publicada, portanto, a portaria nº 666 pelo Comandante do Exército, sendo o documento oficial que originou o Centro de Defesa Cibernética do Exército. A portaria foi publicada oficialmente na 2ª parte (atos administrativos) do Boletim nº 31 de 2010 do Exército, distribuído somente a partir do dia 06 de agosto de 2010.

No mesmo documento podemos observar, também, a publicação da portaria nº 667 pelo mesmo Comandante do Exército que, por sua vez, originou o Núcleo do Centro de Defesa Cibernético, na mesma data.

Cabe elucidar que os Boletins do Exército Brasileiro são documentos publicados pela Secretaria Geral do Exército com funções essencialmente administrativas: faz autorizações, ativa novos Centros e Núcleos, prevê alterações, faz nomeações e designações, entre outros, com o objetivo de formalizar cada uma destes eventos. Dessa forma, é comum que pelo menos um Boletim seja publicado mensalmente pela Secretaria Geral do Exército.

Por se tratar de um documento sucinto e objetivo de uma das Forças, os Boletins do Exército, especialmente nestes casos como o da criação e ativação do CDCiber e do NuCDCiber, respectivamente, não previram outras funções para os órgãos para além de sua autorização de funcionamento (BRASIL, 2010, p. 07; BRASIL, 2010a, p. 08).

Sendo assim, os principais objetivos do Centro de Defesa Cibernético e do Núcleo do Centro de Defesa Cibernético são descritos, oficialmente, apenas no site oficial do Governo Federal, na seção de Defesa¹⁰⁴. Entre os objetivos do CDCiber, consideram: “[...] a capacitação de militares para atuação em situações críticas, o desenvolvimento de sistemas e aplicações duais e a parceria com a indústria nacional para a produção de sistemas inovadores” (SETOR CIBERNÉTICO, 2019, s/p).

Nesta página também podemos observar que, enquanto justificativa para as ações do Centro de Defesa Cibernético tem-se, especialmente o *sigilo* e a *proteção de infraestruturas críticas* (SETOR CIBERNÉTICO, 2019).

A criação dos Centro de Defesa Cibernético e do Núcleo do Centro de Defesa Cibernético, conforme entendemos, foi uma iniciativa importante para que a proteção do espaço cibernético brasileiro chegasse aos níveis operacional e tático (BRASIL, 2014, p. 17). Isto significa que houve capacitação e emprego de pessoal na causa e operações foram estabelecidas. A própria Estratégia Nacional de Defesa, já havia previsto a capacitação deste pessoal no setor estratégico, como já destacado anteriormente (BRASIL, 2008).

Ativado em agosto de 2010, o CDCiber e o NuCDCiber se tornaram operacionais em 2011, após o treinamento de pessoal – militar – autorizado em questões de segurança cibernética.

Enquanto suas capacidades, como afirmaram os pesquisadores do Instituto Igarapé Muggah, Glenn e Diniz: “O CDCiber possui um simulador de *ciberguerra*, um laboratório

¹⁰⁴ Disponível em: <https://www.defesa.gov.br/ciencia-e-tecnologia/setores-estrategicos/setor-cibernetico>. Acesso em: 24 jan. 2020.

de análise códigos virtuais maléficos, além de quase cem especialistas com treinamento em cibersegurança” (MUGGAH; GLENN; DINIZ, 2014, p. 99, grifo nosso).

Como veremos posteriormente, o termo “ciberguerra”, ou Guerra Cibernética, será bastante empregado pelos responsáveis pela cibersegurança, assim como observado em documentos como a Doutrina Militar de Defesa Cibernética (2014) e a Política Cibernética de Defesa (2014), produtos do próprio Centro de Defesa Cibernético.

Ainda sobre a operacionalização do Centro de Defesa Cibernético, desde seu funcionamento em 2011, podemos apenas afirmar que, oficialmente, vem trabalhando em operações que busquem a segurança cibernética ao que se refere ao sigilo, proteção de dados, e de infraestrutura estratégica brasileira, além de trabalhos focados em grandes eventos internacionais esportivos tais como a Copa do Mundo FIFA, através do monitoramento de qualquer atividade suspeita que poderia no âmbito do ciberespaço (SETOR CIBERNÉTICO, 2019; MUGGAH; GLENN; DINIZ, 2014).

Por se tratar de um órgão relativamente novo no âmbito governamental, e com proteção e sigilo de funcionamento garantido pelo Ministério da Defesa, na medida em que o espaço cibernético é considerado setor estratégico, temos poucas informações oficiais a respeito do funcionamento dos CDCiber e NuCDCiber disponíveis.

Quando consultado através do Sistema de Acesso a Informações do Governo Federal¹⁰⁵ pela autora, o Ministério da Defesa, através da Assessoria da Seção de Informação ao Cidadão do Centro de Comunicação Social do Exército afirmou que informações a respeito do efetivo, ou seja, a quantidade de pessoal envolvido no CDCiber, são sigilosas e não forneceu nenhum outro desenvolvimento a respeito do questionamento a respeito da organização.

O que podemos afirmar a respeito destes órgãos, entretanto, é que têm caráter essencialmente militar por ser de responsabilidade do Exército Brasileiro e contar com uma Doutrina Militar específica para a Defesa Cibernética que norteia sua atuação, documentos os quais discutiremos posteriormente neste trabalho.

A dificuldade de se obter informações a respeito de seu funcionamento e efetivo apenas reforça o caráter militar da organização.

¹⁰⁵ O protocolo de solicitação de informação no Sistema de Acesso a Informação é de nº 60502.002337/2020-84.

4.4 Produtos das políticas de cibersegurança

Compreendemos que a Estratégia Nacional de Defesa foi um elemento importante para a cibersegurança no Brasil, pois apresentou o setor cibernético como estratégico e, com a atualização feita em 2012, explicitou a necessidade de investimento no setor, além de dar liberdade às Forças Armadas atuarem na área.

Os Centro de Defesa Cibernética e Núcleo do Centro de Defesa Cibernética também desempenharam papel importante no estabelecimento de uma equipe brasileira militar focada na proteção cibernética.

Com “produtos das políticas de cibersegurança”, queremos analisar o último elemento ou passo para o processo de securitização ocorrer com sucesso: os efeitos na relação entre as unidades.

Retomando o pensamento da Escola de Copenhague apresentado no item 2 desta investigação, os autores afirmaram que uma securitização de sucesso deve ter “três elementos (ou passos): [postular a] ameaça existencial; [tomar a] ação emergencial; e [observar os] efeitos na relação entre as unidades após se libertarem das regras” (BUZAN; WÆVER; DE WILDE, 1998, p. 26, tradução nossa¹⁰⁶).

Entendemos que a ameaça existencial ocorreu com a construção do discurso de segurança entre 2002 e 2007 que, por sua vez, levou às condições que possibilitaram a promulgação da Estratégia Nacional de Defesa em 2008 e a criação do Centro de Defesa Cibernética e do Núcleo do Centro de Defesa Cibernética em 2010 – as ações emergenciais.

Dessa forma, buscamos aqui inferir o que o governo brasileiro, no âmbito do Ministério da Defesa, promoveu depois de aprovar a Estratégia Nacional de Defesa e autorizar a criação e o investimento no CDCiber e no NuCDCiber.

São cinco os produtos que nos propusemos a analisar nesta seção do capítulo a saber: Política Cibernética de Defesa (2012), Doutrina Militar de Segurança Cibernética (2014), Marco Civil da Internet (2014), Guia de Defesa Cibernética na América do Sul (2017) e Política Nacional da Segurança da Informação (2018). Os apresentaremos de forma cronológica, conforme foram publicados ao longo da última década.

¹⁰⁶ No original: “A successful securitization thus has three components (or steps): existential threats, emergency action, and effects on interunit relations by breaking free of rules” (BUZAN; WÆVER; DE WILDE, 1998, p. 26).

4.4.1 Política Cibernética de Defesa (2012)

Entendemos que, após a consideração do Ciberespaço enquanto setor estratégico de Segurança e Defesa pela Estratégia Nacional de Defesa de 2008 e da Criação do Centro de Defesa Cibernético (CDCiber) em 2010, a produção de uma Política que tratasse especificamente das ações voltadas ao setor cibernético seriam promovidas eventualmente na medida em que ciberataques ocorriam no nível internacional com certa frequência, como tratado no capítulo anterior.

A Política Cibernética de Defesa foi um documento aprovado em 2012 através da Portaria Normativa nº 3.389 do Ministério da Defesa em 21 de dezembro, pelo então Ministro Celso Amorim. A Portaria foi publicada no Diário Oficial da União no dia 27 de dezembro do mesmo ano.

A Política Cibernética de Defesa foi, portanto, um produto do Centro de Defesa Cibernético e se trata de um documento conciso, com quatro capítulos, a saber: Introdução, Objetivos, Diretrizes e Responsabilidades e Atualização (BRASIL, 2012).

De acordo com o próprio documento, a Política Cibernética de Defesa teve como finalidade: “[...] orientar, no âmbito do Ministério da Defesa (MD), as atividades de *Defesa Cibernética*, no nível estratégico, e de *Guerra Cibernética*, nos níveis operacional e tático, visando a consecução dos seus objetivos” (BRASIL, 2012, p. 11, grifo nosso).

O termo “Guerra Cibernética” utilizado, apesar de já ter sua definição inclusa no primeiro volume da Doutrina de Operações Conjuntas, elaborada pelo Estado-Maior Conjunto das Forças Armadas (BRASIL, 2011), não apresenta, neste documento, uma explicação explícita. Dessa forma, o que pode ser inferido é que a Guerra Cibernética se relaciona aos níveis operacional e tático, ou seja, *na ação efetiva* das Forças Armadas no ciberespaço.

Uma definição do conceito de Guerra Cibernética¹⁰⁷ foi formulada na publicação de 2014 da Doutrina Militar de Defesa Cibernética, bem como outros termos referentes a atuação no ciberespaço. Entendemos que a Doutrina Militar de Defesa Cibernética se trata de um documento mais extenso com a finalidade de *uniformizar* o pensamento do MD e das

¹⁰⁷ Apresentamos a definição de Guerra Cibernética de acordo com as Forças Armadas Brasileiras e Ministério da Defesa em nossa Introdução, mas o conceito será retomado do tópico seguinte (4.4.2) em nossa retomada histórica e construção argumentativa.

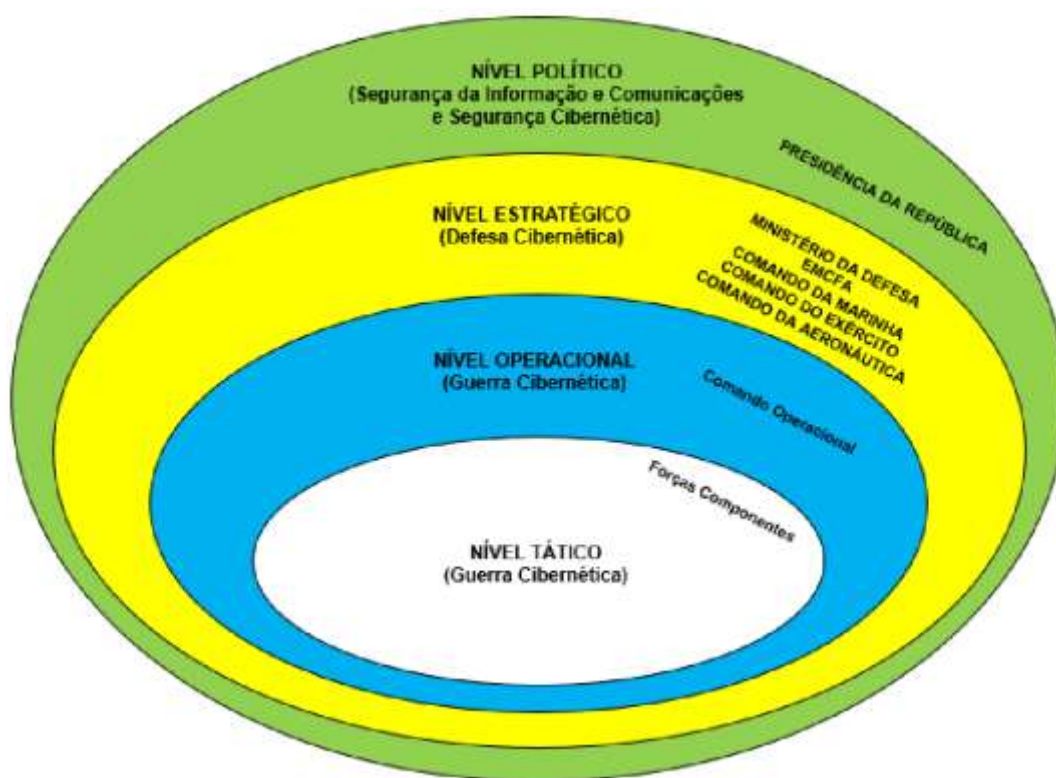
FFAA na compreensão de questões envolvendo a cibersegurança. Abordaremos a Doutrina no tópico seguinte.

No caso Brasileiro, as diferenças entre Defesa Cibernética e Guerra Cibernética se encontram nos níveis de tomada de decisão. Em termos gerais, a Defesa Cibernética cabe ao Ministério da Defesa, ao Estado Maior Comando das Forças Armadas e aos Comandos das Três Forças, pois este é o nível *operacional* da cibersegurança.

A Guerra Cibernética, por sua vez, cabe ao Comando e as Forças Componentes, ou seja, os militares designados para a cibersegurança efetivamente, nos níveis *operacional* e *tático* (BRASIL, 2014).

A Guerra Cibernética, dessa forma está relacionada à atuação no ciberespaço efetivamente pelo Comando Componente e pelas Forças Componentes, pessoal que deveria ser treinado na cibersegurança (BRASIL, 2014; BRASIL 2012).

FIGURA 1: NÍVEIS DE DECISÃO



Fonte: BRASIL, 2014, p. 17.

Ao que se refere aos objetivos específicos da Política Cibernética de Defesa, como o documento postula, tem-se:

a) assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FA) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional; b) capacitar e gerir talentos humanos necessários à condução das atividades do Setor Cibernético (St Ciber) no âmbito do MD; c) colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR); d) desenvolver e manter atualizada a doutrina de emprego do St Ciber; e) implementar medidas que contribuam para a Gestão da SIC no âmbito do MD; f) adequar as estruturas de C,T&I das três Forças e implementar atividades de pesquisa e desenvolvimento para atender às necessidades do St Ciber; g) definir os princípios básicos que norteiem a criação de legislação e normas específicas para o emprego no St Ciber; h) cooperar com o esforço de mobilização nacional e militar para assegurar a capacidade operacional e, em consequência, a capacidade dissuasória do St Ciber; e i) contribuir para a segurança dos ativos de informação da Administração Pública Federal (APF), no que se refere à Segurança Cibernética, situados fora do âmbito do MD (BRASIL, 2012, p. 13).

Podemos inferir, dessa forma, que a Política Cibernética de Defesa previu um maior investimento em ciência e tecnologia, considerando a relevância da cibersegurança e necessidade de preparo das Forças Armadas, em específico, para lidar com as ameaças do setor.

A Política Cibernética de Defesa, de 2012, portanto, deveria ser “aplicada a todos os componentes da expressão militar do Poder Nacional” (BRASIL, 2012, p. 11), na medida em que a tutela da segurança cibernética, como já vimos, coube às Forças Armadas, e em específico, ao Exército Brasileiro. O documento também previu que outros agentes envolvidos na Defesa Cibernética também seguissem as diretrizes que foram propostas pelo CDCiber.

A partir de um amadurecimento maior do MD envolvendo a cibersegurança a partir da criação do CDCiber, a Política Cibernética de Defesa partiu de *sete pressupostos* básicos envolvendo o espaço cibernético enquanto setor estratégico e matéria de segurança. São eles:

a) a eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa; b) as atividades de Defesa Cibernética no MD são orientadas para atender às necessidades da Defesa Nacional; c) as ações cibernéticas de caráter ofensivo deverão estar em conformidade com o planejamento elaborado em atendimento às Hipóteses de Emprego (HE); d) a capacitação tecnológica do Setor Cibernético deve ser buscada de maneira harmônica com a Política de Ciência, Tecnologia e Inovação para a Defesa Nacional (C,T&I); e) a eficácia das ações de Defesa Cibernética no MD depende diretamente do grau de conscientização alcançado junto às

organizações e pessoas acerca do valor da informação que detêm ou processam; f) a Segurança da Informação e Comunicações (SIC) é a base da Defesa Cibernética e depende diretamente das ações individuais; não há Defesa Cibernética sem ações de SIC; e g) as ações cibernéticas no contexto do MD visam a assegurar o uso do espaço cibernético, impedindo ou dificultando seu uso contra os interesses do País e garantindo, dessa forma, a liberdade de ação (BRASIL, 2012, p. 11).

Os chamados “Pressupostos Básicos” foram importantes de serem postulados, pois passariam a orientar as ações voltadas ao ciberespaço, bem como influenciariam na já mencionada Doutrina Militar de Defesa Cibernética em 2014.

Dentre os pressupostos destacamos o de letra F, referente à importância dada a Segurança da Informação e Comunicações. Ao afirmar que a SIC é “base da Defesa Cibernética” (BRASIL, 2012, p. 11), o Ministério da Defesa reforçou a importância proteção de dados e de informações sensíveis.

Podemos traçar um paralelo com o acontecimento do Caso Snowden, em 2013, no qual revelou-se que o Brasil sofreu ciberespionagem no nível Federal com a Presidência da República à época. Dessa forma, o próprio Gabinete de Segurança Institucional da Presidência da República (GSI/PR) passou a receber maior atenção com os investimentos em cibersegurança.

Dessarte, as revelações de espionagem e a conseguinte atenção ao GSI/PR podem ter levado à publicação do Decreto Presidencial 9.637/18 que instituiu a Política Nacional de Segurança da Informação. O Decreto 9.637/18 será abordado ainda nesta seção posteriormente.

No que diz respeito a Política Cibernética de Defesa, seu principal objetivo, como interpretamos, foi assegurar que as Forças Armadas garantissem, efetivamente, os interesses brasileiros no espaço cibernético e evitassem quaisquer possíveis ameaças à Defesa Nacional (BRASIL, 2012, p. 13).

Entretanto, podemos argumentar também, analisando de uma maneira mais geral, ou seja, olhando a *bigger picture*, que a Política Cibernética de Defesa foi responsável por atrair investimentos ao setor cibernético no que se refere tanto aos equipamentos a serem utilizados pelo CDCiber quanto à capacitação das forças envolvidas na segurança cibernética. Dessa forma, a Política Cibernética de Defesa funcionou como uma forma de justificar os gastos na área de ciência e tecnologia, bem como no treinamento de pessoal especializado e na promoção de projetos que pudessem garantir a cibersegurança.

O ponto de maior destaque da Política, entretanto, como compreendemos, não foram os objetivos, mas sim as *diretrizes* estabelecidas para cumpri-los, na medida em que explicitaram as atividades a serem implementadas pelo Ministério da Defesa e, em especial pelas Forças Armadas, no setor cibernético que ganhava cada vez mais destaque pelo governo brasileiro (BRASIL, 2012, p. 15).

Conforme postulado pela própria Assessoria de Comunicação Social do Ministério da Defesa em nota¹⁰⁸, tais diretrizes já seriam aplicadas nos grandes eventos esportivos sediados no Brasil a partir de 2012: a Copa das Confederações, de 2013, a Copa do Mundo, de 2014 e os Jogos Olímpicos, de 2016 (BRASIL, 2012b).

Outra diretriz da Política Cibernética de Defesa de 2012 que merece destaque é aquela que previu o Sistema Militar de Defesa Cibernética (SMDC) que foi melhor elucidada na Doutrina Militar de Defesa Cibernética de 2014, ganhando capítulo exclusivo (BRASIL, 2014).

Conforme o documento, o Sistema Militar de Defesa Cibernética seria uma das maneiras de garantir o objetivo número um da Política: “assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FFAA) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional” (BRASIL, 2012, p. 15).

Podemos inferir que este Sistema seria implementado através de investimentos do Ministério da Defesa no setor cibernético a fim de coordenar as atividades de defesa cibernética a ser feito, a princípio, pelas Forças Armadas com a colaboração civil.

Na nota publicada pela Assessoria de Comunicação Social do MD e na Política de 2012, foi afirmado que o Sistema Militar de Defesa Cibernética teria a *possibilidade* da atuação de civis (BRASIL, 2012; BRASIL, 2012b).

Ainda segundo a mesma nota publicada em dezembro em 2012:

É atribuição do SMDC [Sistema Militar de Defesa Cibernética] coordenar e integrar as ações de defesa cibernética, no âmbito do MD, nas áreas de inteligência, ciência e tecnologia, operacional, doutrina e recursos humanos. A implementação e gestão do novo sistema é responsabilidade do Estado-Maior Conjunto das Forças Armadas (EMCFA) (BRASIL, 2012b, s/p).

¹⁰⁸ Disponível em: <https://www.defesa.gov.br/noticias/4205-28-12-2012-defesa-md-aprova-politica-cibernetica-de-defesa>. Acesso em: 10 jan. 2020.

Dessa forma, a atuação do Sistema Militar de Defesa Cibernética também aparece em outras diretrizes que visam cumprir os objetivos da Política Cibernética de Defesa. Idealizou-se que tal sistema estaria em coordenação com o Sistema de Inteligência de Defesa (SINDE) para a Segurança da Informação e Comunicação (SIC) e da Defesa Cibernética, na medida em que a produção de conhecimento de inteligência foi um dos objetivos da Política de 2012 (BRASIL, 2012).

Podemos elucidar que, assim como a maior parte das questões envolvendo a cibersegurança no Brasil, o SMDC seria composto por “pessoal com competências ou habilidades, existente nos ambientes interno e externo das FA [sic]” que deveria estar treinado e capacitado para a atuação no setor cibernético (BRASIL, 2012, p. 15).

A “capacitação e geração de talentos humanos” necessária para o desenvolvimento das atividades de segurança e defesa no setor cibernético no âmbito do Ministério da Defesa foi também postulado e estimulado pelas diretrizes da Política Cibernética de Defesa (BRASIL, 2012, p. 15).

A Política Cibernética de Defesa também previu a necessidade da criação de uma Doutrina Militar de Defesa Cibernética já citada neste tópico. De acordo com o documento: “3.2.4 Diretrizes atinentes ao Objetivo Nr IV - *desenvolver e manter atualizada a doutrina de emprego do St Ciber* [Setor Cibernético]: a) criar a doutrina de Defesa Cibernética mediante proposta do órgão central do SMDC [...]” (BRASIL, 2012, p.16, grifo do autor).

Dessa forma, o Sistema Militar de Defesa Cibernética teria como produto a criação de uma Doutrina Militar de Defesa Cibernética responsável por uniformizar a compreensão em níveis Estratégico, Operacional e Tático de operações no Setor Cibernético.

Como veremos na seção seguinte, a criação de uma doutrina militar focada na cibersegurança brasileira foi importante para a compreensão da atuação das Forças Armadas no setor cibernético, bem como a forma como a instituição entende as dinâmicas do setor.

A Política Cibernética de Defesa, por sua vez, previu, através de diretrizes voltadas à CT&I, que fossem coordenados estudos com instituições civis e militares de Pesquisa e Desenvolvimento a fim de compreender as necessidades de capacidade tecnológica voltadas à cibersegurança (BRASIL, 2012, p. 17).

Dessa forma, as estruturas de Ciência, Tecnologia e Inovação passariam a coordenar, também, com as Forças Armadas Brasileiras. Tais diretrizes pressupõem, em última

instância, a necessidade do investimento de recursos no âmbito do Ministério da Defesa para a cibersegurança.

Podemos inferir, ainda, que os assuntos de Ciência, Tecnologia e Inovação no Brasil seguem uma tendência de militarização crescente, tendo em vista os objetivos militares com a especialização nessa área e o crescente envolvimento das Forças Armadas.

4.4.2 Doutrina Militar de Defesa Cibernética (2014)

Um dos principais produtos que oficializou a militarização da cibersegurança no Brasil foi a Doutrina Militar de Defesa cibernética publicada em 2014, documento qual objetivava postular as orientações no tratamento do ciberespaço pelo Ministério da Defesa e pelas Forças Armadas.

A Doutrina Militar de Defesa Cibernética foi promulgada através da Portaria Normativa nº 3.010 do Ministério da Defesa em 18 de novembro de 2014 pelo então Ministro Celso Amorim, sendo publicada ainda no mesmo mês pelo Diário Oficial da União.

Desenvolvida pelo Ministério da Defesa e pelo Estado-Maior Conjunto das Forças Armadas, a Doutrina Militar de Defesa Cibernética é documento anexo à Portaria Normativa e teve como objetivo a compreensão de alguns conceitos relacionados ao ciberespaço no âmbito da defesa.

Considerando o contexto militar qual foi desenvolvida, a Doutrina Militar de Defesa Cibernética se trata de um documento robusto (em comparação a Política Cibernética de Defesa, de 2012) que apresentou cinco capítulos e um organograma em seu Apêndice. Os capítulos são: Introdução, Fundamentos, Sistema Militar de Defesa Cibernética, Defesa e Guerra Cibernética nas Operações e Disposições Finais (BRASIL, 2014, p. 09).

De acordo com a Doutrina Militar de Defesa Cibernética, sua finalidade foi:

Estabelecer os fundamentos da Doutrina Militar de Defesa Cibernética, proporcionando unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa (MD), e contribuindo para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético (BRASIL, 2014, p. 13).

Podemos observar, ao longo do documento, que diversos conceitos foram apresentados de acordo com a visão do Ministério da Defesa à época, e destacamos que 22 exemplares da Doutrina foram distribuídos no total, sendo 13 deles internamente e nove deles externamente, ou seja, estes últimos para os órgãos relacionados às Forças Armadas

(BRASIL, 2014, p. 11). Entendemos que esta distribuição de exemplares corresponde a finalidade original da Doutrina de *uniformizar o pensamento* a respeito da cibersegurança no Brasil.

Ainda em suas Considerações Preliminares, o documento resgatou a ideia já debatida anteriormente da ampliação da agenda de segurança. A presença de atores não estatais como elementos de segurança foi considerada pelo Ministério da Defesa quando tomamos por base o item 1.2.2 da Doutrina Militar de Defesa Cibernética:

Na atual conjuntura mundial, caracterizada por *incerteza, mutabilidade e volatilidade* das ameaças potenciais, bem como pela presença de *novos atores não estatais* nos possíveis cenários de conflito, a sociedade brasileira, em particular a expressão militar do Poder Nacional, deverá estar permanentemente preparada, considerando os atuais e futuros contenciosos internacionais. Para tal, medidas deverão ser adotadas de forma a capacitá-la a responder oportuna e adequadamente, antecipando os possíveis cenários adversos à Defesa Nacional (BRASIL, 2014, p. 13, grifo nosso).

O Ministério da Defesa brasileiro, como podemos observar, estabeleceu o contexto internacional à época como sendo caracterizado por “incerteza, mutabilidade e volatilidade” (BRASIL, 2014). Ao fazer este tipo de afirmação, o governo brasileiro reforça o discurso da necessidade de atuação das Forças Armadas em novas questões, ou seja, a necessidade de *flexibilização* da atuação das FFAA como já apresentamos no início deste capítulo.

A proposta, portanto, da Doutrina, é de preparar o que é compreendido como “expressão militar do Poder Nacional” frente às novas ameaças estabelecidas na figura de “atores não estatais” (BRASIL, 2014, p. 13). A capacitação do Exército Brasileiro frente aos novos desafios de segurança também foi mencionada enquanto uma necessidade na garantia dos interesses do País.

Dessa forma, podemos inferir que houve um senso de urgência de que as Forças Armadas no Brasil ressignificassem sua atuação para melhor atuar frente às mudanças na conjuntura mundial, conforme a Doutrina Militar de Defesa Cibernética reforçou.

Como já argumentado brevemente, a partir do século XXI, entendemos que houve uma militarização dos assuntos de Ciência e Tecnologia no Brasil, legitimada por uma sociedade habituada à presença das FFAA em âmbitos civis. Tal militarização justifica que investimentos sejam crescentes no âmbito militar para a capacitação de pessoal nas áreas da ciência e da tecnologia.

Com o objetivo da uniformidade do pensamento em relação à Defesa Cibernética, o documento trouxe a definição de alguns conceitos que deveriam nortear a atuação das Forças Armadas no âmbito cibernético, são eles: Ameaça Cibernética, Artefato Cibernético, Ativos de Informação, Cibernética, Defesa Cibernética, “Dia-Zero”, Domínios Operacionais, Espaço Cibernético, Fonte Cibernética, Guerra Cibernética, Infraestrutura Crítica da Informação, Infraestruturas Críticas, Operação de Informação, Poder Cibernético, Resiliência Cibernética, Risco Cibernético, Risco Cibernético, Segurança Cibernética, e Segurança da Informação e Comunicações¹⁰⁹.

Dentre todos estes conceitos apresentados na Doutrina Militar de Defesa Cibernética, destacamos os já mencionados Espaço Cibernético e Guerra Cibernética os quais delimitaram a visão do Ministério da Defesa e das Forças Armadas no âmbito cibernético.

Ressaltamos que a Guerra Cibernética, conforme sua própria definição, está relacionada aos níveis operacional e tático, uma vez que a Guerra Cibernética implica que ações estão sendo tomadas no espaço cibernético. Ou seja, como postulado pela Doutrina Militar de Defesa Cibernética, a Guerra Cibernética “[...] abrange, essencialmente, Ações Cibernéticas” (BRASIL, 2014, p. 19).

Destacamos, ainda, duas definições importantes que são recorrentes ao tratar do espaço cibernético e que foram esclarecidas no documento, a saber: a *Infraestrutura Crítica de Informação* e a *Infraestruturas Críticas*.

A Infraestrutura Crítica da Informação foi definida sucintamente como: “subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade” (BRASIL, 2014, p. 19).

As Infraestruturas Críticas, por sua vez, foram definidas como “instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade” (BRASIL, 2014, p. 19).

Entendemos que a compreensão destes conceitos (apesar de terem sido apresentados de forma vaga) é importante na medida em que a cibersegurança está relacionada à *segurança de infraestruturas*. Como já apresentado no capítulo anterior, alguns casos de ciberataques

¹⁰⁹ Como se imaginaria de um documento oficial das Forças Armadas, todos estes conceitos que mencionamos não são definidos extensivamente nem com termos técnicos da Tecnologia da Informação, mas passam uma ideia geral de como as Forças Armadas devem se comportar frente às novas tecnologias.

que ganharam notoriedade danificaram gravemente algumas infraestruturas, como foi o Stuxnet em 2010 ou o *malware* que afetou a Ucrânia em 2015.

A vagueza da apresentação destes conceitos vai ao encontro de uma compreensão militarizada dos assuntos relacionados à tecnologia na medida em que se trata de um assunto relativamente novo para as Forças Armadas, e pode permitir uma abrangência de ação maior, dando mais liberdade às FFAA atuarem no âmbito cibernético.

Cabe também mencionar que estes conceitos relacionados à cibersegurança que foram definidos e organizados pela Doutrina também apareceram na versão de 2015 do glossário das Forças Armadas (BRASIL, 2015).

Ainda a respeito das definições apresentadas podemos dizer que, além de defesa e segurança cibernéticas, o Ministério da Defesa também estabeleceu, através da Doutrina Militar de Defesa Cibernética, a preocupação com proteção cibernética, pois deveria ser o conceito a guiar as ações das FFAA no âmbito do ciberespaço. A Proteção Cibernética foi definida como:

Ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética em face de uma situação de crise ou conflito. É uma atividade de *caráter permanente*” (BRASIL, 2014, p. 23, grifo nosso).

Destacamos a ideia do caráter permanente que existe ao tratar da proteção cibernética, assim como a ação de *neutralização* de possíveis ameaças. Tendo em vista estas características, a Proteção Cibernética se encaixou no que a Doutrina Militar de Defesa Cibernética classificou como “Tipos de Ações Cibernéticas” (BRASIL, 2014, p. 23).

Dessa forma, os Tipos de Ações Cibernéticas, tais como postulados pela Doutrina foram os seguintes: “Ataque Cibernético, Proteção Cibernética e Exploração Cibernética” (BRASIL, 2014, p. 23). Estes tipos de ações, também relacionadas aos níveis operacional e tático das campanhas militares no âmbito cibernético, são ações de guerra cibernética, ou seja, o emprego da força militar em uma operação no ciberespaço.

As ações cibernéticas podem ser de caráter permanente e de neutralização, como já mencionada pela Proteção Cibernética; de caráter de inteligência, como é o caso da Exploração Cibernética, na qual visa coleta de informações e possíveis vulnerabilidades; ou de caráter ofensivo contra um inimigo, como é o caso do Ataque Cibernético (BRASIL, 2014, p. 23-24). A tabela a seguir busca esclarecer os Tipos de Ação Cibernética apresentados.

Tabela 07: O caráter das Ações Cibernéticas pelas Forças Armadas Brasileiras

Tipo de Ação Cibernética	Caráter
Proteção Cibernética	Permanente e de neutralização
Exploração Cibernética	Inteligência
Ataque Cibernético	Ofensiva contra inimigo

Fonte: Elaborado pela autora com base em BRASIL, 2014, p. 23-24.

Dentre os Princípios de Emprego da Defesa Cibernética, o documento da Doutrina Militar de Defesa Cibernética estabeleceu quatro deles que deveriam ser considerados pelas Forças Armadas enquanto possibilidade de uma campanha militar no ciberespaço, a saber. São eles: os Princípios do Efeito, Dissimulação, Rastreabilidade e de Adaptabilidade (BRASIL, 2014, p. 20).

Com definições sucintas, os Princípios de Emprego da Defesa Cibernética no Brasil segundo a Doutrina objetivaram, conforme entendemos, preparar as Forças Armadas sobre algumas características intrínsecas do próprio espaço cibernético. Por exemplo, deve-se, segundo o Princípio da Dissimulação, dificultar a rastreabilidade de ações ofensivas contra um inimigo no ciberespaço (BRASIL, 2014, p. 20).

Outrossim, de acordo com o Princípio do Efeito, as ações militares empregadas no ciberespaço devem ter efeito no “mundo real” (BRASIL, 2014, p. 20).

As Forças Armadas, ainda de acordo com os Princípios, devem se atualizar e se adaptar às transformações que também ocorrem no âmbito do ciberespaço, tendo em vista o desenvolvimento tecnológico e as explorações de vulnerabilidades que atingem o espaço cibernético.

Novamente podemos observar uma necessidade das Forças Armadas se capacitarem tecnologicamente para atuarem no ciberespaço. Durante o documento fica cada vez mais claro o “dever” das Forças Armadas em garantirem a cibersegurança.

Vejamos agora o que o documento estabeleceu a respeito do já mencionado Sistema Militar de Defesa Cibernética (SMDC).

Tendo em vista a responsabilidade das Forças Armadas de assegurar a segurança do setor cibernético de acordo com a Estratégia Nacional de Defesa publicada em 2008, a Política Cibernética de Defesa de 2012 previu que um Sistema Militar de Defesa Cibernética

fosse desenvolvido a fim de organizar de forma definitiva os aparatos do Ministério da Defesa na cibersegurança.

A Doutrina Militar de Defesa Cibernética teve um capítulo dedicado à compreensão deste Sistema. De acordo com o documento:

3.1.4 O Sistema Militar de Defesa Cibernética (SMDC) é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas FA, bem como impedindo ou dificultando sua utilização contra interesses da Defesa Nacional. 3.1.5 Cabe também ao SMDC assegurar a proteção cibernética do SISM² [Sistema Militar de Comando e Controle], assegurando a capacidade de atuar em rede com segurança, bem como coordenar e integrar a proteção das infraestruturas críticas da Informação de interesse da Defesa Nacional, definidas pelo MD (BRASIL, 2014, p. 25).

Podemos inferir, portanto, que o SMDC foi idealizado considerando a necessidade de centralização das operações voltadas ao setor cibernético. Ainda de acordo com o documento, o Sistema Militar de Defesa Cibernético foi instituído como órgão central do Centro de Defesa Cibernética (CDCiber) (BRASIL, 2014, p. 26).

Conforme o documento elaborou a respeito do Sistema Militar de Defesa Cibernética:

3.3.1 O EMCFA [Estado Maior-Conjunto das Forças Armadas] é o órgão responsável por assessorar o Ministro de Estado da Defesa na implantação e na gestão do SMDC, com a finalidade de garantir, no âmbito da Defesa Nacional, a capacidade de atuação em rede, a interoperabilidade dos sistemas e a obtenção dos níveis de segurança necessários [...] 3.3.3 O órgão central do SMDC é o Centro de Defesa Cibernética (CDCiber), que passa ao controle operacional do MD nas Operações Conjuntas e conta, permanentemente, com um Estado-Maior Conjunto para realizar o planejamento e o controle das ações planejadas, levando em conta as particularidades de cada Força Armada, de modo a obter uma atuação sinérgica (BRASIL, 2014, p. 26).

Dessa forma, podemos inferir que o Centro de Defesa Cibernético ganhou ainda mais importância, sendo o principal órgão do governo brasileiro responsável pela Segurança e Defesa do ciberespaço no Brasil. Submetido ao Ministério da Defesa, o CDCiber atua nas esferas estratégica, tática e operacional.

Para a coordenação das atividades do CDCiber e do NuCDCiber, o Chefe do Centro de Defesa Cibernética costuma ser um Oficial General¹¹⁰ do Exército, reforçando o caráter

¹¹⁰ Os Oficiais Generais podem ser: General de Brigada, General de Divisão, General do Exército e Marechal, postos e graduações mais altos na hierarquia do Exército Brasileiro.

militar da instituição. Desde 2019 o Chefe do CDCiber é o General de Brigada Ivan de Sousa Corrêa Filho.

Destacamos ainda mais dois pontos estabelecidos na Doutrina Militar de Defesa Cibernética que envolvem o Sistema Militar de Defesa Cibernética e o CDCiber, a saber:

3.3.5 O CDCiber mantém canal técnico para coordenação e integração com os órgãos de interesse envolvidos nas atividades de Defesa Cibernética (CERT.br, CTIR Gov, órgãos de Defesa/Guerra Cibernética das FA [sic], Ministérios, Agências Governamentais, APF e outros). 3.3.6 O CDCiber mantém canal sistêmico/técnico com os órgãos centrais de inteligência das FA [sic], no âmbito do Sistema de Inteligência de Defesa (SINDE), no tocante ao Setor Cibernético, para a difusão e obtenção dos dados obtidos por intermédio da Fonte Cibernética (BRASIL, 2014, p. 26).

Entendemos que a coordenação com outros órgãos de inteligência vai ao encontro dos Tipos de Ação desdobradas no âmbito cibernético, ou seja, a Proteção Cibernética, o Ataque Cibernético, mas, principalmente, a Exploração Cibernética na medida em que esta última está relacionada à coleta de material e informações considerados relevantes com o objetivo final de assegurar a segurança cibernética.

Ainda no âmbito do Sistema Militar de Defesa Cibernética (SMDC), assim como em outros setores em que as Forças Armadas Brasileiras atuam, existem os níveis de alerta para as possíveis ameaças detectadas que foram determinados pela Doutrina Militar de Defesa Cibernética.

Em termos gerais, tem-se os níveis: baixo, moderado, médio, alto e muito alto, representados pelas cores branca, azul, amarelo, laranja e vermelho, respectivamente. Destacamos que “É prerrogativa do Chefe do EMCFA ratificar o nível de alerta cibernético acima de amarelo, sugerido pelos órgãos de Defesa Cibernética das FFAA. Durante operações, os níveis até amarelo, inclusive, serão estabelecidos pelo Chefe do CDCiber” (BRASIL, 2014, p. 28).

Dessarte, podemos inferir que, mesmo com “a possibilidade de participação civil” no CDCiber, as tomadas de decisão e a atuação, efetivamente, ocorrem no nível militar, seja pelo Chefe do Centro de Defesa Cibernética ou pelo Chefe do Estado Maior-Conjunto das Forças Armadas.

Passemos ao quarto e último capítulo da Doutrina Militar de Defesa Cibernética que diz respeito à “defesa e guerra cibernética nas operações” (BRASIL, 2014, p. 29).

No quarto capítulo da Doutrina Militar de Defesa Cibernética, existem algumas disposições a respeito das operações cibernéticas pelas Forças Armadas. Quando uma operação em nível tático ou operacional é realizada no âmbito do ciberespaço, esta é denominada de Guerra Cibernética (ou “G Ciber”, como se referem nos documentos oficiais), conceito que já delimitamos (BRASIL, 2014).

Apesar das operações de defesa cibernética serem tratadas neste documento de 2014, algumas considerações a respeito da defesa cibernética já haviam sido feitas no primeiro volume (de três) da Doutrina de Operações Conjuntas, publicado em 2011 também pelo Estado-Maior Conjunto das Forças Armadas (EMCFA) (BRASIL, 2011).

O documento da Doutrina de Operações Conjuntas foi elaborado quase que simultaneamente com as funções do Centro de Defesa Cibernético e, por este motivo, as considerações a respeito da atuação no âmbito cibernético pelas Forças Armadas ainda é superficial, apresentando apenas alguns conceitos que também foram trabalhados posteriormente na Doutrina Militar de Defesa Cibernética (BRASIL, 2011).

Já ficou estabelecida em 2011, entretanto, a diferenciação a respeito da denominação da operação em relação aos níveis de decisão, questão que já afirmamos previamente. Ou seja, “[...] Defesa Cibernética quando as FA [sic] estiverem planejando e executando ações cibernéticas afetas ao nível estratégico de decisão. Da mesma forma, será utilizada a denominação Guerra Cibernética quando o nível de decisão considerado for o operacional ou tático” (BRASIL, 2011, p. 55).

Aquilo que apareceu no documento da Doutrina de Operações Conjuntas de 2011 a respeito da Defesa Cibernética é reforçado na Doutrina Militar de Defesa Cibernética (BRASIL, 2011; BRASIL, 2014). A diferença é que a Doutrina Militar de Defesa Cibernética aprofundou alguns temas e estabeleceu o já apresentado Sistema Militar de Defesa Cibernético (SMDC) e sua relação com o CDCiber.

É interessante notar que, no que se refere às operações cibernéticas a serem desempenhadas pelas equipes das FFAA responsáveis, foi afirmado que “O ponto focal normalmente será a obtenção da Superioridade da Informação¹¹¹” (BRASIL, 2014, p. 30) nas

¹¹¹ Vantagem operacional resultante da habilidade de coletar, processar e disseminar um fluxo ininterrupto de informação, enquanto explora ou nega ao oponente a capacidade de fazer o mesmo (BRASIL, 2014, p. 30).

Operações de Informação no Estado-Maior Conjunto do Comando Operacional e no Destacamento Conjunto de Defesa Cibernética e Destacamentos de Guerra Cibernética.

Para a obtenção de informações, por sua vez, aquilo entendido como Fonte Cibernética tem relevância singular para aqueles que atuam na ciberdefesa e na cibersegurança. A Fonte Cibernética foi definida como:

[...] recurso por intermédio do qual se pode obter dados no Espaço Cibernético utilizando-se ações de busca ou coleta, normalmente realizadas com auxílio de ferramentas computacionais. A Fonte Cibernética poderá ser integrada a outras fontes (humanas, imagens e sinais) para produção de conhecimento de Inteligência (BRASIL, 2014, p. 19).

Finalmente, podemos inferir que a Doutrina Militar de Defesa Cibernética foi documento fundamental na uniformidade de pensamento a respeito da ciberdefesa e na garantia da cibersegurança.

Em termos oficiais, é prioridade do governo brasileiro obter informações e “estar preparado” para quaisquer possíveis eventos que envolvam ações no ciberespaço, sejam elas de Proteção, Exploração ou Ataque Cibernético.

Ficou evidente pela leitura da Doutrina Militar a importância concedida ao ciberespaço e à cibersegurança pelas Forças Armadas Brasileiras, assim como o emprego de *peçoal militar* desde o nível de tomada de decisão até a atuação efetiva no setor cibernético – atuação esta denominada “Guerra Cibernética”.

Podemos concluir que houve uma militarização da cibersegurança no Brasil que foi se construindo de forma mais evidente desde a Estratégia Nacional de Defesa, publicada em 2008, até a Doutrina Militar de Defesa Cibernética, publicada em 2014.

4.4.3 Marco Civil da Internet (2014)

Um produto importante para compreender o comportamento no ciberespaço, em específico, na Internet, foi a regulamentação da Lei 12.965 de 2014, conhecida popularmente como Marco Civil da Internet.

Idealizado ainda em 2009, o projeto de uma lei que regulamentasse a atuação do Estado e também do indivíduo na Internet só foi assinado e posto em prática em 23 de abril de 2014 pela então presidenta Dilma Rousseff.

Em termos gerais, a Lei 12.965/14 estabeleceu “princípios, garantias, direitos e deveres para o uso da Internet no Brasil” (BRASIL, 2014a, s/p). Dessa forma, aquilo que ficou entendido como “governança na Internet” teve seus parâmetros limitados por esta Lei.

Em um relatório completo fomentado pelo Instituto Igarapé, Daniel Arnaudo apontou que o Marco Civil da Internet é inovador em termos cibernéticos internacionais, sendo uma “referência fundamental para o século XXI”, o qual se torna cada vez mais dependente da Internet (ARNAUDO, 2017, p. 02).

A Internet deixou de ser apenas uma ferramenta de envio e recebimento de arquivos para se tornar algo muito mais complexo que se consolidou como entidade presente nas relações sociais. O filósofo e sociólogo Pierre Lévy se debruçou a investigar as transformações que a Internet trouxe e o papel do ciberespaço na sociologia e na realidade social, o que ele chamou de “Cibercultura” (LÉVY, 1999).

A Internet, portanto, passou por essas transformações nas relações sociais muito rapidamente, especialmente no Ocidente. Dessa forma, fez-se necessário marco regulatório que contemplasse os direitos e deveres de seus usuários.

O Marco Civil da Internet no Brasil foi “[...] orientado por um conjunto de dez princípios, entre eles neutralidade da rede, privacidade, liberdade de expressão, segurança e universalidade” (ARNAUDO, p. 03). Tais princípios, podemos inferir, foram importantes para que se incentivasse o acesso à Internet de forma segura a toda a população.

O projeto de lei que deu origem ao Marco Civil da Internet foi idealizado anos antes de seu estabelecimento, em 2009, como já mencionado. Um Comitê Gestor da Internet tinha a proposta de tornar a Internet mais segura para os usuários, pois entendiam que isso fazia parte de uma iniciativa democrática – a governança na Internet (ARNAUDO, 2017; BRASIL, 2014a).

O Marco Civil da Internet foi importante para a história da governança *online*, pois foi um documento elaborado de forma colaborativa. Como afirmou Arnaudo (2017):

De 2009 a 2014, o projeto de lei passou por um longo processo de discussão, debate e edição online por meio de um inédito sistema de participação open source [...] Os participantes trabalharam a partir de uma versão do projeto criada pelo Ministério da Justiça e pela equipe do CTS-FGV, fazendo seus próprios comentários e edições ao projeto. Pessoas, organizações, empresas, órgãos do governo e até outros governos ofereceram contribuições ao longo de todo o processo, melhorando o pioneiro sistema open source online (ARNAUDO, 2017, p. 05).

O “*open source*”, no qual o autor se refere, era um tipo de software em que os diferentes colaboradores tinham acesso para criar, editar e debater sobre a proposta. Por este motivo, o Marco Civil da Internet é compreendido como a principal referência brasileira em termos de democracia e sua relação com a Internet.

Mesmo que o *acesso* à Internet ainda não seja democratizado a toda a população brasileira, a comunidade do Brasil é uma das mais conectadas do Planeta (ARNAUDO, 2017, p. 03). Dessa forma, justifica-se a iniciativa do marco regulatório que se tornou o Marco Civil da Internet.

Destarte, a Lei 12.965/14 estabeleceu seus princípios e fundamentos em 32 artigos distribuídos em cinco capítulos. Dentre suas disposições, a Lei estabeleceu garantias nas áreas de proteção aos registros, dados pessoais e comunicações privadas; de responsabilidade por danos decorrentes de conteúdo gerado por terceiros; e questões de requisição judicial de registros (BRASIL, 2014a, s/p).

Entretanto, um dos capítulos mais importantes estabelecidos pelo Marco Civil da Internet diz respeito a atuação do poder público na Internet. Dentre as diretrizes para a atuação do Estado, União, Distrito Federal e demais municípios, destacamos aquelas que estabeleceram: a transparência do poder público a ser feita através da Internet; a promoção da cultura e da cidadania; a prestação de serviços através da Internet, ou seja, serviços de governo eletrônico; a promoção da inclusão digital; os investimentos na área da informatização; e a publicação e disseminação de dados e informações que são públicas (BRASIL, 2014a, s/p).

Ademais, a questão da *privacidade* foi recorrente na Lei do Marco Civil. Entre os direitos do usuário, sua privacidade, dados e informações não poderiam ser inviolados ou armazenados por terceiros, salvo por questões judiciais ou pelos termos de uso que o usuário deve concordar a fim de se utilizar do serviço (BRASIL, 2014a).

O que pode ocorrer, todavia, é o usuário acessar determinado *website* ou fazer determinado cadastro *online* e concordar com os termos de uso sem os ler por completo e aceitar que quaisquer de suas informações sejam retidas por terceiros.

Ainda que tratado brevemente, o Marco Civil da Internet¹¹² foi documento importante na história da governança democrática *online* no Brasil e por isso foi incluído em nossa investigação. O Marco Civil evidenciou os rumos que estavam sendo tratados na área da Internet pelos governos Lula (2002-2009) e Dilma (2010-2016), de promoção de garantias ao usuário e liberdade de expressão na Internet.

4.4.4 Guia de Defesa Cibernética na América do Sul (2017)

Desenvolvido por pesquisadores das áreas de Relações Internacionais, Ciência Política e Ciências Sociais do Brasil, o Guia de Defesa Cibernética na América do Sul foi publicado na forma de um livro e contou com financiamento do IBED (Instituto Brasileiro de Estudos de Defesa) e do Ministério da Defesa no ano de 2017 (GUEDES DE OLIVEIRA et al., 2017).

Apesar de ser um livro focado em *defesa cibernética*, ou seja, medidas tomadas em *nível doméstico* visando a manutenção da ciberdefesa, esta não pode ser separada totalmente da cibersegurança que, por sua vez, está ligada a medidas que promovem a proteção contra ameaças *externas*. Dessa forma, faz-se relevante a compreensão deste documento para também compreender a cibersegurança brasileira.

O livro foi um produto de uma parceria entre civis e militares que resultou na colaboração entre a ECEME (Escola de Comando e Estado-Maior do Exército), as Universidades Federais de Pernambuco (UFPE), de Santa Catarina (UFSC) e Fluminense (UFF), a Universidade de São Paulo (USP) e a Academia Militar das Agulhas Negras (AMAN).

Considerando a crescente presença do tema na academia, bem como o próprio desenvolvimento da defesa cibernética em âmbito militar, o Guia teve a proposta de apresentar questões que envolvem a ciberdefesa nos países da América do Sul de forma geral e apresentando dados quantitativos. Ao apresentar um panorama geral da defesa cibernética na América do Sul, o Guia teve como objetivo auxiliar tomadores de decisão na área.

Dividido entre oito capítulos, o Guia apresentou generalidades a respeito da relação da América do Sul com a cibersegurança para então se aprofundar em questões domésticas

¹¹² Para mais informações, ver: BRASIL, 2014a. A Lei que estabeleceu o Marco Civil da Internet pode ser acessada integralmente no link: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 jan. 2020.

de cada país. De acordo com os próprios autores: “O guia foi estruturado por países e seções, o que permite tanto uma leitura completa do texto quanto uma consulta seccionada, sem a necessidade de leitura prévia dos capítulos anteriores” (GUEDES DE OLIVEIRA et al., 2017, p. 25).

Os pesquisadores que trabalharam no Guia de Defesa Cibernética na América do Sul se atentaram a questões envolvendo o “contexto e características de cada país, as fragilidades do espaço cibernético, documentos e marcos regulatórios, e a estrutura de defesa cibernética dos países [da América do Sul]” (GUEDES DE OLIVEIRA et al., 2017, p. 25).

Como os próprios pesquisadores afirmaram, o Guia não precisa ser lido por completo para que se obtenha alguma informação objetiva referente a cibersegurança de algum país da América do Sul. Dessa forma, o Guia de Defesa Cibernética na América do Sul foi desenvolvido com a finalidade de ser documento de consulta por outros pesquisadores, mas principalmente por aqueles responsáveis pela cibersegurança no Brasil que, no caso, se trata do Ministério da Defesa e mais especificamente do Estado Maior-Conjunto do Exército (EMCE) e do Centro de Defesa Cibernética (CDCiber).

Dessa forma, o Guia apresentou dados quantitativos a respeito da conexão e da penetração da Internet nos países da América do Sul, bem como a respeito da democratização do acesso à Internet. Informações a respeito da velocidade de conexão e dados técnicos a respeito de provedores também podem ser encontrados no documento.

O foco foi apresentar a forma pela qual os países lidam com a segurança e defesa cibernética, os principais órgãos, civis e militares, e as principais medidas tomadas na esfera pública (GUEDES DE OLIVEIRA et al., 2017).

O Guia de Defesa Cibernética na América do Sul apresentou algum dos principais ciberataques ou delitos cibernéticos que alguns destes países sofreram. Destacamos, entretanto, que à época de sua publicação o ataque envolvendo o *ransomware* *WannaCry* ainda não havia se espalhado e causado os danos que causou em cerca de 150 países, entre eles, os da América do Sul.

Entendemos o Guia de Defesa Cibernética na América do Sul como um importante documento fomentado e financiado pelo governo brasileiro com a finalidade de compreender a conjuntura brasileira em comparação ao seu entorno. Dessa forma, os tomadores de

decisões estariam melhor informados a respeito de medidas e de como se sobressair regionalmente nos quesitos de Defesa e Segurança.

4.4.5 Política Nacional de Segurança da Informação (2018)

Aprovada através do decreto nº 9.637 em 26 de dezembro de 2018, a Política Nacional de Segurança da Informação (PNSI) foi instituída através de 23 artigos distribuídos entre sete capítulos. A Política Nacional de Segurança da Informação teve a: “finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade *da informação a nível nacional*” (BRASIL, 2018, s/p, grifo nosso).

Um dos últimos Decretos assinados pelo ex-presidente Michel Temer, a Política Nacional da Segurança da Informação teve o objetivo de funcionar como um mecanismo legal de proteção de informações e dados do Governo Federal.

De acordo com o documento, a segurança da informação abrange “I - a segurança cibernética; II - a defesa cibernética; III - a segurança física e a proteção de dados organizacionais; e IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação” (BRASIL, 2018, s/p).

Partindo do princípio de *manutenção da soberania* brasileira, a Política Nacional de Segurança da Informação teve, entre os principais objetivos:

[...] contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio da orientação das ações de segurança da informação, observados os direitos e as garantias fundamentais [...] fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação [...] orientar ações relacionadas a: a) segurança dos dados custodiados por entidades públicas; b) segurança da informação das *infraestruturas críticas* [...] (BRASIL, 2018, s/p, grifo nosso).

Novamente podemos observar a presença da preocupação com as “infraestruturas críticas” que guardam informações e dados que devem ser protegidos para que se garanta a soberania do país. Na medida em que a informatização passa a se consolidar e ser recurso recorrente nas relações políticas, econômicas, sociais e militares, aumenta a necessidade da proteção digital e da segurança da informação.

Como já demonstrado no capítulo anterior a respeito dos principais acontecimentos internacionais envolvendo crimes cibernéticos, a dependência da informática, a existência de uma conexão de redes de computadores e a presença do ciberespaço podem gerir

vulnerabilidades consideradas problemas de defesa e de segurança, que exigem maior atenção de governos centrais.

Levando em consideração estes fatores, a proposta da Política Nacional de Segurança da Informação também foi criar um “Comitê Gestor da Segurança da Informação” na tentativa de juntar representantes de todos os Ministérios – que até então existiam – para que reuniões ocorressem no âmbito governamental e que visassem promover e aprimorar a Segurança da Informação e a proteção de infraestruturas críticas (BRASIL, 2018).

Em sua versão original de 2018, o Decreto que instaurou a PNSI ainda previu que especialistas da área da Segurança da Informação, tanto da área privada quanto pesquisadores da área pública, participassem eventualmente das reuniões do Comitê e ajudassem na promoção da segurança¹¹³ (BRASIL, 2018).

Além do Comitê formado que deveria considerar investimentos na área da Segurança da Informação e proteção de dados, a Política Nacional da Segurança da Informação instituiu que uma Estratégia Nacional de Segurança da Informação fosse fomentada no Brasil nos anos seguintes (BRASIL, 2018). A Estratégia Nacional de Segurança da Informação funcionaria como instrumento da Política Nacional de Segurança da Informação.

Podemos observar um paralelo com os acontecimentos da história da Defesa e Segurança no Brasil entre 2005 e 2008. Em 2005, como já apresentado neste capítulo, tivemos a promulgação de uma Política de Defesa Nacional, uma segunda edição em relação àquela de 1996. A PDN de 2005 deu origem a Estratégia Nacional de Defesa de 2008, que funcionou como instrumento da política e do Ministério da Defesa para o estabelecimento de metas e diretrizes na garantia das Segurança e Defesa no Brasil.

Da mesma maneira, a Política Nacional de Segurança da Informação, de 2018, confere importância de atuação do Ministério da Defesa, bem como do Gabinete de Segurança Institucional da Presidência da República e do Ministério da Transparência e Controladoria Geral da União, cada qual com suas funções específicas (BRASIL, 2018, s/p).

O restante dos Ministérios envolvidos com a PNSI tem disposições mais gerais de como agir e auxiliar na implementação da Política. Destacamos duas destas disposições, a saber: “[...] destinar recursos orçamentários para ações de segurança da informação; [...]

¹¹³ Em 2019, o novo presidente da república, no Decreto 9.838, revogou os parágrafos que dispunham sobre tais questões. Pelo que se pode inferir, as reuniões passaram a ser restritas apenas aos representantes de cada Ministério, que também a partir de 2019 passou a ter um número menor.

promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação [...]” (BRASIL, 2018, s/p).

Destacamos estas duas disposições para esclarecer que, além dos gastos do próprio Ministério da Defesa com a cibersegurança, a Política Nacional de Segurança da Informação ainda previu que os Ministérios destinassem recursos orçamentários na área da Segurança da Informação, na medida em que isso pode contribuir para a proteção das infraestruturas críticas e, em última instância, contribui para a própria cibersegurança no Brasil.

Na Política Nacional da Segurança da Informação podemos observar um elemento presente na construção da Teoria de Securitização que é a tomada de medidas em nome de uma “constelação”, ou seja, visando proteger toda uma *coletividade*, seja de subsistemas, unidades, subunidades ou indivíduos (BUZAN; WÆVER; DE WILDE, 1998, p. 36).

Tendo em vista estes elementos, justificamos a importância de compreender a Política Nacional de Segurança da Informação aprovada pelo Decreto 9.637/18, mesmo que brevemente, pois contribui para a nossa argumentação a respeito da promoção da segurança cibernética no Brasil entre 2002 e 2018.

4.5 A cibersegurança no Brasil

Durante este capítulo apresentamos algumas das principais medidas de defesa cibernética adotadas no Brasil que têm como principal finalidade a promoção da cibersegurança. Assim sendo, uma análise a respeito da segurança cibernética não poderia deixar de considerar e buscar compreender, do mesmo modo, o papel da defesa cibernética.

Tomamos como base a *construção social* do ciberespaço como existencialmente ameaçado e, por este motivo, a Teoria de Securitização foi tão adequada quando aplicado seu quadro de análise sob este caso concreto.

Na primeira parte deste capítulo optamos por contextualizar a realidade brasileira para que se compreendesse os motivos que levaram ao discurso de segurança cibernética. Partir desta abordagem vai ao encontro daquilo que McDonald (2008a) afirmou a respeito da Escola de Copenhague: que seu quadro de análise deixava de considerar questões importantes de contexto e *background*, essenciais para uma leitura completa do caso estudado.

Dessa forma, o item 4.1 foi dedicado à uma breve contextualização do cenário brasileiro nos termos que consideramos relevantes para o desenvolvimento da investigação: o incipiente aprofundamento do conceito de segurança promovido pela Política de Defesa Nacional de 1996, a preocupação com a consolidação da informatização e a possibilidade de formação de uma Sociedade da Informação no Brasil, também no fim da década de 1990.

Em um segundo momento, tomamos como objeto referente o ciberespaço do Brasil; os atores securitizadores, o Ministério da Defesa e o Congresso Nacional brasileiro; e os atores funcionais as Forças Armadas Brasileiras. A partir destes elementos desenvolvidos pela EC, buscamos elucidar as formas pelas quais o processo de securitização ocorreu no Brasil entre 2002 e 2018 (BUZAN; WÆVER; DE WILDE, 1998).

Nossa principal referência para desenvolver a argumentação de securitização foi a Estratégia Nacional de Defesa de 2008 e sua sexta diretriz que estabeleceram o setor cibernético como estratégico.

A partir deste documento objetivamos compreender os elementos a ele anteriores – ou seja, quais as condições que levaram a criação de uma END – e os elementos a ele posteriores – quais foram os produtos da END e da determinação do setor cibernético enquanto estratégico.

Dessarte, é possível afirmar que a cibersegurança no Brasil se estabeleceu em três fases que dialogam diretamente com as três etapas propostas pela Escola de Copenhague para análise de um processo de securitização de sucesso (BUZAN; WÆVER; DE WILDE, 1998). Portanto, o processo de cibersegurança no Brasil foi um processo de securitização do ciberespaço.

A primeira fase é aquilo que veio antes da Estratégia Nacional de Defesa e auxiliou no discurso de construção social de ameaça com o limite temporal do ano de 2002. Dessa forma temos, na primeira fase, o Seminário de Política para o Século XXI fomentada pelo Congresso Nacional em 2002; a Declaração Sobre a Segurança nas Américas, promovida pela OEA em 2003; e a Política de Defesa Nacional de 2005, que surgiu no âmbito do MD após sugestões do Seminário de Política para o Século XXI.

A segunda fase é aquela que contém justamente a publicação da Estratégia Nacional de Defesa, pois é a fase central entre as três. Como já abordado, a END conferiu a segurança cibernética ao Exército Brasileiro. A segunda fase também contém a criação dos Centro de Defesa Cibernético e Núcleo do Centro de Defesa, órgãos responsáveis pelas ciberdefesa e consequente cibersegurança no Brasil. Esta segunda fase corresponde a de ação emergencial sendo tomada em nome do coletivo e do “bem maior”.

A terceira e última fase é a de observação da relação entre as unidades. A forma pela qual o *speech-act* e a ação emergencial se relacionam: seus produtos. Após o estabelecimento do CDCiber como órgão fundamental na garantia da cibersegurança, dois documentos de singular relevância foram produzidos: a Política Cibernética de Defesa (2012) e a Doutrina Militar de Defesa Cibernética (2014) que caracterizaram a militarização do ciberespaço, conforme entendemos.

Outras três produções são importantes para caracterizar a terceira fase: o Marco Civil da Internet (2014), o Guia de Defesa Cibernética na América do Sul (2017) e a Política Nacional de Segurança da Informação (2018). Chegando à data limite de nosso recorte temporal de análise, o ano de 2018, entendemos que estes produtos dialogam com o discurso de necessidade de proteção do ciberespaço contra ameaças externas, mas também com a reivindicação de direitos do usuário conectado e do estabelecimento de limites da atuação do Estado na Internet.

A última fase, portanto, é importante para a conceber o tratamento do ciberespaço e da “e-governança” no Brasil, um dos países mais conectados do mundo (GUEDES DE OLIVEIRA et al., 2017).

Tabela 08: Processo de securitização do ciberespaço brasileiro

	Descrição	Documentos analisados
1ª Fase	<i>Speech-act</i> : identificação de novas ameaças tecnológicas e construção do discurso de segurança cibernética.	- Seminário Política de Defesa para o Século XXI (2002); - Projeto Declaração Sobre a Segurança nas Américas (2003); - Política de Defesa Nacional (2005).
2ª Fase	Ação emergencial: medidas tomadas visando a cibersegurança; estabelecimento do setor cibernético como estratégico e criação de um Centro de Defesa Cibernético e envolvimento oficial das FFAA.	- Estratégia Nacional de Defesa (2008); - Boletim nº 31/10 do Exército Brasileiro (2010).
3ª Fase	Produtos do processo de segurança cibernética: elaboração de uma Política e uma Doutrina Militar voltadas à Defesa cibernética que definem o papel das FFAA brasileiras na cibersegurança; aprovação do Marco Civil da Internet que garante direitos aos usuários; Decreto que estabelece a proteção de dados e informações desde.	- Política Cibernética de Defesa (2012); - Doutrina Militar de Defesa Cibernética (2014); - Marco Civil da Internet (2014) - Guia de Defesa Cibernética na América do Sul (2017); - Política Nacional da Segurança da Informação (2018).

Fonte: elaborado pela autora.

Em conclusão, o processo de securitização do ciberespaço brasileiro pode ser analisado, metodologicamente, a partir do setor militar proposto pela Escola de Copenhague na medida em que a cibersegurança se justifica na manutenção da soberania. Entretanto,

autores como Lene Hansen já sugeriram que houvesse um setor de análise específico voltado ao ciberespaço na teoria de Securitização (HANSEN; NISSENBAUM, 2009).

Dessa forma, nos utilizamos do quadro de análise proposto pela Escola de Copenhague na análise do processo de segurança cibernética no Brasil observado entre os anos de 2002 a 2018.

CAPÍTULO 4

5 OS DESDOBRAMENTOS DA SECURITIZAÇÃO NO BRASIL

Como evidenciou o filósofo e sociólogo Pierre Lévy (2010, p. 54): “por muito tempo os informatas consideraram-se especialistas em máquinas” e, mesmo com a extensa penetração da informatização nas sociedades, muitos informatas mantiveram esse pensamento (LÉVY, 2010). Do ponto de vista da Sociologia e das Relações Internacionais, a consolidação da informatização representou uma verdadeira transformação nos meios de produção, nas relações sociais e no comportamento individual.

Estas transformações ocorreram no Brasil de forma simultânea a uma transformação da conjuntura: a redemocratização brasileira. Os ideais de democratização e universalização do acesso às Tecnologias de Informação e Comunicação passaram a fazer parte da agenda dos governos que passariam a se eleger.

Uma consideração importante deve ser feita sobre este período. As Forças Armadas Brasileiras, durante a redemocratização pós-ditadura militar, passaram por um momento de “crise de identidade”.

Como elucidou Adriana Marques, ainda em 2003:

A crise de identidade militar brasileira que se manifestou nos primeiros anos da década de 1990 deu-se em função de um conjunto de mudanças estruturais no contexto internacional e da quebra do padrão de tutela militar sobre o governo. Estas mudanças relacionavam-se à visão do governo, do Parlamento e da sociedade civil sobre as demandas militares e também à visão da instituição militar acerca da sua própria identidade [...] (MARQUES, 2003, p. 73).

No cenário internacional, o fim do imbróglio entre Estados Unidos e União Soviética em 1991 transformou a concepção “tradicional” que se tinha a respeito de conflitos, da possibilidade de uma Guerra Nuclear e do papel do Estado em meio a tudo isso.

Dessa forma, a crise de identidade das FFAA também emergiu a partir da falta explícita de um inimigo, como outrora era a União Soviética ou a “ameaça comunista”, e fez com que fosse repensado o papel das Forças Armadas no Brasil.

O ataque às Torres Gêmeas de Nova Iorque em 11 de setembro de 2001 foi um *turning point* para Segurança Internacional no Ocidente. As ameaças passaram a ser o terrorismo, o crime organizado, o tráfico de drogas e o engendrar das Tecnologias de Informação e Comunicação.

A apresentação de “novas ameaças” à segurança do Brasil passou, gradualmente, a ressignificar a atuação das Forças Armadas antes em crise. Na medida em que se via o crime organizado e o tráfico de drogas, por exemplo, como novas ameaças, o Exército Brasileiro passou a se dedicar ao seu combate. É o caso de ocupação de favelas pela Polícia Militar e pelo Exército que ocorrera nos anos 1990 e que se estendeu até os dias atuais (MARQUES, 2003).

Somado a isso, as novas tecnologias e suas vulnerabilidades, em termos de Segurança e Defesa, também passaram a ser consideradas oficialmente nas Políticas e Estratégias expedidas pelo Ministério da Defesa no Brasil a partir dos anos 1990 até a segunda metade da década de 2000, seguindo uma tendência internacional de promoção de cuidados com “novas ameaças”.

Como se evidenciou no segundo capítulo, referente a contextualização internacional de ciberataques, o ciberespaço se validou como ambiente passível de crimes que poderiam desestabilizar sistemas e afetar infraestruturas consideradas críticas. Ademais, a prática de espionagem comum no período da Guerra-Fria não havia acabado, mas se remodelado em ciberespionagem.

Tendo em vista tal contexto doméstico e internacional, o governo brasileiro, a partir do século XXI, promoveu um discurso de cibersegurança e ciberdefesa, ressignificando o papel das Forças Armadas, que passaram a se organizar no combate às *novas ameaças*.

A partir de uma proposta do Ministério da Defesa e do Congresso Nacional de flexibilização da ação das Forças Armadas Brasileiras e do papel do Exército Brasileiro na tutela do ciberespaço e na segurança de ameaças cibernéticas, reforçou-se este papel das FFAA cada vez mais presente no cotidiano brasileiro para além de suas funções tradicionais.

Destacamos, ainda, que o Ministério da Defesa criou um canal na plataforma de compartilhamento de vídeos *YouTube* ainda em 2010, publicando conteúdo referente a atuação das Forças Armadas em diferentes setores, exaltando sua importância¹¹⁴. Dentre alguns dos vídeos publicados no canal do *YouTube*, destacamos os seguintes: “o papel das

¹¹⁴ O canal está disponível em: <https://www.youtube.com/user/VideosDefesa>. Acesso em: 18 jul. 2020.

Forças Armadas nas eleições”¹¹⁵, “Forças Armadas contra o mosquito *Aedes aegypti*”¹¹⁶ e “Exército auxilia crianças com necessidades especiais por meio da equoterapia”¹¹⁷.

Entendemos que não é função oficial das Forças Armadas atuar em contextos tais como as eleições, o combate à Dengue e o auxílio de crianças com necessidades especiais, como apresentado nos vídeos publicados. Entretanto, um canal em uma rede social com este tipo conteúdo pode promover a aproximação das FFAA com a sociedade civil. Isso faz parte de uma estratégia de apresentar as Forças Armadas Brasileiras como essenciais em alguns aspectos na garantia da segurança da população, mesmo que estas funções estejam distantes de seu trabalho original.

Compreendemos que essa presença constante das Forças Armadas advém de um discurso que atribui prestígio a sua atuação no cenário Brasileiro. Discurso este que é legitimado por uma sociedade que, no período de redemocratização, passou por um processo político conservador e que não condenou a presença constante dos militares em funções diversas. Ao contrário: exigia-se que as Forças Armadas assumissem mais responsabilidades. Como se evidenciou a partir da década de 2010, uma parcela conservadora da sociedade brasileira fez manifestações públicas antidemocráticas exigindo a intervenção militar no governo (FELLET, 2018; PORTINARI; MENDES, 2020).

Ao observar o processo de securitização do ciberespaço no Brasil, devemos ter em mente este contexto social e as demandas de caráter conservador que emergem das classes sociais mais altas no Brasil.

À vista disso, podemos inferir, analisando a *bigger picture*, que o processo de securitização do ciberespaço no Brasil reforça uma tendência que vem crescendo: a participação militar em funções diversas. Ocorreu, sobretudo, uma militarização das defesa e segurança cibernética no Brasil.

Podemos afirmar, considerando este cenário, que houve, portanto, uma ressignificação das funções das Forças Armadas nas últimas décadas. No caso específico do setor cibernético, este “novo papel” foi reforçado após a publicação da Estratégia Nacional de Defesa que oficializou as novas funções do Exército Brasileiro.

¹¹⁵ Disponível em: <https://www.youtube.com/watch?v=z-ih9f0q9jQ>. Acesso em: 18 jul. 2020.

¹¹⁶ Disponível em: <https://www.youtube.com/watch?v=hghcZxZjcZY>. Acesso em: 18 jul. 2020.

¹¹⁷ Disponível em: https://www.youtube.com/watch?v=hw8Z1_YMqLM. Acesso em: 18 jul. 2020.

Considerando, dessa forma, a crescente importância das Forças Armadas Brasileiras, entendemos que o comportamento do governo brasileiro foi de aumentar as despesas do Ministério da Defesa. Os seguintes dados corroboram com essa afirmação:

Tabela 09: Despesas do Ministério da Defesa entre 2012 e 2018

Ano	Despesas	Ano	Despesas
2012	R\$ 66.378.794.000,00	2016	R\$ 77.025.164.375,26
2013	R\$ 70.880.965.000,00	2017	R\$ 85.488.885.936,72
2014	R\$ 68.515.311.689,32	2018	R\$ 88.199.571.610,67
2015	R\$ 71.607.827.931,24		

Fonte: Elaborado pela autora com base em www.portaltransparencia.gov.br, 2020¹¹⁸.

Podemos observar, de acordo com os dados da Tabela 09, um crescimento das despesas do Ministério da Defesa ao longo dos anos, sobretudo após o *impeachment* da ex-presidenta Dilma Rousseff, em 2015. Embora haja dificuldade em precisar os gastos específicos com a cibersegurança no Brasil, é possível inferir que as despesas do Ministério da Defesa cresceram tal-qualmente cresceu a importância dada ao setor cibernético e às atividades de cibersegurança.

Não significa, contudo, que o aumento das despesas do MD corresponda a um aumento das operações cibernéticas e investimento na área de cibersegurança no Brasil. Isso demonstra a crescente importância conferida à Defesa e Segurança no Brasil nos últimos anos, ponto que é válido na construção de nossa argumentação a respeito do processo de securitização.

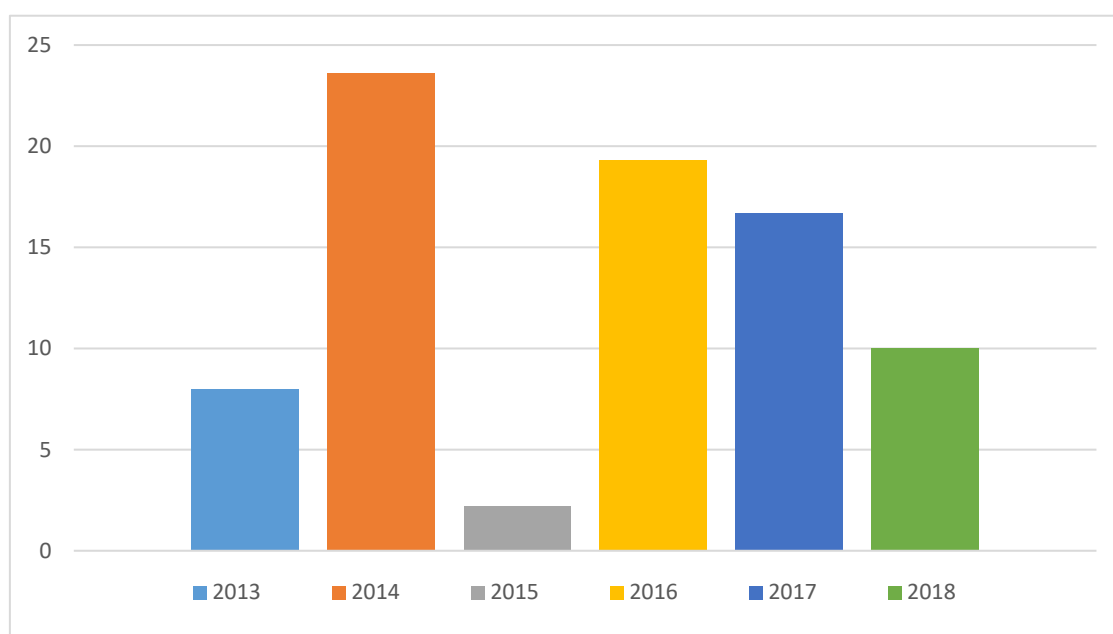
Quando pesquisado pelo orçamento realizado usando o termo “Defesa Cibernética” no Portal da Transparência do Governo Federal, obtém-se grande quantidade de resultados, mas todos eles tendo o Ministério da Defesa como órgão superior que realizou tais despesas.

¹¹⁸ As informações foram coletadas no site do Portal da Transparência do Governo Federal em 11 de abril de 2019 e conferidos em 18 de julho de 2020.

A partir dos resultados, inferimos que o governo brasileiro, em termos de ciberdefesa, destinou cerca de R\$ 70,8 milhões ao setor entre 2013 e 2018¹¹⁹. As despesas por ano foram: 2013, cerca de R\$ 8 milhões; 2014, cerca de R\$ 23,60 milhões; 2015, cerca de R\$ 2,20 milhões; 2016, cerca de R\$ 19,30 milhões; 2017, cerca de R\$ 16,70 milhões; e 2018, cerca de R\$ 10 milhões.

Utilizamos o gráfico a seguir como suporte visual na elucidação dos gastos com defesa cibernética.

Figura 02: Despesas com Defesa Cibernética no Brasil entre 2013 e 2018 em milhões de Reais



Fonte: Elaborado pela autora com base em www.portaltransparencia.gov.br, 2020¹²⁰.

Para a implementação do Centro de Defesa Cibernética, em 2010, o órgão recebeu R\$ 400 milhões que devem ser considerados como gastos com cibersegurança (SENADO FEDERAL, 2014, s/p).

Entendemos que 2014 representou o pico dos gastos quando considerado o período entre 2013 a 2018, pois foi o ano da Copa do Mundo FIFA realizada no Brasil e o primeiro grande “teste” do CDCiber no controle de ameaças que pudessem emergir do ciberespaço.

¹¹⁹ Houve dificuldade em recuperar dados confiáveis a respeito dos gastos com ciberdefesa e cibersegurança em 2011 e 2012.

¹²⁰ As informações foram coletadas no site do Portal da Transparência do Governo Federal em 11 de abril de 2019 e conferidos em 18 de julho de 2020.

As despesas cresceram novamente em 2016, como interpretamos, pelo mesmo motivo: o Brasil sediou as Olimpíadas naquele ano, o que exigiu esforço do Centro de Defesa Cibernética na garantia da proteção das possíveis ameaças no setor cibernético.

Dessa forma, podemos observar que houve um crescimento em termos absolutos das despesas do Ministério da Defesa, o que pode demonstrar maior investimento no Ministério¹²¹. Ademais, de todo o recurso destinado ao Ministério da Defesa nos últimos 4 anos, pelo menos 40% foram repassados ao Comando do Exército.

Podemos interpretar, a partir dos dados, que o Exército Brasileiro tem mais despesas do que a Marinha e a Força Aérea, pois arca com equipamentos eletrônicos que servem na manutenção da cibersegurança, bem como com os equipamentos de monitoramento de fronteiras, função também atribuída ao Exército.

Compreender o dispêndio de recursos com Segurança e Defesa é importante em um país como o Brasil, definido pelo próprio Ministério da Defesa como sendo “pacífico por tradição e convicção” (BRASIL, 2012a, p. 41). O discurso de novas ameaças, somado à importância conferida ao papel das Forças Armadas pela sociedade, justifica as despesas com o setor.

Outro desdobramento importante do processo de securitização do ciberespaço brasileiro foi a Estratégia Nacional de Segurança Cibernética, aprovada pelo Decreto nº 10.222 de 2020. Da mesma maneira em que o Decreto 6.703/18 aprovou a Estratégia Nacional de Defesa e apresentou o texto completo no anexo do documento, a Estratégia Nacional de Segurança Cibernética (E-Ciber) está anexa ao Decreto 10.222/20.

Considerando que as “ameaças cibernéticas [...] colocam em risco a administração pública e a sociedade”, o governo brasileiro desenvolveu, com o auxílio de grupos de trabalho, a Estratégia Nacional de Segurança Cibernética com validade no quadriênio 2020-2023 (BRASIL, 2020, s/p).

De acordo com o documento: “foram estabelecidos os objetivos estratégicos nacionais, e as respectivas ações estratégicas, segundo sete eixos de atuação que demonstram

¹²¹ Evidente que análise mais detalhada e comparações mais aprofundadas dos dados são necessárias para compreender se de fato houve aumento de recursos para o MD, considerando todas as unidades do Ministério. Nossas considerações têm caráter superficial e correspondem apenas aos dados absolutos coletados.

à sociedade brasileira os pontos considerados relevantes para o país na área da segurança cibernética” (BRASIL, 2020, s/p).

A partir de um diagnóstico da segurança cibernética, baseado nos cenários internacional e nacional, a Estratégia Nacional de Segurança Cibernética teve como objetivos estratégicos: “1. Tornar o Brasil mais próspero e confiável no ambiente digital; 2. Aumentar a resiliência brasileira às ameaças cibernéticas; e 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional” (BRASIL, 2020, s/p).

As ações estratégicas, por sua vez, foram dez. Entre elas, destacamos quatro: “[...] Elevar o nível de proteção do Governo [...] Elevar o nível de proteção das Infraestruturas Críticas Nacionais [...] Aprimorar o arcabouço legal sobre segurança cibernética [...] Ampliar a cooperação internacional do Brasil em Segurança cibernética” (BRASIL, 2020, s/p).

Apontamos que na ação estratégica correspondente a “Elevar o nível de proteção do Governo” tem-se a recomendação aos órgãos públicos de manter atualizadas as máquinas e de possuir “cópias de segurança atualizadas e segregadas de forma automática em local protegido”¹²² (BRASIL, 2020, s/p). Podemos entender essas recomendações como um efeito do ataque do *ransomware WannaCry* em 2017 que criptografou as informações de diversas máquinas de repartições públicas tornando-as quase impossível de serem recuperadas¹²³.

As outras ações estratégicas que destacamos, conforme interpretamos, estão relacionadas a uma tendência internacional de investimento e cooperação na segurança cibernética, bem como na atualização da tipificação de crimes cibernéticos, o que favorece a promoção da confiança do ciberespaço brasileiro. Ademais, as infraestruturas críticas continuam sendo elemento importante nas ações estratégicas voltadas à cibersegurança.

Finalmente, os sete eixos foram separados em duas categorias, a saber: o de proteção e segurança e o de transformação. Os eixos referentes à proteção e segurança são: governança da segurança cibernética nacional; Universo Conectado e Seguro: Prevenção e Mitigação de Ameaças Cibernéticas; e Proteção Estratégica.

¹²² Essa sugestão poderia ser entendida, em outros termos, como “manter um *backup* de informações importantes *off-line*”.

¹²³ Ver item 3.8.

Os eixos referentes à transformação são: Dimensão Normativa; Pesquisa, Desenvolvimento e Inovação; Dimensão Internacional e Parcerias Estratégicas; e Educação (BRASIL, 2020).

Em uma análise geral da E-Ciber, podemos inferir que o governo brasileiro, a partir de 2019, passou a estabelecer diretrizes e ações mais específicas voltadas ao espaço. O documento aponta que o objetivo de tornar o Brasil “mais próspero e confiável no ambiente digital” promove o crescimento econômico e desenvolvimento social no País (BRASIL, 2020, s/p).

Tomando como base uma perspectiva mais crítica deste objetivo, podemos afirmar que a criação de um ambiente digital confiável atrai não só investimentos ao Brasil, mas também empresas transnacionais que têm na informatização o elemento central de seu funcionamento ou de seu modelo de negócios.

Por fim, um desdobramento importante que observamos do processo de securitização do ciberespaço brasileiro diz respeito a Segurança da Informação.

De acordo com a Estratégia Nacional de Segurança Cibernética,

Em nível superior aos debates sobre a segurança no espaço cibernético está a Segurança da Informação, área sistêmica e diretamente relacionada à proteção de um conjunto de informações e ao valor que estas possuem para um indivíduo ou para uma organização. Desse modo, segundo o art. 2º do Decreto nº 9.637, de 2018, a Segurança da Informação abrange a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais, e tem como princípios fundamentais a confidencialidade, a integridade, a disponibilidade e a autenticidade (BRASIL, 2020, s/p).

Tendo em vista a relevância conferida à Segurança da Informação, foi proposta, também no Decreto nº 9.637/18, que instituiu a Política Nacional de Segurança da Informação (PNSI), a elaboração de uma Estratégia Nacional de Segurança da Informação (BRASIL, 2018).

Como pôde ser observado no art. 6º da Política Nacional de Segurança da Informação:

A Estratégia Nacional de Segurança da Informação conterá as ações estratégicas e os objetivos relacionados à segurança da informação, em consonância com as políticas públicas e os programas do Governo federal, e será dividida nos seguintes módulos, entre outros, a serem definidos no momento de sua publicação: I - segurança cibernética; II - defesa cibernética; III - segurança das infraestruturas críticas; IV - segurança da informação sigilosa; e V - proteção contra vazamento de dados. Parágrafo único. A construção da Estratégia Nacional de Segurança da Informação

terá a ampla participação da sociedade e dos órgãos e das entidades do Poder Público (BRASIL, 2020, s/p).

Dessa forma, podemos esperar a publicação de uma Estratégia Nacional de Segurança da Informação que contemple as questões envolvendo as Novas Tecnologias da Informação e Comunicação pelo Ministério da Defesa nos próximos anos.

Em síntese, o processo de securitização do ciberespaço brasileiro desenvolveu uma orientação a ser seguida pelo Governo Federal na medida em que a informatização se consolida e o desenvolvimento tecnológico ocorre: a cibersegurança e a segurança da informação serão consideradas como matérias de Segurança e Defesa, fundamentais na manutenção da *soberania nacional*.

Outra tendência que se confirma é a presença das Forças Armadas nos diversos âmbitos da sociedade, aumentando seu escopo de atuação. A concorrência ao cargo de Presidente da República pelo capitão reformado do Exército, Jair Bolsonaro, estimulou que mais militares concorressem a cargos públicos. As candidaturas de militares cresceram 113% nas eleições de 2018 (NEGRISOLI, 2018).

O próprio presidente Jair Bolsonaro, quando eleito, ampliou a presença militar em pelo menos 30 órgãos federais nos primeiros nove meses de 2019 (MATTOSO; BRAGON, 2019). No ano de 2019 havia, pelo menos, “[...] 325 militares a mais [do que no ano anterior] no governo Bolsonaro, entre ministros e assessores” (MATTOSO; BRAGON, 2019, s/p).

A mesma tendência de alargamento da presença militar não é observada em países vizinhos ao Brasil, como Argentina, Chile e Uruguai. Apesar de também terem passado por um período de regime militar, estes países tiveram um processo histórico de redemocratização distinto do Brasil. Entendemos que a memória da ditadura militar é valorizada nestes países, o que explica a relação entre os militares e os civis ser diferente da do Brasil.

Entretanto, quando consideramos os elementos referentes a cibersegurança nos países da América do Sul, existem algumas semelhanças no tratamento da questão.

No caso da Argentina, por exemplo, algumas das responsabilidades de segurança cibernética estão a cargo do Estado Maior Conjunto, mas não de forma exclusiva. A participação civil também ocorre no âmbito do Ministério da Defesa argentino (GUEDES DE OLIVEIRA et al., 2017).

No caso do Chile, tal-qualmente, a ciberdefesa está submetida ao Ministério de Defesa Nacional. Ainda a respeito do Chile:

As únicas abordagens sobre o espaço cibernético acontecem quando o documento [Livro Branco do Chile] trata da política militar e da política de defesa. Na política militar, o espaço cibernético é tratado dentro do conceito de *campo de batalla*. Nessa concepção, o espaço cibernético é uma dimensão deste, com profundidade, altura e o espectro eletromagnético (GUEDES DE OLIVEIRA et al., 2017, p. 102).

Apesar desta abordagem, o governo chileno ainda está em vias de elaborar documentos mais detalhados a respeito do tratamento do ciberespaço e da compreensão oficial do governo a respeito da cibersegurança, como apontaram no site oficial do Ministério de Defesa Nacional¹²⁴.

O governo do Uruguai, por sua vez, reconheceu que as vulnerabilidades que se apresentam no ciberespaço podem comprometer a segurança dos Estados, contudo não tomou medidas específicas ou de cunho militar visando a cibersegurança (GUEDES DE OLIVEIRA et al., 2017). Como afirmaram Guedes de Oliveira et al. (2017), o Uruguai tem a intenção de “[...] desenvolver uma cultura de segurança cibernética nas Américas. Para isso, o país se dispõe a adotar medidas de prevenção eficazes para prever, tratar e responder aos ataques cibernéticos” (GUEDES DE OLIVEIRA et al., 2017, p. 119-120).

A cibersegurança nos Estados Unidos, por sua vez, se distancia, ainda que em partes, das realidades do Sul do continente. São várias as condições para isso, como entendemos: a quantidade de pessoas conectadas nas redes de computadores, a penetração da Internet no país, o acesso às novas tecnologias, etc. À vista disso, os EUA são alvo constante de ataques cibernéticos.

Entendemos que eventos que envolveram a exposição da Agência Nacional de Segurança dos Estados Unidos em 2013 podem ter estimulado que medidas fossem tomadas para reforçar sua cibersegurança. Entretanto, o País já vinha investindo no discurso de segurança cibernética há muito tempo. Como afirmou Gills Lopes (2013): “[...] o caso estadunidense se projeta como particular, pois é o que figura em praticamente todos os *frameworks* e análises relacionados à defesa cibernética, bem como é um dos primeiros atores a tratar as ameaças ciberespaciais como ‘de segurança nacional’” (LOPES, 2013, p. 49).

¹²⁴ Disponível em: <https://www.defensa.cl/temas-de-contenido/ciberdefensa/>. Acesso em: 19 jul. 2020.

O Departamento de Segurança Interna dos Estados Unidos (*Homeland Security*) e a própria Agência Nacional de Segurança (NSA, na sigla em inglês) eram os órgãos responsáveis pela Defesa e Segurança do espaço cibernético, mas, em 2018, o Departamento de Segurança Interna dos Estados Unidos elaborou sua própria Estratégia de Cibersegurança e criou a Agência de Cibersegurança e Segurança de Infraestrutura (CISA, na sigla em inglês).

A Estratégia de Cibersegurança do *Homeland Security* tinha como principal objetivo de, até 2023, aperfeiçoar o “gerenciamento de riscos de segurança cibernética, aumentando a segurança e a resiliência em toda a rede do governo e nas infraestruturas críticas” (ESTADOS UNIDOS, 2018, capa, tradução nossa¹²⁵).

Além da Estratégia de Cibersegurança, a Casa Branca publicou, em setembro de 2018, a Ciberestratégia Nacional dos Estados Unidos da América, responsável por garantir a segurança da população americana e o “*American Way of Life*”¹²⁶ (ESTADOS UNIDOS, 2018a, p. 06).

Ambos documentos estabelecem princípios e diretrizes na garantia da segurança cibernética, da proteção da privacidade da população americana e da preservação das infraestruturas críticas, além da preocupação com o “ciberterrorismo”.

Após essa breve leitura, podemos afirmar que alguns dos elementos estipulados pelos documentos de cibersegurança norte-americanos se assemelham à Estratégia Nacional de Segurança Cibernética brasileira, principalmente no que se refere aos objetivos da Estratégia de Cibersegurança do Departamento de Segurança Interna.

Dessa forma, inferimos que as tomadas de decisão a respeito da cibersegurança no Brasil estão mais próximas da realidade dos Estados Unidos do que de seus vizinhos da América do Sul. O panorama que antecipamos é de que esta tendência permaneça no futuro próximo brasileiro pelos motivos que já expusemos no início deste capítulo.

Essa tendência brasileira de se aproximar mais de uma política norte-americana do que de uma política sul-americana advém de uma experiência histórica autoritária. O

¹²⁵ No original: “By 2023, the Department of Homeland Security will have improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure [...]” (ESTADOS UNIDOS, 2018, capa).

¹²⁶ “Modo de Vida Americano”. Lema que ficou popular a partir dos anos 1950, nos EUA, para descrever o estilo de vida conservador dos americanos.

processo histórico brasileiro, especialmente no que se refere ao período de redemocratização, difere dos seus vizinhos sul-americanos.

A Guerra das Malvinas, por exemplo, elucida a forma pela qual a ditadura argentina chegou ao fim. A população argentina, já insatisfeita com problemas econômicos e políticos que ocorriam durante o regime militar viu na empreitada militar da Argentina nas Malvinas mais um motivo para o fim do regime militar.

A rendição argentina na Guerra das Malvinas colocou fim ao governo da junta militar que já durava dez anos naquele País principalmente pela força da opinião popular (PHILLIPS, 2014). O governo brasileiro, à época, também na condição de um regime militar, apoiou o governo argentino na campanha militar na Ilha das Malvinas.

O resultado do fim do governo da junta militar argentina pautou o sentimento que a população argentina nutre até hoje a respeito da atuação das Forças Armadas na política daquele País. Processo histórico, reforçamos, que foi diferente daquele que ocorreu no Brasil.

Outro exemplo de diferentes processos de redemocratização na América do Sul diz respeito ao Chile. O fim da ditadura Pinochet que durou 17 anos no País fez com que a questão da memória fosse bastante valorizada no Chile. Observa-se a valorização da memória no Chile até os dias atuais a partir de uma organização e mobilização social.

Como já afirmado anteriormente, os papel e atuação das Forças Armadas no território brasileiro difere nestes aspectos em relação a outros países sul-americanos, na medida em que uma intervenção militar já foi pauta de manifestações populares.

Deve-se considerar, entretanto, tais condições que levaram a presença militar e legitimação de ações das Forças Armadas em funções diversas no Brasil pela sua sociedade conservadora.

Tal argumentação a respeito dos diferentes processos históricos que moldaram as sociedades atuais do Brasil e de seu vizinho não será desenvolvida neste capítulo, mas se trata de uma questão que pode justificar uma proximidade maior entre Brasil e EUA em detrimento de uma aproximação Brasil e América do Sul. A presença norte-americana em assuntos culturais, de Política Externa ou econômicas do Brasil permaneceram mesmo após o fim da ditadura militar.

6 CONSIDERAÇÕES FINAIS

Quando idealizados com a finalidade de melhorar a comunicação entre os soldados durante o período da Guerra Fria, não se imaginava que os computadores, telefones celulares, Internet e outras Tecnologias de Informação e Comunicação teriam a popularidade que teriam no século XXI.

As TICs não apenas se popularizaram, mas também transformaram os meios de produção, as relações sociais e o comportamento dos indivíduos, além de criar um novo estilo de vida dependente dos aparatos tecnológicos e da informatização.

O ciberespaço foi produto destas transformações. Como afirmaram Guedes de Oliveira et al. (2017): “Por ser fruto das mãos humanas, o espaço cibernético foi explorado como uma ferramenta importante desde sua constituição”. Contudo, entendemos que não foi só uma ferramenta explorada: a relação entre a sociedade e o ciberespaço foi – e continua sendo – recíproca. A humanidade transforma o ciberespaço e, tal-qualmente, o ciberespaço transforma a humanidade.

A década de 1990 foi importante para as TICs se popularizarem e se consolidarem em todos os níveis da sociedade. Foi nesta década, também, que o mundo assistiu o fim da bipolaridade advinda da concorrência entre Estados Unidos e URSS, e as preocupações internacionais de um conflito armado ou nuclear deram lugar a novas ameaças. O fim do século, portanto, trouxe significativas transformações a nível mundial.

Dessa forma, ocorreu uma perda do referencial do Estado e a ampliação da agenda de Segurança Internacional que as teorias *mainstream* de Relações Internacionais não puderam prever. A exploração das Novas Tecnologias de Informação e Comunicação também entraram na agenda de novas ameaças que eram levadas em consideração.

A Escola de Copenhague, à vista disso, desenvolveu uma teoria híbrida, que ofereceu um quadro de análise que buscou compreender o papel destes novos elementos de segurança sem desconsiderar aqueles tradicionais. Isso fez com que fosse possível tentar compreender de que maneira se passou a invocar o ciberespaço como questão de segurança e de manutenção de soberania.

O governo brasileiro, ainda que o País esteja na condição distante dos grandes centros, começou a reconhecer a sensibilidade de seu setor cibernético e incentivou estudos a respeito do avanço tecnológico a sua relação com a Sociedade da Informação ainda na década de

1990. A preocupação alcançou os níveis de defesa nacional após as transformações engendradas pelo ataque terrorista, em 2001, à Nova Iorque. Tal evento suscitou Seminário de Política de Defesa para o Século XXI, em 2002, com o objetivo de gerar ações contra as ameaças “não ortodoxas”, conforme foram denominadas pelo então Ministro da Defesa.

O Seminário de Política de Defesa para o Século XXI resultou em uma nova Política de Defesa Nacional publicada pelo Ministério da Defesa em 2005 que, por sua vez, resultou em uma Estratégia Nacional de Defesa, em 2008, documento que também resultou em outras Políticas, Doutrinas e Decretos que se dedicaram a promover a cibersegurança.

Na tentativa de compreender estas transformações no quadro de defesa brasileiro, nos baseamos no quadro analítico da Teoria de Securitização, a teoria híbrida desenvolvida pela Escola de Copenhague.

Tomando como ponto de partida os três componentes para que o processo de securitização ocorra com sucesso - “a ameaça existencial, a ação emergencial e os efeitos na relação entre as unidades [...]” (BUZAN; WÆVER; DE WILDE, 1998, p. 26) -, podemos sugerir que o governo brasileiro securitizou seu espaço cibernético em três fases: a primeira entre os anos de 2002 e 2007, a segunda, entre os anos de 2008 e 2011, e a terceira entre os anos de 2012 a 2018.

A teoria da Securitização foi relevante na medida em que apresenta uma perspectiva de *construção social* daquilo que é entendido como ameaça e, por conseguinte, como questão de segurança nacional (BUZAN; HANSEN, 2012, grifo nosso). Em nossa análise, tentamos demonstrar de que forma ocorreu a construção da cibersegurança no Brasil nestas três fases.

Ressaltamos, entretanto, que a securitização é um processo e que a separação entre fases é uma ferramenta metodológica utilizada na tentativa de compreendê-lo

Durante a primeira fase do processo securitizatório, entre 2002 e 2007, fora realizado o Seminário de Política para o Século XXI (2002) e a conseguinte publicação da Política de Defesa Nacional (2005) em âmbito brasileiro, além dos debates regionais a respeito de *novas ameaças* e o papel da tecnologia em nível da OEA (2003). Entendemos que este momento pode ser associado ao *speech-act*, ou o discurso, fase que se apresenta uma matéria – no caso o espaço cibernético – como existencialmente ameaçado. Foi neste momento que o Ministério da Defesa iniciou sua articulação visando a segurança cibernética. As Tecnologias

de Informação e Comunicação ganharam espaço nessa época como elementos de segurança nos debates que se sucediam.

A segunda fase da securitização do espaço cibernético ocorreu entre 2008 e 2011. Foi neste período em questão que houve a publicação da Estratégia Nacional de Defesa (2008) que, em sua sexta diretriz, aponta o espaço cibernético como vulnerável e que deve ser assegurado pelo Exército Brasileiro. Foi neste intervalo, do mesmo modo, que foram criados o Centro de Defesa Cibernético e o Núcleo de Defesa Cibernético, instrumentos no esforço pela segurança cibernética brasileira. Entendemos esta fase como o momento da *ação emergencial*, a tomada de decisão de levar a segurança cibernética “para além das regras do jogo”, assim como afirmam os autores da Escola de Copenhague (BUZAN; WÆVER; DE WILDE, 1998, p. 23).

Esta fase é importante para se interpretar o processo de securitização, pois podemos observar que o governo postulou o setor cibernético como infraestrutura estratégica e até indicou que a Segurança Cibernética se equiparava às Segurança Nuclear e Segurança Espacial.

A terceira e última fase é compreendida pelos acontecimentos de 2011 a 2018, pois evidenciaram os *produtos* do processo de securitização a partir da publicação das Política Cibernética de Defesa e Doutrina Militar de Defesa Cibernética. Ambos documentos, produtos de um CDCiber já implementado, demonstraram a visão do Ministério da Defesa a respeito do espaço cibernético e consolidaram um aspecto emergencial de tratamento do setor.

Nesta última fase, podemos observar também o repasse de recursos do Ministério da Defesa ao setor cibernético que, em alguns momentos, foi mais elevado do que em outros. Ademais, neste último período que vai até 2018, tivemos a publicação do Marco Civil da Internet (2014), do Guia de Defesa Cibernética na América do Sul (2017) e do Decreto que instituiu a Política Nacional da Segurança da Informação (2018).

Ou seja, a privacidade e o direito do usuário também se intensificaram no debate público do uso das tecnologias. Informações sigilosas, classificadas ou sensíveis também tiveram novo tratamento com a Política Nacional da Segurança da Informação (BRASIL, 2014a; BRASIL, 2018).

Estas três fases vão ao encontro daquilo que foi enunciado pelos autores da Escola de Copenhague das Relações Internacionais. O Ministério da Defesa brasileiro agiu na condição de agente securitizador e o objeto de referência foi o próprio espaço cibernético. No papel dos atores funcionais, por sua vez, observamos as próprias Forças Armadas, em específico o Exército Brasileiro, que desde o início do século aumentava seu prestígio frente a sociedade brasileira e ganhava cada vez mais responsabilidades, entre elas, a proteção do setor cibernético.

Ao que se refere às condições facilitadoras (BUZAN; WÆVER; DE WILDE, 1998, p. 36), entendemos que o próprio desenvolvimento tecnológico agiu dessa maneira, assim como a preocupação internacional com ameaças não tradicionais desde setembro de 2001.

Ainda cabe argumentar que, uma vez que as novas tecnologias e o ciberespaço podem ser entendidos, pelo sistema internacional, como meios que constituem ameaças, o Brasil viu a necessidade de proteger o espaço cibernético tal como o próprio sistema internacional. Ataques a infraestruturas críticas tais como houveram no Irã, na Ucrânia e o Brasil até os casos de ciberespionagem evidenciados pelo vazamento de informações deram sentido de urgência as questões que envolvem a ciberdefesa e a cibersegurança.

Ademais, evidenciou-se a tentativa do Brasil em se aproximar, em termos de cibersegurança, aos Estados Unidos nos últimos três anos. Existem semelhanças entre os objetivos do Brasil com a publicação da Estratégia Nacional de Segurança Cibernética e a Estratégia de Cibersegurança dos Estados Unidos publicada em 2018. Entendemos que a relação EUA-Brasil deve permanecer nesse sentido, especialmente no que se refere aos assuntos militares, dado o alinhamento entre os dois governos a partir de 2018 com a eleição do presidente Jair Bolsonaro.

Podemos, ainda, incitar como debate uma questão já apresentada anteriormente sobre as Forças Armadas no Brasil. O processo de segurança cibernético, analisado em uma perspectiva mais ampla, reforça a ressignificação do papel das Forças Armadas, em especial o Exército Brasileiro, frente à sociedade brasileira, de acordo com os imperativos de flexibilidade e elasticidade postulados pelo Ministério da Defesa a partir deste século.

Esta ressignificação vem ocorrendo desde a década de 1990 e foi legitimado pela sociedade conservadora brasileira. Assim sendo, ocorreu uma “normalização” de que cada vez mais funções sejam atribuídas às Forças Armadas Brasileiras. A Estratégia Nacional de

Defesa teve como principal objetivo reorganizar e reorientar as Forças Armadas, incentivando que houvesse uma transformação em seu escopo de atuação (BRASIL, 2008).

Em linhas gerais, podemos afirmar que houve uma tentativa de tornar o ciberespaço mais seguro, tanto por uma questão de defesa e segurança nacionais, como por uma perspectiva social e econômica. A justificativa que se observou, entretanto, para os investimentos em cibersegurança, foi a manutenção da soberania nacional.

Os esforços brasileiros em relação à segurança no ambiente digital e no ciberespaço obtiveram um caráter militar entre 2002 e 2018, como evidenciamos. Mas também podemos inferir que a inclusão digital, a proteção do usuário na Internet e a confiança no espaço cibernético para investidores estrangeiros também vêm sendo debatidos, especialmente com a publicação da Estratégia Brasileira para a Transformação Digital, a recente Estratégia Nacional de Segurança Cibernética e a futura Estratégia Nacional de Segurança da Informação (BRASIL, 2018; BRASIL, 2018a; BRASIL, 2020).

Evidente que a proteção do usuário na Internet – e no ciberespaço de forma geral – é importante, assim como a criação dos mecanismos legais para o uso das tecnologias, mas isso não é o suficiente. Considerando os principais ataques cibernéticos que o Brasil sofre, muitos deles advêm de uma dificuldade do próprio usuário em identificar aquilo que pode ser uma ameaça. Os ataques de *phishing*, por exemplo, acontecem porque o usuário legítimo, voluntariamente, informa suas informações pessoais e senhas ao usuário mal-intencionado. À vista disso, compreendemos a necessidade da educação dos usuários a respeito das boas práticas na Internet.

REFERÊNCIAS

AKBANOV, Maxat; VASSILAKIS, Vassilios G.; LOGOTHETIS, Michael D. WannaCry ransomware: Analysis of Infection, Persistence, Recovery, Prevention and Propagation Mechanisms. **Journal of Telecommunications and Information Technology**, v. 01, 2019. Disponível em: <https://www.il-pib.pl/czasopisma/JTIT/2019/1/113.pdf>. Acesso em: 11 jul. 2020.

ALMEIDA, João Marques de. A União Europeia e a Rússia após a crise da Geórgia: o fim do paradigma pós “Guerra Fria”. **Relações Internacionais (R: I)**, n. 20, p. 17-29, 2008.

ARNAUDO, Daniel. O Brasil e o Marco Civil da Internet: O Estado da Governança Digital Brasileira. **Artigo Estratégico**, n. 25, Rio de Janeiro: Instituto Igarapé, 2017. Disponível em: https://igarape.org.br/marcocivil/assets/downloads/igarape_o-brasil-e-o-marco-civil-da-internet.pdf. Acesso 20 maio 2020.

BAEZNER, Marie. **Cyber and Information warfare in the Ukrainian conflict**. 2ª ed. Center for Security Studies (CSS), Zurique: 2018. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf. Acesso em: 30 maio 2020.

BALL, James; BORGER, Julian; GREENWALD, Glenn. **Revealed: how US and UK spy agencies defeat internet privacy and security**. Theguardian.com, 2013. Sem paginação. Disponível em: <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>. Acesso em: 18 ago. 2019.

BALZACQ, Thierry; LÉONARD, Sarah; RUZICKA, Jan. ‘Securitization’ revisited: theory and cases. **International Relations**, v. 30, n. 04, p. 494-531, 2016.

BARTOT, Jéssica F. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. **VirtuaJus**, Belo Horizonte, v. 2, n. 2, p. 338-362, 2017.

BBC. **Cyber attack hits South Korea websites**. Bbc.com, 2013. Sem Paginação. Disponível em: <https://www.bbc.com/news/world-asia-23042334>. Acesso em: 25 maio 2019.

BBC. Sony cyber-attack: **North Korea faces new US sanctions**. Bbc.com, 2014. Sem Paginação. Disponível em: <https://www.bbc.com/news/world-us-canada-30661973>. Acesso em: 26 maio 2019.

BRASIL. DECRETO Nº 5.484, DE 30 DE JUNHO DE 2005. Aprova a Política de Defesa Nacional, e dá outras providências. **Presidência da República**: Casa Civil, Brasília, 2005. (Originalmente publicado no Diário Oficial da União). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm. Acesso em: 01 out. 2019.

BRASIL. DECRETO Nº 6.703, DE 18 DE DEZEMBRO DE 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. **Presidência da República**: Casa Civil, Brasília, 2008. (Originalmente publicado no Diário Oficial da União). Sem Paginação.

Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm. Acesso em: 30 set. 2019.

BRASIL. DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, *caput*, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

Câmara dos Deputados: Centro de Documentação e Informação, Brasília, 2018. (Originalmente publicado no Diário Oficial da União). Sem Paginação. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/2018/decreto-9637-26-dezembro-2018-787537-norma-pe.html>. Acesso em: 26 jan. 2018.

BRASIL. DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020. Aprova a Estratégia Nacional de Segurança Cibernética. **Presidência da República:** Secretaria-Geral, Brasília, 2020. Sem Paginação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 19 jul. 2020.

BRASIL. **Doutrina Militar de Defesa Cibernética.** Ministério da Defesa. Brasília, 2014. Disponível em: https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_de_fesa_cibernetica_1_2014.pdf. Acesso em: 16 maio 2018.

BRASIL. **Doutrina de Operações Conjuntas:** 1º Volume. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. Brasília, 2011. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/134/1/MD30_M01_v1.pdf. Acesso em: 02 maio 2019.

BRASIL. **Estratégia Brasileira para a Transformação Digital.** Brasília: Ministério da Ciência, Tecnologia, Inovações e Comunicações, 2018a. Disponível em: <http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf>. Acesso em 26 ago. 2019.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012:** Dispõe sobre a tipificação criminal de delitos informáticos. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 14 jan. 2020.

BRASIL. **Lei 12.965, de 23 de abril de 2014:** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. 2014a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 26 jan. 2020.

BRASIL. **Plano Plurianual 2004-2007:** Projeto de Lei. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Planejamento e Investimentos Estratégicos. Brasília: MP, 2003. Disponível em: <https://www2.camara.leg.br/orcamento-da-uniao/leis-orcamentarias/ppa/2004-2007/ppa-2004-2007/proposta/anexo1.PDF>. Acesso em: 20 jan. 2019.

BRASIL. **Política de Defesa Nacional**. Presidência da República. Brasília: 1996. Disponível em: <http://www.biblioteca.presidencia.gov.br/publicacoes-oficiais/catalogo/fhc/politica-de-defesa-nacional-1996.pdf>. Acesso em 23 jan. 2020.

BRASIL. POLÍTICA NACIONAL DE DEFESA E ESTRATÉGIA NACIONAL DE DEFESA. **Ministério da Defesa**: Brasília, 2012a. Disponível em: https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf. Acesso em: 30 set. 2019.

BRASIL. POLÍTICA NACIONAL DE DEFESA E ESTRATÉGIA NACIONAL DE DEFESA. **Ministério da Defesa**: Brasília, 2020a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 14 out. 2020.

BRASIL. **Portaria nº 666, de 4 de agosto de 2010**. Cria o Centro de Defesa Cibernética do Exército e dá outras providências. Boletim do Exército nº 31/2010, de 06 de agosto de 2010. Comandante do Exército: Brasília, 2010. Disponível em: <http://www.sgex.eb.mil.br/sistemas/be/boletins.php>. Acesso em: 24 jan. 2020.

BRASIL. **Portaria nº 667, de 4 de agosto de 2010**. Ativa o Núcleo do Centro de Defesa Cibernética do Exército e dá outras providências. Boletim do Exército nº 31/2010, de 05 de agosto de 2010. Comandante do Exército: Brasília, 2010a. Disponível em: <http://www.sgex.eb.mil.br/sistemas/be/boletins.php>. Acesso em: 24 jan. 2020.

BUMILLER, Elisabeth. **Video Shows U.S. Killing of Reuters Employees**. The New York Times, MiddleEast, 2020. Sem Paginação. Disponível em: <https://www.nytimes.com/2010/04/06/world/middleeast/06baghdad.html>. Acesso em: 03 maio 2020.

BUZAN, Barry. **People, States and Fear**: The National Security Problem in International Relations. Brighton: Wheatsheaf Books, 1983. 262 p.

BUZAN, Barry. Rethinking Security after de Cold War. **Cooperation and Conflict**, v. 32, p. 5-28. 1997.

BUZAN, Barry; HANSEN, Lene. **A evolução dos estudos de Segurança Internacional**. São Paulo: Editora Unesp, 2012. 576 p.

BUZAN, Barry; WÆVER, Ole. **Regions and Powers**: The Structure of International Security. Cambridge University Press, 2003.

BUZAN, Barry; WÆVER, Ole; DE WILDE, Jaap. **Security**: A New Framework for Analysis. Colorado: Lyenne Rienner Publishers, 1998. 239 p.

CAPELAS, Bruno. **No Brasil, órgãos públicos foram os mais afetados pelo WannaCry**. Link, Cultura Digital, Estadão, 2017. Sem Paginação. Disponível em: <https://link.estadao.com.br/noticias/cultura-digital,no-brasil-orgaos-publicos-foram-os-mais-afetados-pelo-wannacry,70001816480>. Acesso em: 02 jan. 2020.

CERT. **Incidentes reportados ao Cert.br em 2015:** tipos de ataques. Brasília: Nic.br., 2016. Disponível em: <http://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque.html>. Acesso em: 02 jan. 2020.

CLARKE, Richard A; KNAKE, Robert A. **Cyber War: The Next Threat to National Security and What to do About It**. New York: HarperCollins Publishers, 2012.

DESIMONE, Antonio; HORTON, Nicholas. **Sony's Nightmare Before Christmas:** The 2014 North Korean Cyber Attack on Sony and Lesson for US Government Actions in Cyberspace. The Johns Hopkins University Applied Physics Laboratory, 2017.

EDDY, Paul. LINKLATER; Magnus; GILLMAN, Peter. **The Falklands War** – The Full Story. Sphere: 1982.

ENGELKE, Daniel. **The real war against the press: Julian Assange as public enemy number one**. DiEM25.org, Democracy in Europe, 2020. Sem Paginação. Disponível em: <https://diem25.org/the-real-war-against-the-press-julian-assange-public-enemy-number-one>. Acesso em: 04 jul. 2020.

ESTADOS UNIDOS. **Cybersecurity Strategy**. U.S. Department of Homeland Security, 2018. Disponível em: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf. Acesso em: 19 jul. 2020.

ESTADOS UNIDOS. **National Cyber Strategy of the United States of America**. White House, 2018a. Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. Acesso em: 19 jul. 2020.

FALLET, João. **A Constituição prevê a possibilidade de intervenção militar?** BBC.com, BBC Brasil. São Paulo: 2018. Disponível em: <https://www.bbc.com/portuguese/brasil-44335337>. Acesso em: 18 jul. 2020.

FALLIERE, Nicolas; O'MURCHU, Liam; CHIEN, Eric. **W32.Stuxnet Dossier**. Symantec Security Response, Symantec Corporation, 2015. Disponível em: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Acesso em: 23 ago. 2019.

FERREIRA, Oliveira S. Ideias Para Uma Concepção Estratégica: A Defesa Nacional e O Projeto Nacional. In: REBELO, Aldo; FERNANTES, Luís (org). **Seminário Política de Defesa Para o Século XXI**. Brasília: Câmara dos Deputados, Coordenação de Publicações, 2003. 285p.

FIGUEIREDO, Lucas. **Ministério do Silêncio:** A História do Serviço Secreto Brasileiro de Washington Luís a Lula. Rio de Janeiro: Record, 2005. 595 p.

FOLHA DE SÃO PAULO. **Governo na Estônia é alvo de hackers**. Folha de São Paulo, Mundo. Da Redação. 2007. Sem Paginação. Disponível em: <https://www1.folha.uol.com.br/fsp/mundo/ft1805200713.htm>. Acesso em: 16 ago. 2019.

G1. **'Bombardeio virtual' de hackers deu início ao ataque contra a Geórgia**. G1 Globo.com, Tecnologia, 2008. Sem Paginação. Disponível em:

<http://g1.globo.com/Noticias/Tecnologia/0,,MUL729549-6174,00-BOMBARDEIO+VIRTUAL+DE+HACKERS+DEU+INICIO+AO+ATAQUE+CONTRA+A+GEORGIA.html>. Acesso em: 16 ago. 2019

G1. **Brasil é o país que recebe mais ataques cibernéticos da América Latina.** Bom dia Brasil, Globo.com, 2016. Sem Paginação. Disponível em: <http://g1.globo.com/bom-dia-brasil/noticia/2016/12/brasil-e-pais-que-recebe-mais-ataques-ciberneticos-da-america-latina.html>. Acesso em: 02 jan. 2020.

G1. **Ciberataques em larga escala atingem empresas no mundo e afetam Brasil.** G1.globo.com, Economia, Tecnologia, 2017. Sem Paginação. Disponível em: <https://g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sao-alvo-cyber-ataques-em-larga-escala.ghtml>. Acesso em: 18 jun. 2020.

G1. **Documentos da NSA apontam Dilma Rousseff como alvo de espionagem.** G1.com, 2013. Sem Paginação. Disponível em: <http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html>. Acesso em 18 ago. 2019.

G1. **Veja as mensagens vazadas pelo WikiLeaks que citam o Brasil.** São Paulo: G1, 2010. Sem paginação. Disponível em: <http://g1.globo.com/mundo/noticia/2010/12/veja-mensagens-vazadas-pelo-wikileaks-que-citam-o-brasil.html>. Acesso em: 03 maio 2020.

G1. **WikiLeaks divulga locais vitais para a segurança nacional dos EUA.** G1, Mundo. 2010a. Sem Paginação. Disponível em: <http://g1.globo.com/mundo/noticia/2010/12/wikileaks-divulga-lista-de-locais-vitais-para-seguranca-nacional-dos-eua.html>. Acesso em: 04 maio 2020.

GAYLEN, Damien. **Julian Assange “told Edward Snowden not to seek asylum in Latin America”.** Theguardian.com, 2015. Sem Paginação. Disponível em: <https://www.theguardian.com/media/2015/aug/29/julian-assange-told-edward-snowdon-not-seek-asylum-in-latin-america>. Acesso em: 05 maio 2020.

GIBSON, William. **Neuromancer.** Trad. Fábio Fernandes. 5ª ed. São Paulo: Aleph, 2016. 320 p.

GREENWALD, Glenn. **NSA collecting phone records of millions of Verizon customers daily.** Theguardian.com, 2013. Sem Paginação. Disponível em: <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>. Acesso em 18 ago. 2019.

GREENWALD, Glenn; MACASKILL, Ewan. **NSA Prism program taps in to user data of Apple Google and Others.** Theguardian.com, 2013. Sem paginação. Disponível em: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 18 ago. 2019.

GREENWALD, Glenn; MACASKILL, Ewan; POITRAS, Laura. **Edward Snowden: the whistleblower behind the NSA surveillance revelations.** Theguardian.com, 2013. Sem paginação. Disponível em: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acesso em: 18 ago. 2019.

GREENWALD, Glenn; KAZ, Roberto; CASADO, José. **EUA espionaram milhares de e-mails e ligações de brasileiros**. Oglobo.com, 2013. Sem Paginação. Disponível em: <https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>. Acesso em: 18 ago. 2019.

GUEDES DE OLIVEIRA, Marcos A.; PORTELA, Lucas Soares. As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil. **Revista Brasileira de Estudo de Defesa**, v. 4, n. 2, p. 77-99, 2017.

GUEDES DE OLIVEIRA, Marcos A.; PAGLIARI, Graciela D. C.; MARQUES, Adriana A.; PORTELA, Lucas S.; NETO, Walfredo Bento Ferreira. **Guia de Defesa Cibernética na América do Sul**. Recife: Ed. UFPE, 2017. 162 p.

HAGGARD, Stephan; LINDSAY, Jon R. North Korea and the Sony Hack: Exporting Instability Through Cyberspace. **Analysis from East-West Center**, n. 117, 2015. Disponível em: https://www.jstor.org/stable/resrep06456?seq=1#metadata_info_tab_contents. Acesso em 25 maio 2019.

HANSEN, Lene. **Security as a Practice**: Discourse Analysis and the Bosnian War. The new international relation series. New York: Routledge, 2006. 259 p.

HANSEN, Lene. The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School. **Millennium: Journal of International Studies**, v. 29, n. 2, 2000. p. 285-305.

HANSEN, Lene; NISSENBAUM, Helen. Digital disaster, cyber security, and the Copenhagen School. **International studies quarterly**, v. 53, n. 4, 2009. p. 1155-1175.

HAMANN, Eduarda Passarelli; TEIXEIRA, Carlos A. Ramires. (Org.) A participação do Brasil na MINUSTAH (2004-2017): Percepções, lições e práticas relevantes para futuras missões. Edição Especial: coletânea de artigos. Rio de Janeiro: Instituto Igarapé, 2017. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/03/2018-03-06-AE-MINUSTAH-PT.pdf>. Acesso em: 11 out. 2019.

HARDING, Luke. **Os arquivos Snowden**: A história secreta do homem mais procurado do mundo. São Paulo: LeYa Brasil, 2014. E-book.

HARLEY, Nicola. **North Korea behind WannaCry attack which crippled the NHS after stealing US cyber weapons, Microsoft chief claims**. Telegraph.co.uk, 2017. Sem Paginação. Disponível em: <https://www.telegraph.co.uk/news/2017/10/14/north-korea-behind-wannacry-attack-crippled-nhs-stealing-us/>. Acesso em: 11 jul. 2020.

HERZOG, Stephen. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. **Journal of Strategic Security**, v. 04, n. 02, p. 49-60, 2011. Disponível em: https://www.researchgate.net/publication/229014537_Revisiting_the_Estonian_Cyber_Attacks_Digital_Threats_and_Multinational_Responses. Acesso em: 16 ago. 2019.

HUYSMANS, Jef. Revisiting Copenhagen: Or, On the Creative Development of a Security Studies Agenda in Europe. **European Journal of international Relations**, v. 04, n. 04, p. 479-505, 1998.

KAZ, Roberto; CASADO, José. **NSA e CIA mantiveram em Brasília equipe para coleta de dados filtrados de satélite**. Oglbo.com, 2013. Sem Paginação. Disponível em: <https://oglobo.globo.com/mundo/nsa-cia-mantiveram-em-brasilia-equipe-para-coleta-de-dados-filtrados-de-satelite-8949723>. Acesso em: 18 ago. 2019.

KORYBKO, Andrew. **Guerras híbridas**: das revoluções coloridas aos golpes. Trad. Thyago Antunes. São Paulo: Expressão Popular, 2018. Disponível em: <https://www.expressaopopular.com.br/loja/wp-content/uploads/2020/05/guerras-hibridas.pdf>. Acesso em: 20 maio 2020.

LANDLER, Mark; MARKOFF, John. **Estônia protagoniza primeira virtual**. Trad. Cláudia Freire. G1 Globo.com, Tecnologia. 2007. Sem Paginação. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL45961-6174,00-ESTONIA+PROTAGONIZA+PRIMEIRA+GUERRA+VIRTUAL.html>. Acesso em: 16 ago. 2019.

LAUFER, Rafael; MORAES, Igor; VELLOSO, Pedro; BICUDO, Marco; CAMPISTA, Miguel; CUNHA, Daniel; COSTA, Luís Henrique; DUARTE, Otto. **Negação de Serviço: Ataques e Contramedidas**. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS 5. (Organizaador: Luciano Paschoal Gaspary). 2005. Disponível em: <https://www.gta.ufrj.br/ftp/gta/TechReports/LMVB05a.pdf>. Acesso em 16 ago. 2019.

LÉVY, Pierre. **As Tecnologias da Inteligência**: O Futuro do Pensamento na Era da Informática. Trad. Carlos Irineu da Costa. São Paulo: Editora 34, 2010.

LÉVY, Pierre. **Cibercultura**. Trad. Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LÉVY, Pierre. **O que é o virtual?** Trad. Paulo Neves. São Paulo: Editora 34, 1996.

LIMA, Lioman. **Como a energia elétrica se tornou o novo campo de batalha entre EUA e Rússia**. Bbc.com, BBC News Mundo, 2019. Sem Paginação. Disponível em: <https://www.bbc.com/portuguese/internacional-48691284>. Acesso em: 30 maio 2020

LOJKINE, Jean. A revolução informacional. Trad. José Paulo Neto. 3. ed. São Paulo: Cortez, 2002. 316 p.

LOPES, Gills. **Reflexos da Digitalização da Guerra da Política Internacional do Século XXI**: Uma Análise Exploratória da Securitização do Ciberespaço nos Estados Unidos, Brasil e Canadá. 2013. Dissertação (Mestrado em Ciência Política) – Universidade Federal do Pernambuco, Recife. 2013.

MAIER, Friedrich. **GRAMSCI ONLINE?** : Uma tradução gramsciana da cibersegurança. 2019. Dissertação (Mestrado em Ciências Sociais) – Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília. 2019. Disponível em:

https://www.marilia.unesp.br/Home/Pos-Graduacao/CienciasSociais/Dissertacoes/maier_f_me_mar.pdf. Acesso em 19 jan. 2020.

MARKOFF, John. **Geórgia inaugura era da ciberguerra**. Estadão, Notícias, 2008. Sem Paginação. Disponível em: <https://www.estadao.com.br/noticias/geral,georgia-inaugura-era-da-ciberguerra,1298>. Acesso em: 16 ago. 2019.

MAGALHÃES, Daniel. Da WikiLeaks aos Panama Papers: como os vazamentos de dados ajudaram a reconfigurar o jornalismo. **Temática**, v. 13, n. 02, 2017. Disponível em: <https://periodicos.ufpb.br/ojs2/index.php/tematica/article/view/33007>. Acesso em: 02 maio 2020.

MARQUES, Adriana A. Concepções Estratégicas Brasileiras no Contexto Internacional do Pós-Guerra Fria. **Revista de Sociologia e Política**, n. 20. Curitiba: 2003. Disponível em: <https://www.scielo.br/pdf/rsocp/n20/n20a7.pdf>. Acesso em: 10 julho 2020.

MATTOSO, Camila; BRAGON, Ranier. **Bolsonaro amplia presença de militares em 30 órgãos federais**. Folha.uol.com.br, Folha de São Paulo, 2019. Sem Paginação. Disponível em: <https://www1.folha.uol.com.br/poder/2019/10/bolsonaro-amplia-presenca-de-militares-em-30-orgaos-federais.shtml>. Acesso em: 15 jul. 2020.

MCDONALD, Matt. Construtivism. In: WILLIAMS, Paul D. (Ed.). **Security Studies: An Introduction**. Oxon: Routledge, 2008.

MCDONALD, Matt. Securitization and the Construction of Security. **European Journal of International Relations**, v. 14, n. 04, p. 563-587, 2008a.

MERCAU, Ezequiel. **The Falklands War: An Imperial History**. Cambridge: Cambridge University Press, 2019. E-book. Sem Paginação.

MIYAMOTO, Shiguenoli. **Geopolítica e poder no Brasil**. Campinas: Papirus, 1995.

MORGAN, Steve. **Global Cybersecurity Spending Predicted To Exceed \$1 Trillion From 2017-2021**. Cybersecurityventures.com, Cybercrime Magazine, 2019. Sem Paginação. Disponível em: <https://cybersecurityventures.com/cybersecurity-market-report/>. Acesso em: 30 maio 2020.

MUGGAH, Robert; GLENN, Misha; DINIZ, Gustavo. Securitização da Cibersegurança no Brasil. **Cadernos Adenauer XV**, n.4, p. 69-109, 2014. Disponível em: https://www.kas.de/c/document_library/get_file?uuid=e01ed6d1-a531-2d8d-58a3-dae713a1af78&groupId=265553. Acesso em 03 jun. 2019.

NEGRISOLI, Lucas. **Eleições 2018: Candidaturas de militares crescem 113%**. Em.com.br, Estado de Minas, Política, 2018. Sem Paginação. Disponível em: https://www.em.com.br/app/noticia/politica/2018/10/04/interna_politica,994063/eleicoes-2018-candidaturas-de-militares-crescem-113.shtml. Acesso em: 15 jul. 2020.

NUNES JUNIOR, Edson Mendes. WikiLeaks: o vazamento de informações secretas como forma de contra-hegemonia. **Fronteira**, v. 17, n. 33, Belo Horizonte, 2018. p. 63-72.

OEA. **Projeto de Declaração Sobre a Segurança Nas Américas**. Conferência Especial Sobre Segurança. México: 2003. 14 p. Disponível em: http://www.oas.org/juridico/portuguese/decl_security_pt.pdf. Acesso em: 14 ago. 2019.

OLIVEIRA, Anderson L.; SHIMA, Walter T. Um estudo sobre a sociedade da informação do Brasil no paradigma tecno-econômico das TICS. **Revista Capital Científico** – Eletrônica, v. 10, n. 2, 2012.

OLIVEIRA FRAZÃO, Pedro Henrique. **Um Big Brother Global? Os Programas de Vigilância da NSA à Luz da Securitização dos Espaços Sociotecnológicos**. 2016. Dissertação (Mestrado em Relações Internacionais) – Universidade Estadual da Paraíba (UEPB), João Pessoa, 2016. Disponível em: <http://pos-graduacao.uepb.edu.br/ppgri/files/2012/02/Pedro-Fraz%C3%A3o.pdf>. Acesso em: 18 fev. 2020.

OPPERMANN, Daniel. Virtual attacks and the problem of responsibility: the cases of China and Russia. **Carta Internacional**, p. 11-25, dez. 2010.

PACHECO, Liliana. WikiLeaks e Internet: O que poderá mudar no jornalismo a partir daqui. **Estudos em Comunicação**, n. 09, 2011. p. 31-43.

PASSARINHO, Nathalia; BONIN, Robson. **Presidente Lula critica prisão de fundador do site WikiLeaks**. Brasília: G1, 2010. Sem Paginação. Disponível em: <http://g1.globo.com/politica/noticia/2010/12/presidente-lula-critica-prisao-de-fundador-do-site-wikileaks.html>. Acesso em: 03 maio 2020.

PHILLIPS, Russel. **Foi Por Pouco: Breve História da Guerra das Malvinas**. Trad. Aline L. de Abreu. Babelcube Inc., 2014. E-book. Sem Paginação.

PORTINARI, Natália; MENDES, Adriana. **Bolsonaro vai a ato com aglomeração de manifestantes e pedidos de intervenção militar**. OGlobo.com, Globo, 2020. Disponível em: <https://oglobo.globo.com/brasil/bolsonaro-vai-ato-com-aglomeracao-de-manifestantes-pedidos-de-intervencao-militar-24382154>. Acesso em: 18 jul. 2020.

QUINTÃO, Geraldo M. da Cruz; A Política De Defesa Para O Século XXI e A Missão Constitucional Das Forças Armadas. In: REBELO, Aldo; FERNANTES, Luís (org). **Seminário Política de Defesa Para o Século XXI**. Brasília: Câmara dos Deputados, Coordenação de Publicações, 2003. 285p.

REBELO, Aldo; FERNANTES, Luís (org). **Seminário Política de Defesa Para o Século XXI**. Brasília: Câmara dos Deputados, Coordenação de Publicações, 2003. 285p.

REZENDE, Lucas Pereira; AZEVEDO, Cesar Augusto Lambert de. Sobre o Sistema de Segurança Coletiva e a Legitimidade das Operações de Paz da ONU. **Carta Internacional**, v. 6, n. 1, p. 26-38, 2011. Disponível em: <https://cartainternacional.abri.org.br/Carta/article/view/22/9>. Acesso em: 25 jan. 2020.

RODRIGUES, Renato. **Há um ano, WannaCry infectava mais de 200 mil sistemas**. Kaspersky.com.br, Blog, 2018. Sem Paginação. Disponível em:

<https://www.kaspersky.com.br/blog/um-ano-wannacry-ransomware/10282/>. Acesso em: 18 jun. 2020.

ROHR, Altieres. **Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia**. G1 Globo.com, Tecnologia, 2010. Sem Paginação. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html>. Acesso em: 23 ago. 2019.

SAINT-PIERRE, Hector. “Defesa” ou “Segurança”? Reflexões em torno de Conceitos e Ideologias. **Contexto Internacional**, v. 33, n 02, p. 407-433, 2011.

SANG-HUN, Choe. **Computer Networks in South Korea Are Paralyzed in Cyberattacks**. Thenewyorktimes.com, 2013. Sem Paginação. Disponível em: <https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html>. Acesso em: 25 maio 2019.

SANG-HUN, Choe; MARKOFF, John. **Cyberattacks Jam Government and commercial Web Sites in U.S. and South Korea**. Thenewyorktimes.com, 2009. Sem Paginação. Disponível em: <https://www.nytimes.com/2009/07/10/technology/10cyber.html>. Acesso em 15 maio 2019.

SENADO FEDERAL. Brasil investe pouco em inteligência. **Em discussão**, n. 21, 2014. Disponível em: <https://www12.senado.leg.br/emdiscussao/edicoes/espionagemcibernetica/realidadebrasil-sem-cultura-de-inteligencia/brasil-investe-pouco-em-inteligencia>. Acesso em: 06 jul. 2018.

SETOR CIBERNÉTICO (Brasil). **Ministério da Defesa**. Governo Federal, 2019. Sem Paginação. Disponível em: <https://www.defesa.gov.br/ciencia-e-tecnologia/setores-estrategicos/setor-cibernetico>. Acesso em: 24 jan. 2020.

SOBEL, CLIFFORD. **2008 U.S.-BRAZIL POLITICAL-MILITARY CONSULTATIONS AGENDA**. Brasília, 2008. Sem Paginação. Disponível em: https://search.wikileaks.org/plusd/cables/09BRASILIA34_a.html. Acesso em: 05 maio 2019.

SOBEL, Clifford. **BRAZIL’S NEW DEFENSE STRATEGY – STRATEGY FOR DEVELOPMENT**. Brasília, 2009. Sem Paginação. Disponível em: https://search.wikileaks.org/plusd/cables/09BRASILIA34_a.html. Acesso em 05 maio 2019.

SOBEL, Clifford. **CONSTRAINING IRANIAN INFLUENCE IN BRAZIL**. Brasília, 2008a. Sem Paginação. Disponível em: https://search.wikileaks.org/plusd/cables/08BRASILIA896_a.html. Acesso em: 04 maio 2019.

SOBEL, Clifford. **THE FX2 COMPETITION – THE GLIDEPATH TO SUCCESS**. Brasília, 2009a. Sem Paginação. Disponível em: https://search.wikileaks.org/plusd/cables/09BRASILIA41_a.html Acesso em: 04 maio 2019.

SOBEL, Clifford. **THOUGHTS ON THE VISIT OF DEFENSE MINISTER JOBIM TO WASHINGTON**. Brasília, 2008b. Disponível em: https://search.wikileaks.org/plusd/cables/08BRASILIA429_a.html. Acesso em: 04 maio 2019.

SOARES, Adalgisa Bozi. Separatismo na Geórgia: considerações geopolíticas e etnicidades. **Meridiano** 47, v. 9, n. 93. 2008, p. 31-33.

SKIDMORE, David. Security: A New Framework for Analysis. By Barry Buzan, Ole Weaver, and Jaap de Wilde. Boulder, CO: Lynne Rienner, 1998. 239p. \$55.00 cloth, \$19.95 paper. **American Political Science Review**, v. 93, n. 04, p. 1010-1011, 1999.

TAKAHASHI, Tadao (org). **Sociedade da Informação no Brasil**: Livro Verde. Brasília: Ministério da Ciência e Tecnologia, 2000. Disponível em: www.governodigital.gov.br/documentos-e-arquivos/livroverde.pdf. Acesso em: 18 maio 2018.

TALLEY, Ian; VOLZ, Dustin. U.S. **Targets North Korean Hacking as National-Security Threat**. Msn.com, The Wall Street Journal, 2019. Sem Paginação. Disponível em: <https://www.msn.com/en-us/news/world/us-targets-north-korean-hacking-as-national-security-threat/ar-AAHkAGU?ocid=iemptp>. Acesso em 25 maio 2019.

TANNO, Grace. A Contribuição da Escola de Copenhague aos Estudos de Segurança Internacional. **Contexto Internacional**, v. 25, n. 01, p. 47-80, 2003. Disponível em: <http://www.scielo.br/pdf/cint/v25n1/v25n1a02.pdf>. Acesso em 22 jan. 2020.

THE GUARDIAN. **Russia accused of unleashing cyberwar to disable Estonia**. The Guardian, World, Europe. 2007. Sem Paginação. Disponível em: <https://www.theguardian.com/world/2007/may/17/topstories3.russia>. Acesso em: 16 ago. 2019.

UN NEWS. **In Wake of ‘WannaCry’ attacks, UN cybersecurity expert discusses Internet safety**. News.un.org, 2017. Sem Paginação. Disponível em: <https://news.un.org/en/story/2017/05/557712-wake-wannacry-attacks-un-cybersecurity-expert-discusses-internet-safety>. Acesso em: 11 jul. 2020.

VILLA, Rafael Duarte; REIS, Rosana Rocha. A Segurança Internacional no pós-Guerra: Um balanço da Teoria Tradicional e das Novas Agendas de Pesquisa. **BIB**, n. 62, p. 19-51, São Paulo: 2006. Disponível em: <http://www.anpocs.com/index.php/edicoes-antiores/bib-62/588-a-seguranca-internacional-no-pos-guerra-fria-um-balanco-da-teoria-tradicional-e-das-novas-agendas-de-pesquisa/file>. Acesso em: 23 jan. 2020.

WÆVER, Ole; BUZAN, Barry; KELSTRUP, Morten; LEMAITRE, Pierre. **Identity, Migration and the New Security Agenda in Europe**. London: Pinter, 1993.
WILLIAMS, Paul D. (Ed.). **Security Studies: An Introduction**. Oxon: Routledge, 2008.

WEBER, Max. **Ensaio de Sociologia**. Trad. Waltenesir Dutra. 5ª ed. LTC Editora: Rio de Janeiro, 1982.

WIKILEAKS. **What is WikiLeaks**. WikiLeaks.org, 2015. Sem paginação. Disponível em: <https://wikileaks.org/What-is-WikiLeaks.html>. Acesso em: 03 maio 2020.

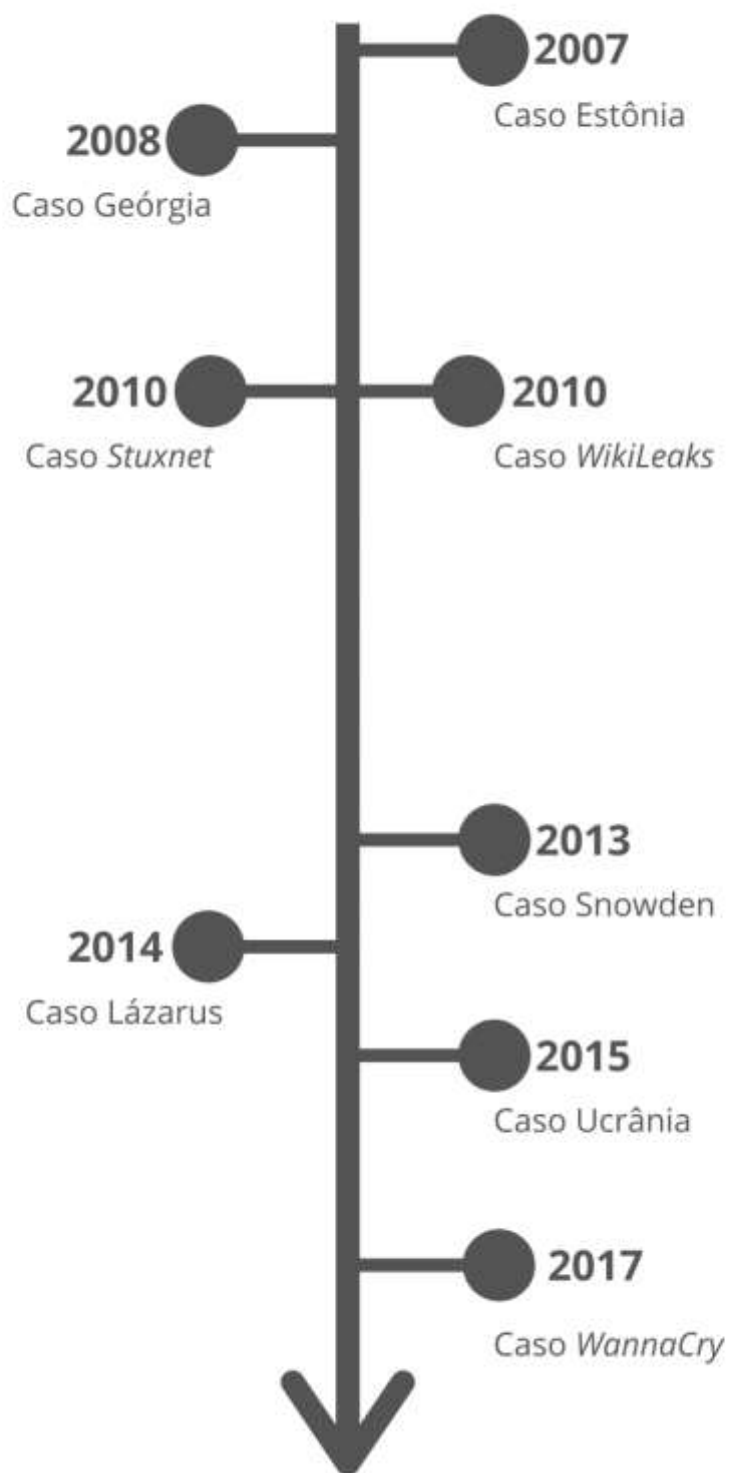
WILLIAMS, Paul D. (Ed.). **Security Studies: An Introduction**. Oxon: Routledge,

XAVIER, João Ricardo G. Z. A política externa da Rússia: O Referendo da Criméia e os efeitos na região do Nagorno-Karabakh. **Conjuntura Global**, v. 04, n. 03, 2015.

Disponível em: <https://revistas.ufpr.br/conjglobal/article/download/45302/27542>. Acesso em: 30 maio 2020.

ZETTER, Kim. **Contagem regressiva até Zero Day: Stuxnet e o lançamento da primeira arma digital do mundo**. Rio de Janeiro: Brasport, 2017. 417 p.

APÊNDICE A – Linha do Tempo da Contextualização Internacional



APÊNDICE B - Linha do Tempo do Processo de Segurança Cibernética do Brasil

