UNIVERSIDADE FEDERAL DA INTEGRAÇÃO
LATINO-AMERICANA (UNILA)
INSTITUTO LATINO-AMERICANO DE
ECONOMIA, SOCIEDADE E POLÍTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM
RELAÇÕES INTERNACIONAIS (PPGRI)

SEGURANÇA CIBERNÉTICA NO BRASIL: UMA ANÁLISE DOS FATORES INSTITUCIONAIS QUE PRECEDEM A POLÍTICA DE SEGURANÇA CIBERNÉTICA ENTRE 2008 – 2020

Luiz Gustavo Lavandoski da Silva

Foz do Iguaçu

2024

Luiz Gustavo Lavandoski da Silva

SEGURANÇA CIBERNÉTICA NO BRASIL: UMA ANÁLISE DOS FATORES INSTITUCIONAIS QUE PRECEDEM A POLÍTICA DE SEGURANÇA CIBERNÉTICA ENTRE 2008 – 2020

Defesa apresentada no âmbito do Programa de Pós-Graduação em Relações Internacionais (PPGRI) do Instituto Latino-Americano de Economia, Sociedade e Política (ILAESP) da Universidade Federal da Integração Latino-Americana (UNILA) como requisito para a obtenção do título de Mestre em Relações Internacionais.

Área de Concentração: Segurança Internacional

Orientador: Prof. Dr. Mamadou Alpha Diallo.

Foz do Iguaçu

2024

Luiz Gustavo Lavandoski da Silva

SEGURANÇA CIBERNÉTICA NO BRASIL: UMA ANÁLISE DOS FATORES INSTITUCIONAIS QUE PRECEDEM A POLÍTICA DE SEGURANÇA CIBERNÉTICA ENTRE 2008 – 2020

Defesa apresentada no âmbito do Programa de Pós-Graduação em Relações Internacionais (PPGRI) do Instituto Latino-Americano de Economia, Sociedade e Política (ILAESP) da Universidade Federal da Integração Latino-Americana (UNILA) como requisito para a obtenção do título de Mestre em Relações Internacionais.

Área de Concentração: Segurança Internacional

COMISSÃO EXAMINADORA

_____

Prof. Dr. Mamadou Alpha Diallo

ILAESP - UNILA

Orientador

_____

Professor Dr. Lucas Ribeiro Mesquita

ILAESP – UNILA

_____

Professor Dr. Ramon Blanco de Freitas

ILAESP - UNILA

AGRADECIMENTOS

Aos meus familiares por todo o apoio e suporte dado neste período acadêmico. A minha mãe Jane, meu irmão Masakazu e minha avó Zelide: obrigado por valorizarem e apoiar minha educação, mesmo que nem sempre merecendo. Sou grato por toda a paciência, amor e investimento que vocês me propuseram nos momentos fáceis e, principalmente nos difíceis. Ao meu tio Isaias, que infelizmente não sobreviveu ao Covid, mas que me incentivou a buscar novos caminhos.

A minha segunda família, ao qual inclui minha namorada Gabriella, seus pais, primos e tios, que me acolheram sem pensar duas vezes e ajudaram em tudo que precisava, as vezes até o que não precisava.

Aos meus grandes amigos, Juliana Cardoso, Brenda Moreira, Patrícia Camargo, Andriele Aparecida e Gabriella Leandro, que ao longo dessa trajetória me aguentaram e ajudaram, sendo com críticas em relação ao trabalho ou encontros para fofocar, sorrir e chorar. Levarei vocês para sempre comigo. Em especial ao meu “time de suporte emocional e técnico”, Jhennyfer Rayssa e Eduardo Izycki, vocês me ajudaram de uma forma que eu não tenho nem palavras para agradecer. Aos meus eternos professores, Mayane Bento e Mario Amim (você realmente tinha razão quando falava que o ciberespaço seria a problemática do século XXI).

Ao meu orientador, professor Mamadou Alpha Diallo, por persistir na busca da qualidade do trabalho desde 2020. Agradeço por acreditar no meu potencial e pelo suporte no programa.

A Universidade Federal da Integração Latino-Americana (UNILA), por me ajudar com o financiamento e apoio relacionado a inscrições em cursos e eventos e pelo incentivo em educação e pesquisa.

Aos professores membros do Programa de Pós-graduação em Relações Internacionais, por dedicação e apoio para formação acadêmica.

Por fim, ressalto o agradecimento ao nosso Sistema Único de Saúde, por ter sido fundamental quando precisei de ajuda nesta pandemia.

“O DESENVOLVIMENTO CIENTÍFICO & TECNOLÓGICO ESTÁ INTIMAMENTE LIGADO À PROSPERIDADE DE UM PAÍS”

- ALMIRANTE ÁLVARO ALBERTO

RESUMO

Esta dissertação tem como objetivo discutir quais fatores no âmbito institucional do Estado brasileiro limitam a consolidação da política nacional de segurança cibernética. Como marco teórico, elegem-se os Estudos de Segurança Internacional e pesquisadores que compreendem a segurança cibernética não somente como um fenômeno conceitual do século XXI, mas como uma ferramenta necessária e crítica ao se entender o poder dos Estados na área. Dessa forma, o trabalho está dividido em três capítulos além da introdução. Na introdução, apresenta-se a problemática e o tema, tratando da relevância atualmente e definições importantes para contextualizar o assunto. No segundo, traz-se a revisão teórica, onde se apresenta o contexto histórico-teórico na qual se é inserida a questão da evolução dos Estudos de Segurança Internacional, como a ideia dos complexos de segurança frente ao caso do ciberespaço, com autores que são referência das Relações Internacionais, como Buzan e Waever. Assim como apresentar o contexto que envolve os estudos de segurança cibernética como subcampo da Segurança Internacional. No terceiro capítulo, trata-se da segurança voltada para o Brasil, onde se analisa o processo de criação, desenvolvimento e melhorias das políticas de segurança cibernética. E em quarto se tem a descrição da importância desse processo para o desenvolvimento e crescimento do País. Para fazer a análise deste trabalho, seguiu-se a abordagem qualitativa com o uso do método hipotético-dedutivo, onde o falseamento das hipóteses será feito através de revisão literária e documental para identificar, descrever e concluir o problema. Dessa forma, como resultado, é abordada a ideia de que existem fatores que limitam a consolidação da PNSC e apresentados quais são eles.

PALAVRAS-CHAVE: Segurança Cibernética; Relações Internacionais; CiberRI; Brasil; Política Nacional De Segurança Cibernética.

ABSTRACT

This dissertation aims to discuss which factors within the institutional scope of the State limit the consolidation of the national cyber security policy. As a theoretical framework, International Security Studies and researchers are chosen who understand cybersecurity not only as a conceptual phenomenon of the 21st century but as a necessary and critical tool when understanding the power of States in the area. Thus, the work is divided into three chapters in addition to the introduction. In the introduction, the problem and the theme are presented, dealing with the relevance in the present day and important definitions to contextualize the subject. In the second, a theoretical review is presented, where the historical-theoretical context is presented, in which the issue of the evolution of International Security Studies is inserted, such as the idea of security complexes in the face of the case of cyberspace, with authors who are reference in International Relations, such as Buzan and Waever. As well as presenting the context that involves cybersecurity studies as a subfield of International Security. The third point deals with security focused on Brazil, where the process of creation, development, and improvement of cybersecurity policies is analyzed. And fourth, there is a description of the importance of this process for the development and growth of the country. To make the analysis of this work, followed the qualitative approach with the use of the hypothetical-deductive method, where the falsification of the hypotheses will be done through literary and documentary review to identify, describe and conclude the problem. Thus, as a result, the idea that there are factors that limit the consolidation of the PNSC is addressed and what they are is presented.

KEYWORDS: Cyber Security; International relations; CyberRI; Brazil; National Cyber Security Policy.

LISTA DE FIGURAS E TABELAS

LISTA DE SIGLAS

ABIN	Agência Brasileira de Inteligência
ANATEL	Agência Nacional de Telecomunicações
ANPD	Agência Nacional de Proteção de Dados
CGIPR	Conselho Gestor da informação da Presidência da República
COMDCIBER	Comando de Defesa Cibernética
CRS	Complexo Regional de Segurança
DSIC	Departamento de Segurança da Informação
DPF	Departamento de Polícia Federal
EB	Exército Brasileiro
END	Estratégia Nacional de Defesa
ENSC	Estratégia Nacional de Segurança Cibernética
ESI	Estudos de Segurança Internacional
EUA	Estados Unidos da América
FA	Forças Armadas
GSI	Gabinete de Segurança Institucional
LBSN	Livro Branco de Segurança Nacional
LGPD	Lei Geral de Proteção de Dados
LVSC	Livro Verde de Segurança Cibernética
MD	Ministério da Defesa
MENA	Middle East and North Africa
OTAN	Organização do Tratado do Atlântico Norte
OI's	Organizações Internacionais
PND	Política Nacional de Defesa
PNSC	Política Nacional De Segurança Cibernética
RI	Relações Internacionais
SI	Sistema Internacional
SOCS	Centros De Operações De Segurança Avançados

Sumário

INTRODUÇÃO

A segurança cibernética é um fenômeno resultante da evolução tecnológica que norteia a Segurança Internacional. Desde o final da década de 1980, esse fenômeno passou a fazer parte da globalização. Para compreender o que entendemos por globalização, o autor deste trabalho buscou três definições com relevância no contexto teórico das Relações Internacionais (RI).

Na primeira definição, Nye (1998) afirma que a globalização é o resultado do desenvolvimento e investimento de novos atores – entendidos como OI's, empresas multinacionais, ONG's e outras entidades - em meios de crescimento no Sistema Internacional. Dessa forma a cooperação entre estes mantém funcionalidade e pacificidade que garantem relações entre Estados e atores não estatais, tais como a capacidade de manutenção da paz nas relações impactando no desenvolvimento. Por outro ponto de vista, Lévy (1999), fala que a globalização é um avanço possibilitado pela evolução da tecnologia ruminada pela sociedade. Este avanço social acontece mais rápido do que a evolução de meios e ferramentas de desenvolvimento do Estado, possibilitando um ambiente informacional que "encurta" distâncias e cria novas dimensões, como a internet.

Para Buzan (1998), a globalização é o resultado do investimento no desenvolvimento de formas de poder para os Estados. Esse poder causa a evolução de ferramentas que geram corridas no Sistema Internacional, sejam elas tecnológicas, financeiras ou armamentistas. Ambas as descrições realçam a ideia de que a globalização e a segurança cibernética possuem como principal elo a evolução do desenvolvimento das tecnologias. Ou seja, é um processo que gera uma interconectividade e interdependência através do avanço tecnológico e que influencia no âmbito social, econômico, político e cultural.

Com o ápice da evolução tecnológica marcando a atualidade, o uso dos meios informacionais – como internet, GPS (Sistema de Posicionamento Global), smartphones e computadores - se tornou essencial no cotidiano dos indivíduos, sociedades e Estados (IZYCKI 2021, 11). Esse tema ganhou grande relevância a partir da Guerra Fria por conta da competição econômico-tecnológica-militar que fez com que as grandes potências buscassem uma inovação para os setores militares, tendo como grandes exemplos a corrida aeroespacial e a tecnologia de espionagem

e bélica (LOBATO e KENKEL 2015, 636).

Ainda no período da Guerra Fria, as Relações Internacionais passavam por longos debates[1] que tratavam da perspectiva positivista de pensar no Estado como o único ator de importância para o sistema. Com isso muitos estudiosos, como Keohane, Waltz e Morgenthau tinham como concepção na agenda de Segurança Internacional[2] pensamentos de diferentes matrizes teóricas, mas que concordavam com a ideia do Estado protegendo valores fundamentais. Lippmmann (1944) *apud* Bueno (2019), falava que o conceito de segurança era "uma capacidade de um Estado proteger os seus valores fundamentais".

Esta afirmação pode ser simplificada na ideia de que segurança é uma ferramenta para proteger e influenciar a soberania de um Estado. Baldwin (1997) apud Bueno (2019), dizia que "para garantir a segurança de um Estado, é necessário, às vezes, sacrificar valores internos, onde se incluem valores marginais e valores primos". O valor marginal é a segurança pelos meios políticos, com a solução de um problema por meio de alocação de recursos. Os valores primos (primordiais), seriam a garantia de determinar o resultado pela lógica, nesse caso a segurança é um meio para se desfrutar prosperidade e liberdade.[3]

No fim da década de 1980, esses pensamentos sobre as perspectivas tradicionalistas de segurança[4] geraram a dúvida de que o Estado podia não ser o principal ator do sistema, ou melhor, o sistema poderia nem ser formado por atores e sim por agentes. De acordo com Seitenfus (2004), os atores são aqueles que influenciam e manifestam o que acontece no Sistema Internacional. Eles controlam e moldam as práticas a partir da sua capacidade de poder, que como define Nye (1998), é a habilidade ou potencial de uma instituição - como um Estado, organização ou o indivíduo - para desempenhar influência, controle ou até mesmo autoridade sobre situações, recursos e/ou outros agentes diferentes contextos. Já Buzan (2012) descreve que os agentes são parte

[1] Os grandes debates das Relações Internacionais, foram expressões da evolução do pensamento de poder no sistema internacional que alavancaram os paradigmas expandindo a linha teórica. Para ler mais, ver Sarfati – Teoria das Relações Internacionais, 2005 p.304.

[2] Termo utilizado pela academia de Relações Internacionais para discutir assuntos que podem gerar conflito na governabilidade regional, local e global.

[3] Ler mais em BALDWIN, David A. The concept of security. Review of International Studies (1997), p. 21 – 24.

[4] Seriam as vertentes teóricas que buscavam explicar a guerra partindo de analises racionais, ligadas as tradições que envolviam o pensamento de hostilidade e Estado. Ver mais em Buzan; Hansen, A evolução dos Estudos de Segurança Internacional, 2012.

dessa relação internacional, o que faz com que cada organização, Estado e indivíduo tenha uma importância diferencial. Parte-se da ideia de que eles não seguem um roteiro, e sua próxima ação pode até mesmo desencadear um conflito ou caos no sistema.

Pensando que o SI é formado por agentes, a Segurança Internacional incorporou além dos Estados, as Organizações Internacionais (OI's) – como a Organização das Nações Unidas e o Fundo Monetário Internacional, por exemplo - e o indivíduo – que seria a representação das pessoas individualmente e através da sociedade - (ADLER 2006).

Esta nova perspectiva, tinha como um dos pontos principais para análise de evolução do sistema internacional, a concepção de problemas que iam além do pensamento clássico de segurança, que envolvia poder, guerra e Estado (ADLER 2006, ABREU 2011, LAVANDOSKI DA SILVA 2018) e que refletiam agora em problemas modernos (como por exemplo a fome e desastres naturais) colocando o indivíduo para ser um dos agentes desse sistema, através da importância da sua atuação em grandes eventos. Buzan (2012) explica que o modo de pensar em segurança se transformou, com a introdução das questões ambientais, pandêmicas e sociais, assim como o espaço nuclear, espacial e o cibernético.

Assim, Lavandoski (2018) e Izycki (2021) apontam que a criação de novos espaços de domínio para os Estados fez com que se gerassem novas perspectivas para o ciberespaço. Todavia esse desafio nasce bem antes da criação e aperfeiçoamento da internet no século XX. Ayres (2017) aponta que com o aperfeiçoamento do uso operacional de ferramentas que fazem parte do espectro eletromagnético, podem ter sido o primeiro 'degrau' para esta realidade, assim como o aperfeiçoamento do GPS, telégrafos e telefones, talvez podendo ser considerado então o início de uma terceira revolução industrial.

Neste trabalho, o autor classifica dois tipos de perspectivas. A) As capacidades técnicas de um agente (Estado, organização e indivíduo), definidas como ferramentas básicas de uso social, que agregam para crimes cibernéticos, *cyberbullying*, invasão de privacidade, fraudes, *fake-news* e golpes. B) As capacidades ofensivas e defensivas. A segunda perspectiva engloba esta ideia de exercício de poder por irem além do uso de *softwares* e *malwares*, para engajar-se

em espionagem, crises e conflitos com ataques cinéticos (IZYCKI e BRANDÃO 2019). Assim, de acordo com Al-Mashat (1985), o conceito de capacidades de segurança é explicado como ações voltadas para conduzir ou assegurar um objetivo através da compreensão das ferramentas que garantem a segurança do Estado. Na perspectiva de Buzan (1998), o conceito de capacidade de segurança refere-se à habilidade de um agente de garantir sua própria segurança e promover seus interesses de maneira eficaz, pensa-se que a segurança é algo que existe além da básica ideia do pensar militar e inclui várias dimensões, como segurança política, econômica, societal e ambiental. A capacidade de segurança abrange, assim, a habilidade de um agente lidar com ameaças e desafios em todas essas áreas.

As duas perspectivas de capacidades, possuem algo em comum, elas podem ser utilizadas pelo Estado, organizações e pelo indivíduo. Além de, se alguma destas ações forem feitas 'corretamente', podem ser disfarçados ou contestados, expandindo a ideia criada no 11 de setembro, de que existe um inimigo sem rosto e digitais, mas que agora tem um novo ambiente de ações, que seria o espaço cibernético (CLARKE e KNAKE 2010).

Mas como surgiu esse novo ambiente? Bem, historicamente o termo "*cyberspace*" passa a ser utilizado pela primeira vez na obra de William Gibson, na década de 1980, no livro *Neuromancer*, onde o autor instiga que o ciberespaço era algo que ia além do corpo humano e que seria um ambiente cujos dados não poderiam ser quantificados ou controlados (GIBSON 1984, 53).

> "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. Uma complexidade impensável. Linhas de luz alinhadas no não espaço da mente, aglomerados e constelações de dados. Como luzes da cidade, se afastando... (GIBSON 1984, 53)"

Embora o ciberespaço tenha sido impulsionado nos debates das Relações Internacionais nas últimas duas décadas do século XX (GRAY 1997)[5] foi somente no final da primeira década do século XXI que o Brasil, de fato adotou o ciberespaço, por conta da relevância estratégica e devido ao significante crescimento nas tecnologias e conectividades. Além disso, neste mesmo período, o Brasil passou a considerar as

[5] Gray instiga em seus trabalhos que a tecnociência é uma ferramenta baseada no princípio organizacional das novas eras do conflito moderno.

questões nucleares e aeroespaciais como demandas que necessitavam de um olhar mais crítico do Estado (BRASIL 2008).

Sendo assim, o país passou a criar planos para o desenvolvimento destes novos espaços de domínio (BRASIL 2008). Primeiro, a criação da Estratégia Nacional de Defesa (END) (BRASIL 2020) e a Política Nacional de Defesa (PND) (BRASIL 2018), onde o Brasil entrou no conjunto de Estados que estavam dispostos a gerar desenvolvimento em uma área que era nova e arriscada, devido o investimento e ações de outros países na área (IZYCKI e BRANDÃO 2019). Dessa forma, vista como espaço de domínio tal qual a terra, o ar e as águas, o Governo brasileiro optou por divisão de controle, pesquisa e defesa, dando origem a uma Política Nacional De Segurança Cibernética a partir da estratégia nacional de segurança cibernética.

Nesta estratégia, entendida como uma forma de orientação de operações e atividades relacionada à defesa nacional, as forças armadas (BRASIL 2008) ganharam novas atribuições baseadas no cenário de conflitos e guerras e outras instituições governamentais (como as polícias, a agência de inteligência e empresas públicas de desenvolvimento) ficaram com a responsabilidade principal pelo controle nacional do ciberespaço.

Em suma, o Exército Brasileiro (EB) trabalha as capacidades ofensivas e defensivas do espaço cibernético. Já as capacidades técnicas envolvendo questões legislativas e normativas, a agenda de prioridade é de órgãos ligados diretamente aos três poderes (executivo, legislativo e judiciário), como por exemplo o Conselho Gestor de Informações (CGI) e a Agência Nacional de Telecomunicações (ANATEL 2021).

Neste panorama, este trabalho busca responder a seguinte questão: quais fatores institucionais limitam a consolidação da Política Nacional de Segurança Cibernética?

A fim de responder à pergunta de pesquisa, aponta-se como objetivo geral: Identificar fatores institucionais que limitam a efetividade da Política Nacional de Segurança Cibernética.

Destaca-se como objetivos específicos:

1. Descrever os aspectos institucionais envolvidos na criação da Política Nacional de Segurança Cibernética no Brasil, abordando seu histórico e os obstáculos enfrentados.

2. Identificar a estrutura e a divisão institucional entre os órgãos que participam da segurança cibernética no Brasil.

3 Analisar os problemas que afetam a interação entre os agentes nacionais no âmbito da segurança cibernética, incluindo a questão dos investimentos.

Para chegar na resposta do trabalho, pensou-se em três possíveis hipóteses:

H1 – A falta de coordenação e interação entre os agentes nacionais impede o desenvolvimento de um processo político coeso e eficaz para a implementação da Política Nacional de Segurança Cibernética

H2 – Os investimentos em segurança cibernética no Brasil são insuficientes quando comparados a outros setores estratégicos, prejudicando a consolidação da política.

H3 – Há uma limitação na integração entre governo e sociedade civil no desenvolvimento de políticas voltadas para a segurança cibernética, dificultando a criação de uma estratégia abrangente e eficaz.

1.1 – Procedimentos Metodológicos

O presente trabalho trata como temática principal um estudo a respeito da segurança cibernética, com base na busca dos fatores que limitam a consolidação da política de segurança cibernética no Brasil. Mais objetivamente, este trabalho consiste na proposta de analisar as dificuldades institucionais que causam essa demora na viabilização de uma política tão necessária e esperada para a segurança cibernética em âmbito nacional.

Para alcançar os objetivos propostos, será utilizado o Método Hipotético-Dedutivo (MHD) com uma abordagem descritiva. O MHD é um método de investigação científica que parte da formulação de hipóteses, as quais são testadas através da observação e análise de dados para verificar sua validade. Neste caso, as hipóteses serão exploradas e descritas com base em uma análise detalhada dos

fatores institucionais, considerando o contexto específico da segurança cibernética no Brasil. A abordagem descritiva permitirá compreender e documentar como esses fatores influenciam a consolidação da política, oferecendo uma visão clara dos obstáculos institucionais enfrentados.

Dessa forma, ao utilizar o MHD, o falseamento das hipóteses será realizado através da análise descritiva e comparativa dos dados coletados com as previsões pensadas pelas hipóteses formuladas. Inicialmente, as hipóteses foram criadas a partir da observação preliminar sobre o assunto e reformuladas de forma que possam ser testadas de maneira objetiva. Ao longo do texto, as hipóteses serão apresentadas pela contextualização da temática dentro da estrutura teórica da pesquisa.

A pesquisa será caracterizada como uma pesquisa qualitativa, com foco na análise de fontes secundárias, incluindo artigos acadêmicos, livros, políticas públicas, relatórios oficiais, e manuais de doutrinas. Essa combinação de métodos permitirá não apenas testar as hipóteses formuladas, mas também fornecer uma descrição rica e contextualizada do cenário institucional brasileiro em relação à questão proposta da política de segurança cibernética nacional.

Este trabalho busca contribuir para o campo da segurança cibernética e para os estudos sobre políticas públicas na área. Ao identificar e descrever os fatores institucionais que limitam a efetividade da política nacional de segurança cibernética, este trabalho incrementa a base acadêmica para o desenvolvimento de estratégias que possam ajudar a controlar e mitigar os obstáculos existentes. Além disso, as análises das interações institucionais fornecem compreensões que podem ser utilizados em futuras pesquisas, não só no contexto da segurança cibernética, mas também no que tange os estudos de cooperação interinstitucional. A abordagem metodológica adotada também pode servir de referência para outros estudos que busquem explorar e descrever fenômenos em contextos institucionais específicos.

Ao longo do desenvolvimento desta pesquisa, houve dificuldades que marcaram a implementação, dentre eles o de maior gravidade foi a pandemia, que além de ser a maior fonte de vontade de desistência acabou nos abalando pelas perdas pessoais.

Este trabalho é composto por 4 capítulos. O Capítulo um (1) corresponde à introdução, onde são apresentados o contexto, os objetivos da pesquisa e a justificativa. No Capítulo dois (2), abordaremos o desenvolvimento teórico utilizado para discutir segurança cibernética no Brasil e sua perspectiva como ponto de poder no Sistema Internacional.

A estratégia nacional de segurança cibernética e a política nacional de segurança cibernética são discutidas no capítulo três (3), mediante a análise entre a estrutura de gerenciamento da segurança cibernética no Brasil e a ideia das capacidades de segurança.

No capítulo quatro (4), traz-se a análise contextualizada das características que afetam a interação entre os agentes que fomentam a segurança cibernética no Brasil. Por fim, estão dispostas as considerações finais.

CAPÍTULO 2 - A EMERGÊNCIA DO DEBATE DOS ESI FRENTE A INSERÇÃO DA SEGURANÇA CIBERNÉTICA NA AGENDA INTERNACIONAL

O presente capítulo aborda o conceito da evolução dos Estudos de Segurança Internacional (ESI), na perspectiva do desenvolvimento cibernético frente à Segurança Internacional. Assim, será feita uma descrição teórica para sustentar a linha de pensamento aplicada para a análise do trabalho.

Este capítulo, está organizado em três pontos. O primeiro apresenta a evolução da segurança internacional, abordando as mudanças frente ao pensamento da segurança**,** principalmente no que trata da discussão de segurança regional e capacidades de segurança e defesa. A importância desta teoria ao se falar de segurança cibernética no Brasil fundamenta-se no argumento de Costa (2020) que destaca o potencial do país nesse campo, ao mesmo tempo em que ressalta sua tendência à autossabota[6] no âmbito do poder global.

No segundo, trazemos a ideia da aplicação das Relações Internacionais Cibernéticas como uma das áreas chaves para entender o Sistema Internacional e como isso impacta na formação dos estudos de segurança para a área. E em terceiro, a discussão mais apropriada de como a segurança cibernética se tornou peça fundamental para entender o poder atualmente.

2.1 - Perspectivas na Segurança Internacional Moderna

Quando abordamos a segurança internacional, a primeira consideração que deve ser feita é: qual é o meio que conduz à transformação das perspectivas sobre o que entendemos por segurança internacional ao longo do tempo? Nesse contexto, a globalização surge como uma das principais características do desenvolvimento do mundo em relação às questões de segurança contemporâneas (BUZAN, B., WAEVER, O., & WILDE, J. D 1998).

Referindo-se à segurança internacional, outras características que devem ser consideradas são aquelas relacionadas à representação de uma ameaça existencial

[6] Cita-se as barreiras internas, tais como a insuficiência de investimentos, políticas inconsistentes ou desafios estruturais, que atuam como impedimentos para que o Brasil atinja plenamente seu potencial no contexto global de segurança cibernética.

dirigida a um objeto que emerge no poder dentro da estrutura do sistema. Griffiths (2007), exemplifica que indivíduos, sociedade e Estados, constam nessa perspectiva, uma vez que qualquer assunto que ponha em risco algum desses três objetos, pode ser uma representação de ameaça à segurança.

Na virada das décadas de 1980 e 1990, a narrativa em foco não era apenas a preocupação convencional com a segurança voltada para os conflitos armados e ameaças militares. Em vez disso, expandia-se para uma perspectiva mais abrangente, como desafios mais amplos relacionados ao desenvolvimento humano, como a fome e o meio ambiente, por exemplo. Em 1990, um marco significativo foi a reunião dos representantes de Estados em Nova York, organizada pelas Nações Unidas (ALVES 2018, 46), com o propósito de discutir o futuro do planeta, concentrando-se em desafios globais relacionados ao desenvolvimento humano, meio ambiente, segurança e direitos das mulheres, entre outros. Esse diálogo impulsionou uma liberdade dos Estados para se reunirem e debaterem sobre uma variedade de questões securitárias. (ALVES 2018).

Com isso, os Estudos de Segurança Internacional se tornaram preceitos conhecidos antes mesmo de serem popularizados como uma subárea de estudos nas Relações Internacionais (BUZAN e HANSEN 2012, 70). Inicialmente concebidos como análises estratégicas, concentravam-se na avaliação do poder e conflitos entre Estados, fundamentados nas discussões positivistas do século XX (ibdem; p. 73).

Assim, durante os grandes debates que foram palco para as discussões conservadoras envolvendo realistas e liberais, durante 1940 a 1990, diante de novas perspectivas teóricas das Relações Internacionais, com a ideia de que o mundo estava vivenciando os efeitos da globalização e, portanto, novas ideias sustentariam ou fariam parte do processo evolutivo do mundo. As novas teorias (construtivismo, pós-estruturalismo e estudos pós-coloniais e de coloniais) trouxeram à tona que as concepções de segurança iam além de Estado e de guerra e até mesmo armas nucleares (ABREU 2011).

Com essas novas teorias tonteando o SI, o Parlamento Dinamarquês em 1998, buscou inovar os estudos da paz dando criação a uma escola que a partir de

então ficaria conhecida pelos seus estudos tanto na questão da busca para a paz quanto nos estudos da segurança internacional, como a Escola de Copenhague (BUZAN, B., WAEVER, O., & WILDE, J. D 1998).

A Escola de Copenhague, como unidade política do Estado, passou a ter presença na academia visando o incentivo nessas discussões e, além disso, aderindo a novos pensamentos que pudessem construir novas práxis de segurança internacional, tal qual: os pensamentos feministas, a inserção de diálogos que envolvessem outros continentes – como a América Latina, Africa, Asia e Oriente Médio - e a inserção da problemática sobre a questão das novas dimensões de conflito (BUZAN e HANSEN 2012).

Isso se torna interessante ao examinarmos as teorias de Relações Internacionais, pois parte-se da ideia de que a realidade muitas vezes não se alinha com as expectativas teóricas (ibidem; p.64). Logo, essa 'disparidade' entre teoria e prática é influenciada por fatores como mudanças globais e ações imprevisíveis que podem ser desencadeadas pela atuação do Estado, de indivíduos e até mesmo pelo meio ambiente.

Compreender esse funcionamento demanda uma análise aprofundada, especialmente considerando o processo de evolução histórico-teórico. As teorias, embora proporcionem diversas perspectivas, não conseguem capturar totalmente a complexidade das interações dos agentes internacionais. Isso ressalta a importância de uma abordagem crítica e flexível na busca de avaliar e questionar diferentes perspectivas. Explicar esse tipo de problemática requer uma compreensão do processo de evolução histórico-teórico, tratado neste capítulo, para se aprofundar na questão, uma vez que podemos tirar inúmeros resultados ou formas de entender o mundo a partir das teorias (GRIFFITHS 2007), como por exemplo a Guerra Fria a partir do realismo, os movimentos civis sociais pelo construtivismo ou até mesmo a dependência econômica Latino-Americana pelo Marxismo.

É nesse contexto que se tem o desenvolvimento da abordagem que trata dos Complexos Regionais de Segurança (CRS), que faz parte da evolução dos estudos de segurança internacional no que tange o mundo além do norte global. Segundo Wæver (2003), a proposta é entender que os problemas que envolvem regiões diferentes tendem a ser traçados diferentemente. A teoria aponta que o sistema

carece de uma interpretação de polaridade – distribuição de poder no Sistema Internacional - após a guerra fria, isso porque a diferença nos aspectos de segurança serve como análise para a distinção no que tange o nível de interação dos Estados. A teoria em si possui traços do realismo ofensivo – como relação de poder, anarquia internacional e a natureza de conflito e competição -, uma vez que analisa o poder relativo do Estado e sua sobrevivência. Entretanto sua criação foi o contexto para mudar a forma que se compreendia a dinâmica de cooperação e desenvolvimento de países do terceiro mundo.

A importância desse viés teórico está na abertura para se estudarem novas estruturas de segurança em locais onde a política de segurança de um Estado acaba dependendo do seu vizinho[7]. Logo, esta teoria explica que um conjunto de unidades cujo principais processos de securitização[8], des-securitização[9] ou ambos, são tão interligados que faz com que seus problemas de segurança não possam ser moderadamente analisados ou resolvidos se os Estados não trabalharem juntos (BUZAN e WÆVER 2003).

Entende-se que existem três níveis de pensar em segurança: o nível global, onde a agenda de segurança internacional se desenvolve em relação a problemas que envolvem potências com grande poder, seja ele econômico, militar ou político; e o nível regional, que abrange Estados com capacidades consideráveis, mas que atuam predominantemente em esferas regionais. Por fim, o nível doméstico (nacional), onde a prioridade é a segurança individual do Estado, frente a proteção contra ameaças internas e externas sobre soberania, estabilidade política, economia e outros aspectos individuais (ibidem; p.13).

Dessa forma, ao calcular a ideia de poder no que o autor chama de 'nível superior', esses Estados inseridos no nível regional podem não exercer uma influência direta em processos em escala global. No entanto, isso não os exclui de serem considerados como riscos ou rivais em nível global, evidenciando a complexidade das

[7] Buzan e Waever explicam em *Regions and Powers*, 2003, que conflitos internos ou ameaças externas em uma região pode afetar na tomada de decisões da dinâmica regional, gerando inclusive rivalidades. Um exemplo clássico talvez seja a o envolvimento da Rússia no conflito na Síria, desencadeando tenções com refugiados em países como Turquia e Líbano.
[8] Processo onde um agente identifica uma questão como ameaça à sua segurança.
[9] Processo oposto, onde uma questão tratada como ameaça é normalizada através de atividades políticas.

Relações Internacionais, onde Estados regionais podem desempenhar papéis cruciais na estabilidade global, mesmo que sua influência primária seja regional. Além disso, a avaliação de riscos e rivalidades pode abranger uma variedade de fatores, transcendendo o âmbito militar e incorporando elementos como dimensões econômicas, políticas e culturais, entre outros (BUZAN e WÆVER 2003).

Por conta disto, quando se trata de ciberespaço, entende-se que há dois extremos, ou o país tem um bom domínio do desenvolvimento e produção de tecnologia, o que cria margem para exportação de tecnologia de segurança e defesa, ou ele importa essa tecnologia e trava a batalha no aperfeiçoamento da mesma (IZYCKI e CORTINHAS 2021). De acordo com Ayres (2017), o mundo pós-guerra-fria acabou experimentando várias novas perspectivas sendo elas sociais, políticas e econômicas, o que acabou gerando consequências como a ideia de que o ciberespaço e a cibersegurança são conceitos voltados para a percepção dos agentes internacionais, a priori o Estado.

Assim, se têm tido como premissa a definição de quem são os agentes responsáveis pelo movimento da estrutura que sustenta o Sistema Internacional, qual o posicionamento e comportamento deles, assim como suas intenções (ADLER 2006). Dessa forma, buscam também entender e explicar como essa configuração do atual poder mundial pensa e encara os fenômenos existentes (GRIFFITHS 2007). Esse poder, difuso no Sistema Internacional, faz com que alguns fatores tendenciem a instabilidade no que tange a proteção e segurança dos Estados e OIs.

Sendo assim, a criação de meios que no geral tendem a estabelecer vínculos que mantenham a sobrevivência estatal, também é a mesma que protege os Estados fortes (GRIFFITHS 2007). Ao se pensar na questão da segurança internacional, precisa-se entender que com o passar dos anos, a evolução dos estudos na área passou a desmistificar que a guerra é o ponto chave. Diversos novos fatores incluídos na década de 80 e 90 mostraram que existem outras razões que podem desestabilizar os Estados tal qual as guerras, dentre eles a questão do tráfico de drogas, pandemias, problemas voltados ao meio ambiente e o ciberespaço – que é o objeto de estudo.

Izycki (2021) diz que o ciberespaço se tornou emergente por conta de processos técnicos que envolviam a corrida de desenvolvimento global durante a guerra fria em diante. A nova ordem geopolítica mundial passa a ter um caráter

binário, onde além de não haver fronteiras, existe uma interdependência econômica e infraestruturas que fortalecem ou enfraquecem os Estados, fazendo com que aquele Estado que tenha uma melhor tecnologia esteja à frente de ações dissuasivas (p. 3).

A consideração da relevância do tema fez com que ainda no fim da década de 1980, analistas de segurança dos EUA, como Clarke e Knake (2010) iniciaram pesquisas fomentando que o ciberespaço tinha tudo para ser a problemática do século XXI, uma vez que envolve diretamente questões econômicas, movimenta a indústria de defesa de todos os Estados com as aquisições de aparatos tecnológicos e soma na prática de espionagem.

Por ser algo novo e imaterial, pode ser um lugar onde não há clareza sobre como se dará a aplicação do direito internacional, não existem fronteiras e acima de tudo não se tem controle, faz com que o espaço cibernético seja uma enorme referência para novas modalidades de conflitos. Lobato e Kenkel (2015), argumentam que por conta do aumento significante no número de ações que se alastraram no ciberespaço, os Estados começaram a se questionar a respeito da securitização do espaço cibernético. A securitização é um processo que demanda ações de segurança quando um problema passa das medidas de ações que estão no limite do Estado. Em síntese, um assunto é securitizado quando gera medo para os Estados (BUZAN, B., WAEVER, O., & WILDE, J. D 1998). De acordo com Buzan (1998), a securitização é um processo de viés político e social que identifica um objeto como uma ameaça real no sistema, uma vez relacionada ao envolvimento do assunto com a agenda de segurança internacional.

O capítulo 8 do livro *A new framework for analysis*[10] - que explica sobre setores compilados nas novas ópticas envolvendo os complexos de seguranças regionais - traz para os estudos de segurança internacional pela primeira vez a visão da academia sobre o olhar que tanto EUA quanto OTAN (Organização do Tratado do Atlântico Norte) passaram a ter sobre o distanciamento que existe no ciberespaço e o investimento militar realizado na área. Clarke e Knake (2010), mencionam que nesse período da década de 1990, os primeiros projetos Norte Americanos que visavam estabelecer uma nova corrida armamentista acabaram envolvendo outros países em assuntos nucleares.

[10] Buzan *at al,* 1998.

Como exemplo, Clarke e Knake (2010) falam sobre o alvoroço causados em 2007, quando foi anunciado na mídia, através de fontes anônimas, que a Síria estaria fazendo uma bomba nuclear em fábricas clandestinas no seu território. Na época, o reconhecimento contou com análises de especialistas que através da tecnologia e de inteligência, conseguiram identificar e conter esta ameaça. A combinação dessas duas ferramentas - inteligência e tecnologia -, foram responsáveis por fazer com que os EUA intervirem e acabassem com as fábricas clandestinas de produção de armamento. A dúvida, no entanto, era saber como os radares e os sistemas de defesa aérea poderiam ter sido cegados exatamente no momento dos ataques ao País.

A descrição do que seriam as reações de uma possível guerra de caráter cibernético tinha então acabado de nascer, envolvendo novamente Estados como EUA e Israel, pelo lado atacante e Síria, Rússia e Irã, no lado atacado (CLARKE e KNAKE 2010). A guerra informacional começou a ganhar expressão no mundo, por conta dos “guerreiros cibernéticos” que surgiam, sem rosto, sem nação e sem endereço. A perspectiva do ciberespaço se tornou algo que passou a gerar um medo, porém sem chances de controles, porque agora o ciberespaço era uma ferramenta que por questões como “0’s” e “’1’s” podiam acabar com defesas antiaéreas com um simples feixe de pulsos envolvendo luz e eletricidade.

Por esse lado, pensar em segurança cibernética atualmente é algo intrínseco na academia, devido a fatores como alta demanda em estudos de ameaças e dependência da tecnologia e/ou estudos sobre legislações na área. Entende-se que quando se fala segurança, o debate sempre chega à defesa, entretanto são conceitos paralelos que remetem o mesmo pensamento, só que trabalhados em setores distintos.

Nota-se que a equiparação entre segurança e defesa na segurança cibernética é quase inevitável, dada a interconexão de ambos os conceitos na salvaguarda de sistemas e do Estado contra sensibilidades e vulnerabilidades. Embora distintos, esses termos estão intrinsecamente conectados, com a defesa frequentemente integrada às estratégias e ações de segurança cibernética. Se destaca também que o debate sobre segurança cibernética frequentemente chega à defesa, indicando a interconexão desses termos.

De acordo com Cepik (2014), a segurança é uma condição baseada no status

de proteção, cujo objetivo é a capacidade de neutralizar ameaças contra existência de alguma coisa ou alguém. Por outro lado, o ato da defesa está amplamente ligado à ideia de se repelir um ataque.

Estudar defesa e segurança cibernéticas hoje no Brasil se tornou algo desafiador. Isso porque a região da América do Sul é um local cujo problemas de geopolítica limitam a possibilidade de abertura intelectual[11] entre o Estado e o indivíduo. Wæver (2003) explica que o complexo de segurança formado nas regiões com problemas políticos tende a gerar uma dinâmica que faz com que o Estado tenha tantos problemas com conflitos políticos, problemas de más divisões de riquezas e crimes relacionados a tráficos, que gere uma própria insegurança no Estado para manter relações diretas com o indivíduo.

Lógico que este não é um problema que existe só aqui na América do Sul, entretanto é um dos empasses que o autor identifica para justificar o porquê de as análises de segurança do norte global não poderem ser 100% aplicadas em questões de assuntos regionais.

Parando para pensar nesse argumento, reflete-se que a América do Sul até tenta abordar mecanismos baseados na Europa para gerar desenvolvimento regional, entretanto isso acaba não funcionando, já que os governos tendem a levar seu viés político antes de acordos ou tratativas entre Estados, não possuem políticas conjuntas para trabalhar segurança e mal fazem uso dos acordos já existentes de interesse mútuo (PENTEADO 2022).

Por esse fato, o desenvolvimento de segurança cibernética para o Brasil acaba agregando no status de desenvolvimento existente na região. De acordo com Ayres (2017) regionalmente o Brasil é um dos Estados mais visados quando se trata de ataques e crimes cibernéticos. Isso se dá pelo fato de ser um país populoso e amplamente ativo na rede mundial. Por outro lado, a dinâmica de segurança e defesa para resposta a essas ameaças fica a cargo dos agentes ligados à segurança e defesa da esfera pública. Nesse quesito, vê-se que os estudos acerca do poder voltado para

[11] Trata-se da prontidão e habilidade de um ambiente, sociedade ou sistema em incentivar e facilitar a livre troca de ideias, conhecimento e informações entre várias partes, incluindo o Estado e os indivíduos.

o ciberespaço é algo que se faz necessário para o Brasil002E

2.2 - As Ciber Relações Internacionais

As Relações Internacionais Cibernéticas, defendida por Lopes (2016) é baseada na defesa de que há um subcampo nas R.I, cujo objetivo é tratar do impacto do desenvolvimento e das questões cibernéticas no Sistema Internacional, idealizado nos estudos modernos de segurança internacional, atrelando o poder, a guerra, economia e o espaço cibernético.

Essa literatura trata da exploração da justificativa de que o tema – as relações internacionais cibernéticas – é algo genérico e por isso é algo que se torna necessário, já que sua formulação se deu por base sistematizada, que “exige além de revisão de literatura um produto que venha ser parte de um processo de investigação e que constitui um suprassumo político social” (LOPES 2016).

A constituição dessa ideia parte do que seria o 'ciber internacionalista’, explicado como uma forma de expandir as ciências que engloba as Relações Internacionais, dando permeabilidade a busca crítica de uma visão globalizada na especialidade que trata o ‘cibernético’ e o ‘internacionalista’ (LOPES 2016, 31-33). Assim, o objeto central de estudo pode ser delimitado, uma vez que seus termos homográficos têm tanto campo científico quanto um objeto direto de estudo, no qual o autor ainda cita a presença empírica de fato histórico, desenvolvimento industrial e singularidade com a segurança internacional (ibidem p. 32).

A ideia enquadra as características de fenômenos para construir estudos completos sobre as relações internacionais cibernéticas. O autor utiliza esse pensamento como justificativa, já que o subcampo liga temas extremamente importantes nas R.I como governança, Organizações Internacionais, Segurança Internacional e diplomacia, sendo assim um leque de abordagem em relação ao ambiente informacional criado no século XXI.

Lopes (2016) apresenta que por mais que a temática seja interessante para as R.I, deve-se entender que o espaço cibernético é algo essencialmente fictício, portanto, possui várias interpretações e mesmo que possamos fazer ações no

ambiente dimensional é necessário entender que isso é um produto do desenvolvimento.

O autor também destaca que não foi somente as ciências naturais que ganharam na fundamentação dos estudos do desenvolvimento tecnológico, uma vez que as ciências humanas tiveram um grande avanço na questão do relacionamento tanto deste espaço com o homem, quanto entre os homens em si. Assim, esse desenvolvimento também ajudou na construção das relações sociais.

Quando se analisa o desenvolvimento da temática no âmbito da segurança internacional, percebe-se que se trata de um assunto complexo e vasto. A literatura, segundo Lopes (2016) é ilimitada, tanto em relação às localizações, quanto a fronteiras geofísico-políticas, o que dá a característica do assunto ser multifacetário, onipresente e com suas próprias diretrizes. Nesse contexto, é possível identificar pelo menos dois princípios que impulsionam a concepção de uma teoria voltada para a Segurança Cibernética nas Relações Internacionais.

Em primeiro lugar, uma teoria se origina a partir de um desafio. Neste caso, o desafio está relacionado ao contexto dos efeitos da globalização, já que esse campo é capaz de analisar ameaças e cenários de estabilidade para o Sistema Internacional. Conforme Rid (2011) argumenta, uma teoria pode ser caracterizada como um conjunto de princípios, hipóteses, suposições e explicações destinadas a analisar um fenômeno específico. No contexto da segurança cibernética nas Relações Internacionais, busca-se compreender aspectos que envolvem o Soft Power relacionado à segurança, o que representa uma nova perspectiva nos estudos de segurança internacional.

O segundo ponto a ser destacado é a importância da interdisciplinaridade. Segundo Kello (2013), ‘a interpretação dos fenômenos cibernéticos requer a análise de um novo conjunto de experiências que as teorias existentes podem não ser capazes de esclarecer’. Como consequência, Kello aponta que houve uma demora na adaptação estratégica às realidades cibernéticas. O autor também destaca que, se os decisores estiverem corretos - e suas opiniões não forem ambíguas - o mundo contemporâneo enfrenta uma ameaça cibernética de proporções enormes. Nesse sentido, teorias que abrangem a análise de política externa, Relações Internacionais

e Segurança Internacional necessitam de uma abordagem holística, uma vez que uma ameaça cibernética pode ser mais grave do que o terrorismo global, alertando para o potencial de um catastrófico ciberataque.

2.3 - A segurança cibernética como ferramenta de poder no sistema internacional

Neste ponto, trabalhamos a discussão da segurança cibernética dentro da teoria de segurança internacional, tendo como análise dois tipos de situações, as de cunho técnico e as de caráter bélico. Antes de tudo, como entendemos essas tais "capacidades" e como a definimos? Para entender como se avalia as diferenças e o que são as capacidades, escolhemos autores das Relações Internacionais, cujo as obras foram de grande importância para o desenvolvimento da temática na atualidade.

A começar por Rid (2011, 1-28), que em seu trabalho, define que as capacidades cibernéticas podem ser vistas de duas formas. A primeira trata das capacidades de nível técnico, que envolvem crimes, políticas e normas constitucionais e a segunda é a que tange a esfera do conflito internacional, como poder ofensivo e defensivo. Rid aponta que as ações de cunho ofensivas do ciberespaço, são instrumentos que correspondem aos objetivos políticos de um Estado. Nesse caso entende-se que para um conflito alcançar esse caráter ofensivo, é necessário a violência e a morte no mundo real, onde se engloba tanto as caraterísticas ofensivas e defensivas, que seria ao nível extremo, a guerra (T. RID 2011).

Mensurar as capacidades cibernéticas é um trabalho diferente de calcular o poder nuclear de um Estado. Para mensurar, é necessário entender que por se tratar de uma ferramenta silenciosa (algo que pode ser feito a partir de qualquer lugar com um dispositivo ligado ao ciberespaço), modular uma investida no ciberespaço necessita de energia, paciência, até mesmo calma, onde se envolve frequências do uso de poder, buscando se aproveitar da inocência e da fraqueza dos Estados (CLARKE e KNAKE 2010). Nesse caso, o coeficiente para calcular esta equação, tem sido o investimento em empresas que constroem e melhoram ferramentas cibernéticas, uma vez que se um Estado "A" financia empresa "B" e vende para um país "C", o Estado "A" tem a 'vantagem' em relação ao outro país.

Há pelo menos três definições de poder voltados ao ciberespaço. A primeira

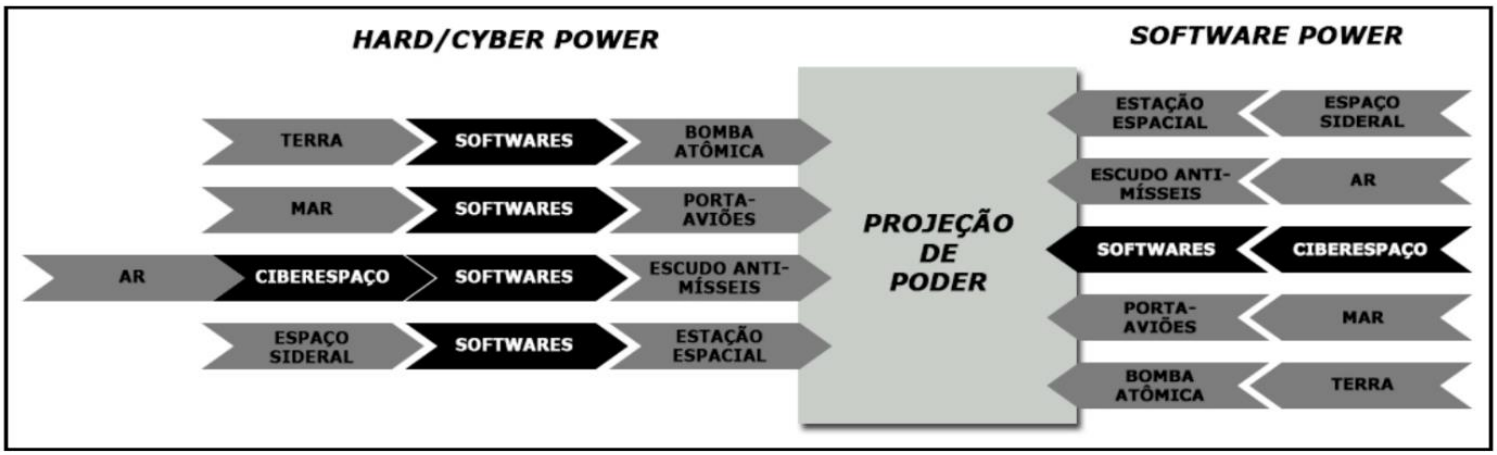
dimensão, Izycki (2021) descreve que envolve a condição de impor a terceiros a execução de ações suas do jeito que você estabelece. A segunda, trata de uma dimensão de poder que acontece na ação prática e que não tem a necessidade de se utilizar a coerção. Já a terceira, o autor explica que seria onde aqueles que moldam ideias e disseminam crenças conseguem reproduzir o poder para os que já exercem, sem se expor. Essas facetas, tal qual descreve Nye (2010) envolvem conceitos conhecidos nas Relações Internacionais e são parte do que o autor nomeia de Softpower.

Quando Clarke e Knake (2010) avaliaram as capacidades ofensivas no ciberespaço, levaram em consideração tudo que envolvia a dimensão cibernética, como espionagem, questões políticas e ataques reais. Entendeu-se que à nível de Sistema Internacional, até o indivíduo que faz parte da sociedade estava confrontando os Estados no ciberespaço.

De 2000 a 2010, os Estados Unidos e a Rússia foram os países detentores das mais sofisticadas e complexas redes de segurança cibernética (CLARKE e KNAKE 2010). Os autores colocam que em segundo lugar poderia ser colocado a China e França, porém a relevância do cenário era tão alta que surpreendentemente países potencialmente ‘relevantes’ como Brasil, Irã e Coreia do Norte conseguiam destaques por seus desenvolvimentos na área.

Lopes (2016), desenvolveu uma tabela que mostra a construção de ferramentas de segurança cibernéticas atuais no Sistema Internacional, onde é importante destacar que a projeção de poder é aplicada por duas formas tradicionais das R.I, o *Softpower* e *Hardpower* (conceitos desenvolvidos para explicar formas de exercer o poder). Porém além destas, o autor descreve uma terceira, o *Software Power* (Lopes identifica que esse seria o resultado de quando se exerce poder no ciberespaço) para provar seu pensamento incluindo a ideia da necessidade das ciberRI até no viés brando da demonstração de poder.

Figura 1: Aplicação da segurança cibernética em meios convencionais de poder.



Fonte: Lopes, 2016 p.107.

Esta subseção desenvolvida pelo autor, mostra a interação das ciberRI não somente pela prova teórica da necessidade de estudos, mas também com análise empírica de que as bases estruturais do conceito de segurança internacional e relações internacionais cibernéticas podem ajudar na investigação e aperfeiçoamento das RI para Estados, como o Brasil.

2.3.1 – A Construção de Capacidades da Segurança Cibernética

Como os Estados têm pensado a respeito da segurança cibernética? Para responder isso, tendo como base o estuzdo realizado por Izycki (2021), foram analisados, a partir de dados coletados por *scripts* personalizados em *python*, dois tipos de informações. Primeiro, como se entende a segurança cibernética no Sistema Internacional? Já em segundo buscou-se entender em dois conjuntos de dados como o desenvolvimento do ciberespaço vem acontecendo, ou seja, como os Estados estão se armando para isso?

Os Estados no geral entendem a necessidade da segurança cibernética como algo fundamental para o desenvolvimento e segurança interna (E. A. IZYCKI 2021). Nesta afirmação, tem se deparado com um ponto de análise interessante, os Estados mensuram o ciberespaço como uma ferramenta que funciona como a antiga concepção de balança de poder[12]. Segundo Waltz (WALTZ 1979), entende-se que a

[12] Ler mais em Waltz K. Theory of International Politics, 1979.

balança de poder é a forma que os Estados buscam para garantir sua proteção no Sistema Internacional. O alinhamento entre Estados fracos faz com que haja um equilíbrio contra Estados mais fortes. Por esse ponto de vista, Cortinhas (2021), apresentou em seu trabalho que os Estados mais fracos tendem a concentrar seus recursos investindo em capacidades cibernéticas. Enquanto isso, os Estados mais fortes buscam melhorar o que já possuem e colocar em contrapartida os limites das capacidades de seus rivais.

De 2008 a 2020, destacamos os seguintes 45 países que investiram em aquisição múltiplas de capacidades ciber-ofensivas, com fornecedores de fontes Estatais e empresas privadas:

TABELA 1: Lista de países que adquiriram capacidades ciber-ofensivas

Nome	**Region**	**Purchases**[13]
Mexico	Americas	13
UAE	MENA[14]	8
Egypt	MENA	7
Saudi Arabia	MENA	6
United States	Americas	5
Kazakhstan	Central Asia	5
Bahrain	MENA	5
Nigeria	Africa	5
Oman	MENA	5
Ethiopia	Africa	4
Uzbekistan	Central Asia	4
Hungary	Europe	4
Pakistan	Southeast Asia	3
Turkey	MENA	3
Syria	MENA	3
Morocco	MENA	3
Thailand	Southeast Asia	3
Panama	Americas	3
Qatar	MENA	3
Singapore	Southeast Asia	3
Spain	Europe	3
Malaysia	Southeast Asia	3
Italy	Europe	3
Sudan	Africa	3
Lebanon	MENA	2
Vietnam	Southeast Asia	2
India	Southeast Asia	2
Philippines	Southeast Asia	2
Zambia	Africa	2
Yemen	MENA	2
Indonesia	Southeast Asia	2

[13] Número de compras dentro do período analisado.
[14] Oriente Médio e Norte da África.

Mongolia	Central Asia	2
Bangladesh	Southeast Asia	2
Switzerland	Europe	2
Kuwait	MENA	2
Czechia	Europe	2
Lithuania	Europe	2
Uganda	Africa	2
Luxemburg	Europe	2
Latvia	Europe	2
Turkmenistan	Central Asia	2
Honduras	Americas	2
Jordan	MENA	2
Poland	Europe	2
Colombia	Americas	2

Fonte: Izycki, 2021 p.45.

Nestes dados, fica em evidente que a busca por meios que aumentem a capacidade ofensiva (como ataques e roubo de dados) é uma consequência estratégica pensada nos futuros meios de conflito. De acordo com Izycki (2021) A aquisição dessas “soluções” também implica dizer que os países pretendem expandir seu repertório, uma vez que os fornecedores privados fazem parte da estratégia de explorar vulnerabilidades, melhorar e revender uma nova solução.

No que diz respeito a como os Estados vêm se armando para responder às ameaças do SI no meio cibernético, foram analisados a partir de um *script* desenvolvido por Izycki (2021) dois conjuntos de Estados. O primeiro conjunto trata de Estados, que apresentam as capacidades cibernéticas caracterizadas pelo uso real – quer dizer que são Estados que eventualmente atacam ou fazem testes contra outros agentes -, o resultado foi de 34 (trinta e quatro) Estados-nações, ou seja, 34 Estados têm em seu arsenal, além de armamentos, porta-aviões e jatos, ferramentas que envolvem o ciberespaço para uso imediato.[15]

O segundo conjunto, por sua vez, cuja apresentação se dá em dados detalhados destas capacidades ofensivas (por meio de ataques ou conflitos), tratam de 85 países, porém estes não foram evidencialmente comprovados com um uso real em meio a sua segurança interna (E. A. IZYCKI 2021, 23). Se entende então que as capacidades de desenvolvimento e segurança cibernética tem sido uma ferramenta tão importante quanto o desenvolvimento de armas nucleares ou de ferramentas

[15] Izycki aponta sobre a distinção dos países referidos em relação a esta capacidade ofensiva diretamente associada ao Estado. No trabalho são citados uma média de 30 Estados contando com a Belarus. Alguns destes países demonstram capacidade ofensiva local, porém não associados ao governo, normalmente são grupos criminosos.

maquináveis, isso porque o custo é relativamente menor e pode ser desenvolvido sem necessidade matéria prima industrial, como aço ou urânio.

Ao analisar o estudo feito por Izycki (2021), percebeu-se que ambos os países que fizeram parte do estudo realizaram um processo de aquisição com fornecedores privados – para aqueles onde o desenvolvimento da ciência nacional não é tão avançado assim - e pelo que o autor apresenta, não é um processo que tem uma data para acabar. Neste ponto, uma característica bem interessante de se comentar é a aplicação prática da diferença entre desenvolvimento cibernético e segurança cibernética. A diferença entre ambos se dá enquanto um trata da ciência, estudos e investimento, o outro trata de questões práticas de segurança e defesa, como por exemplo no caso do desenvolvimento o LVSC (Livro Verde de Segurança Cibernética) e na segurança o programa Guardião Cibernético do Exército Brasileiro[16].

Em seu trabalho, Izycki (2021) ainda afirma que além do armamento convencional, temos a presença de um aparato que atua a partir da interoperabilidade, algo que envolve um desenvolvimento contínuo em três pontos chaves, que são: comunicação, armazenamento e disseminação de informação. Esses três pontos são resultado massivo da ideia de as CiberRI se tornaram uma peça oportuna nas RI. Além disso, desencadeiam a perspectiva de conceitos de segurança do século XX e do século XXI, como espionagem e sabotagens. A natureza que envolve o poder para todos estes Estados é fruto de uma concepção que traz um novo patamar para o pensamento de segurança moderno, onde agora quem não consegue se proteger com mísseis ou com acordos com aliados mais fortes estava fadado a recorrer ao desenvolvimento de doutrinas informacionais, como a doutrina de guerra eletrônica ou a de guerra cibernética já que a modernidade está aproximando o mundo (IZYCKI e CORTINHAS, Conflito Cibernético - Evolução ou Revolução? 2021).

A partir disso, Estados passaram a utilizar como ferramenta os próprios ciber criminosos (CLARKE e KNAKE 2010) – podendo ser citado os famosos casos nos EUA, os anúncios da Rússia, ou até mesmo os grandes casos noticiados por Israel, ou os “patriotas” hackers iranianos que de ‘boa-fé’ ajudam o País a se manter forte frente às ameaças do Ocidente - (IZYCKI e CORTINHAS, Conflito Cibernético -

[16] Programa criado pelo ComDCiber, cujo o intuito é garantir resiliência em ações de caráter de defesa e segurança cibernéticas. Ler mais em: www.dct.eb.mil/comdciber.br

Evolução ou Revolução? 2021). Assim, utilizamos o conceito de segurança cibernética desenvolvido por Hosang (2011, 7), que diz que a segurança cibernética "pode ser entendida como a arte de garantir a existência do espaço cibernético pela adoção de ações que assegurem disponibilidade, integridade, confidencialidade e autenticidade das informações de interesse do Estado".

Pensando assim, quando se fala do ciberespaço, é interessante abordar a perspectiva da sua criação, sendo um dos mais perfeitos avanços da tecnologia no século XXI, já que passou a ser essencial na vida de pessoas e Estados (LÉVY 1999). O ciberespaço também acaba sendo perigoso, porque como ainda está em evolução não pode ser controlado ou mensurado, uma vez que isso acabaria invadindo a liberdade e direitos de outros agentes (LOBATO e KENKEL 2015, 39).

O fato de haver um espaço de domínio dos Estados que não possui controle faz com que seja uma ferramenta de espionagem e sabotagem tendenciosa, onde se pode atribuir a responsabilidade de atos para um outro Estado ou até mesmo um indivíduo (ibidem; p. 23)[17].

Por esse motivo, Buzan (2012) oferece aporte teórico, alegando que pelo fato de o ciberespaço ser algo desenvolvido pelas necessidades da guerra, se torna algo complexo e importante para as Relações Internacionais. Spiri (2020) defende que por conta da ampliação da agenda de Segurança Internacional, o ciberespaço e o desenvolvimento tecnológico acabaram sendo enquadrados como elementos de ameaça e por isso passam a ser tratados nas perspectivas dos ESI, logo podem ser analisados a partir da sua geolocalização.

Nesse viés, entende-se que o ciberespaço pode ser considerado um problema que se enquadra nos princípios de securitização descritos nos ESI, uma vez que se torna uma ameaça real e que afeta as relações entre indivíduos e Estados, já que acaba se tornando uma ferramenta de poder no Sistema e com o aperfeiçoamento de Estados menores, tem-se a ideia de um aumento na questão do poder regional, o que também gera insegurança.

Falando da abordagem regional, quando se trata do enfoque na América do

[17] Izycki (2021) explica que há um nome para essa ideia de se atuar sem necessariamente receber uma penalização militar, econômica ou geopolítica, se chama '*plausible deniability'*.

Sul, alguns indicadores agregam a ideia do CRS, além da importância do crescimento da pesquisa na temática para as Relações Internacionais. De acordo com Portela (2017), a caracterização dos estudos voltados para o ciberespaço tem sido importante para o desenvolvimento científico. O autor indica três conjuntos de pesquisa: (a) estruturação e configurações teóricas; (b) estudos voltados à políticas e relações interestatais envolvendo regulamentação, e; (c) segurança e defesa cibernética.

Dessa forma, ao analisarmos o ciberespaço no âmbito da América do Sul, é fundamental levar em conta elementos essenciais para compreender a dinâmica desse ambiente na região. Um exemplo notável é a marcante disparidade na adesão ao espaço cibernético, onde apenas 70% da população possui acesso. Isso se destaca como um fator crucial que impacta a distribuição de poder e as oportunidades no ciberespaço (OLIVEIRA, et al. 2017).

Além disso, ainda de acordo com os autores, a porcentagem de pessoas com acesso, a velocidade e a qualidade da conexão desempenham um papel fundamental na capacidade dos Estados de explorar e utilizar eficazmente as tecnologias cibernéticas (OLIVEIRA, et al. 2017). Ou seja, a atenção dada aos livros de segurança e defesa cibernética, bem como às doutrinas relacionadas, desempenha um papel vital na preparação da região para lidar com as ameaças e oportunidades que o ciberespaço oferece.

Portanto, ao considerarmos esses elementos, temos uma visão mais completa das implicações do ciberespaço nas Relações Internacionais na América do Sul e da sua diferença quando comparado a problemas direcionados ao Norte global.

Em um estudo sobre (in)segurança cibernética, Izycki (2023) buscou discutir justamente a respeito desse acesso à tecnologia e noções básicas de segurança, tanto em âmbito de agencias e órgãos, quanto para a sociedade focados na América Latina. Com base no trabalho, identificou-se que "muitos países da região não possuem a infraestrutura necessária para lidar com as ameaças cibernéticas, o que implica na falta de políticas públicas eficientes e regulatórias relacionadas à segurança cibernética" (p.04).

Em suma, a América Latina enfrenta uma lacuna na implementação de

políticas públicas integradas que fomentem a colaboração entre os setores público e privado, bem como estratégias eficazes de conscientização e capacitação. Isso resulta na falta de uma abordagem estratégica abrangente para lidar com as ameaças cibernéticas, o que dificulta a proteção de informações sensíveis e a resposta eficiente aos ataques.

Com base no que foi apresentado sobre a falta de infraestrutura e políticas públicas eficientes na América Latina para enfrentar ameaças cibernéticas, podemos pensar no Brasil como uma das principais nações da região, que enfrenta desafios semelhantes em sua abordagem à segurança cibernética. Por isso, a necessidade urgente de uma estratégia integrada, que envolva colaboração entre os setores público e privado, além de conscientização e capacitação, destaca a importância de o Brasil implementar medidas específicas para lidar com as complexidades do ciberespaço e assegurar a eficaz proteção de seu território.

CAPÍTULO 3 - A ELABORAÇÃO DA ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA NO BRASIL

A segurança cibernética no Brasil é algo que começou a ser desenvolvido em 2008, quando o governo entendeu que precisavam investir em capacidades e ações mais robustas para poder acompanhar os avanços internacionais. Nesse caso, o investimento precisava ir além da segurança e defesa tradicional, que seriam blindados, armamentos e munições, viabilizando um tempo de produção curto. Com isso, pensou-se nas tecnologias voltadas para o ciberespaço, como simuladores, treinamentos, políticas e *softwares* de segurança e defesa (HOSANG, 2011; BRASIL, 2020).

Desta forma, ao se tratar do ciberespaço como algo que constantemente está evoluindo, além de envolver diretamente dados de estruturas críticas – sistemas e ativos extremamente essenciais para a sociedade, como hospitais, hidrelétricas e outros -, a segurança cibernética se tornou foco para iniciar um processo que até o presente momento ainda está em fase de construção, que seria a ideia de uma segurança cibernética viável para a proteção do Brasil (HOSANG, 2011, p. 35).

Essa por sua vez é uma necessidade que ainda carece de consolidação, uma vez que a proteção dos meios cibernéticos não é algo sólido, nem tangível para o Brasil (Senado Federal, 2014). Isso porque parte dessa segurança faz parte da agenda do ministério da defesa, outra parte é intercalada a agências do executivo, tais como Gabinete de Segurança Institucional (GSI) e outros órgãos que fazem por metodologia própria, como o Departamento de Segurança da Informação (DSI), PF, Anatel, BACEN e outros. O problema nisso tudo é que todos os órgãos de alguma forma trabalham com segurança cibernética, todavia existe a falta de comunicação entre ambos os órgãos e, ainda pior, fazem segurança cibernética para o que lhes convém (*ibid* p.40).

A ideia de se criar uma Política Nacional De Segurança Cibernética surge primeiramente a partir da Estratégia Nacional de Segurança Cibernética (ENSC) em 2018, regida pelo decreto nº 9.637, de 26 de dezembro de 2018 (BRASIL 2018). Que tem como finalidade a proteção e segurança das instituições e indivíduos do País. A tratativa inicial, atribuída ao GSI, como órgão gestor do papel de governança e

produção de segurança foi algo que deu origem a três pontos focais na estrutura atual.

1 – Gestão de riscos. Com isso, a agenda nacional precisou criar uma equipe de tratamento e respostas a incidentes;

2 – Aos ativos cibernéticos. Identificar meios de melhorar a nossa segurança cibernética. Com isso o Brasil adota uma postura baseada na ‘imitação’, ou seja, o Estado ‘imita’ o que se tem de melhor de outros países com base no conhecimento gerado a partir de cooperações Internacionais, além do investimento nacional em pesquisa e desenvolvimento (PENTEADO 2022).

3 – Pontos Críticos. Seriam as proteções estratégicas, proteção do Governo e proteção às infraestruturas, trabalhar a governança cibernética, dimensão normativa, pesquisa, desenvolvimento e inovação, educação, dimensão internacional e parcerias estratégicas (BRASIL 2018).

O interessante disso é que até 2020, essa ENSC desenvolveu a ideia da Política Nacional De Segurança Cibernética, entretanto não conseguiu ainda uma aprovação legal, algo que não aconteceu quando a Autoridade Nacional de Proteção de Dados (ANPD) foi criada, com base na Lei Geral de Proteção de Dados Pessoais (LGPD), criada a partir da Medida Provisória nº 869, de 2018 (BRASIL 2018). Onde o objetivo seria o de regular o modo que tratamos a segurança dos dados dos indivíduos e das empresas, buscando criar um consentimento, tanto em relação a prazo para alertar o governo sobre incidentes, quanto para aprimorar os ecossistemas digitais do Brasil. Esta por outro lado independente da Política Nacional De Segurança Cibernética

Baseado nos trabalhos do Senado Federal (2014), de Hosang (2011) e a Revisão Sobre Cibersegurança (2018), identifica-se que o primeiro problema do Brasil, se dá na dificuldade em se elaborar uma política de segurança cibernética, visto problemas governamentais que inviabilizam a continuidade de investimento e aperfeiçoamento de setores estratégicos. Também é o mesmo problema que atrapalha nas leis. Isto porque existem tantos setores e tanta divisão na tentativa de ser algo completo, que acaba havendo lacunas, deixando falhas quando se trata na jurisdição de atuação dos órgãos, onde claramente um é criado com o princípio de

tratar dados de empresas e indivíduos e o outro do Estado, sendo que em teoria este também incluiria empresas e indivíduos (IZYCKI, AYRES PINTO e LAVANDOSKI DA SILVA 2023).

Assim, neste capítulo trata-se da discussão da Política Nacional De Segurança Cibernética no Brasil, onde traz-se a abordagem histórica e os processos utilizados para se pensar neste modelo de segurança. Para esse capítulo, serão abordados em dois subcapítulos, a evolução das capacidades de segurança, dentro desta estratégia e a estrutura a qual se encontra e é coordenada.

3.1 - Evolução Das Capacidades De Segurança Cibernética No Brasil

No Brasil, as primeiras propostas voltadas para a segurança cibernética começaram tardias em relação aos outros países citados. Oficialmente, foi só em 2008 que o Brasil decretou que o espaço cibernético era algo a ser trabalhado e que a partir de então ganharia visibilidade (BRASIL 2008). A divisão feita, tratava da prerrogativa de defesa e segurança cibernéticas. A defesa, que envolvia desenvolvimento, Comando e controle (C2), ferramentas à nível de conflito armado, foram destinadas aos órgãos do ministério da defesa, no caso a força terrestre (exército brasileiro), que em seguida rearticulou e passou a ter funcionalidade tanto da marinha quanto da força aérea, assim como o apoio dos órgãos de segurança pública.

A parte normativa, que cuidava de segurança relacionada a crimes e golpes (fraudes e chans[18] com venda de dados de cartões são os mais comuns), foi passada para agências como a GSI e ANATEL, que no âmbito da sua agenda tratam de forma multissetorial a abordagem e o enfoque com base nas leis gerais de telecomunicações para políticas públicas (ANATEL 2021).

Considera-se que a ANATEL tem apoio de outros órgãos, como o Gabinete de Segurança Institucional da Presidência da República (GSIPR) (através da representação do Departamento de Segurança da Informação e Comunicações (DSIC) e Agência Brasileira de Inteligência (ABIN), assim como Ministério da Justiça

[18] chans são fóruns virtuais na deep web que tem por objetivo mercado negro e conversas sem controle.

(tanto pelos departamentos do Ministério da Justiça (MJ) quanto pelo Departamento de Polícia Federal (DPF) que coordenam atividades de inteligência e segurança da informação (BRASIL 2010).

Nesse ponto, uma crítica pessoal em relação a essa estrutura organizacional nacional, é que o Brasil consegue diferenciar, porém não consegue gerenciar bem o papel das instituições, falta um modelo de governança e uma metodologia viável para tratar assuntos de segurança cibernética[19]. Isso porque vários órgãos trabalham em um espectro geral de segurança e defesa cibernética, indo desde o Comando de Defesa Cibernética (ComDCiber), ou o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CtirGov) e até pela ANPD, mas não existe uma clareza quando se trata das regras do jogo, já que quando ocorre um incidente e as coisas não fluem como deveriam.

Utilizando como exemplo: "houve um ataque cibernético voltado aos dados de usuários da COPEL[20]". Por ser um incidente, é tratado como um incidente criminal, quem investiga é a polícia federal ou um órgão público estadual (nesse caso a polícia civil)? Mas nesse caso, a COPEL é uma infraestrutura crítica, seria o ComDCiber quem trata do caso? Será que pela circunstância ser baseada em ataques voltados aos usuários a ANPD é quem trataria? Em resumo, como apresentado em documentos como END, PND ou LVSC por exemplo, as descrições são "bonitas", mas quando se trata de casos reais, é possível enxergar com clareza que existe um labirinto burocrático e isso acontece pelo fato de as atribuições não estarem claramente dispostos, gerando um conflito de competências.

Na teoria, pode-se pensar em pelo menos duas formas de se “fazer” a segurança cibernética no Brasil. A primeira, está relacionada com o que o DSIC trata dessa normativa. Ou seja, a produção de informações de inteligência e segurança cibernética, tratamento de incidentes. Nesse caso é importante citar a abrangência operacional do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), que junto do GSI e ANATEL, tem desenvolvido

[19] Compartilha-se a crítica apontada por Izycki (2021) de que a ausência de diretrizes claras e a falta de um modelo de governança e metodologia eficazes podem comprometer a eficiência do país em lidar com incidentes cibernéticos.
[20] Companhia de Energia Elétrica do Paraná.

normativas para as atividades de segurança nacional relacionadas à informação (2020). A funcionalidade desse primeiro ponto se dá nas análises de infraestruturas críticas do Brasil, como usinas hidrelétricas, hospitais e até mesmo sites, notificando vulnerabilidades e, se caso haja, incidentes e finalizando com recomendação de correções.

A segunda, é a utilização das forças policiais na prática. A partir da persecução criminal[21], onde se gera aquele efeito preventivo geral, com a ideia de investigação de crimes, fraudes e prisão. No entanto, tal qual o Senado Federal (2014) apresenta, a falta de comunicação quando se trata de defesa cibernética e segurança cibernética fazerem alusões a coisas longínquas, faz com que as informações e as ações sejam negligenciadas e acabam por resultar em incidentes graves, como nos acontecimentos de 2013 e 2014[22], quando foi revelado que os EUA possuía dados de caráter sigilosos de membros do executivo e de dados de empresas públicas e privadas do Brasil, como a Petrobrás.

A ampliação do ciberespaço começou a ser pensado de fato na primeira década dos anos 2000 (BRASIL 2008, 11), onde se tiveram os principais documentos que explicam, descrevem e aplicam políticas de uso e segurança na rede interna e externa do país. Assim é fácil mensurar a quantidade de documentos oficiais - através de pesquisa, revisão bibliográfica e documental - que mostram essa perspectiva, desde a sua criação até os dias atuais, isso porque, como apresentado por Favero (2022), de 2008 até 2020 foram escritos trinta e três documentos que no fim das contas visam explicar o que o Brasil entende por ciberespaço, crimes cibernéticos e como deve-se agir.

A evolução das capacidades de segurança cibernética e a ideia de interação dos agentes nacionais no Brasil são pontos que podem ser evidenciados na base destes trinta e três documentos, conforme apresentados a seguir.

[21] Termo utilizado para o ato de quando o Estado utiliza todos os meios necessários para punir, já que apenas ele pode exercer tal função.
[22] Senado Federal questiona a comunicação entre os órgãos de segurança e inteligência em relação a dados extremamente confidenciais que foram parte da revelação de espionagem pelos EUA em 2013 e 2014.

3.1.1 Política Cibernética de Defesa de 2012

Na Política Cibernética de Defesa (PCD) (2012), conhecida também por *MD31-P-02*, as estratégias e diretrizes adotadas para a segurança das redes, sistemas e as infraestruturas críticas visão o nível estratégico e de guerra cibernética. O pressuposto básico desta está na eficácia das ações cibernéticas com a atuação colaborativa da sociedade brasileira, onde se diz incluir também a comunidade acadêmica, setor público e privado (2012, 11).

O MD elaborou o documento quatro anos após a indicação da END de que o ciberespaço deveria ser uma prioridade. Ao contrastar com o programa nuclear de 2011, o documento deixou evidente que o setor estratégico seria negligenciado, uma constatação que se confirmou em 2014.[23]

Conforme estabelecido pelo MD31-P-02, os objetivos relacionados à cibernética e defesa buscavam estabelecer princípios de atuação em relação às estruturas, à Ciência e Tecnologia (C&T) e à criação de legislação e normas para o emprego no setor cibernético (2012, 15).

3.1.2 Lei Nº12.737 de 2012

A lei referenciada se tornou um marco no que tange os delitos informáticos. Se tratando da primeira lei aplicada no Brasil pelo legislativo que buscou como objeto a penalização para invasão de dispositivos e redes, adultério de informações, roubo e obstrução de dados digitais (2012).

A relação desta lei com a evolução das capacidades de segurança cibernética no Brasil está no desempenho para o fortalecimento da segurança e privacidade do indivíduo. Isso porque foi a partir desta que o governo passou a buscar uma resposta efetiva para a crescente ameaça digital. Dentre os aspectos que contribuíram para o aprimoramento de nossas capacidades, cita-se: 1- as penalidades graduadas presentes no artigo 154-B, no que tange a ação penal, as penalidades para delitos cibernéticos passaram a ser executadas com base na gravidade dos crimes. 2- O aumento da conscientização para o caso. Com a repercussão do assunto, houve

[23] Exposição da NSA.

também a conscientização sobre a importância dos conceitos básicos de segurança de credenciais e senhas. Em suma, a base foi criada e a partir desta aperfeiçoada para delitos e ações futuras.

3.1.3 Doutrina Militar de Defesa Cibernética de 2014

O manual MD31-M-07 retomou a definição do espaço cibernético conforme estabelecido pelo MD (2014). Sua principal missão foi padronizar os princípios do conflito cibernético nas Forças Armadas (FA) destacando o seu papel na progressão das capacidades e o conceito de defesa cibernética, integrando as responsabilidades no âmbito operacional das FA de maneira conjunta.

O impacto da criação do MD31-M-07 é evidenciado quando o Estado reforça as competências das FAA na reação proativa diante das ameaças cibernéticas. reflete na integração efetiva das responsabilidades operacionais, promovendo uma abordagem coordenada na defesa cibernética e segurança das infraestruturas. Esse impacto não só aprimora as capacidades militares, mas também repercute de maneira positiva em toda a estrutura de segurança cibernética do Brasil, fornecendo orientações nítidas e integração para enfrentar os desafios em constante mutação no cenário cibernético (BRASIL 2014).

A partir deste manual, o Brasil também teve impacto nas ações de cooperação internacional, no aperfeiçoamento e formação técnica de oficiais do quadro de comunicações das forças armadas, assim como na melhoria de práticas e informações no âmbito de atividades de segurança e defesa dentro das nossas FA. Isso porque com a capacitação de pessoal, há também a atualização das práticas e normas internas que garantem o fortalecimento da capacidade de resposta para eventuais incidentes.

3.1.4 Estratégia de Segurança da Informação e Comunicação e Segurança Cibernética da Administração Pública Federal de 2015 e a Política Nacional de Inteligência (PNI) de 2016.

Ambos os documentos de natureza político-estratégica se originam do Gabinete de Segurança Institucional (GSI), teoricamente delineando a divisão entre segurança e defesa cibernética em níveis. A Estratégia, por um lado, adicionalmente,

também busca facilitar pontos como articulação, coordenação e aprimoramento dos esforços entre os diversos agentes que fazem parte da Administração Pública Federal (APF).

Por outro lado, a PNI apresenta um panorama um tanto quanto interessante, destacando, no ponto 6.5 referentes à inteligência do Estado, a abordagem de ataques cibernéticos. O documento prevê o uso de recursos tecnológicos para interromper, penetrar, adulterar ou destruir redes, incluindo a infraestrutura crítica nacional, diante de ameaças à segurança nacional.

Novamente, um dos fatos que tem se destacado ao longo desses anos foi a forma como estas políticas foram aplicadas, por falta de continuidade e consistência, muitas vezes influenciadas pelas trocas de governos. Isso revela que, ao longo destes períodos não houve políticas contínuas direcionadas ao investimento e à proteção desse espaço estratégico e de domínio dos estados.

Dessa forma, se tornam extremamente importantes os estudos que tratam da questão cibernética, sendo inclusive um marco interessante, já que é um dos fatores que tem aproximado as relações civis-militares por conta da importância dos estudos na área. Mais do que isso, o interesse crescente na discussão, tanto na parte teórica quanto na construção de ferramentas de TI, tem feito com que as instituições que antes mantinham a confidencialidade do avanço, hoje em dia careçam de novas perspectivas para problemas que mesmo não sendo ocorrente, possam já se ter alternativas para soluções emergentes quando empregados agregando na mitigação de incidentes futuros (HOSANG 2011, 20).

Na região da América do Sul, o Brasil foi visto como vanguarda no desenvolvimento de projetos (BRASIL 2020, 20), justamente pela iniciativa rápida na criação da END, PND, Livro Branco de Defesa Nacional (LBDN) e o Livro Verde de Segurança Cibernética (LVSC). O pensamento era de atenção para o ciberespaço como um forte ponto estratégico em relação a espionagem, algo que infelizmente foi comprovado em 2014, quando os projetos de segurança e defesa da área ainda eram implementados (BRASIL 2014, 15) e foram divulgados no mundo pelos esquemas de segurança dos EUA, o que impactou no desenvolvimento estrutural da área para o país.

Para o governo, o setor cibernético faz parte de um conjunto de novos espaços de domínios que, assim como explicado antes, envolvem a nova perspectiva de Segurança Internacional, dessa forma organizado e comandado pelas forças armadas, com acréscimo da portabilidade[24] das agências de segurança do Executivo, tal qual a ANATEL, GSI e as forças de segurança policiais.

Para contribuir para o aprimoramento do setor de segurança cibernética no Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) surgiu como uma agência especializada na regulamentação de leis e ações que envolvem a proteção de dados. Apesar de sua dedicação à segurança de dados pessoais, a ANPD desempenha um papel relevante, uma vez que grande parte dos crimes cibernéticos no Brasil hoje tem como alvo esse tipo de ativo, conforme apontado pelo LVSC (2010). Dessa forma, como afirma Moraes (2021) é pertinente considerar a ANPD como um novo ator no processo de amadurecimento desse setor no país. Isso porque devido à sua natureza estratégica e à função específica no âmbito da proteção de dados a agência não apenas se dedica à segurança de dados, mas também aborda a crescente relevância da proteção da privacidade, um aspecto essencial para a segurança cibernética contemporânea.

Ainda de acordo com o autor, a falta de clareza nas responsabilidades das instituições na área de segurança cibernética no Brasil constitui um desafio iminente que merece atenção. Quando confrontada com situações reais, essa complexidade é agravada pela presença de um labirinto burocrático, que obscurece as linhas de ação e tomada de decisão diante de incidentes cibernéticos (MORAES 2021).

Por conta disso, a ausência de um modelo eficaz de governança é evidente nesse contexto, criando um terreno propício para conflitos de competência e ineficiências operacionais. A existência de vários órgãos, como ComDCiber, CtirGov, ANPD, GSI, ANATEL, Ministério da Justiça e outros, sugere uma fragmentação de esforços que, apesar de sua aparente especialização, muitas vezes resulta em sobreposições e lacunas que comprometem a resposta imediata a incidentes (FERREIRA 2020).

[24] Entende-se como portabilidade à capacidade de transferir ou adaptar as funções, responsabilidades ou recursos de uma agência ou organização para diferentes áreas e setores, da feita que necessário.

A necessidade urgente de um modelo de governança mais eficiente torna-se evidente à medida que a complexidade das ameaças cibernéticas aumenta. É vital estabelecer protocolos claros para a atribuição de responsabilidades em casos específicos, a fim de evitar a ambiguidade que caracteriza a estrutura atual. A implementação de um sistema que estabeleça diretrizes claras, com definições nítidas dos papéis de cada entidade envolvida, seria um passo crucial rumo à eficácia operacional (J. S. OLIVEIRA 2019).

Além disso, é crucial estabelecer mecanismos de comunicação e coordenação mais eficazes entre os diversos órgãos. Essa iniciativa não só agilizará a resposta a incidentes, mas também fomentará uma abordagem unificada e integrada para enfrentar as ameaças cibernéticas em constante evolução. A colaboração entre as instituições torna-se indispensável para lidar de maneira efetiva com a natureza dinâmica das ameaças digitais, assegurando uma defesa resiliente e adaptativa. (SILVA 2022).

3.2 As Estruturas de Gerenciamento e Apoio de Segurança Cibernética no Brasil

Depois de apresentar algumas das principais instituições e documentos que introduzem e desenvolvem os estudos e práticas da área, neste trecho comenta-se sobre a execução da política de segurança cibernética no Brasil.

Em 2019, o IPEA em parceria de outras instituições criou o index “Desafios contemporâneos para o Exército Brasileiro”, onde falava no âmbito de defesa, os maiores desafios que o país estava buscando superar. Neste mesmo index, Izycki e Brandão (2019) falam sobre a nuance das vulnerabilidades e sensibilidades do Estado. Ao analisar o index como um todo, percebe-se que o Brasil ao mesmo tempo que progride em criar um órgão específico para conjunto de pontos, também peca por ter um monte de ferramentas e setores e não haver uma conversação entre eles.

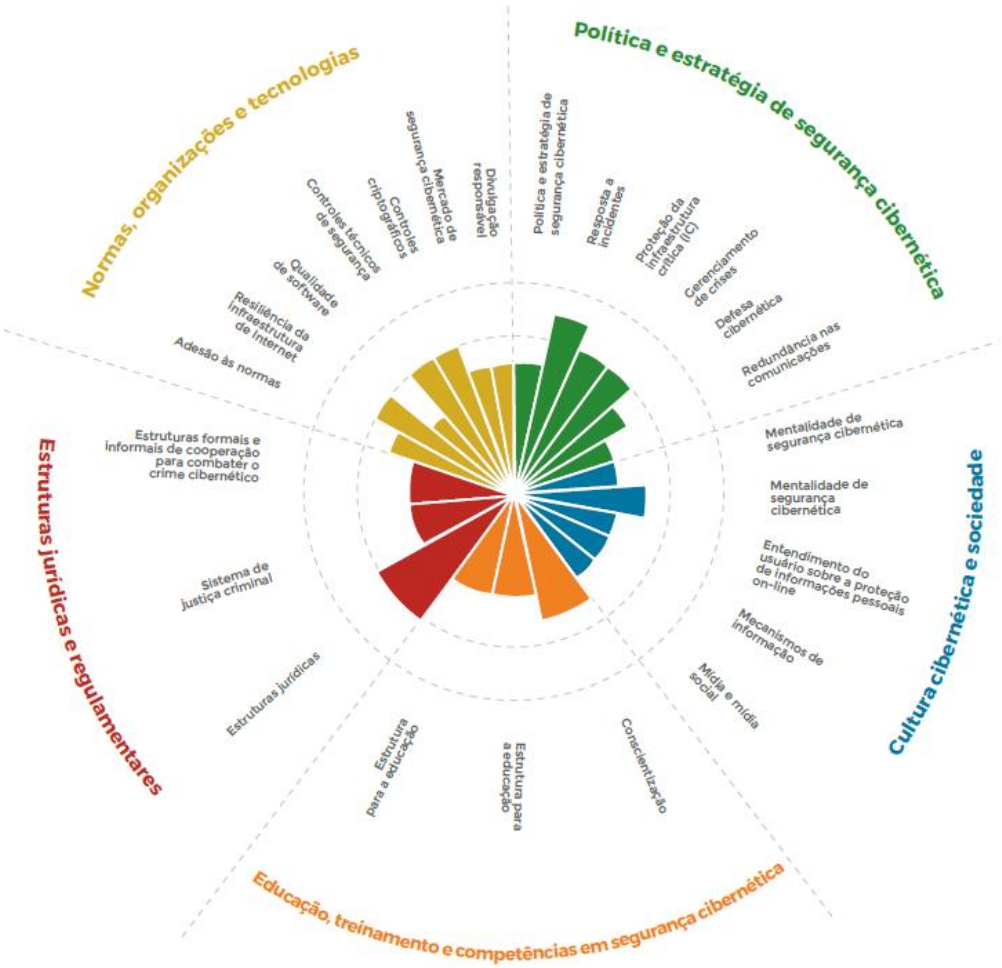
Na realidade, esse esquema, como apresentado na revisão da capacidade de cibersegurança do Brasil (2018), acaba fazendo parte do tripé da segurança, que em teoria deveria funcionar da seguinte forma.

1 – Inteligência Cibernética: Por ser parte da estratégia de inteligência Estatal, tanto o GSI e a ABIN têm vez e voz para ações de caráter de segurança;

2 – Incidentes externos, ciberterrorismo e poder nas capacidades cibernéticas: Por sua vez o Comando de Defesa Cibernética (ComDCiber) teria a autonomia para intervir e mediar ações em caráter de segurança;

3 – Segurança Cibernética e Crimes: Nesse caso em teoria, ANATEL, CGI, as polícias, ANPD, CTIR, GSI e outras unidades dentro de órgãos específicos atuam para conter as atividades. Além destas, outras funções como estrutura, educação, conscientização são representadas na imagem abaixo.

Figura 2 – Organização Estrutural das Capacidades de Segurança Cibernéticas no Brasil



Fonte: Revisão das Capacidades de Cibersegurança do Brasil, 2018 p. 38.

Assim, entende-se que o planejamento acima divide todos os principais pontos de desenvolvimento de segurança cibernética em cinco dimensões:

1- Normas, organizações e tecnologias;
2- Política e estratégia de segurança cibernética;
3- Cultura cibernética e sociedade;
4- Estruturas jurídicas e regulamentares e;
5- Educação, treinamento e competências em segurança cibernética.

Isso, em teoria, é algo muito bom, algo complexo, bem dividido, porém ainda assim o Brasil, ao comparar com Estados Unidos por exemplo, possui tecnologias defasadas e vulneráveis (BRASIL 2017), indo desde o pouco conhecimento em cadastro público para a autenticação de 2 fatores até a própria infraestrutura em rede e sistemas operacionais do governo.

A questão é, o Brasil consegue dividir bem os setores, assim como consegue pensar nas projeções de futuro na área, além de estarmos por dentro dos principais países que têm medido esforços para agregar ações de transparência, combate a crimes, inovações e respostas a incidentes para o desenvolvimento do ciberespaço, mas o que ainda nos segura nessa perspectiva de país vulnerável?

Para isso, seria necessário fazer uma análise temporal, onde se apresenta a evolução do desenvolvimento para esta política cibernética, utilizando como base os governos e o investimento destes. Por tanto, o foco deve ser o fortalecimento e a melhoria das políticas cibernéticas atuais, juntamente com a resolução de lacunas específicas, que são fundamentais para reduzir a vulnerabilidade do Brasil no ciberespaço.

Nesse contexto, ao considerar as vulnerabilidades associadas ao ciberespaço brasileiro, nota-se uma semelhança em relação a países como o Chile e a Argentina, que compartilham o objetivo de aprimorar suas capacidades de segurança cibernética. Embora estes países tenham a questão de um complexo de segurança abrangente, com uma ampla variedade de ameaças e desafios para a segurança na América Latina, percebe-se que as ameaças cibernéticas nem sempre ocupam uma posição de destaque (SPIRI 2020). Isso ocorre porque esses países frequentemente priorizam questões como pobreza, corrupção e tráfico de drogas em detrimento do enfoque nas ameaças cibernéticas (RÜDELL 2003).

Ao examinar os padrões de políticas públicas nos países mencionados, torna-se evidente um enfoque que prioriza desafios imediatos, mas que, a longo prazo, cede espaço para os significativos problemas sociais enfrentados pela América Latina (Izycki, 2023).

Essa abordagem é destacada ao analisarmos a perspectiva de um complexo

de segurança para o ciberespaço no Brasil, revelando um padrão que associa as capacidades cibernéticas com as práticas adotadas por países como Argentina e Chile. Este padrão ressalta a importância crucial de considerar fatores regionais que influenciam as esferas de segurança e as estratégias implementadas desde 2008.

Isso demonstra que, embora o desenvolvimento na área de segurança cibernética tenha avançado, as ameaças e atividades criminosas conseguem superar a capacidade de resposta do Estado, por conta de questões como o anonimato em ações, diferença tecnológica que envolve as regiões e outros (SILVA 2022). Em meio a esse cenário, questões tradicionais de segurança, como pobreza, corrupção e tráfico de drogas, também persistem e evoluem.

Numa avaliação subjetiva, por vezes parece que as autoridades subestimam a complexidade da segurança cibernética, acreditando que é possível fortalecê-la com recursos e especialistas limitados, mesmo sabendo que os recursos são escassos, especialmente quando não há uma pressão iminente ou uma controvérsia específica.

Essa visão, por sua vez, pode resultar em uma abordagem menosprezada em relação à segurança cibernética, desconsiderando sua importância estratégica e a necessidade de investimentos contínuos para enfrentar os desafios emergentes nesse domínio.

Nessa perspectiva, voltando para o arcabouço deste trabalho, no próximo capítulo é apresentado como está dividida a estrutura que compõe o corpo de segurança cibernética no Brasil na atualidade. Isso será descrito através da análise da política cibernética brasileira.

CAPÍTULO 4 - A IMPORTÂNCIA DA MANUTENÇÃO DO CIBERESPAÇO BRASILEIRO

A necessidade de manter atualizados os meios de segurança informacional é um dos princípios fundamentais em gastos relacionados à segurança e defesa em todo o mundo. De acordo com uma tabela comparativa entre grandes Estados[25], compilada pelo GSI, o Brasil conseguiu avançar do septuagésimo primeiro para o décimo oitavo lugar no índice global de cibersegurança[26] (2021). Essa melhoria é ainda mais notável quando avaliamos a situação nas Américas, onde o país ocupa o terceiro lugar, ficando atrás apenas dos EUA e Canadá (ITU 2021).

Não é novidade que a demanda por esforços na área de segurança cibernética tem crescido em todo o mundo. A crescente complexidade dos futuros conflitos internacionais sugere uma mudança de paradigma, afastando-se da ênfase exclusiva em mísseis, armas nucleares e poder naval. O cenário futuro indica que nações incapazes de competir diretamente nesses domínios podem optar por investir no desenvolvimento de capacidades em segurança cibernética, ciberataques e até mesmo na ciberdiplomacia[27] (IZYCKI e CORTINHAS 2021) (CLARKE e KNAKE 2010).

Nesse viés, Lobato e Hurel (2018) destacam a crescente inquietação em relação à "política de segurança cibernética", especialmente no Brasil, impulsionada pelo aumento significativo de ataques e incidentes cibernéticos que o país enfrentou desde 2011, juntamente com as medidas adotadas pelo Estado para enfrentar essas ameaças. Essa constatação mostrou a sensibilidade do país para participar ativamente, em meio às grandes potências mundiais, no desenvolvimento de diretrizes e políticas voltadas para o enfrentamento dessas ameaças.

Pensando nesse contexto de colaboração internacional, à medida que o desenvolvimento coletivo tem o intuito de elaboração de políticas de segurança,

[25] Ler mais em: Cyber Offensive Capabilities: A Glimpse Into A Multipolar Dimension, 2021.
[26] Documento publicado pela ITU que geralmente publica relatórios e índices relacionados à segurança cibernética no globo
[27] A ciberdiplomacia pode ser definida através do uso de técnicas e medidas no ciberespaço, com a finalidade de estabelecer regras, comportamentos e confiança, seja de Estados, indivíduos e organizações. Ler mais em: IBICT: Cibersegurança na União Europeia: a ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos, 2022.

também enfrentam desafios ligados a ameaças a partir dos limites entre atuação nacional e regional/internacional, como políticas de capacidades para proteção de infraestruturas e dados de segurança e, ou desequilíbrios resultantes de necessidades específicas.

Como resposta a esse cenário, o Brasil empenhou-se no planejamento de processos visando o aprimoramento da segurança nacional, como a criação da LGPD, ENSC e o projeto da PNSC. As autoras, Lobato e Hurel (2018), ressaltam dois desses processos, conforme mencionado abaixo:

> "...identificou-se dois processos que culminaram na diversificação e no amadurecimento da atual arquitetura da governança da segurança cibernética no país: (i) a criação de novas instituições, dedicadas a questões de natureza técnica, estratégica e/ou operacional específicas dessa área; e (ii) a reorientação de instituições já existentes, que passaram a incluir aspectos da segurança cibernética e vigilância das redes em seu rol de responsabilidades." (LOBATO e HUREL 2018).

Nesse sentido, foi com a oportunidade de sediar os grandes eventos no país[28] que se desenvolveu no âmbito da cooperação interna entre agências o maior esquema de coordenação técnica e de defesa para tratar de questões voltadas para ameaças à segurança e defesa nacional, ciberterrorismo e incidentes contra estruturas críticas.

Dessa forma, torna-se necessário realizar investimentos críticos para garantir a sustentação da estrutura e a eficácia das políticas dedicadas à segurança cibernética. De acordo com Favero e Pagliari (2023), o cálculo para compreender o poder cibernético de um Estado é, de certa forma, 'simples': o poder cibernético está intrinsecamente ligado ao investimento de um país; no entanto, a correlação entre o montante investido e a sofisticação efetiva da segurança cibernética deve ser relativizada. A alocação de recursos não garante, por si só, as capacidades e condições técnicas adequadas. Embora o investimento seja um fator "significativo", afirmar que quanto maior o gasto, mais sofisticada é a segurança cibernética de um país pode não refletir com precisão a complexidade real desse setor. Além disso, os autores reforçam que essa relação direta se manifesta no desenvolvimento e na

[28] Copa do Mundo de 2014, Jogos Olímpicos em 2016, entre outros.

incorporação de hardwares, softwares e outras tecnologias relevantes.

Assim, os aportes na capacidade cibernética do país traçam um quadro particular no progresso da segurança cibernética nacional. Com base no decreto nº 10.569, de dezembro de 2020, o governo estabeleceu um ponto de ênfase crucial na proteção das infraestruturas críticas. Foi implementada a Estratégia Nacional de Segurança das Infraestruturas Críticas (ENSIC), encarregada de preparar setores como comunicações, energia, transporte, sistemas de água, finanças, entre outros, para integrarem o conjunto de organismos de capacidade nacional (LUCAS 2023). Portanto, a implementação da ENSIC representa um marco significativo que colaborou na questão do fortalecimento das capacidades cibernética. É pouco conhecida, todavia é vista como um esforço para proteger setores vitais e assegurar a “resiliência” do país diante das ameaças.

De acordo com o Security Report (2019), no período entre 2012 e 2018, o investimento no setor de segurança cibernética foi notoriamente negligenciado, totalizando apenas 125 milhões de Reais. Surpreendentemente, em contraste, o setor nuclear recebeu uma alocação substancial de cerca de 7 bilhões de Reais. Este desequilíbrio financeiro levanta um paradoxo intrigante, destacado por um senador da República, que questionou e ficou sem uma resposta clara, o porquê de o investimento no setor nuclear ser maior do que no cibernético, considerando que o setor nuclear carece de segurança cibernética, especialmente ao se pensar na infraestrutura crítica (Senado 2019).

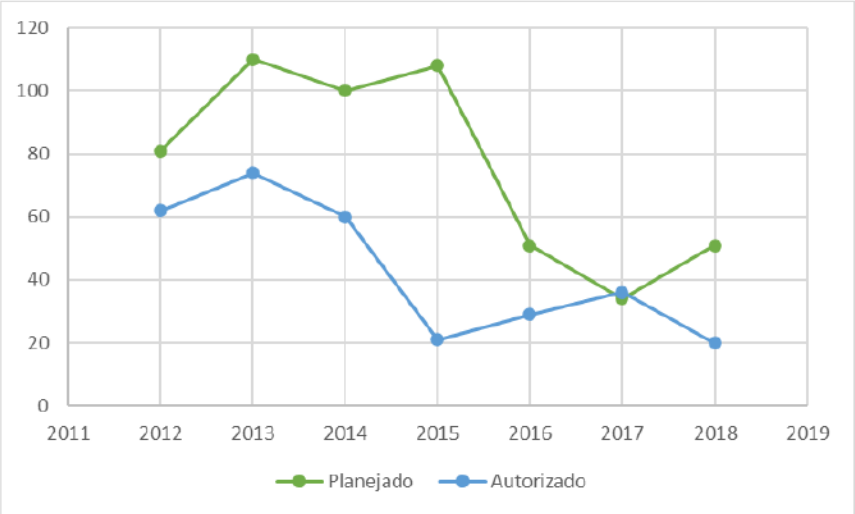
Com base na proposta da segunda hipótese, entende-se que os setores estratégicos do país passam por dificuldades em relação aos valores estimados para as áreas. Por tanto, aqui faz-se-rá uma apuração dos dados para comprovação da hipótese.

Uma análise mais aprofundada revela que a diferença entre o planejado e o autorizado pode ser atribuída a uma falta generalizada de conhecimento sobre as ameaças cibernéticas, prioridades estratégicas desalinhadas e influências políticas, que poderia ser solucionada com treinamentos e implementações de medidas de segurança, 2FA por exemplo. No entanto, ao julgar o argumento sobre o setor nuclear,

por exemplo, é crucial destacar que essa diferença não apenas evidencia um descaso em relação ao setor à cibernética, mas também ressalta a necessidade urgente de ações corretivas para abordar as lacunas existentes já que não se tem sido autorizado os valores planejados para investimento na área, o que por consequência interfere na falta de qualificação, pesquisa e desenvolvimento.

Apesar de ser considerada uma prioridade para o Estado Brasileiro, observa-se em evidente a relação ao setor de segurança cibernética, conforme ilustrado no gráfico abaixo.

FIGURA 3: Gastos do Brasil em Defesa e Segurança Cibernéticas entre 2012 e 2018



Fonte: BRASIL, 2018.

A partir do gráfico, assim como entende Pagliari e Favero (2023), fica claro que o governo adota uma estratégia de investimento com baixa consistência, alocando um montante significativamente inferior ao planejado. Para se ter uma ideia, segundo o Senado (2019), o orçamento destinado à cibernética no Brasil em 2020 teve um déficit de R$41 milhões, conforme indicado por um relatório[29] sobre a Política

[29] Ver mais em: https://www12.senado.leg.br/noticias/audios/2019/12/cre-aprova-relatorio-com-sugestoes-para-a-politica-de-defesa-cibernetica > CRE aprova relatório com sugestões para a política de defesa cibernética, Agência Senado, 2019.

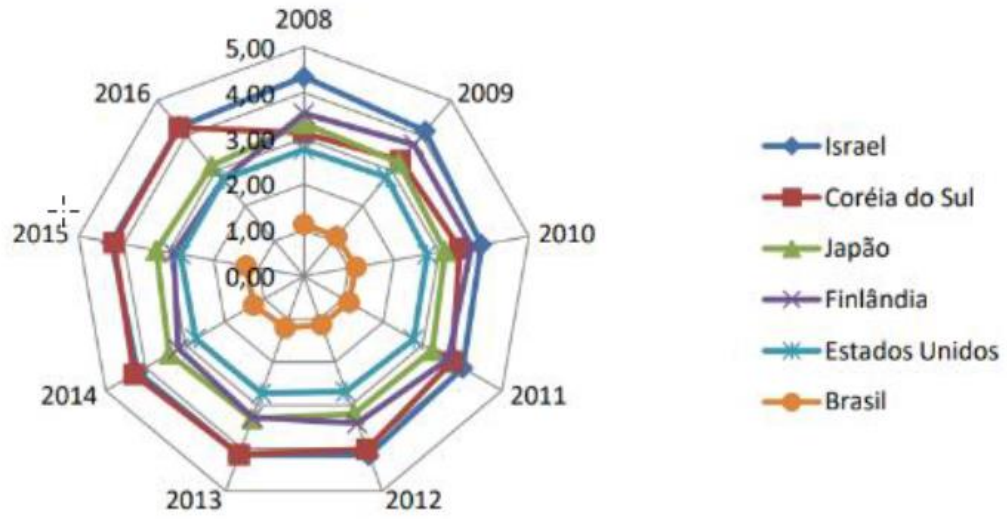
Nacional de Defesa Cibernética. No documento, revela-se que o Executivo alocou apenas R$19 milhões para esse fim, enquanto a recomendação mínima apontava a necessidade de pelo menos R$60 milhões. Ainda segundo o relatório, a escassez de recursos financeiros direcionados à cibernética no Brasil em 2020 reflete a negligência política e burocrática, evidenciando uma lacuna na abordagem governamental para enfrentar os desafios emergentes.

O investimento, sendo a variável fundamental do planejamento estratégico nos traz a relação com a criação de capacidades (2018). A concepção fundamental sobre a relação entre poder e investimento é ilustrada por Faver (2022, 65), indicando que “um aumento nos investimentos resulta em uma ampliação correspondente das capacidades”. Ainda segundo o autor, é necessário direcionar investimentos para recursos de "ordem material e imaterial" (FARIAS e FERRAZ 2018), como sistemas de segurança e informação, redes de transmissão, softwares e hardwares, para além da especialização técnica (P. H. FAVERO 2022).

A visibilidade da relação entre capacidade e investimento é retratada por Favero (2022, 66), quando é explicado sobre o estudo das nossas estruturas defasadas de segurança cibernética, onde o autor conclui que elas não são eficientes e necessitam urgentemente de uma atualização e novos investimentos. Para o autor, se fossem gerados investimentos para inteligência cibernética, certamente isso aumentaria a capacidade de dissuasão do Brasil.

Com base no estudo, é possível ainda apresentar uma outra variável, a própria tecnologia. No Brasil, o investimento em P&D é tão baixo que, em comparação com a discrepância de recursos destinados a outras áreas é possível até equiparar aos gastos do congresso. De acordo com a figura abaixo é possível notar a diferença de investimento de seis países diferentes na segurança cibernética.

Figura 4 – Investimento em porcentagem do PIB de Brasil, Israel, Coréia do Sul, Japão, Finlândia e Estados Unidos



Fonte: Fonseca, 2018 (apud Favero 2022)

Conforme os dados da figura, identifica-se que o investimento anual do Brasil é de cerca de 1% do PIB para P&D. Esse baixo investimento tem sido pauta de debates no senado pois tem sido algo que interfere nos projetos das áreas estratégicas do país, culminando também no baixo repasse para a área cibernética. Em comparação aos países da imagem, tem-se nos Estados Unidos, o investimento em porcentagem do PIB chega a 4,85% (Cisco 2020) somente para segurança cibernética e, ainda mais engajado, Israel com o investimento médio de 15% do PIB (GlobalXT 2022).

Por sua vez, segundo os dados do IPEA (2023), o montante destinado à toda área de pesquisa e desenvolvimento (P&D) no Brasil equivale a cerca de R$11 bilhões ao ano. Esse valor é considerado baixo ao ser contrastado com os recursos destinados por exemplo para o Congresso Nacional, onde este por sua vez tem arrecadado R$10,8 bilhões anualmente (ConvergenciaBrasil 2022).

Portanto, até o momento, e devido a limitações de dados, não se confirma e nem se nega a veracidade da segunda hipótese, no que persiste o desafio de assegurar um orçamento adequado para a segurança cibernética. Com recursos substancialmente inferiores ao que era esperado, torna-se uma tarefa complexa alcançar objetivos de longo prazo, especialmente os vinculados ao desenvolvimento de tecnologia de vanguarda. Apesar de a segurança cibernética figurar como um setor

estratégico nos documentos de defesa e segurança do Brasil, observa-se um desequilíbrio entre a prioridade estabelecida na política e o investimento efetuado no avanço desse campo.

4.1 - Desafios e Avanços na Legislação Brasileira de Segurança Cibernética: Da Incerteza à Evolução Contínua

Ao realizar uma análise comparativa entre o artigo “Desafios Estratégicos para a Segurança e Defesa Cibernética” (BRASIL, SAE 2011) da Secretaria de Assuntos Estratégicos da Presidência da República e o artigo “Proposta de Avaliação da Política Nacional de Segurança da Informação” (SANTOS, et al. 2022), observa-se que, ao focar nos dados relacionados ao âmbito da administração pública, torna-se evidente que nosso principal desafio persiste na incerteza em relação ao progresso da legislação brasileira na área.

Ambos os documentos, produzidos após espaçamento temporal de uma década, destacam a crescente importância da "era da informação" e a necessidade imperativa de proteção dos interesses nacionais no espaço cibernético (SANTOS, et al. 2022). Ao observar essa evolução temporal, aparecem algumas questões, relativamente críticas, sobre a eficácia nas respostas dadas desde a introdução do ciberespaço na agenda de segurança do Brasil até o presente momento, frente à complexidade destas ameaças cibernéticas.

De acordo com o artigo da SAE (BRASIL, SAE 2011), aponta-se a incerteza sobre o avanço da legislação brasileira na área como o principal desafio à época[30]. No entanto, ao longo da última década, a persistência dessa ‘análise’ indicado em 2011 sugere que nós passamos por uma 'inércia'[31] no desenvolvimento destas mesmas políticas. Todavia, quando um caso desses cai na mídia ou está sendo discutido pela representação da sociedade, traz à tona questionamentos quanto à nossa (governo) capacidade em antecipar e enfrentar adequadamente as ameaças cibernéticas (BRASIL, SAE 2011). Ao mesmo tempo, nota-se um aumento alarmante de crimes cibernéticos cujos prejuízos financeiros impactam tanto a indivíduos quanto as empresas (SANTOS, et al. 2022).

[30] Isso já tinha sido levado em consideração em 2011, e mesmo assim só mais para frente que surgiram as leis na área.
[31] Lê-se negligencia.

Segundo a fortinet *ibidem* Jornal da USP (2023) com um exemplo mais recente, só em 2022 presume-se que ultrapassaram 100 bilhões de ameaças e tentativas de ataques no Brasil, e ainda que estamos passando por uma crescente de 94% por semestre (CLARANET 2022). No entanto, apesar do governo reconhecer esses desafios, a eficácia das medidas adotadas até agora é limitada, voltando ao que já foi apresentado no capítulo 3, de que a resposta atual - tanto política quanto de segurança e defesa - não acompanhou a crescente incidência desses casos.

Ressalta-se que tanto Claranet, quanto a Forinet enfatizam a necessidade de uma abordagem proativa e coordenada para lidar com estas ameaças, mas que a aparente falta de coordenação efetiva entre as instituições públicas, órgãos e instituições privadas responsáveis pela segurança cibernética no Brasil levantam dúvidas sobre a capacidade do país de responder de forma eficaz e rápida a incidentes cibernéticos, especialmente em uma era de crescente interconexão e dependência tecnológica (NYE 2010).

> "Diante desses desafios, instituições públicas e privadas precisaram regular as atividades de segurança através de políticas, visando orientar os procedimentos referentes à segurança cibernética. Diversos países têm suas políticas e estratégias relacionadas à segurança cibernética publicadas de forma ostensiva. De igual forma, o meio acadêmico também tem acompanhado as discussões nacionais e internacionais acerca do tema, tanto no aspecto da elaboração de políticas quanto na criação de medidas de natureza cibernética que ampliem a segurança das instituições e das sociedades, em última análise" (SANTOS, et al. 2022)

Assim, justifica-se não apenas o que foi apresentado ao longo do capítulo 3, mas também a proposta apresentada neste capítulo, que visa compreender como o Brasil pode fortalecer suas capacidades de enfrentar os desafios emergentes no campo cibernético, sobretudo assegurando a proteção de seus interesses nacionais, através do investimento do valor planejado para desenvolvimento, treinamento atualização de tecnologia existentes e na pesquisa e criação de políticas de segurança robustas.

Mediante a revisão das políticas de segurança cibernética estabelecidas até 2020, a análise da classificação governamental em relação à segurança cibernética e a exposição do progresso das nossas capacidades, argumenta-se que a chave desse problema está não somente, mas na coordenação e reestruturação de atribuições.

Além da importância em se ponderar sobre a necessidade de colaboração entre Estado-Empresas-Sociedade civil, dada a natureza do problema, através de editais de projetos, abertura para pesquisa e até mesmo pregões eletrônicos para parcerias.

É necessário entender que a legislação de políticas de segurança cibernética e as doutrinas de segurança cibernética deveriam ser elaboradas pelo Brasil como um todo e não apenas de órgãos ou agências individualmente, para evitar invalidar ou até mesmo reduzir a operacionalidade de outras entidades (BRASIL 2020).[32] A ideia de segurança do ciberespaço gera muita indagação sobre “quem atua com o quê?”, onde até então, antes de 2014, nem existiam leis que punissem crimes cibernéticos, sendo estes aplicados e julgados como outros crimes previstos na Constituição e invalidados juridicamente por não haver sessão específica (CUNHA 2018).

Nos últimos anos, houve um aumento significativo no número de crimes relacionados à segurança cibernética. Paralelamente, instituições privadas têm solicitado a implementação de uma política institucional específica para lidar com conflitos, invasões e crimes cibernéticos (BRASIL 2014). Estes pedidos, de acordo com Dupas e Vigevani (1999) inclusive fizeram parte de um movimento internacional que tratava da criação de leis internacionais para problemas desta natureza. Atualmente, têm chamado atenção golpes relacionados à venda de terrenos, serviços e produtos, e até mesmo prometendo uma nova vida no metaverso criado no espaço cibernético.

Por conta disso, no Brasil, as legislações que tratam dos crimes cibernéticos só foram passar por um processo de evolução constante por volta de 2018. Como dito anteriormente, durante um período de oito anos, houve incerteza sobre a base legal de condução destes crimes, já que não existiam leis específicas para lidar com eles. No entanto, a situação muda de forma significante a partir da lei Nº 12.737/2012 (Lei Carolina Dieckmann), que definiu punições específicas para crimes como invasões de dispositivos e sistemas, bem como para a divulgação não autorizada de informações pessoais na internet.

Em 2018, entrou em vigor a Lei Nº 13.709/2018, intitulada "Lei Geral de

[32] Acredita-se que concentrar essas políticas em nível nacional, ao invés de distribuí-las em diversas entidades, pode resultar em uma abordagem mais eficaz e consistente para a segurança cibernética.

Proteção de Dados" (LGPD), que regula o tratamento de dados pessoais, impondo obrigações e responsabilidades claras para as instituições que lidam com informações pessoais. Essa legislação não busca só proteger a privacidade dos indivíduos, mas também impor sanções para, se caso, ocorra o vazamento de dados e violações de privacidade de segurança cibernética. Estas leis marcam avanços significativos na consolidação da legislação brasileira relacionada à segurança cibernética e à proteção dos dados pessoais. Isso porque elas estabelecem um alicerce jurídico mais sólido para abordar os crescentes desafios no cenário digital.

Contudo, a evolução legislativa nesse campo ainda está se desenvolvendo, uma vez que tanto a tecnologia quanto as ameaças cibernéticas permanecem em constante evolução. Portanto, torna-se imperativo manter uma adaptação contínua das políticas e regulamentações vigentes para acompanhar essa dinâmica em evolução.

Neste contexto, surge uma crítica intrigante. Para abordar o problema dos crimes cibernéticos, não é suficiente apenas investir em tecnologia avançada e software de segurança. É essencial também promover a educação. Ao contrário da simples ideia de que alguém que cometa um roubo será preso, deveria haver uma conscientização de que cada indivíduo precisa adotar medidas de segurança cibernética. Podendo exemplificar a autenticação de 2 fatores (2FA), backup de dados e conscientização sobre senhas e phishing.

Em suma, as capacidades de segurança cibernética no Brasil têm avançado consideravelmente ao longo dos anos, culminando na implementação de leis específicas e regulamentações (como a Lei Carolina Dieckmann e a LGPD). No entanto, o desafio persiste, pois, as ameaças cibernéticas continuam mudando. Para garantir a proteção eficaz dos dados e a mitigação de riscos cibernéticos, é crucial que o Estado trabalhe em iniciativas e que defina com clareza o papel dos órgãos que tratam dessa temática.

4.2 - O Cenário Brasileiro de Segurança Cibernética, das Instituições aos Desafios Atuais

Chegamos a um ponto crucial em nossa pesquisa, no qual discutiremos nossa situação atual. Nesse aspecto, surgem duas premissas importantes. A primeira

aborda o tópico anterior: qual é a realidade das capacidades de segurança cibernética no Brasil? A segunda explora como isso afeta o dia a dia do país. Além disso, trata-se também das reflexões voltadas para a primeira hipótese tratada.

No âmbito territorial hoje, podem ser citados pelo menos onze composições[33] que trabalham segurança cibernética, conforme mostra a tabela 2 a seguir:

TABELA 2 – Composição de agencias com base nas suas funções principais e ano de criação.

Órgão/Agência/Lei	Funções Principais	Ano de Criação
Gabinete de Segurança Institucional da Presidência da República (GSI/PR)	Formulação e coordenação de políticas de segurança cibernética em nível federal.	Não especificado
Centro de Tratamento de Incidentes de Segurança Cibernética (CTIR)	Monitoramento e coordenação de respostas para incidentes de segurança cibernética em âmbito do Estado.	-
Agência Nacional de Telecomunicações (ANATEL)	Regulação do setor de telecomunicações com interesse em questões de segurança cibernética relacionadas a redes de comunicação.	1997
Polícia Federal	Investigação de crimes cibernéticos e crimes na internet.	1944 (Polícia Federal)

[33] Diz-se ‘composições’ pela possibilidade de influenciarem outras agências, por exemplo PRF, MJ, BACEN e outros.

Forças Armadas (Exército, Marinha, Aeronáutica)	Participação na defesa cibernética, especialmente em relação à infraestrutura crítica. (ComDCiber; CDCiber)	-
Agência Brasileira de Inteligência (ABIN)	Dizem eles que fazem coleta de informações relacionadas à 'segurança cibernética, inteligência e contrainteligência'.	1999
Ministério da Ciência, Tecnologia e Inovações	Desenvolvimento de iniciativas de pesquisa em segurança cibernética.	-
Governos Estaduais e Municipais	Responsável por 'iniciativas' e órgãos relacionados à segurança cibernética a nível estadual e municipal (polícia civil).	-
NIC.br (Núcleo de Informação e Coordenação do "ponto br")	Monitoramento sobre os domínios ".br", coordenação de IPv6, pesquisa e desenvolvimento, educação e conscientização sobre Internet.	2005
Lei Geral de Proteção de Dados (LGPD)	Responsável pela regulamentação de proteção de dados pessoais e privacidade.	2018
Comitê Gestor da Internet no Brasil (CGI--BR)	Aquele quem deveria cuidar de políticas públicas, diretrizes e princípios éticos e técnicos para a Internet no Brasil.	1995

Fonte: Elaborado pelo autor a partir de dados extraídos de GSI/PR. ANATEL, DPF, ABIN, Ministério da Ciência, Tecnologia e Inovações, NIC.br, LGPD, CGI.br e diário oficial do estado do Pará, São Paulo e DF.

A análise da imagem pode se tornar ainda mais valiosa se a categorizarmos com base na distinção entre aqueles que se dedicam à segurança cibernética, como ANATEL, CTIR ou a própria LGPD e aqueles que estão envolvidos com a defesa cibernética, como o MD e as FA – ComDCiber, CDCiber ou GSI/PR -. Entender a composição de agências e órgãos, conforme detalhado na imagem anterior, que tem responsabilidade no que tange segurança cibernética no Brasil é essencial para compreender como o país aborda problemas críticos relacionados à área.

O impacto dessas organizações na sociedade é significativamente direto quando se pensa na influência que geram para o dia a dia de pessoas e empresas. Entende-se que é necessária uma estrutura bem-organizada e eficiente para fortalecer a proteção contra ataques, assim como promover um ambiente cibernético seguro e confortável para aqueles que fazem uso (FERREIRA 2020).

Por outro lado, as lacunas e falhas que existem nesta estrutura por conta da questão da competência de ações resultam na vulnerabilidade e exposição de crimes e ameaças além de impactar na governança – administração e coordenação - que norteia o brasil, afetando investigações e desenvolvimento de estratégias na área (COSTA, FERREIRA e CABRAL 2022).

A estrutura atual de leis e organizações relacionadas à segurança cibernética no Brasil parece enfrentar dificuldades para se manter atualizada diante dos desafios em constante evolução do ciberespaço (CISCO 2021). Leis como LGPD, que regem essa área e as instituições, como ANATEL ou ANPD, e encarregadas de sua aplicação e supervisão constituem os pilares desta estrutura e elas estão fragilizadas devido ao grande número de golpes e crimes que crescem no Brasil, assim como ataques e malwares na infraestrutura nacional.

Na tabela anterior é possível observar uma notável abertura temporal que ocorre em momentos nos quais a capacidade do Estado em assegurar a segurança cibernética é posta à prova, e a própria base legal, representada pela doutrina e livro verde, ressalta a necessidade de trabalharmos para anteciparmos os problemas.

No entanto, ainda de acordo com o estudo da CISCO (2021) o rápido avanço das ameaças cibernéticas e a crescente complexidade das tecnologias digitais revelam uma lacuna significativa entre as necessidades atuais e a capacidade da infraestrutura existente para lidar eficazmente com elas. Como resultado, há uma urgente necessidade de reformas, atualizações e abordagens inovadoras para fortalecer a segurança e proteger os sistemas contra ameaças cada vez mais sofisticadas (CISCO 2021).

Malagutti (2022) em seu livro[34], conduz uma análise comparativa desses aspectos com outros cinco países. Essa análise revela que, é por conta do ComDCiber e do GSI, que o Brasil ainda consegue possuir uma presença limitada em um setor estratégico em comparação com outros Estados.

TABELA 3 – Comparação de USA, China, França, UK, Alemanha e Brasil sobre agencias e estrutura de segurança e defesa Cibernéticas.

País	Intel.	Contra Intel.	Segurança	Defesa	Ataque	1ª NCSS	Ativos
USA	NSA CIA NGA	FBI	DHS NIST	NSA	USCyberCom	2003	7.000 (NSA) 6.200 (USCyberCom)
China	3rd Dep (EM-EPL)	3° Dep (EM-EPL)	3° Dep (EM-EPL)	4° Dep (EM-EPL)	4° Dep (EM-EPL)	2003	"centenas ou milhares" (Unit 61398)
França	DGSE	DGSI	ANSSI	CALID	ComCyber	2008	3.500 (CyberCom) 600 (ANSSI)
UK	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ & MoD	2009	1.900+ (NCSC) 2.000 (NCF)
Alemanha	BND BSI KSA	BfV	BSI	CIR	CIR	2011	13.600 (CIR)
Brasil	N/A	N/A	GSI/DSIC	ComDCiber	ComDCiber	2020	180~

Fonte: Malagutti, 2022, p.20

Um aspecto que pode ser percebido no trabalho de Malagutti (2022) é que quando comparamos no âmbito da inteligência e contrainteligência do Brasil com estes outros países, nossos órgãos responsáveis - tanto a ABIN quanto as forças

[34] leitura rica em dados sobre segurança cibernética. O autor faz uma análise comparada entre a segurança cibernética no Brasil e outros países que possuem uma agência nacional para segurança cibernética.

policiais - não conseguem ter o mesmo destaque em inteligência e contrainteligência (UCHOA 2013).

Isso é justificado quando temos o fato de que as agências têm suas atividades condicionadas e/ou limitadas através de leis e regulamentos específicos (COSTA, FERREIRA e CABRAL 2022), diferentemente de países como os EUA, onde as agências de segurança podem operar com maior autonomia em casos de percepções de caos, incluindo a necessidade de ações domésticas (ACLU 2013).

No entanto, existem restrições legais - como exemplo básico tem-se a própria constituição federal, que estabelece limites para as atividades de investigação e coleta de informações, justificando garantir direitos individuais como a privacidade e a inviolabilidade do domicílio - e diferenças em suas atribuições que podem afetar suas atividades nesses campos. Além disso, o autor destaca que alguns dos países analisados atuam através de instituições independentes, enquanto outros atuam com comandos específicos que reúne indivíduos de outros órgãos do governo para montar um ‘comando unificado’ (MALAGUTTI 2022, 19).

Este tipo unificação parece ser interessante quando pensamos em vantagens como eficiência em coordenação de atividades, compartilhamento bruto e direto de recursos, além da flexibilidade existente para adaptação a mudanças de cenários. O que também traz como desvantagens pontos como burocracia e complexibilidade de camadas para ações e dependência de estrutura, podendo agregar em falhas ou problemas internos.

Tomando a ABIN como exemplo, ela assume um papel institucional tanto em inteligência quanto em contrainteligência. No entanto, a execução dessas responsabilidades no âmbito cibernético é pouco conhecida ou divulgada, não somente pela natureza de sigilo, até porque no Brasil hoje “não há na legislação brasileira uma definição precisa do que seja segredo de Estado” (CONDEIXA 2015), mas porque a atividade oferecida ao longo dos anos foi voltada para o asseguramento do acesso de informações para o executivo (COSTA, FERREIRA e CABRAL 2022). Consequentemente essa falta de transparência dificulta a colaboração com outras entidades e o setor privado, criando lacunas na segurança e defesa cibernéticas nacional.

Como exemplo disso podemos analisar a gestão do governo liderado pelo executivo durante o período de 2019 a 2022. Nas tabelas abaixo podemos considerar várias denúncias que apontam para o uso da agência governamental para atividades políticas partidárias. Isso foi evidenciado em reportagens de veículos de imprensa como:

Origem	Reportagem	Local	Ano
FOLHA DE SÃO PAULO	"Abin sob Bolsonaro rastreou juiz e jornalista, suspeita PF"	São Paulo	2023
CORREIO BRAZILIENSE	"Moro diz que há desvio de finalidade na ação da Abin em benefício de Flávio Bolsonaro"	Brasília	2020
CBN	"Abin sob Bolsonaro teria sido usada para monitorar aliados, caminhoneiros e ambientalistas"	Rio de Janeiro	2023

Não somente isso, também existem as constantes denúncias de uso de softwares espiões pela agência:

Origem	Reportagem	Local	Ano
GLOBO	"Programa espião usado pela Abin para monitorar celulares deixou expostos dados estratégicos em servidor em Israel"	Rio de Janeiro	2023
BBC	"Pegasus: o que é o sistema que espionou jornalistas, ativistas e advogados"	Londres	2021
JORNALP360	"Governo avalia punir empresas de espionagem que não têm aval da Abin para agir"	DF	2020

As denúncias levantadas sugerem possíveis abusos de poder e desvio de finalidade por parte da ABIN para o Executivo. Estas alegações de uso político da agência, incluindo monitoramento de opositores e exposição de dados sensíveis, levantam sérias preocupações sobre a integridade da instituição e a proteção dos direitos individuais dos cidadãos. Essas acusações destacam a confiança e põe em jogo a transparência do órgão

Por outro lado, a Polícia Federal, um dos órgãos mais prestigiados do país, é uma instituição vinculada ao Ministério da Justiça com o objetivo de cumprir a lei, tendo jurisdição sobre uma ampla gama de crimes, incluindo crimes cibernéticos, contrabando, tráfico de drogas e corrupção. No entanto, na prática, além da falta de tecnologia (equipamentos e softwares) e até mesmo pessoal capacitado (ADPF 2017) para lidar com crimes cibernéticos, a atuação da Polícia Federal está sujeita a

salvaguardas legais, exigindo autorização judicial para realizar atividades nesse âmbito. No âmbito da política de segurança cibernética, implica dizer que esse desafio evidencia a necessidade de formação e desenvolvimento para investigação e punição de crimes cibernéticos, assegurando eficácia e mostrando respeito aos direitos civis na questão de preservação de leis e minimizando a questão do problema com abuso de poder que isso pode gerar.

Dessa forma, percebe-se que se trata das limitações operacionais que envolve a Polícia Federal em relação aos crimes cibernéticos, se nota uma lacuna significativa na capacidade do Estado de lidar adequadamente com ameaças cibernéticas, caracterizada pelo fato de o Brasil ser um dos países com maior número de golpes e crimes relacionados ao ciberespaço, sendo na américa latina o segundo (exame 2023).

Isso evidencia a necessidade de uma revisão – de políticas e leis - urgente das políticas e estratégias de segurança cibernética, a fim de fortalecer – regulamentação e segurança - as capacidades de resposta do país diante da emergência. De forma direta, a maioria das nossas capacidades (financeira e pessoal) de segurança cibernética está direcionada para a defesa contra ameaças cibernéticas, em vez de para a segurança cibernética em si. Enquanto as ameaças cibernéticas representam os potenciais perigos ou ataques que visam comprometer a segurança dos sistemas, redes ou dados que gerenciamos, a segurança cibernética abrange não só a defesa contra essas ameaças, mas também a implementação das medidas e das práticas responsáveis por garantir a proteção, integridade e disponibilidade das informações e infraestruturas (FARIAS e FERRAZ 2018).

Conforme ressaltado por Malagutti (2022), desde a criação do CDCiber até o lançamento de uma estratégia de segurança cibernética (E-Ciber), o Brasil tem alocado recursos para o fortalecimento de sua infraestrutura de defesa cibernética. Com isso, surge a E-ciber, que, em vez de se apresentar como um manual ou uma estratégia para uma questão complexa, acaba se assemelhando a um artigo acadêmico que busca explicar um eixo temático voltado para a proteção e segurança

cibernética no país[35] (PECK 2020). Segundo Malagutti (2022), o documento possui o alicerce de uma carta de boas intenções e não apresenta claramente as responsabilidades e recursos das ações às quais se propõe complementar, ao contrário do que espera de uma Estratégia, onde precisa ser um documento forte, mostrando os pilares, deveres e medidas de análise, contenção e mitigação dos problemas. Assim, voltando a questão da hipótese proposta, é possível identificar que existem problemas nas interações entre os agentes, podendo delimitar a afirmação da primeira hipótese.

O autor ainda compara o documento com o projeto similar de outras 14 economias e, nessa comparação, algo interessante é observado, além do Brasil ter desenvolvido uma 'estratégia' cibernética muito atrasada, quando comparado com outros países como Itália, França e Reino Unido, o plano exclui explicitamente a ideia da ciberdefesa, impactando na falta de informações para o futuro da defesa cibernética pelo Brasil.

Se entende por uma 'estratégia atrasada' quando está defasada em relação às práticas reais, tecnologias e políticas adotadas por outras entidades e/ou países em um determinado campo, que neste caso, considera-se a segurança cibernética. Concordando com Malagutti (2022), a estratégia cibernética brasileira é considerada atrasada em relação a países como Itália, França e Reino Unido.

> Além de bastante atrasada, a e-Ciber ‘fica aquém’, falhando em todos os quatro pilares que constroem uma boa estratégia nacional de defesa e segurança. Em primeiro lugar, não comunica o que é essencial para o exercício da influência estatal e a consecução dos fins pretendidos. É, de fato, ‘tímida’ em suas intenções, com muitos ‘faria’ e poucos ‘fará’. Em segundo lugar, não mantém a coesão linguística para criar significado e unidade. Terceiro, não considera que as ações propostas sejam de longo prazo e que sua correção ou adequação em caso de erro seja um processo demorado e desafiador. Quarto, embora indique os objetivos pretendidos, não especifica responsabilidades e recursos para que as ações pretendidas atinjam (e mantenham) seus objetivos. A e-Ciber parece, na prática, uma carta de (boas) intenções, não uma estratégia nacional. A jabuticaba de

[35] Diferente de um texto de relatório de política nacional, a E-Ciber não tem a destinação de comunicar as decisões em torno do nível estratégico. O texto carece de especificações e diretrizes quando realmente se trata das ações no âmbito da segurança cibernética. Além disso, faz referência ao Marco Civil da Internet e LGPD, mas não traz questões que envolvam segurança e defesa cibernéticas como ponto de segurança e defesa nacional.

> dividir as estratégias de cibersegurança e ciberdefesa corre o risco de fazer com que duas se tornem nenhuma: nem segurança nem defesa. (MALAGUTTI, 2022, p.73).

Neste contexto, as críticas direcionadas ao documento evidenciam que a e-Ciber, enquanto documento de estratégia nacional de defesa e segurança cibernética, apresenta deficiências expressivas. Reconhece-se que há a necessidade imediata de aprimoramento para corrigir falhas estratégicas. Portanto, a e-Ciber, embora seja o primeiro passo para um avanço, carece de refinamentos substanciais “revisão” a fim de atender de forma mais eficaz à complexidade e da realidade que envolve a cultura de segurança cibernética no Brasil, como identificação de lacunas, definição de recursos e responsabilidades e participação de stakeholders.

4.3 – CiberRI e Segurança do Ciberespaço Brasileiro

Após apresentar todos esses aspectos, como podemos compreender a posição negligenciada do Brasil diante da segurança cibernética nas teorias das Relações Internacionais? Será que é vantajoso implementar estratégias para fortalecer a segurança cibernética?

A importância de entender o Brasil como um Estado soberano, com suas fronteiras e leis internas, não exerce influência nas Relações Internacionais Cibernéticas (CUNHA 2018). Isso ocorre porque estamos lidando com um domínio que não conhece limites, que é incontrolável, tornando-se, assim, o nosso maior desafio.

Com um exemplo, entender o Brasil como Estado soberano implica que – comparando com o exemplo de uma pessoa e uma casa -, o país tem o direito e a capacidade de tomar suas próprias decisões sobre como proteger seu território, sistemas, informações e infraestruturas.

É como uma pessoa que tem o controle da sua própria casa e decide como protegê-la contra possíveis ameaças. Assim como um morador pode decidir instalar sistemas de segurança, contratar uma ronda ou comprar uma arma para proteger sua residência, o Brasil, na ideia de Estado soberano, pode implementar estratégias e políticas para fortalecer sua segurança cibernética. Ao mesmo tempo, pode interagir com países vizinhos ou não, na busca de colaboração e conhecimento mútuo para

resolver os desafios compartilhados no século XXI, assim como na relação de vizinhos que podem se ajudar a manter a segurança em um bairro.

Pensando dessa forma, é vantajoso implementar estratégias para fortalecer a segurança cibernética, já que elas protegem nossa infraestrutura contra ameaças como hackers e malwares, prevenindo perdas financeiras, roubo de dados e interrupções nos serviços básicos e fundamentais. A execução de uma estratégia eficaz, tem como consequência a promoção da confiança pública, crescimento econômico e aumenta a segurança para a ideia de privacidade.

Anteriormente, discutimos a história e a ideia de que a securitização ou o desenvolvimento de uma teoria focada na segurança cibernética como parte das Relações Internacionais era algo relevante. Voltando ao debate, o conceito da securitização, segundo Buzan (1998), busca considerar os temas tradicionais que a princípio não tem relação base com segurança convencional e justificar ações exponenciais para transformar esses temas em questões de segurança – o espaço cibernético por exemplo tem sido securitizado devido as ameaças cibernéticas.

No entanto, após analisar e desenvolver este trabalho, percebeu-se que a ideia de se securitizar a cibernética – ou seja, dizer que a cibernética precisa ser gerenciada como um problema de segurança nacional - no brasil está sujeita a inúmeros desafios. Isso ocorre porque a adição de mais uma teoria não necessariamente aumentaria a prioridade da área no país, uma vez que, como explica Barragan (2008) as teorias servem para nos ajudar a entender as estruturas conceituais e utilizá-las como ferramentas de análises para compreender e até mesmo explicar os fenômenos. Todavia, uma teoria a mais pode não ser o suficiente para determinar a existência ou consistência de uma política cibernética no Brasil. O que deve ser entendido é que a qualidade e a relevância desta teoria oferecem uma maior capacidade de conscientização e apoio de profissionais, possibilitando o desenvolvimento e a implantação de políticas eficazes.

Além disso, é importante reconhecer que a segurança cibernética é um tema que, em sua maioria, atrai um público muito específico[36]. Essa observação também

[36] Meio que as RI estão mais ligadas com diplomacia, análises de políticas internacionais ou comércio exterior.

se relaciona com a abordagem da securitização do ciberespaço, que seria transformar questões ligadas à segurança cibernética em preocupações de segurança e importância nacional.

Por tanto, pensar nessa integração para o setor cibernético nas CiberRI, implica destacar que sim, é de estrema importância implementar novas estratégias para o setor cibernético em âmbito nacional. Isso porque acredita-se que o Brasil está progredindo rumo à segurança cibernética devido ao aumento da conscientização sobre os desafios e riscos relacionados à proteção de indivíduos e do Estado.

Dentro desse contexto, investir em infraestrutura tecnológica é uma peça de extrema importância, isso pode ser feito com o desenvolvimento de centros de operações de segurança avançados (SOCs) e a adoção de tecnologias emergentes, como gestores de vulnerabilidades – ferramentas de avaliação e identificação que podem ser configuradas em sistemas, redes e estruturas de organizações -, são essenciais para detectar e mitigar as ameaças de forma eficaz.

No entanto, ao refletirmos sobre CiberRI e a securitização do ciberespaço, torna-se evidente a relação de causa e efeito, graças ao aumento das ameaças cibernéticas e pela resposta do Estado em securitizar esse ambiente. Com a ideia da causa, afirma-se que o processo de securitização envolve uma variedade de medidas, que vão desde o aumento expressivo das ameaças cibernéticas até a rápida incorporação de tecnologias digitais no país. Porém diante de uma evolução constante dos meios informacionais, imagina-se que se gera também uma pressão para priorizar a segurança no ciberespaço.

Os efeitos dessa securitização, em teoria seriam promissores, já que além da proteção da soberania, um ambiente cibernético seguro estimula a inovação e o desenvolvimento tecnológico, impulsionando a economia digital do país, investimento externo e integração entre sociedade-empresas-Estado. No entanto, talvez seja precisamente por essas razões que ela não seja aplicável no Brasil.

Sabe, quando alguém sai da graduação em Relações Internacionais e está entusiasmado com a ideia de estudar segurança internacional, a securitização pode parecer a abordagem mais adequada para todas as discussões. No entanto, a

realidade é mais complexa, uma vez que nem todos os tópicos se encaixam nessa teoria. Mesmo que um tema possa suscitar preocupações no âmbito estatal, devemos reconhecer que a securitização não é a abordagem mais adequada para todos os casos.

Essa perspectiva se torna especialmente relevante quando buscamos identificar os fatores que limitam a efetividade de políticas voltadas para a segurança cibernética em âmbito institucional. Se percebe então que a questão no Brasil não se restringe apenas à ausência de investimentos e ao aprimoramento das políticas. Há também uma carência na busca de conhecimento por parte da população, justificado por desinformação e baixa priorização do tema em consideração outros assuntos como meio ambiente e corrupção. Comparando com a proposta da terceira hipótese, percebe-se que a falta de confiança em assuntos de segurança com a população acaba prejudicando a relação existente entre o Estado e a sociedade, fazendo com que de fato os outros problemas 'básicos' se tornem complexos.

Neste ponto, retornamos à discussão das hipóteses apresentadas. Apesar de o Estado criar leis para prevenir o roubo de dados, golpes e phishing, a ausência de estímulos para iniciativas e a falta de educação cibernética dificultam a eficácia desse processo de segurança (SILVA 2022). No âmbito institucional, é desejável que uma política de segurança cibernética no Brasil seja uma variável constante - uma política de segurança cibernética no Brasil deve ter uma presença contínua e consistente, não apenas um documento estático- , indo além de ser apenas mais um documento explicativo sobre os diversos conceitos modernos relacionados ao conflito cibernético e suas ações correspondentes.

Por isso pensar nas CiberRI, não deve só ser um ponto que ocorre porque existem pessoas apaixonadas pela área e que sentem e sabem que deve ter mais importância nos estudos das Relações Internacionais. Isto deve acontecer mediante o reconhecimento da complexibilidade do ciberespaço, destacando a natureza incontrolável e limitada do desafio que é mapear a abordagem de segurança em um ambiente virtual, isso quando se reconhece a complexidade e os desafios de segurança no ciberespaço (LUCAS 2023).

A proposta de uma abordagem mais abrangente na política de segurança cibernética no Brasil vai além da simples elaboração de um documento explicativo (MALAGUTTI 2022). Busca-se transformar a segurança cibernética em uma variável constante, integrada em diversos níveis e setores da sociedade. O intuito disto é reconhecer a complexidade intrínseca do ambiente cibernético e a necessidade de uma resposta multifacetada para enfrentar os desafios emergentes (conflitos e crimes) (FERREIRA 2020).

Nesse sentido, a sugestão de torná-la uma constante reflete no entendimento de que “as ameaças no ciberespaço estão em constante evolução” (CAVELTY e WENGER 2022), assim visando não apenas reagir aos incidentes específicos, mas também estruturar uma mentalidade proativa que antecipe e se adapte continuamente às mudanças nas táticas dos atacantes (AYRES PINTO 2017).

A integração da segurança cibernética em diferentes níveis e setores da sociedade reconhece que a responsabilidade por proteger o ciberespaço não deve recair exclusivamente sobre entidades governamentais ou especializadas (IZYCKI, AYRES PINTO e LAVANDOSKI DA SILVA 2023). Em vez disso, propõe-se uma colaboração ampla que envolva o governo, o setor privado, instituições acadêmicas e a sociedade civil. Se isso ocorrer, criar-se-ia um ecossistema resiliente em que o conhecimento e os recursos são compartilhados, promovendo uma defesa mais robusta contra ameaças cibernéticas.

CONCLUSÃO

No contexto da segurança cibernética no Brasil, emerge um cenário complexo, caracterizado por uma série de desafios críticos que impactam a eficácia das políticas e a proteção das infraestruturas do país. Em resumo, pode-se afirmar que, apesar dos crescentes esforços de estudo e pesquisa, a segurança cibernética no Brasil ainda é um tema complexo e desafiador, por uma série de fatores. Entre eles, destaca-se a evolução dos ataques e ameaças, limitações orçamentarias e de investimento em tecnologias de defesa e segurança.

Neste trabalho, procuramos esclarecer quais fatores institucionais que impedem a consolidação eficaz da Política Nacional de Segurança Cibernética. Estes desafios incluem a falta de investimento adequado, uma distribuição de responsabilidades entre os órgãos de segurança e defesa considerada inadequada, bem como a carência de conscientização e educação na área. Além disso, constatamos que os objetivos propostos neste trabalho na introdução, desempenharam um papel crucial na obtenção das respostas, conforme detalhado e analisado ao longo do texto. Dessa forma, as principais questões enfrentadas pelo Brasil no âmbito da segurança cibernética (falta de desenvolvimento, políticas incompletas, falta de recursos e outros) podem ser claramente identificadas na confirmação das hipóteses a seguir.

Começando pela ideia de que existe uma fragmentação institucional na segurança cibernética[37]. O Brasil conta com diversos órgãos e agências governamentais envolvidos na segurança cibernética, o que resulta em uma fragmentação de responsabilidades e recursos, gerando também falta de coordenação e ação quando necessário. No âmbito legal, a legislação e regulamentação incompletas representam um desafio adicional. O país ainda carece de leis específicas e regulamentações claras relacionadas à segurança cibernética, o que dificulta a aplicação de medidas de proteção. Isso também pode ser destacado quando se refere às ações políticas e orçamentárias, que impactam na continuidade

[37] Hipótese 1: A falta de interação entre os agentes nacionais inviabiliza o condicionamento sobre o processo de moldagem político que daria efetividade na criação da política.

das políticas de segurança cibernética, fenômeno visível quando ocorre a mudança de governos.

Além disso, outro fator que limita as intenções na área é a falta de recursos adequados[38]. Este é um obstáculo significativo que, infelizmente, não afeta apenas a segurança cibernética, mas também setores-chave do Estado, como educação e saúde, a cibersegurança envolve mais do que apenas tecnologia. A alocação insuficiente de recursos financeiros e humanos para a área de segurança cibernética limita a capacidade governamental de desenvolver e implementar programas, sistemas, mecanismos e ações abrangentes. Com isso, a falta de conscientização e educação em relação à segurança cibernética é uma das maiores preocupações existentes. A ausência de educação cibernética nos próprios órgãos (como a própria Polícia Federal) mostra que as vulnerabilidades não se limitam à falta de equipamentos ou ao desenvolvimento de tecnologias.

Por fim, temos uma coordenação interinstitucional fraca, que se manifesta como um problema persistente entre diferentes órgãos governamentais, bem como entre o setor público e privado. A falta de confiança na sociedade e no setor privado representa um obstáculo significativo à colaboração entre empresas, instituições acadêmicas e o governo na proteção das infraestruturas críticas. É importante ressaltar que não se espera que a sociedade tenha 100% de participação nas atividades de segurança cibernética, pois isso também envolve questões de inteligência e contrainteligência do país. No entanto, a construção de confiança mútua é fundamental para o sucesso das iniciativas de segurança cibernética.[39]

Nesse quesito, cabe dizer que a fraqueza do Brasil também é sua força. Ao mesmo tempo em que o país enfrenta altos índices de violações cibernéticas, como crimes e golpes digitais, além de malwares e roubo de dados, o país também é reconhecido por sua capacidade de mitigar incidentes e por exportar pensadores e desenvolvedores de soluções na área.

[38] Hipótese 2: Os investimentos existentes na área são baixos quando comparados a outros setores estratégicos.

[39] Hipótese 3: Não existe uma liberdade intelectual voltada para a relação governo-sociedade no que tange o desenvolvimento para segurança cibernética.

Referências

ABREU, A. F. *A Política Internacional de Controle de Armamentos: Novos Atores, Novos Referenciais.* Scielo, 2011.

ACLU. “More About Intelligence Agencies (CIA/DNI) Spying.” *ACLU.org.* 2013. https://www.aclu.org/documents/more-about-intelligence-agencies-ciadni-spying.

ADLER, E. *Constructivism and International Relations.* London: Sage Publications, 2006.

ADPF. “Combate ao crime cibernético.” *Associação Nacional dos Delegados da Polícia Federal*, 2017.

Al-Mashat, A M.M. *National Security In The Third World.* Routledge, 1985.

ALOIA, J. E. *MaratonaCiberEducação Cybersecurity Essentials.* Cisco Network Academy, 2022.

ALVES, J. A. L. *A Década das Conferências - 1990 - 1999.* Brasilia: Fundação Alexandre de Gusmão, 2018.

ANATEL, A. N. “Segurança Cibernética.” *Governo Federal.* 2021. https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica.

AYRES PINTO, Danielle Jacon. “Segurança e Defesa Cibernética: Desafios e Perspectivas para os Países da América do Sul.” *6º Encontro da Associação Brasileira de Relações Internacionais – ABRI*, 25 - 28 de Julho de 2017.

BARRAGAN, R., Salman, T., Ayllón, V., Córdova, J., Langer, E., Sanjinés, J., & Rojas, R. *Guía Para la Formulación y Ejecución de Proyectos de Investigación.* La Paz: PIEB, 2008.

BRASIL. *Cenário de Defesa 2020 - 2039.* Brasília, 2017.

—. *Estratégia Nacional de Defesa.* Brasília: Governo Federal, 2020.

—. “Estratégia Nacional de Segurança Cibernética.” *Presidência da República, sub chefia para assuntos jurídicos.* 26 de dezembro de 2018.

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm (acesso em 14 de junho de 2022).

—. “Lei Geral de Proteção de Dados Pessoais, Medida Provisória nº 869, de 2018.” *Presidência da República Subchefia para Assuntos Jurídicos.* 14 de Agosto de 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm (acesso em 14 de Maio de 2022).

BRASIL. “LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.” *Presidência da República - Subchefia para Assuntos Jurídicos*, 2012.

—. *Livro Branco de Defesa Nacional.* 2012.

—. *Livro Verde de Segurança Cibernética no Brasl.* Brasilia: Governo Federal, 2010.

—. *Ministério da Defesa - Doutrina Militar de Defesa Cibernética.* Brasilia: ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS, 2014.

—. *Política Nacional De Defesa.* Brasília: Governo Federal, 2008.

—. *Revisão da Capacidade de Cibersegurança.* Brasília: Governo Federal, 2018.

—. *Senado Federal - Análise de Espionagem Cibernética.* Governo Federal, 2014.

BRASIL, Ministério da Defesa. “Política Cibernética de Defesa.” *MD31-P-02*, 2012.

BRASIL, Ministério da Economia. *Brasil sobe 53 posições no Índice Global de Segurança Cibernética.* Serviços e Informações do Brasil, Brasilia: Governo Federal, 2021.

BRASIL, SAE. “Os Desafios Estratégicos para a Segurança e Defesa Cibernética.” Distrito Federal: Governo Federal, 2011.

BUENO, Guilherme. “Escola Superior de Relações Internacionais.” *ESRI.* 2019. https://relacoesinternacionais.com.br/seguranca-internacional-importancia-e-evolucao/?msclkid=ee41e6c4c50611ec80166b3cbf1667c9.

BUZAN, B., e L HANSEN. *A Evolução dos Estudos de Segurança Internaiconal.* São Paulo: Unesp, 2012.

BUZAN, B., WAEVER, O., & WILDE, J. D. *Security: A New Framework for Analysis.* Lynne Rienner Publishers Inc, 1998.

BUZAN, Barry, e Ole WÆVER. *Regions and Power - The Structure of International Security.* UK: Cambridge, University Press, 2003.

CAVELTY, M. D, e A. WENGER. *Cyber Security Politics. Socio-Technological Transformations and Political Fragmentation.* Routledge, 2022.

CEPIK, M, D CANABARRO, e T. BORNE. “A Securitização do Ciberespaço e o Terrorismo: Uma Abordagem Crítica do 11 de Setembro à Guerra ao Terror.” *ipea*, 2014.

CISCO. *CyberTech Report - Desafios da Cibersegurança no Brasil.* Report, Cisco, 2021.

Cisco. *Orçamento dos EUA para ciberdefesa alcança US$ 9,8 bilhões.* 2020. www.ciscoadvisor.com.br/orcamentos-dos-eua-para-ciberderfesa/.

CLARANET. *Cibersegurança: veja os setores mais críticos no Brasil.* 2022. https://www.claranet.com/br/blog/ciberseguranca-veja-os-setores-mais-criticos-no-brasil.

CLARKE, R., e R. KNAKE. *Cyber War: The Next Threat to National Security and What to Do About It.* HarperCollins e-books, 2010.

CONDEIXA, F. M. S. P. “Espionagem e Direito.” *Revista Brasileira de Inteligência*, 2015.

ConvergenciaBrasil. *Convergencia Brasil.ORG.* 2022. https://convergenciabrasil.com.br/blog/congresso-nacional.

COSTA, A. *ISH Tecnologias.* 2020. https://www.ish.com.br/blog/nao-e-a-seguranca-digital-no-brasil/.

COSTA, A. L, A. L FERREIRA, e V. J. Q CABRAL. “A Criação de Uma Agência Brasileira de Segurança Cibernética como Estratégia de Defesa Nacional.” *Escola Superior de Defesa*, 2022.

CTIR Gov, GSIPR. *Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.* 2020.

CUNHA, H. V. “A Soberania na Era da Informação: Impactos na Política e no Direito.” 2018.

DUPAS, G., e T. VIGEVANI. *O Brasil e as Novas Dimensões da Segurança Internacional.* São Paulo: Alfa-Omega, 1999.

exame, revista. *R$ 103 bilhões roubados: Brasil é o 2º país que mais sofre crimes cibernéticos na América Latina.* 2023. https://exame.com/future-of-money/r-103-bilhoes-roubados-brasil-e-o-2o-pais-que-mais-sofre-crimes-ciberneticos-na-america-latina/.

FARIAS, D, e V FERRAZ. “Saber e poder na atualidade: questão cibernética.” *Décimo Encontro Nacional da Associação Brasileira de Estudos de Defesa*, 2018.

FAVERO, P. H. “O amanhecer do poder cibernético brasileiro? Uma análise documental sobre defesa e segurança cibernética no Brasil de 2018 a 2020.” 2022.

FAVERO, P. H. P, e G. D. C. PAGLIARI. “A DEFESA NACIONAL NO SÉCULO XXI: A INFLUÊNCIA DA CIBERNÉTICA NO PODER DAS POTÊNCIAS MÉDIAS - UM ESTUDO SOBRE O CASO BRASILEIRO.” *ABRI*, 25 de 07 de 2023.

FERREIRA, C. R. “ Governança em Segurança Cibernética: Uma Análise Crítica da Fragmentação de Órgãos no Brasil.” *Anais do Congresso Brasileiro de Segurança Cibernética*, 2020.

GIBSON, W. *Neuromancer.* Aleph, 1984.

GIL, A. C. *Como elaborar projetos de Pesquisa.* São Paulo: Atlas, 1996.

GlobalXT. *Segurança cibernética em Israel - Fortalecimento das defesas digitais em meio a riscos elevados.* 2022. www.globalxefts.com.br/.

GRAY, Chris Hables. *Postmodern War: The New Politics of Conflict.* NewYork: Guilford Press, 1997.

GRIFFITHS, Martin. *International Relations Theory for the Twenty-First Century.* Brisbane: Routledge, 2007.

HOSANG, Alexandre. “Política Nacional De Segurança Cibernética: Uma Necessidade Para O Brasil.” *Escola Superior de Guerra*, 2011.

IPEA. “Centro de Pesquisa em Ciência, Tecnologia e Sociedade.” Gasto tributário para P&D no Brasil, 2023.

ITU, I. “Global Cybersecurity Index.” *ITU Publications*, 2021.

IZYCKI, E. A, D. J AYRES PINTO, e L. G. LAVANDOSKI DA SILVA. “(IN)SEGURANÇA CIBERNÉTICA OU FALTA DE INTERESSE PARA CRIAR POLÍTICAS PÚBLICAS NESSE SETOR NA REGIÃO LATINO AMERICANA?” 2023.

IZYCKI, E. A. *Cyber Offensive Capabilities: A Glimpse Into A Multipolar Dimension.* Brasilia: Universidade de Brasilia, 2021.

IZYCKI, E. A., e J. D. CORTINHAS. “Conflito Cibernético - Evolução ou Revolução?” *Encontro Nacional da Associação Brasileira de Estudos de Defesa. ABED*, 2021.

IZYCKI, Eduardo Arthur. “A nuance binária e a nova ordem geopolítica mundial.” *A nuance binária e a nova ordem geopolítica mundial*, 2021.

IZYCKI, Eduardo Arthur, e José Eduardo Malta de Sá BRANDÃO. “Poder Ofensivo No Espaço Cibernético.” Em *Desafios Contemporâneos para o Exército Brasileiro*. IPEA, 2019.

KELLO, L. *The Meaning of the Cyber Revolution.* MIT Press Journals, 2013.

LAVANDOSKI DA SILVA, L. G. *O Brasil E O Ciberespaço: Um Estudo Acerca Do Planejamento Estratégico De Defesa Cibernética A Partir Do Escândalo Da Nsa.* Belém, 2018.

LÉVY, Pierre. *As Tecnologias Da Inteligência.* São Paulo: 34 LTDA, 1999.

LOBATO, L. C, e L. M. HUREL. *Uma Estratégia para a Governança da Segurança Cibernética no Brasil.* Instituto Igarapé, 2018.

LOBATO, L., e K. KENKEL. “Discourses of Cyberspace securitizacion in Brazil and in United States.” *Scielo*, 2015: 23 - 43.

LOBATO, Luisa, e Kai Michael KENKEL. “A Ciberguerra É Moderna! Uma Investigação sobre a Relação entre Tecnologia e Modernização na Guerra.” *Contexto Internacional - PUC Rio*, 2015: 629-660.

LOPES, G. V. *As Relações Internacionais Cibernéticas (CiberRI): Um Defesa Acadêmica a Partir dos Estudos de Segurança Internacional.* Recife: Universidade Federal de Pernambuco, 2016.

LUCAS, F. S. “A Ameaça Cibernética Às Infraestruturas Críticas Nacionais.” *Escola Superior de Guerra - Curso Superior de Segurança e Defesa Cibernética*, 2023.

MALAGUTTI, M. *Ciberdefesa e Cibersegurança. Um Olhar Brasileiro.* Brasília: Instituto Vegetius, 2022.

MORAES, A. B. “Segurança Cibernética no Brasil: Desafios e Perspectivas.” *Revista Brasileira de Segurança Cibernética, v. 15, n. 3,*, 2021: 45-62.

NYE, J. “Cyber Power. Belfer Center for Science and International Affairs.” *Harvard Kennedy School*, 2010.

NYE, J., e R. KEOHANE. “Power and Interdependence in the information age.” *Foreign Affais* (Foreign Affairs), 1998: 81-94.

OLIVEIRA, J. S. “Desafios na Governança de Segurança Cibernética no Contexto Brasileiro.” *Journal of Cybersecurity Studies, v. 7, n. 1*, 2019: 112-129.

OLIVEIRA, M. A., G. C. PAGLIARI, A. A. MARQUES, L. S. PORTELA, e W. B. FERREIRA NETO. *Guia de Defesa Cibernética na América do Sul .* UFPE, 2017.

PECK, P. *E-Ciber é aprovada, mas redação deixa a desejar.* 2020. https://securityleaders.com.br/e-ciber-e-aprovada-mas-redacao-deixa-a-desejar/.

PENTEADO, Carlos J. R. A. “Estratégia Nacional de Segurança Cibernética e a Lei Geral de Proteção de Dados.” *IV Congresso de Segurança e Defesa Cibernética.* São Paulo: FIESP, 2022.

REPORT, SECURITY. “Governo brasileiro investe pouco em segurança cibernética.” 2019.

RID, T. *Cyber War Will Not Take Place.* London: King's College, 2011.

RID, Thomas. *"Cyberwar não acontecerá.".* Journal of Strategic Studies, 2011.

RÜDELL, I. *Cibersegurança no Brasil em 2023.* 2003. https://www.lumiun.com/blog/ciberseguranca-no-brasil-em-2023/.

SANTOS, C. S. A, L. O GAVIÃO, L. A. S OLIVEIRA, e J. C. PEREIRA. “Proposta de Avaliação da Política Nacional de Segurança da Informação.” Em *Perspectivas em Ciência da Informação*, 108 - 145. 2022.

SEITENFUS, R. *Os atores das Relações Internacionais.* Barueri: Manole, 2004.

Senado. *Agencia Senado.* 2019. https://www12.senado.leg.br/noticias/videos/2019/12/falta-de-recursos-para-defesa-cibernetica-preocupa-senadores-da-comissao-de-relacoes-exteriores (acesso em 02 de 08 de 2023).

SILVA, R. A. “Cooperação Interinstitucional em Segurança Cibernética: Um Estudo de Caso no Brasil.” *Conferência Internacional de Tecnologia da Informação*, 2022.

SPIRI, Raquel T. *Cibersegurança No Brasil: Uma Análise De Seus Desdobramentos À Luz Da Securitização .* Marília: Universidade Estadual Paulista, 2020.

UCHOA, Pablo. *Para especialista americano, 'espionagem do Brasil não se compara à da NSA'.* Washington, 2013.

USP, JORNAL DA. *Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos no último ano.* São Paulo, 2023.

WALTZ, K. *Theory of International Politics.* 1979.