UNIVERSIDADE FEDERAL DE SERGIPE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS

MATHEUS CARVALHO ALEXANDRE PEREIRA

SEGURANÇA CIBERNÉTICA BRASILEIRA: UMA ANÁLISE DOCUMENTAL NO RECORTE DE 2012 A 2016

São Cristóvão/SE
2023

MATHEUS CARVALHO ALEXANDRE PEREIRA

SEGURANÇA CIBERNÉTICA BRASILEIRA: UMA ANÁLISE DOCUMENTAL NO RECORTE DE 2012 A 2016

Trabalho de Conclusão de Curso II apresentado ao Departamento de Relações Internacionais como requisito parcial para obtenção do título de Bacharel em Relações Internacionais.
Orientadora: Profa. Dra. Bárbara Vasconcellos de Carvalho Motta.

São Cristóvão/SE

2023

TERMO DE APROVAÇÃO

MATHEUS CARVALHO ALEXANDRE PEREIRA

SEGURANÇA CIBERNÉTICA BRASILEIRA: UMA ANÁLISE DOCUMENTAL NO RECORTE DE 2012 A 2016

Trabalho de Conclusão de Curso II apresentado ao Departamento de Relações Internacionais como requisito parcial para obtenção do título de Bacharel em Relações Internacionais.
Orientadora: Profa. Dra. Bárbara Vasconcellos de Carvalho Motta.

BANCA EXAMINADORA

Professora Dra. Bárbara Vasconcellos de Carvalho Motta
Orientadora - Universidade Federal de Sergipe

Professor Dr. Cairo Gabriel Borges Junqueira
Examinador Interno - Universidade Federal de Sergipe

Professor Dr. Jonathan de Araújo de Assis
Examinador Externo - Programa de Pós-Graduação San Tiago Dantas

Nota:_____

São Cristóvão,_____de _____ de 2023

“Nem todos que trabalham duro são recompensados. Mas! Todos aqueles que obtiveram sucesso trabalharam duro!” - Treinador Kamogawa (MORIKAWA, 1998, p. 156, tradução nossa)

AGRADECIMENTOS

Primeiramente, gostaria de agradecer ao Prof. Dr. Jonathan de Araújo de Assis por se disponibilizar a compor ambas as bancas de TCC I e TCC II, contribuindo com excelentes comentários acerca do trabalho e do tema de pesquisa. Gostaria de estender esses agradecimentos aos professores Dra. Bárbara Vasconcellos de Carvalho Motta e Dr. Cairo Gabriel Borges Junqueira, há um carinho especial quanto esses dois, a Professora Dra. Bárbara que atuou como minha orientadora fiel em meio a períodos turbulentos, se assim posso dizer. Enquanto o Professor Dr. Cairo me remonta aos primeiros períodos da graduação, em que o mesmo havia iniciado há pouco na Universidade Federal de Sergipe e que com isso possuo muitas memórias de suas aulas. De todo modo, ambos são a representação ética e profissional que tenho como modelo para minha vida.

O trabalho de conclusão de curso II simboliza o encerramento de uma jornada de quatro anos (cinco anos com os contratempos) em busca da diplomação em Relações Internacionais. Durante todo esse percurso eu fui muito feliz por estar acompanhado de um departamento com professores extremamente dedicados, que pelo fato de ser um departamento pequeno se comparado a outros, me permitiu ter uma relação bem próxima dos professores, na medida em que acompanhei professores já instalados no departamento, bem como aqueles que iniciaram sua jornada durante a minha graduação. A todos vocês, meu muitíssimo obrigado ao amor e profissionalismo que vocês empenham diariamente ao curso de Relações Internacionais da Universidade Federal de Sergipe.

Assim como disse um professor em uma das muitas aulas que vivenciei, a faculdade é melhor vivida quando acompanhada por amigos. Obviamente a frase não foi dita exatamente assim, mas é assim que eu me recordo dela, até porque eu carreguei essa mensagem comigo do primeiro período até o último no formato dos meus amigos Maria Milena, Maria Rafaela, Brena, Ellen, Paula Renata, Enio, João Pedro e Adler. Todos foram presentes que ganhei na graduação e que me renderam ótimas memórias e vivências que levarei comigo sempre.

Ademais, não tenho palavras para descrever minha alegria em chegar até aqui e saber que posso trilhar um caminho estável para o futuro, tudo isso devido às inúmeras e imensuráveis contribuições que meus pais, Edinete e Sandro batalharam para garantir que eu obtivesse as melhores oportunidades e acesso a educação de qualidade. Além de todo o apoio emocional durante a graduação e minha vida por completo.

Por último, não há como listar todas as pessoas que me ajudaram a pavimentar a estrada que me trouxe até aqui. Porém, desejo registrar meu profundo agradecimento a Ághata

Gabrielle por atuar como mais um porto seguro em minha vida, me permitir viver diversas experiências e realizar uma longa viagem ao seu lado por todas as sensações que a vida pode nos proporcionar.

À todos, inclusive aqueles não citados nominalmente, meu MUITO OBRIGADO!

RESUMO

O entendimento de segurança internacional como um campo capaz de abarcar temas diversos é relativamente recente. Um desses temas é a segurança cibernética, que envolve a percepção de riscos advindos do espaço cibernético. Apesar do alargamento de temas e atores da segurança internacional, o Estado continua sendo objeto de análise preponderante. Assim sendo, ao falarmos de segurança cibernética no Brasil é necessário olhar para a atuação do Estado sobre a temática, sua percepção dos riscos e suas ações. O presente trabalho pretende realizar uma análise do desenvolvimento da pauta de segurança cibernética no Brasil pautada no período dos megaeventos que o Brasil sediou de 2012 a 2016, utilizando da análise documental e sua correlação com o fenômeno de securitização, descrito pela Escola de Copenhagen. Para tal, será feita a leitura dos documentos oficiais, juntamente ao resgate da literatura especializada em segurança cibernética brasileira e da teoria de securitização voltada para o setor de segurança cibernética.

Palavras-chave: Segurança Cibernética; Brasil; Securitização; Espaço Cibernético; Megaeventos.

ABSTRACT

The understanding of international security as a field capable of encompassing diverse topics is relatively recent. One of these themes is cybersecurity, which involves the perception of risks arising from cyberspace. Despite the broadening of themes and actors in international security, the State continues to be the preponderant object of analysis. Therefore, when we talk about cybersecurity in Brazil, it is necessary to look at the State's performance on the subject, its perception of risks, and its actions. The present work intends to carry out an analysis of the development of the cybersecurity agenda in Brazil based on the period of the mega events that Brazil hosted from 2012 to 2016, using document analysis and its correlation with the securitization phenomenon, described by the Copenhagen School. To this end, the official documents will be read, along with the rescue of the literature specialized in Brazilian cybersecurity and the theory of securitization focused on the cybersecurity sector.

Key-words: Cybersecurity; Brazil; Securitization; Cyberspace; Mega-events.

LISTA DE ABREVIATURAS E SIGLAS

ABIN - Agência Brasileira de Inteligência

CDCiber - Centro de Defesa Cibernética

CDN - Conselho de Defesa Nacional

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

ComDCiber - Comando de Defesa Cibernética

CREDEN - Câmara de Relações Exteriores e Defesa Nacional

CTIR.Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo

DSIC - Departamento de Segurança da Informação e Comunicações

E-Ciber - Estratégia Nacional de Segurança Cibernética

EB - Exército Brasileiro

END - Estratégia Nacional de Defesa

ENISA - The European Union Agency for Cybersecurity

EUA - Estados Unidos da América

GSI-PR - Gabinete de Segurança Institucional da Presidência da República

ITU - International Telecommunication Union

LBDN - Livro Branco de Defesa Nacional

MD - Ministério da Defesa

NSA - National Security Agency

OND - Objetivos Nacionais de Defesa

PDN - Política de Defesa Nacional

PND - Política Nacional de Defesa

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O fim da Guerra Fria representou um marco nas relações internacionais. A última década do século passado foi um período de extensa produção acadêmica, debates teóricos e inovações conceituais para que houvesse uma compreensão da realidade hodierna. Isso se deve às mudanças nas relações de poder e a revolução da informação (NYE, 2010, p.3). O impacto desses dois elementos foi percebido nos diversos temas de Relações Internacionais, inclusive na pauta de segurança.

Ao falar em segurança e poder no período da Guerra Fria, havia uma imediata analogia com as temáticas de armamentos nucleares e uma clara identificação de dois atores no sistema internacional, Estados Unidos da América e a União das Repúblicas Socialistas Soviéticas (VILLA; REIS apud SOUZA, 2013, p. 25). Com o fim da bipolaridade e a chegada da revolução da informação, as dinâmicas de poder no sistema internacional se modificaram, sobretudo com a emergência de novos atores e novas temáticas, bem como com um maior contexto de interdependência e a aparição de um espaço cibernético cada vez mais presente na vida dos indivíduos e nas extensões do Estado (SOUZA, 2013; NYE, 2010).

Segundo Souza (p.25, 2013), a chegada do século XXI traz consigo a emergência da pauta de segurança cibernética, em que "as ameaças cibernéticas transbordam do setor societário e atingem o político e militar"; com isso, uma das "consequência[s] para a política internacional hodierna (...) é a formulação de políticas exteriores e de defesa nacional que elevam o status das ameaças cibernéticas à alçada de assuntos pertinentes à segurança nacional".

O espaço cibernético representa um ambiente de incerteza, desterritorialização e difusão de poderes (MEDEIROS; CARVALHO; GOLDONI, 2019), e que, segundo Nye (2010), o Estado foi compelido a atuar no espaço cibernético e considerá-lo um “novo” domínio, assim como o “domínio terrestre” e “domínio aéreo”. No entanto, os elementos supracitados do espaço cibernético requerem que o Estado atue de modo particular neste domínio, devido à multiplicidade de atores e à possibilidade de um “indivíduo” (hacker) de produzir ameaças ao Estado, podendo gerar danos através de cibercrimes diversos, como fraudes, desinformação e proliferação de malwares (programas maliciosos) (MEDEIROS; CARVALHO; GOLDONI, 2019, p.48-49; NYE apud HUREL, 2018, p.321; OLIVEIRA, 2014, p.14). Isso se traduz também na permeabilidade das fronteiras, devido às conexões entre redes de todo o mundo, o que dificulta o papel do Estado de se resguardar e de mensurar os riscos e possíveis ameaças nesses ambiente de incerteza, em que os efeitos de um ataque são quase que imediatos (MEDEIROS; CARVALHO; GOLDONI, 2019, p.48-49).

A aparição do tema de segurança cibernética inserido nos estudos de segurança internacional se deve bastante à contribuição da Escola de Copenhagen (BUZAN; WAEVER; WILDE, 1998) em expandir o escopo de análise para além da guerra convencional. Ademais, o conceito teórico de securitização se faz presente em muitos estudos voltados à compreensão da construção da agenda de segurança cibernética. A bibliografia utilizada neste estudo usa do conceito de securitização para explicar a emergência da pauta, bem como seu desenvolvimento, efeitos e desafios, em que muitas análises tratam o caso brasileiro como objeto de investigação (SOUZA, 2013; HUREL; LOBATO, 2021; HUREL, 2018; HANSEN; NISSENBAUM, 2009).

Pensando mais especificamente nas ameaças que o Brasil enfrenta no espaço cibernético, bem como na sua percepção dos riscos, a proposta elaborada por Hurel e Lobato (2021) é seminal. As autoras traçam todo o processo em que a pauta de segurança cibernética brasileira foi se desenvolvendo como uma resposta à percepção de risco do Brasil em determinados períodos.

Segundo Hurel e Lobato (2021), a pauta de segurança cibernética brasileira passou por duas dimensões de percepção, sendo a primeira uma forte conotação da percepção do risco como uma ameaça externa. Essa percepção foi marcada pelos ataques cibernéticos que a Estônia, a Geórgia e o Irã sofreram nos anos de 2007, 2008 e 2010, respectivamente. O cenário externo em conjunto com o momento vivido pelo Brasil à época, em que o país sediou 4 megaeventos internacionais de grande escala, respaldam a percepção interna da importância da área cibernética e foram propulsores do desenvolvimento da estrutura institucional de segurança cibernética no Brasil. Estas questões explicam o surgimento de instituições e órgãos com ênfase em segurança cibernética no período, mas que estavam preocupados com as ameaças externas da guerra cibernética e do ciberterrorismo (HUREL, 2018, p. 330-331; HUREL; LOBATO, 2021, p. 506-507).

Essa percepção da ameaça cibernética externa fez com que não fosse dada atenção ao debate de segurança pública tido como urgente: a questão do cibercrime, fraudes e proteção de dados (DINIZ; MUGGAH; GLENNY apud HUREL; LOBATO, 2021, p. 507). Após os escândalos de espionagem revelados por Snowden, em que a National Security Agency (NSA) dos Estados Unidos realizava monitoramento de e-mails e ligações de funcionários do alto escalão da administração pública, da Petrobrás e da ex-presidente Dilma Roussef (GLEENWALD; KAZ; CASADO, 2013), o Brasil passou por um período de instabilidade política fomentado pelos escândalos de corrupção da Lava a Jato, que culminou no impeachment da então presidente Dilma Roussef, em 2016. Conforme apontam Hurel e

Lobato (2021, p. 509-510), é a partir desse momento de instabilidade política que a dimensão da percepção do risco proeminente do espaço cibernético passa a ser o âmbito interno, com a pauta de segurança cibernética voltando-se à mitigação de ameaças como hacktivismo, fraudes, crimes financeiros, roubo de dados e desinformação (HUREL; LOBATO, 2021, p. 510).

No esteio desse debate, a Estratégia Nacional de Defesa (END) de 2008 representou um marco para a segurança cibernética no Brasil, ao trazer o espaço cibernético como um dos eixos principais da estratégia de defesa do país. No entanto, antes da END de 2008 tivemos a Política de Defesa Nacional (PDN), em 2005, a qual não apontava o cibernético como um eixo principal mas ressaltou a necessidade de defesa e mitigação de vulnerabilidades no espaço cibernético, porém de modo breve e sem a merecida relevância. Por essa razão a END de 2008 é tida como documento inaugurador da temática de segurança e defesa cibernética no Brasil (OLIVEIRA; PORTELA, 2017). Segundo Oliveira e Portela (2017, p. 89-90), os documentos de defesa como a END (2008), a PDN (2005), o Livro Branco de Defesa de 2016 (LBDN) e a Política Nacional de Defesa de 2012 pouco inovam sobre "as tratativas de defesa cibernética do país" (p. 89), mas é manifesta a evolução institucional advinda desses documentos na pauta de segurança cibernética que foram responsáveis por moldar a estrutura de governança da segurança cibernética no Brasil. Desde a aparição do cibernético como eixo estratégico de segurança e defesa no Brasil, que se soma a sobreposição gradual de órgãos e instituições que hoje compõem o sistema de análise e resposta a incidentes cibernéticos, sejam ameaças internas ou externas.

Hurel (2018) compreende que os mega eventos representaram uma verdadeira clivagem na matéria de segurança cibernética, uma vez que, por exemplo, o Centro de Defesa Cibernética (CDCiber) e o Comando de Defesa Cibernética das Forças Armadas (ComDCiber) foram criados em 2012, após a revisão do END no mesmo ano, bem como:

> [...] a portaria No. 2.221 de 20 de agosto de 2012 estabeleceu orientações para a atuação do Ministério da Defesa nas atividades dos Grandes Eventos, dentre estas o emprego temporário das forças armadas na segurança e defesa cibernética para proteção das cidades-sede (GABINETE apud HUREL, 2018, p. 331).

O processo de institucionalização da pauta de segurança cibernética foi acelerado e diretamente impactado pelos megaeventos; no entanto, tem recaído sobre o Ministério de Defesa e as Forças Armadas o papel de guiar o leme do Brasil no tema de segurança cibernética:

> [...] a rápida estruturação de instituições dentro do Ministério da Defesa (por exemplo, GSI e Forças Armadas) traz profundas tensões para uma visão que destaque uma distribuição de competências para órgãos associados à segurança em

> sua dimensão política e operacional. [...] Ao mesmo tempo que segurança cibernética ganha notoriedade dentro da agenda nacional, as respostas se concentram, em grande medida, no papel e estruturas do Ministério da Defesa, Exército e Forças Armadas – mais especificamente, por meio da consolidação do Sistema Militar de Defesa Cibernética (HUREL, 2018, p. 332-333).

Conforme explicitado até aqui, é defendido a relevância do espaço cibernético para as Relações Internacionais e em especial, para a temática de segurança, baseando-se na defesa de autores como Nye (2010) e Souza (2013) sobre a relevância e a incapacidade de desconectar o espaço cibernético das novas dinâmicas nas relações de poder. Além disso, é importante destacar o esforço conjunto de autoras como Hurel e Lobato (2021) em retratar a importância e captar a dinâmica com a qual a pauta de segurança cibernética brasileira tem se moldado. Inclusive, o espaço cibernético tem ganhado expressividade nos temas de Relações Internacionais, inclusive com adeptos da criação do subcampo internacionalista "CiberRI"[1], tendo como foco o espaço cibernético e sua repercussão nas relações internacionais em sua totalidade.

Assim sendo, o presente trabalho se propõe a responder a seguinte pergunta: como se deu a expansão normativa e institucional do Brasil para tratar do tema da segurança cibernética no período dos megaeventos de 2012 a 2016?

Para tal, é feita uma análise documental voltada para os temas de segurança cibernética no Brasil, sob o prisma da teoria de securitização que tem sido elemento recorrente nos estudos de segurança cibernética (HANSEN; NISSENBAUM, 2009; SOUZA, 2013; HUREL, 2018; HUREL; LOBATO, 2021). Utilizando da análise dos documentos oficiais, em conjunto a leitura de literatura especializada sobre os documentos e seus elementos quanto ao espaço, tempo e os temas abordados nos mesmo (SÁ-SILVA; ALMEIDA ;GUINDANI, 2009). A literatura apresenta os megaeventos como um período importante para a expansão normativa e institucional do Brasil em segurança cibernética, no entanto, a análise desse período não é feita com intuito de compreender a especificidade e dinâmica desse período. A proposta deste trabalho é oferecer a discussão sobre segurança cibernética no Brasil uma análise dos documentos oficiais e da literatura específica, voltada para o período dos megaeventos (2012-2016).

O trabalho está estruturado em quatro partes. A primeira parte apresenta uma discussão introdutória sobre as definições de espaço cibernético, segurança cibernética, segurança internacional, defesa cibernética e securitização do espaço cibernético. A segunda

[1] No Brasil, a defesa da criação do CiberRI é tida com afinco pelo Prof. Dr. Gills Vilar Lopes. Para aprofundamento no assunto, olhar o artigo: Relações internacionais cibernéticas (CiberRI): uma defesa acadêmica a partir dos estudos de segurança internacional (LOPES, 2016).

parte discorre sobre a segurança cibernética no contexto brasileiro, de modo a compreender como o setor cibernético tornou-se estratégico para o país através da análise dos documentos e o que a bibliografia interpreta do caso brasileiro. A terceira parte analisa o período em que o Brasil foi sede de megaeventos como a Rio +20 (2012), Copa das Confederações (2013), Copa do Mundo (2014) e as Olímpiadas (2016), com foco nos efeitos produzidos que contribuíram para a expansão normativa e institucional brasileira para lidar com questões de segurança cibernética. Por fim, as considerações finais sobre o tema de segurança cibernética no Brasil e o modo como o período dos megaeventos é importante para a compreensão desse tema.

2 SEGURANÇA INTERNACIONAL E SEGURANÇA CIBERNÉTICA

2.1 Segurança e o Espaço Cibernético

Os estudos de segurança internacional podem ser entendidos pelo anseio da ausência de ameaças e riscos a nível internacional. Ao colocarmos o foco sobre a temática de segurança internacional, o Estado e tudo aquilo que o compõem é tido como o ator de maior relevância e consideramos um incidente de segurança internacional a partir do momento que esse ator é posto sobre ameaça existencial (SAINT-PIERRE; VITELLI, 2018). Se existe uma ameaça à existência do Estado isso faz dele o objeto referente, enquanto àquele que gera a ameaça é tido como agente, o causador da instabilidade (BUZAN; WAEVER; WILDE, 1998). É interessante pensar que a efetiva passagem de ameaça existencial para o fim do Estado afetado, pode incluir ameaças e riscos a outros Estados sensíveis e/ou vulneráveis, demonstrando a capacidade de alastramento da ameaça ao panorama geral do sistema internacional.

O espaço cibernético é um ambiente complexo e dinâmico que evoluiu rapidamente nos últimos anos. É um domínio virtual dentro das redes de computadores[2] e engloba todas as interações digitais entre indivíduos, organizações e governos. Como resultado, o ciberespaço é um elemento importante da sociedade moderna, fornecendo serviços essenciais como comunicação, finanças, saúde e transporte.

Ao procurar pela definição do conceito de espaço cibernético é fácil reconhecer os muitos pontos em comum entre as mais diversas definições, bem como as diferenças de autor para autor. Geralmente o espaço cibernético é entendido como um território sem delimitação clara, o qual possui um enorme tráfego de informação e a capacidade de armazenar uma quantidade ainda maior de informação (VENTRE, 2019). Para Cepik (et al. 2014), o espaço cibernético é um domínio operacional responsável por criar e transportar um grande montante de informações em redes, tendo as tecnologias de informação e comunicação (TIC) atuando como seu principal recurso. A bibliografia não diverge sobre as características centrais do espaço cibernético, sempre apresentando-o como um espaço, campo ou domínio desterritorializado e que comporta um fluxo de informações gigantesco (MEDEIROS; CARVALHO; GOLDONI, 2019).

Como o objeto referente desse trabalho se trata do Estado brasileiro, nada melhor do que buscar a definição utilizada pelo mesmo. A Doutrina Militar de Defesa Cibernética

[2] É necessário notar que o espaço cibernético não está limitado à *internet* (ARPANET), a mesma é um tipo de rede de computadores sendo a mais popularizada, no entanto, a conexão de dois computadores em rede fechada trata-se também de espaço cibernético e/ou ciberespaço.

(MD31-M-07, 2014) é um documento de defesa vigente que trouxe as primeiras definições sobre a segurança e defesa cibernética para o Brasil.

Para a Doutrina Militar de Defesa Cibernética (MD31-M-07, 2014, p.18) o espaço cibernético é entendido como um "espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas." O Glossário de Segurança da Informação (2023) traz uma definição mais completa:

> - espaço virtual composto por um conjunto de canais de comunicação da Internet e outras redes de comunicação, que garantem a interconexão de dispositivos de tecnologia da informação. Engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente (ESPAÇO CIBERNÉTICO, 2023).

Por se tratar de um documento com quase uma década, é esperado que alguns conceitos estejam defasados para os padrões atuais, por isso será complementado pelas definições presentes no Glossário de Segurança da Informação, o qual se trata de uma plataforma mantida e alimentada pela estrutura institucional brasileira sobre assuntos de defesa e segurança cibernética e informação.

O domínio cibernético é por concepção um vasto espaço ausente de fronteiras e delimitações, dificultando o processo de territorialização desse ambiente por parte dos atores, em especial o Estado, o qual se caracteriza por ter explícito suas fronteiras em qualquer domínio que venha atuar, como o mar, o ar e a terra (MEDEIROS; CARVALHO; GOLDONI, 2019).

De modo específico, o ciberespaço ou espaço cibernético é compreendido por meio de três dimensões e/ou camadas:

> Uma primeira camada é constituída pela arquitetura material, física, *hardware*; ela é feita pelo conjunto de computadores, calculadoras, cabos eletrônicos (*hardware layer*). Uma segunda camada, média, denominada software ou aplicativa, é constituída pelo conjunto de programas, códigos, dados e algoritmos que dão vida ao ciberespaço (*software layer*). E uma terceira camada, informacional, é a do sentido, das informações (*news*), dos conteúdos (*meatware layer*) (VENTRE, 2019).

A concepção do que é espaço cibernético em documentos oficiais é importante para a compreensão dos conceitos que virão a seguir, como segurança cibernética e defesa cibernética. Com isso, consequentemente, a interpretação da atuação do Brasil na temática de segurança cibernética está diretamente ligada a compreender o objeto em questão, em especial na visão de quem constrói a estrutura de governança cibernética.

Como dito anteriormente, o espaço cibernético possui uma grande fluidez informacional e tem se tornado parte comum das interações entre as diversas áreas. As

informações pessoais, bancárias, financeiras de pessoas físicas, jurídicas e até dados governamentais se encontram armazenadas e circulando em redes, isso faz com que o acesso à informação e a compilação da mesma seja bastante eficiente e eficaz. No entanto, o ciberespaço também é vulnerável a ameaças cibernéticas como hacking, malware e espionagem. Essas ameaças representam um risco significativo para a segurança e a estabilidade do ciberespaço e podem ter consequências graves para os indivíduos e para a sociedade como um todo.

A vulnerabilidade desse espaço está relacionada ao critério de desterritorialização, mas também à difusão de poder e à incerteza característicos desse domínio. Como dito anteriormente, o espaço cibernético tem por característica a ausência de fronteiras e comporta um enorme fluxo de informações que é alimentado por um grande público/atores. Esse público é composto por diversos atores, das unidades menores (indivíduos) até as maiores (Estado), a interação desses atores em um espaço no qual o Estado não exerce plenamente suas capacidades, faz com que atores não convencionais dos cálculos de segurança tenham liberdade e potencial de gerar riscos e ameaças intencionais ou não intencionais em larga escala. Esse cenário é uma exemplificação da difusão de poder e a incerteza centrada na participação de diversos atores com capacidades de gerar ameaças de pequena a larga escala (MEDEIROS; CARVALHO; GOLDONI, 2019; VENTRE, 2019).

2.2 Segurança Cibernética

Segundo a Agência de Segurança Cibernética da União Europeia (ENISA,2016) há uma variedade de definições possíveis para segurança cibernética, tanto os governos como as organizações internacionais tendem a optar por uma definição que englobe os pontos que julgarem centrais para natureza de sua relação com o espaço cibernético e sua segurança. Por exemplo, o Ministério da Defesa dos Estados Unidos (DOD, 2021, p.55) entende segurança cibernética por proteção dos sistemas de informação, redes e ativos digitais contra ataques cibernéticos, roubos e danos. As medidas de segurança cibernética podem incluir várias ferramentas e técnicas, como firewalls, software antivírus, criptografia e sistemas de detecção de intrusão, a fim de garantir sua disponibilidade, integridade, autenticação, confidencialidade e não repúdio. A International Telecommunication Union (ITU, 2008) enfatiza que segurança cibernética é um aglomerado de medidas políticas, gerenciamento de risco, boas práticas e uso da tecnologia para a proteção do ambiente cibernético e a informação contida nele.

Apesar da abordagem diferente sobre o que é segurança cibernética para as duas organizações, percebe-se que em conteúdo não se difere substancialmente, sendo uma mais

abrangente e a outra mais específica. Ao somar essa informação com a leitura da bibliografia presente, é possível afirmar que ao tratar do conceito de segurança cibernética dois elementos são recorrentes: a proteção da informação/dados e mitigar ameaças a infraestrutura crítica que se constitui como a proteção da infraestrutura de hidrelétricas e barragens, por exemplo.

A definição do Ministério de Defesa do Brasil (MD31-M-07, 2014) para segurança cibernética é sucinta e atende aos dois elementos centrais elencados anteriormente, sendo descrita como a " arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas." Uma outra leitura que pode ser feita é que a segurança cibernética tem como objetivo mitigar possíveis ameaças ao ambiente cibernético, para tal, a definição de ameaça cibernética é complementar e é apresentada como "causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse." (MD31-M-07, 2014, p. 18-19)

O Glossário de Segurança da Informação (2023) contribui com mais detalhes mas não disponibiliza uma definição sobre o que vem a ser uma ameaça cibernética, limitando-se a definir exclusivamente o que é ameaça como um "conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização" (BRASIL).

> - ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (SEGURANÇA CIBERNÉTICA, 2023).

A importância da segurança cibernética cresceu significativamente nos últimos anos, à medida que os ataques cibernéticos se tornaram mais frequentes, sofisticados e destrutivos. Os ataques cibernéticos podem causar danos significativos a indivíduos e organizações, incluindo perdas financeiras, danos à reputação e até mesmo perda de vidas em alguns casos. Desde a década de 70, os Estados têm se preocupado em construir um arcabouço jurídico nacional capaz de traçar fronteiras no espaço cibernético para que fossem capazes de mensurar e minimizar os riscos. Nesse sentido, a busca por segurança desses Estados é responsável pela estrutura do sistema cibernético internacional como conhecemos (VENTRE, 2019).

Mesmo com os esforços por parte dos Estados em manipular o espaço cibernético, a segurança cibernética continua um tema recente e com isso enfrenta alguns desafios:

> [...] o quadro ontológico contemporâneo se tornou ainda mais complexo com a emergência de temas não tradicionais nas agendas de segurança internacional, como podemos observar pela noção de segurança cibernética. É possível, de fato, compreender essa nova dimensão de segurança como um fenômeno de segurança? Na verdade, o fato de seus agentes (os hackers) se transformarem em uma ameaça transnacional, que coloca em risco diferentes objetos referentes, não os torna

> necessariamente “novas ameaças”. Por sua natureza virtual, os estudos em segurança internacional ainda não desenvolveram acuradamente as estruturas analíticas para melhor entender os impactos da segurança cibernética para a segurança internacional e suas consequências (SAINT-PIERRE; VITELLI, 2018)

Conforme apontado em Saint-Pierre e Vitelli (2018), a emergência da temática de segurança cibernética contribui para os estudos de segurança internacional, porém, reside uma dificuldade de leitura da natureza do grau de ameaça e da interação dos diversos atores nesse domínio.

As autoras Hansen e Nissenbaum (2009) apontam a importância da Escola de Copenhagen e sua contribuição para a aparição de novas temáticas de segurança internacional, incluindo segurança cibernética. Porém, sinalizam que nos parâmetros da teoria de securitização, a segurança cibernética trata-se de um setor próprio completamente securitizado e com características únicas. Defendendo a mudança dos estudos de segurança cibernética como subsetor vinculado ao setor militar para se tornar um setor próprio, a análise de segurança cibernética pautada nas sugestões de Hansen e Nissembaum (2009) podem significar respostas ou contribuições para os desafios apontados em Saint-Pierre e Vitelli (2018).

2.3 Defesa Cibernética

A defesa cibernética usa medidas defensivas para proteger a infraestrutura crítica e a segurança nacional contra ataques cibernéticos. A defesa cibernética pode incluir várias atividades, como análise de ameaças, avaliações de vulnerabilidade, planejamento de resposta a incidentes e desenvolvimento de tecnologias e capacidades defensivas. Ela pode ser entendida como:

> conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (MD31-M-07, 2014, p. 18).

A ciberdefesa é essencial para a segurança nacional, pois os ataques cibernéticos podem ter consequências significativas para o poder político, econômico e militar de um país. Os ataques cibernéticos também podem ser usados como uma ferramenta de espionagem ou sabotagem, visando infraestrutura crítica, como redes elétricas, sistemas de transporte e redes de comunicação.

O Estado tem um papel crítico em garantir a segurança cibernética e defesa cibernética de seus cidadãos, infraestrutura crítica e segurança nacional. O Estado pode usar uma

variedade de políticas, estratégias e estruturas para lidar com ameaças cibernéticas e proteger o ciberespaço.

Desenvolver uma estratégia nacional de segurança cibernética é uma das políticas mais importantes para a cibersegurança e a defesa cibernética. Uma estratégia nacional de segurança cibernética descreve as metas, prioridades e medidas para enfrentar as ameaças cibernéticas e proteger a infraestrutura crítica. A estratégia pode incluir uma série de atividades, como o desenvolvimento de regulamentos de segurança cibernética, o estabelecimento de agências de segurança cibernética e a promoção da conscientização e educação sobre segurança cibernética.

Outra política essencial para a segurança cibernética e defesa cibernética é o estabelecimento de agências de segurança cibernética. As agências de segurança cibernética podem fornecer recursos críticos, como análise de ameaças, planejamento de resposta a incidentes e desenvolvimento de tecnologias defensivas. Além disso, essas agências podem coordenar os esforços de segurança cibernética entre departamentos governamentais e organizações do setor privado.

No caso brasileiro, os documentos norteadores da estratégia nacional de segurança cibernética se iniciam com a promulgação da Estratégia Nacional de Defesa em 2008 (END) seguida pela Política Nacional de Defesa em 2012 (PND)[3] e também pelo Livro Branco de Defesa Nacional também em 2012 (LBDN).

2.4 Securitização do Espaço Cibernético

Durante a década de 90 e início do século XXI intensificou-se a preocupação dos Estados acerca do espaço cibernético, a ponto de reconhecer processos de securitização na pauta de segurança cibernética (SOUZA, 2013). Essa situação é tida como efeito do surgimento das novas Tecnologias da Informação (TIC) que hoje permeiam todas as instâncias da vida em sociedade, da interação entre indivíduos até os fluxos de informação entre os Estados (HUREL, 2018).

Joseph S. Nye é um autor renomado nos estudos de relações internacionais, o qual se debruçou em análises sobre o modo como o sistema internacional e os Estados se comportam, tendo em mente que o autor considera a interdependência um fator crucial para a

[3] O Livro Verde de Segurança Cibernética (LVSC) é um manual de segurança cibernética que se originou na Câmara de Relações Exteriores e Defesa Nacional (CREDEN) no ano de 2010 e foi coordenado pelo Gabinete de Segurança Institucional (GSI) e seu Departamento de Segurança da Informação (DSI), apesar de ser anterior a Política Nacional de Defesa de 2012 (PND) se tratava de documento com caráter sugestivo e por isso não é analisado profundamente pela bibliografia.

compreensão do mundo em que vivemos. Não obstante, o desenvolvimento do espaço cibernético como um domínio desterritorializado e difusor de poder, que hoje permeia nos demais setores da vida humana despertou o interesse de Nye, que em 2010 escreveu *Cyberpower* considerando a maestria no espaço cibernético uma extensão do poder e um objeto de análise essencial para as relações internacionais contemporâneas. É importante pensar que o mundo como conhecemos, interdependente com fronteiras perenes se deve a expansão desse domínio cibernético que declara uma vulnerabilidade e dependência desse domínio:

> O funcionamento desse sistema está condicionado à circulação, sem entraves, dos fluxos de dados. Mas se essa fluidez e essa interdependência estão entre os motores essenciais da integração das sociedades modernas ao sistema internacional contemporâneo, elas determinam, ao mesmo tempo, sua exposição a violências veiculadas pelas redes, praticamente inevitáveis. Os Estados sofrem tais violências sem ter condições de antecipá-las, de antevê-las, de enfrentá-las. Elas atingem o próprio seio de suas sociedades, alteram suas economias, sua vida política. Às vezes ameaçam os pontos nevrálgicos dos Estados, suas infraestruturas vitais, sem que eles consigam ativar suas defesas de modo eficaz, sem que consigam rebater, agir, reagir (VENTRE, 2019).

É com base no dilema da interdependência no sistema internacional e a necessidade de se proteger das vulnerabilidades do sistema em que estão inseridos que os Estados acabaram por securitizar a pauta de segurança cibernética (NYE, 2010; VENTRE, 2019).

O estudo do espaço cibernético como tema dos estudos de segurança internacional é recente. Isso se deve à própria concepção do que é segurança internacional, a qual por muito tempo esteve vinculada à imagem política e militar de conservação do *status quo* do Estado (SAINT-PIERRE; VITELLI, 2018). No pós Guerra-Fria, o Estado continuou sendo o principal objeto referente da segurança, porém os estudos de segurança passaram a englobar esforços teóricos para além da via tradicionalista, ampliando os temas de segurança e os objetos de análise. Dessa forma, indivíduos, grupamentos sociais e coletivos passaram a compor os estudos de segurança internacional, bem como temáticas como meio ambiente, energia, segurança alimentar e cibernética (HANSEN; BUZAN, 2012; SAINT-PIERRE; VITELLI, 2018).

Dentre as inovações teóricas que surgiram no campo dos estudos de segurança, a Escola de Copenhagen e a teoria de securitização (BUZAN; WAEVER; WILDE, 1998) são centrais para o presente trabalho, devido a melhor tradução do espaço cibernético como tema de segurança através de seus conceitos elaborados. A gramática presente nos estudos da Escola de Copenhagen, especificamente no livro ***Security****: A New Framework For Analysis* (BUZAN; WAEVER; WILDE, 1998*)* utiliza do tema de segurança cibernética como um tema não securitizado, mas em movimento securitizador. Segundo os autores, o fato do Pentágono

(Departamento de Defesa dos Estados Unidos) ter declarado em 1996 que hackers apresentam uma ameaça à segurança nacional, não significa que haveria uma sucessão de prejuízos que transbordassem o escopo de segurança cibernética e se tornasse uma ameaça com escalabilidade para outros setores; ou seja, naquele momento o discurso securitizador (do hackitivismo) não tinha uma audiência legitimadora e nem se tratava de uma ameaça existencial com capacidade gerar danos em escala para além das questões de segurança que competiam a segurança cibernética (BUZAN; WAEVER; WILDE, 1998, p. 25).

É compreensível a interpretação dos autores à declaração do Pentágono e seus efeitos na época, no entanto, sabe-se que a vida hodierna tem sido invadida pelo espaço cibernético e isso tem acarretado em uma percepção de ameaça advinda do mesmo, por parte do Estado mais sensível. Fazendo com que segurança cibernética tenha se tornado um tema em que é possível atribuir seu desenvolvimento e legitimidade a medidas excepcionais, como argumentam os autores Souza (2013) e sua pesquisa sobre a securitização e militarização do tema de segurança cibernética, bem como Hansen e Nissembaum (2009) que defendem o ambiente cibernético como um setor próprio.

Para a presente pesquisa, o espaço cibernético não só é tema de segurança como também pode-se afirmar ser um ambiente construído sobre discursos securitizantes por parte do Estado (HANSEN; NISSENBAUM, 2009; LOBATO; KENKEL, 2015). Segundo as autoras Hansen e Nissenbaum (2009) a segurança cibernética ganha notoriedade no pós Guerra-Fria devido ao fim das tensões do mundo bipolar, ao advento da globalização, da revolução da informação e sua digitalização gradual do Estado e suas instituições, da economia e da sociedade (NYE, 2010; SOUZA, 2013).

A crescente digitalização dos mais diversos setores é irreversível, em que as relações internacionais e sociais foram grandemente afetadas. Nesse sentido, é comum que a bibliografia sobre segurança cibernética entenda o espaço cibernético como um novo domínio, assim como a terra, o ar e a água. No entanto, a interação do Estado com esse espaço é peculiar devido aos elementos de desterritorialização, incerteza e difusão dos poderes que contrariam a noção de soberania do Estado (MEDEIROS; CARVALHO; GOLDONI, 2019; VENTRE, 2019), fazendo com que o Estado não se sinta seguro nesse espaço.

Somado a isso, a digitalização do mundo, seu relativo grau de horizontalidade e a permeabilidade ou ausência de fronteiras fazem com que ataques específicos de menor grau e em rede se tornem possíveis ameaças com capacidade de dano massivo à indivíduos, firmas e Estados ao redor do mundo, tendo em vista que estão todos conectados e sujeitos ao mesmo espaço, o cibernético. Essas características do tema de segurança cibernética são apresentadas

por Hansen e Nissenbaum (2009) como elementos formadores da necessidade de compreender a segurança cibernética quanto um setor dos estudos de segurança. A Escola de Copenhague detém o feito de ampliar as questões de segurança para além dos temas diretamente ligados ao Estado, adotando cinco setores para a agenda de segurança: militar, ambiental, social, político e econômico (MOTTA, 2014). Hansen e Nissenbaum (2009) propõem a adição da segurança cibernética como o sexto setor, sob a premissa de que a segurança cibernética possui uma gramática própria de interação com os objetos referentes e discursos securitizantes, satisfazendo os elementos de definição dos setores em Buzan, Waever e Wilde (1998).

Para sustentar o argumento de que segurança cibernética é um setor da agenda de segurança internacional, as autoras apontam que a segurança cibernética originou-se do movimento securitizador da segurança da computação, em que esta se compromete com boas práticas e desenvolvimento de softwares que sejam menos suscetíveis a erros/bugs que comprometem dados e redes em menor escala. A segurança cibernética surge no âmbito da segurança nacional sob o pretexto de uma ameaça cibernética possível com capacidade destrutiva em larga escala, que se insere no espectro político no formato de um discurso técnico enfatizando os riscos à segurança nacional (HANSEN; NISSENBAUM, 2009).

O espaço cibernético é o campo em que o setor segurança cibernética está ancorado. Com isso, as características desse campo são transferidas para o seu setor, a exemplo da imersão de indivíduos, firmas e Estados nesse território e o modo como encontram-se ligados (HANSEN; NISSENBAUM, 2009; NYE, 2010). Ele tem por efeito a multiplicidade de objetos referentes e discursos, sendo quatro no total: segurança nacional; segurança estatal; segurança privada e segurança das redes (DEIBERT apud HANSEN; NISSENBAUM, 2009). Essa multiplicidade de discursos e objetos referentes são denominados como uma competição (de discursos) que se conecta a uma constelação (objetos referentes), essa denominação exemplifica que o setor segurança cibernética possui a característica de que os discursos ganham coerência fazendo conexões com discursos e objetos distintos (HANSEN; NISSENBAUM, 2009).

A característica da existência simultânea de múltiplos discursos e objetos referentes não é única ao setor segurança cibernética, sendo encontrada também no setor econômico que possui uma relação de responsabilidade que recai sobre o público-privado também similar. No entanto, o setor econômico surge e recai sobre a figura do mercado liberal, enquanto o setor segurança cibernética está intrinsicamente conectado à manutenção da segurança nacional (HANSEN; NISSENBAUM, 2009).

A gramática do setor de segurança cibernética estaria pautada na capacidade de uma única ameaça afetar diretamente diversos objetos referentes, à título de ilustração, um ataque cibernético às instituições financeiras do Brasil estaria pondo em risco indivíduos, bancos, firmas e o Estado, o vazamento desses dados é prejudicial a todos eles por isso o interesse em securitizar é coletivo (HANSEN; NISSENBAUM, 2009).

As autoras definem três conceitos específicos da gramática de segurança do setor de segurança cibernética: hipersecuritização, práticas de segurança diárias e tecnificação. A hipersecuritização é definida pela percepção exacerbada dos níveis de ameaça. Apesar de ser um conceito com aplicabilidade a outros setores, Hansen e Nissenbaum (2009, p. 1164) entendem que na segurança cibernética a hipersecuritização está em seu ápice, e isso ocorre pela existência de discursos securitizantes que ressaltam o efeito cascata ou desencadeamento de eventos subsequentes a um ataque cibernético de impacto global e dano irreversível. O fato de não haver precedentes de um evento desse tipo, somado a escalabilidade desses possíveis eventos é crucial para instaurar e legitimar discursos securitizantes:

> A extrema confiança no futuro e a enormidade das ameaças que está em jogo torna o discurso suscetível a acusações de "exagero", no entanto, a escala da catástrofe potencial aumenta simultaneamente as apostas em ignorar os avisos. Fazendo com que a ausência de incidências anteriores vá na direção oposta, a dificuldade de dizer que não poderia acontecer também cria um espaço poderoso para a projeção do (im)possível (HANSEN; NISSENBAUM, 2009, p. 1164, tradução nossa).

Quanto às práticas de segurança diárias, as autoras relatam que atores securitizantes privados, como firmas e instituições, utilizam de discursos securitizantes apontando que os indivíduos estão experienciando ameaças durante suas atividades cotidianas. Podemos observar esse apelo no dia-a-dia quando empresas ressaltam a necessidade de não compartilhar dados de caráter confidencial ou a necessidade de adquirir um bom antivírus e o cuidado ao acessar certos conteúdos na internet. Hansen e Nissenbaum (2009) fazem um paralelo da experiência individual e sua capacidade de criar uma ameaça em larga escala no espaço cibernético com o cenário de epidemia, em que um único indivíduo "infectado" pode gerar danos a um grupamento maior. A prática de segurança diária e a hipersecuritização somadas geram a legitimidade para securitizar o espaço cibernético sob pena de prejuízo em outras áreas (HANSEN; NISSENBAUM, 2009, p. 1165).

O terceiro elemento da gramática do setor segurança cibernética trata-se da tecnificação, em que este elemento está relacionado à complexidade do espaço cibernético quanto ao conhecimento do mesmo. Hansen e Nissenbaum (2009) ressaltam a presença de indivíduos que possuem legitimidade para falar sobre segurança cibernética baseado no conhecimento específico que os mesmos possuem sobre o campo. Esses indivíduos podem ser

tidos como bons ou ruins, sendo os hackers enquadrados nos últimos. A tecnificação é responsável por causar a dualidade de, por um lado, a aproximação da audiência com os discursos securitizantes propostos pela hipersecuritização e, por outro, as práticas de segurança diárias, com o afastamento da mesma audiência em entender que é um tema complexo pertencente a figuras de conhecimento específico (HANSEN; NISSENBAUM, 2009). Por outro lado, essas figuras detentoras do conhecimento técnico se tornam atores securitizantes com uma suposta característica de neutralidade, diferenciando-se dos políticos e atores securitizantes públicos, além disso, a tecnificação é responsável por dar legitimidade aos discursos securitizantes (HANSEN; NISSENBAUM, 2009, p. 1167-1168).

A gramática do setor segurança cibernética ilustra a particularidade da relação do público-privado sob jugo da autoridade governamental como agente securitizante, porém tem por mais importante o feito de sua legitimidade está pautada no desconhecimento de um ambiente (espaço cibernético) no qual a sua audiência convive hodiernamente, sendo a inexistência de desastres anteriores seu maior trunfo, não há como se negar a escalabilidade dos danos de um ataque cibernético, porém não há critérios de mensuração do mesmo. O setor segurança cibernética é baseado no paradoxo de se compreender as ameaças cibernéticas com efeitos catastróficos de destruição completa à existência humana, ao passo de não ter nenhum evento anterior que o valide.

3 SEGURANÇA CIBERNÉTICA NO BRASIL

A construção de segurança cibernética no Brasil como eixo estratégico se iniciou na primeira década do século XXI, quando os ataques cibernéticos à Estónia[4] e à Geórgia[5] (2007 e 2008, respectivamente) e o vírus Stuxnet no, em 2010 no Irã[6], foram entendidos como eventos alarmantes, moldando a percepção brasileira e o trato com o tema de segurança cibernética, resultando na promulgação do primeiro documento de defesa e segurança brasileiro que tratava de segurança cibernética estrategicamente, a END de 2008 (HUREL; LOBATO, 2021; CEPIK; CANABARRO; BORNE, 2014).

A END é o primeiro documento brasileiro a tratar o setor cibernético como um tema estratégico, apresentando no corpo do texto que o setor cibernético é compreendido pela Defesa Cibernética e Segurança Cibernética, sendo o último um tema em conjunto com a Segurança da Informação e Comunicações que deve ser aprimorado visando a proteção das estruturas estratégicas da Tecnologia da Informação. Somado a isso, também está disposto que é necessário o fomento à pesquisa, inovação e desenvolvimento de novas tecnologias que permitam a criação e execução de um planejamento estratégico para a defesa cibernética, como também um planejamento que vise a segurança cibernética através da revisão do marco legal e normas afins (BRASIL, 2008).

É importante ressaltar a presença dos temas de defesa cibernética e segurança cibernética como áreas estratégicas correlatas, mas com planejamentos e desafios próprios que evidenciam a autonomia de cada área. Este é o motivo da bibliografia considerar a END (2008) como o marco da segurança cibernética brasileira, uma vez que a separação entre defesa e segurança cibernética não havia aparecido em nenhuma normativa anterior. Um exemplo é a PDN de 2005, que antecede a END como principal documento de defesa. Nela

---

[4] Em 2007, a Estónia estava em um impasse diplomático com a Rússia, após a retirada de uma estátua que representava a campanha do Exército Vermelho em território estoniano. Alguns dias após o ocorrido, houve uma enxurrada de ataques DDos, que são ataques que negam o funcionamento normal de um serviço em rede, nesse caso, ocorreu uma grande quantidade de acessos e solicitações em sites do governo da Estónia que resultou na interrupção desses serviços durante dias (LANDLER; MARKOFF, 2007).

[5] Durante as invasões da Rússia no território da Geórgia em 2008, houveram ataques cibernéticos similares aos que ocorreram na Estónia em 2007. Mais uma vez, se constatou uma grande quantidade de ataques DDos a sítios eletrônicos sob o controle do governo da Geórgia, mas dessa vez os ataques se estenderam aos sítios pertencentes a mídia internacional, instituições financeiras e empresas. Segundo alguns especialistas, esses ataques tinham como objetivo isolar a Geórgia do resto do mundo, bloqueando sua conexão em rede com o exterior. O caso da Geórgia pode ser visto como o primeiro exemplo de uma guerra cibernética, tendo em vista que o ataque cibernético foi utilizado durante um conflito armado (SHAKARIAN, 2011).

[6] No ano de 2010, o Irã sofreu um ataque massivo ao seu espaço cibernético por meio da disseminação do vírus Stuxnet em suas redes privadas do governo, em especial, a rede que continha as informações do projeto de enriquecimento de urânio que o Irã vinha desenvolvendo. Se descobriu que o vírus Stuxnet infiltrou-se na rede de sistemas da Siemens, com o objetivo de vazar informações do programa nuclear do país. O fato de que redes de controle de usinas nucleares podem ser invadidas, causou um temor na comunidade internacional de um ataque cibernético com efeitos físicos em larga escala (PICK, 2010).

não existem menções a segurança cibernética, citando brevemente a necessidade de se minimizar as vulnerabilidades brasileiras a um ataque cibernético, evidenciando que até então o setor cibernético só era visto do ponto de vista da defesa e de importância ocasional (BRASIL, 2008; BRASIL, 2005).

A END (BRASIL, 2008) apresentou a construção da segurança cibernética no Brasil como uma tarefa conjunta entre os diversos setores, militares e civis. É importante ressaltar que a END (2008) foi responsável pela estrutura institucional de defesa e segurança cibernética, em que o Gabinete de Segurança Institucional, vinculado à Presidência da República, trata sobre os assuntos de segurança cibernética, enquanto a área de defesa cibernética é reservada ao Ministério da Defesa e às Forças Armadas (BRASIL, 2008; CARRION, 2022, p. 22).

A PDN (2005) se caracterizou por apresentar "o posicionamento do País em relação à sua defesa e estabelecia os Objetivos Nacionais de Defesa", enquanto a END "orientava todos os segmentos do Estado brasileiro quanto às medidas a serem implementadas para se atingirem os objetivos estabelecidos" (BRASILa, 2012), sendo a PDN (2005) uma declaração de intenção e reconhecimento do espaço cibernético e sua importância para a segurança nacional (BRASIL, 2005; CARRION, 2022, p. 21).

A análise da PDN (2005) e da END (2008) levantam um fator crucial na construção da estrutura institucional e normativa de segurança cibernética brasileira, em que essa estrutura passou a ser composta e gerenciada majoritariamente por instituições ligadas a defesa nacional, com forte presença das Forças Armadas no desenvolvimento e operacionalização de medidas de segurança cibernética. Isso se deve a apresentação dúbia dos conceitos de segurança e defesa, em que os documentos permitem uma interpretação dos temas de segurança como assuntos de defesa, tornando recorrente a atuação das Forças Armadas em diversas temáticas de segurança.

Segundo Donadelli et al (2021), essa opacidade na definição e aplicabilidade dos conceitos de segurança e defesa no Brasil se estende para todas as temáticas de segurança e abre prerrogativa para a interpretação de que a atenção às ameaças externas e à segurança nacional sejam o norte preponderante. A definição na PDN que apresenta o conceito de defesa nacional como correlato à "preponderância de ameaças externas", representa um cenário em que o internacional pode ser tido como mais importante do que os assuntos domésticos, tomando a dianteira do desenvolvimento de uma pauta de segurança voltada para o exterior.

Ao utilizar a definição semântica do conceito de segurança nos documentos de defesa do Brasil, Donadelli et al (2021) elucidam que as Forças Armadas obtiveram maior controle

sobre a pauta de defesa no decorrer do tempo, com as atualizações dos documentos de defesa permitindo a atuação militar de modo mais abrangente e tornando notório a prerrogativa das Forças Armadas nos temas de defesa e segurança. A análise feita pelos autores apresenta que os documentos de defesa, em tese, buscam delimitar e institucionalizar os assuntos de defesa. No entanto, se observa que historicamente esses documentos enfraqueceram a atuação do poder político na pauta defesa e segurança, enquanto houve um fortalecimento dos militares no planejamento da pauta.

Um aspecto dessa dominância dos militares é a própria construção e planejamento desses documentos oficiais de defesa e segurança, que no geral são produzidos quase que exclusivamente pelas Forças Armadas, afastando as contribuições da sociedade civil e da comunidade acadêmica. O segundo aspecto é um resultado do primeiro, já que os militares controlam em grande parte a pauta de defesa e segurança, tornando-se visível uma transmutação dos documentos de defesa em documentos próprios da instituição: "muito embora levem por título 'documentos de defesa', eles se limitam, no melhor dos casos, a documentos militares, restringindo o âmbito semântico da defesa apenas ao seu instrumento específico." (DONADELLI et al, 2021, p. 153)

Infere-se da análise feita pelos autores que há uma predominância da interpretação dos militares acerca dos temas de segurança e defesa. Portanto, é esperado que os princípios de defesa nacional e de combate à ameaça externa, tão importantes à própria concepção das Forças Armadas, sejam elementos preponderantes na construção da pauta de segurança cibernética (DONADELLI et al, 2021). Os autores possuem uma passagem ao final do texto, que apresenta bem o contexto em que a pauta de segurança cibernética se desenvolveu:

> A leitura dos documentos na sua dimensão histórica deixou-nos a impressão da firmeza de projetos das forças armadas de recuperar a posição no palco político nacional da que se afastaram por pouco tempo. Na verdade, parecem querer recuperar sua origem de guardas nacionais voltadas a reprimir manifestações de descontento para manter a lei do mercado e a ordem burguesa. Ver a dissolução dos limites entre defesa e segurança e a preocupação jurídica dos militares para atuar no cenário doméstico nos deixou com a clara impressão de profundo e amargo retrocesso do processo de democratização brasileira da mão amiga dos militares (DONADELLI et al, 2021, p. 154).

Desse modo, a interpretação de uma normativa que pressupõe que os temas de segurança e defesa devem ser observados majoritariamente pela ótica da ameaça externa, fruto da forte presença das Forças Armadas, corrobora com o fenômeno da criação da estrutura institucional e normativa de segurança cibernética brasileira e o modo como o mesmo se desenvolveu, especialmente no período dos megaeventos.

De 2008 em diante o tema de segurança cibernética continuou sendo fomentado e gerenciado por uma estrutura institucional com foco em defesa. Isso se deveu à percepção de ameaça externa fomentada pelos casos da Geórgia, Estónia e Irã, que foram alarmantes e fundamentais para a fundação dessa percepção pautada na capacidade de um ataque cibernético causar danos irreversíveis em uma escala global. No entanto, mesmo estes casos não produziram danos que correspondam ao imaginário de um potencial destrutivo em larga escala. Para Hansen e Nissembaum (2009), os três casos de ataques cibernéticos foram gerenciados com êxito ao mitigar uma possível escalada de danos.

Tendo isto em mente, podemos considerar que esses eventos de ataques cibernéticos que antecederam a aparição do setor cibernético como eixo estratégico no Brasil atuaram como estimuladores da temática de segurança cibernética na administração pública brasileira. Devido à criação da percepção de uma ameaça cibernética de magnitude global, o qual não corrobora com a realidade e que não possui um evento passado de mesma proporção, é apresentado por Hansen e Nissembaum (2009) a partir do conceito de hipersecuritização. No que tange à realidade brasileira, é possível identificarmos o quanto os eventos externos fomentaram processo semelhante, à exemplo da noção brasileira de que a ameaça cibernética é majoritariamente externa e com alta escalabilidade, contrariando a realidade do caso brasileiro.

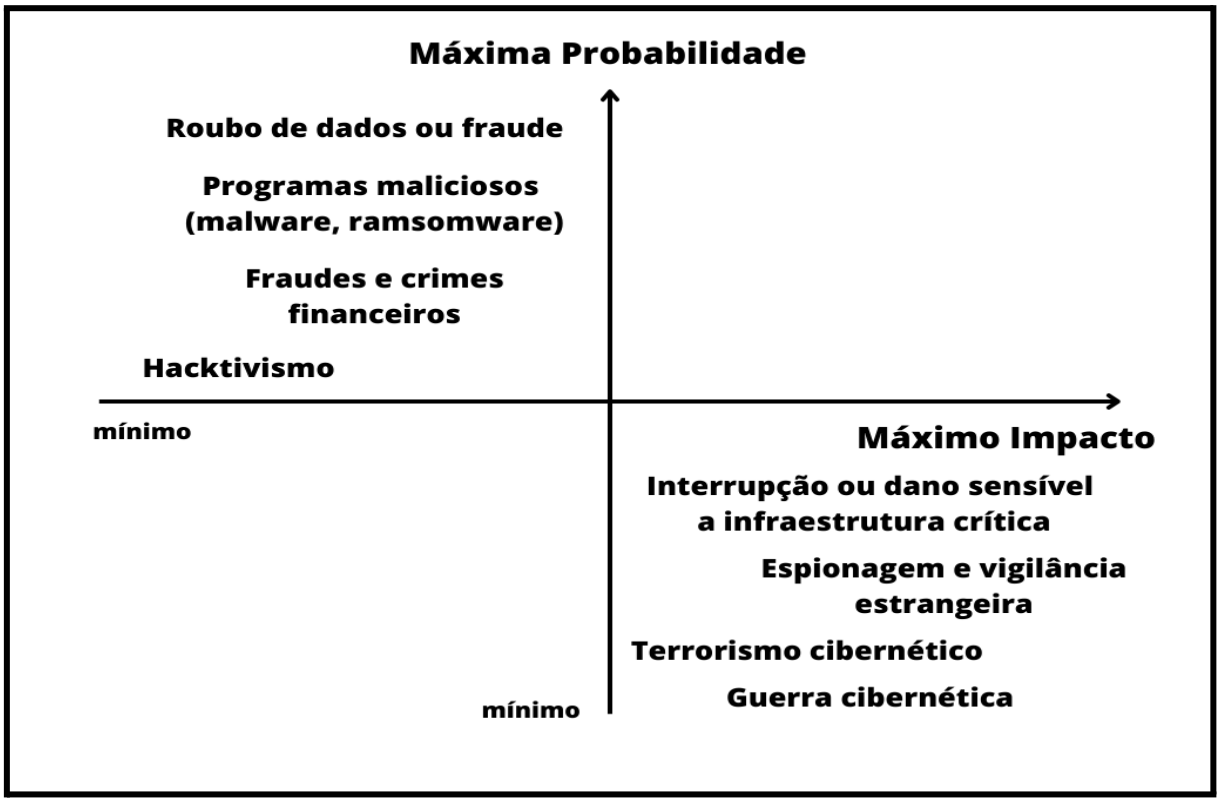
Desse modo, Hurel e Lobato (2021) reforçam que os discursos securitizantes que fomentam a segurança cibernética no Brasil tendem a colocar o risco à segurança nacional como principal elo, quando, na verdade, se sabe que o nível de ameaça cibernética no Brasil advém de ataques cibernéticos de menor expressão, como hacking, fraudes e roubo de dados. Com o intuito de exemplificar a percepção e a realidade do tema de segurança cibernética no Brasil, as autoras apresentam um esquema de análise do risco cibernético brasileiro baseado em impacto e probabilidade. O impacto é a escalada de danos de um ataque, sendo um ataque de impacto máximo aquele que resulte em milhares de mortes e danos irreversíveis, enquanto um ataque com probabilidade máxima aquele em que há uma enorme chance de acontecer com recorrência.

Ainda em Hurel e Lobato (2021), nos é apresentado que se baseando nos dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) há uma crescente exponencial de ataques cibernéticos do tipo fraude e roubo de dados no decorrer dos anos, o que faz com que a probabilidade desse tipo de ataque seja extremamente alta, porém esses tipos de ataque não são de alto impacto. Enquanto ao analisar ataques sensíveis à segurança nacional, como guerra cibernética, ameaça a infraestrutura cibernética e

terrorismo cibernético são ataques de altíssimo impacto mas possuem baíxissima probabilidade, conforme o exposto na figura 1.

Sabendo que a percepção do risco cibernético no Brasil é proveniente da necessidade de proteger a segurança nacional, mesmo que contrariando a realidade do caso brasileiro, é perceptível a forma como o quadro institucional e as discussões em segurança cibernética no Brasil ganham um tom mais voltado à prevalência da segurança do Estado, concedendo a prerrogativa operacional, estratégica e política de segurança cibernética a instituições de caráter de defesa, como o Ministério de Defesa, as Forças Armadas e o Gabinete de Segurança Institucional da Presidência da República (HUREL, 2018; HUREL; LOBATO, 2021).

Figura 1 - Gráfico de probabilidade e impacto de ataques cibernéticos no Brasil



Fonte: Hurel e Lobato, 2021[7].

Os conceitos de segurança e defesa adotados na PDN (2005) e que são recorrentes em documentos de defesa posteriores, somados aos eventos da Geórgia, Estónia, Irã e seus efeitos para a criação da pauta de segurança cibernética brasileira, são elementos analíticos que

[7] A imagem é uma adaptação da figura presente em Hurel e Lobato (p. 508, 2021).

evidenciam a trajetória normativa e institucional do tema de segurança cibernética no Brasil, inclusive nos apresentando que a consolidação da percepção do risco advindo da ameaça externa é resultado da junção desses elementos. Dessa forma, essa dimensão foi um divisor de águas que reforçou os discursos securitizantes na pauta de segurança cibernética (LOBATO; KENKEL, 2015).

4 ANÁLISE DA EVOLUÇÃO NORMATIVA EM SEGURANÇA CIBERNÉTICA NO BRASIL (2012-2016)

Como mencionado no capítulo anterior, a promulgação da Estratégia Nacional de Defesa (END) de 2008, é o marco inicial para a consideração do espaço cibernético como um tema de segurança e defesa no país, tendo em vista que foi o primeiro documento de estratégia de defesa que apresentava o espaço cibernético como elemento transversal ligado ao desenvolvimento industrial e tecnológico, aparecendo no documento também como setor de importância estratégica a ser fortalecido, ao lado do eixo espacial e nuclear (BRASIL, 2008; HUREL; LOBATO, 2021; HUREL, 2018; LOBATO; KENKEL, 2015; OLIVEIRA; PORTELA, 2017; MEDEIROS; CARVALHO; GOLDONI, 2019).

A PDN de 2005 foi complementada pela END (2008) e atualizada para Política Nacional de Defesa (PND) em 2012, que trouxe a ligeira mudança no nome como uma demonstração de que a PDN (2005) deixava de ser um documento setorial do Ministério da Defesa e passava a ser compreendida enquanto documento orientador para os diversos setores de segurança e defesa (BRASIL, 2005; BRASIL, 2008; BRASIL, 2012a; OLIVEIRA; PORTELA, 2017)[8]. Segundo os autores Oliveira e Portela (2017) e a própria observação dos documentos PDN (2005) e PND (2012), o elemento de desenvolvimento de tecnologias autônomas para o ambiente cibernético é um objetivo comum entre esses documentos e que se transfere para os subsequentes, no entanto, é interessante notar que da PDN (2005) para a PND (2012) há uma mudança de percepção sobre essa autonomia tecnológica. Enquanto o documento de 2005 previa uma aspiração mais ideal para o desenvolvimento de tecnologia autônoma, o documento de 2012 já trata dessa questão com uma percepção de que é impossível seguir um caminho de tecnologias completamente nacionais.

Ao tratar da evolução institucional da pauta de segurança cibernética no Brasil é indispensável verificar a primeira aparição do tema no Livro Branco de Defesa (LBDN). Segundo Oliveira e Portela (2017, p. 87) o Congresso Nacional recebeu a incumbência de apresentar o LBDN no ano de 2012 devido a Lei Complementar nº 136/2010. Desse modo:

> [...] O livro seguiu praticamente a mesma estrutura da END de 2012, porém com maior profundidade e detalhes. Nas palavras do então ministro de defesa, Celso Amorim, o objetivo do LBDN era, conjuntamente com a END e a PND, ser "um documento esclarecedor sobre as atividades de defesa do Brasil" [...] Nesse livro, a

[8] É importante lembrar que os documentos de defesa, apesar da denominação, tratam de segurança e defesa. Acontece que o conceito de segurança estava arraigado ao conflito interestatal, com o passar do tempo esse conceito se expandiu para temas políticos, sociais e outros que estão ligados a situação interna. Desse modo, os documentos de defesa se ajustaram a essa mudança e apresentam questões de segurança, voltadas para esses temas internos e de defesa, voltadas a questões externas de resposta a ameaças. A PND 2012, apresenta em seu texto uma distinção de segurança e defesa, bem como os temas que se enquadram em cada uma, além de afirmar que trata de ambos os elementos (BRASIL, p.13, 2012a)

> defesa cibernética começa a ser tratada no tópico que aborda o ambiente estratégico do século XXI. Nessa parte, esse ambiente é abordado como um novo tema ou novas abordagens, que influenciam no sistema internacional do século e, por isso, têm implicações para a soberania dos países (OLIVEIRA; PORTELA, 2017, p. 87).

Para Medeiros, Carvalho e Goldoni (2019, p. 57) e Carrion (2022, p. 23) é interessante apontar que antes da END de 2012, houve o "Livro Verde: Segurança Cibernética no Brasil" de 2010, que foi elaborado com o intuito de servir como orientação para a elaboração do LBDN no tema de segurança cibernética. O Livro Verde já apresentava como premissa o fomento a um espaço cibernético brasileiro desenvolvido e a um panorama de reconhecimento do espaço cibernético enquanto tema sensível de segurança internacional. Além de retomar as premissas sobre a necessidade de programas de cooperação entre governo e sociedade civil, o documento também enfatizou a urgência de uma Política Nacional de Segurança Cibernética, a qual não se concretizou até os dias de hoje[9] (CARRION, 2022).

É com a elaboração do Livro Branco de Defesa (2012) que somos apresentados ao Centro de Defesa Cibernética (CDCiber), responsável pela coordenação das ações de segurança e defesa cibernética no Brasil. O CDCiber está vinculado ao Exército cumprindo com o disposto na Estratégia Nacional de Defesa (2008), a qual definiu a esta instituição como órgão responsável por essa temática. Com a revisão da END, em 2012, o CDCiber adquiriu capacidade de se tornar parte do então criado Comando de Defesa Cibernética das Forças Armadas (ComDCiber), havendo um fortalecimento institucional das Forças Armadas e do Ministério da Defesa, devido as figuras do CDCiber e ComDCiber (HUREL, 2018; MEDEIROS; CARVALHO; GOLDONI. 2019). É importante ressaltar que o ComDCiber é o principal órgão de resposta e coordenação a ataques cibernéticos, tendo como atribuições “planejar, orientar, supervisionar e controlar as atividades operacional, de inteligência, doutrinária, de ciência e tecnologia, bem como de capacitação no Setor Cibernético de Defesa” (BRASIL, 2016b, p. 58), enquanto o CDCiber é um órgão subordinado a ele que contribui com a execução das atividades operacional e de inteligência.

Apesar disso, existem outros órgãos que compõem a governança cibernética brasileira: a Agência Brasileira de Inteligência (ABIN), o Ministério de Defesa (MD), o Exército Brasileiro (EB), a Presidência da República, a Câmara de Relações Exteriores e Defesa Nacional (CREDEN), do Conselho de Defesa Nacional (CDN), o Departamento de

[9] De fato, apesar da previsão legal prevista na END (2012) para a criação de uma Política Nacional de Segurança Cibernética, não houve até os dias de hoje a concretização. No entanto, a Estratégia de Segurança Cibernética (E-Ciber, 2020) é o que se tem de mais próximo desse documento.

Segurança da Informação e Comunicações (DSIC) e o Gabinete de Segurança Institucional da Presidência da República (GSI-PR) (LOBATO; KENKEL, 2015, p. 36).

Desse modo, as primeiras edições da END e PDN (depois PND) inauguraram o setor cibernético como um eixo estratégico. Para a bibliografia, o período que consiste os megaeventos (2012-2016) foi propulsor de práticas e normativas sobre o tema segurança cibernética no Brasil, em que as edições da END, PND e LBDN de 2012 à 2016 são importantes para entender o cenário que estava posto durante os megaeventos e o que se gerou durante esse período (HUREL, 2018; HUREL; LOBATO, 2021). Como dito anteriormente, a PND de 2012 não apresentou uma análise robusta sobre segurança cibernética, sendo um documento muito curto e raso ao tratar de segurança cibernética. Ela é citada apenas indiretamente por meio de termos como "tecnologia" e "informação" para tratar de ameaças e vulnerabilidades a outros setores como o continental, aeroespacial e marítimo que também são afetados pelo setor cibernético (BRASIL, 2012a).

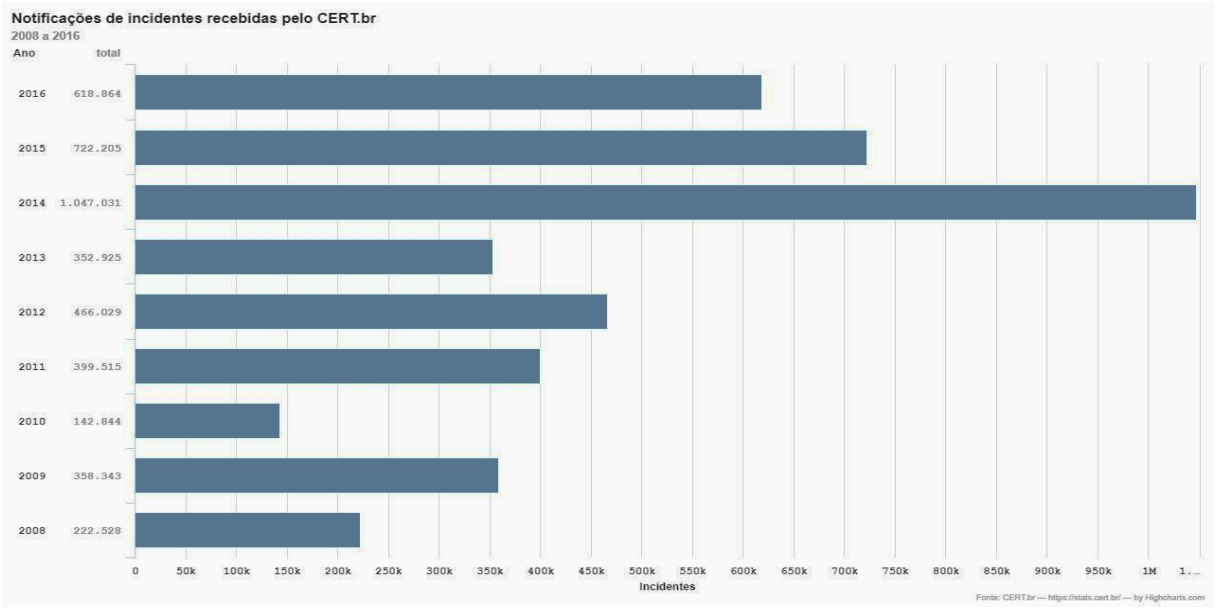
Por outro lado, a END de 2012 serviu como conteúdo base do tema de segurança e defesa cibernética para o que veio a ser o LBDN 2012. Apesar de suas contribuições para a prescrição do ComDCiber, o aprimoramento da Segurança da Informação e Comunicação e para alertar sobre a necessidade de se proteger os dados administrativos do país, a END não ofereceu especificidades e detalhes sobre segurança cibernética, sempre retomando a necessidade de se proteger a "infraestrutura crítica" através de "medidas", sem detalhar como tal iniciativa seria realizada, fazendo com que esses termos se tornassem repetitivos durante a leitura do documento (BRASIL, 2012a). Do mesmo modo, o LBDN 2012 não se diferencia da END 2012 em conteúdo informativo e prescricional em segurança e defesa cibernética (BRASIL, 2012b).

A END, a PND e o LBDN de 2012 juntos representam um arcabouço normativo que reforçam o setor cibernético como matéria de defesa nacional, formando uma estrutura em que as instituições de defesa cibernética atuam majoritariamente na temática de segurança cibernética, transpondo a lógica de defesa nacional e da ameaça da guerra cibernética para a segurança cibernética.

De 2012 a 2016 o Brasil sediou a Rio+20, a Copa do Mundo e as Olimpíadas, cada uma com um intervalo de dois anos. Durante esse período o país se preocupou com a possibilidade de algum ataque cibernético de grande magnitude, tendo em vista a imensa quantidade de visitantes internacionais que receberia. De fato, houve durante esse período um aumento exponencial de notificações de ataques cibernéticos recebidos pelo CERT.br, o que nos apresenta que, apesar do aumento natural de ocorrências no decorrer dos anos, o ano de

2014, ano este em que ocorreu a Copa do Mundo, representou um pico anormal de notificações, como podemos ver na tabela 1 a seguir.

Tabela 1 - Notificações de incidentes recebidas pelo CERT.br (2008-2016)



Fonte: CERT.br

Nesse cenário foi aprovada a portaria número 2.221/2012 em que o Ministério da Defesa designou as Forças Armadas como responsáveis pela segurança e defesa cibernética durante os megaeventos (BRASIL, 2012c; HUREL, 2018).

Segundo Hurel (2018), durante a Rio+20 alguns dos sites correlatos ao evento sofreram ataques cibernéticos que tiveram sua autoria requisitada pelo grupo Anonymous, os quais se mostraram descontentes com a conferência e o modo como esta vinha sendo conduzida. Apesar da resposta do Brasil aos ataques ter sido composta por um grupo que envolveu as Forças Armadas, o CDCiber, a Polícia Federal, o CERT.br e o CTIR.gov, a coordenação a nível estratégico e operacional ficou a mando das instituições ligadas ao Ministério da Defesa e o GSI/PR.

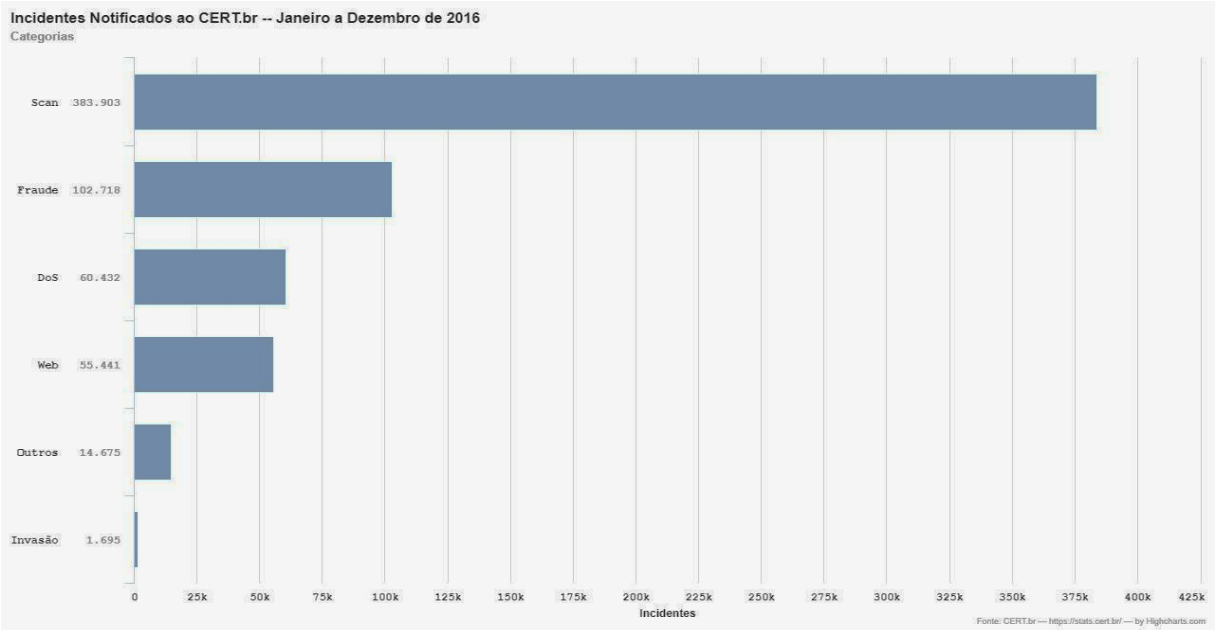
O período dos megaeventos foi composto por ações conjuntas entre os órgãos de defesa cibernética subordinados ao MD e ao GSI/PR com órgãos governamentais independentes (CERT.br, CTIR.gov), em resposta à crescente de ataques cibernéticos. Porém, apesar das ações conjuntas entre os diferentes órgãos, a estrutura de segurança e defesa cibernética que nos é apresentada pela END, PND e LBDN permite que as Forças Armadas, o MD e o GSI/PR continuem tendo o controle sobre a construção da pauta de segurança e defesa cibernética Esse domínio reservado nos aponta para uma maior possibilidade de

securitização da segurança cibernética no Brasil (HUREL, 2018; LOBATO; KENKEL, 2015). A denúncia de espionagem dos EUA em relação ao Brasil, em 2013, também serviu de catalisador para a cristalização de um discurso securitizante da guerra cibernética, reforçando a identificação de uma ameaça externa, elemento presente nos documentos de segurança que norteiam a pauta de segurança cibernética no país (HUREL, 2018; Greenwald *et al*, 2013).

É interessante olhar para o elemento da ameaça externa que paira sobre toda a construção da segurança cibernética no Brasil e comparar com o aumento dos ataques cibernéticos no decorrer dos anos. O CERT.br dispõe de dados referentes aos tipos de ataques cibernéticos que ocorrem por ano e também do local em que esses ataques são provenientes. Infelizmente o CERT.br só possui dados sobre os locais em que os ataques foram originados a partir de 2016. Sendo assim, ao compararmos a tabela 1 sobre o montante de ataques cibernéticos anuais com as tabelas 2 e 3 que são, respectivamente, os tipos de ataques e o local do qual partiram, podemos visualizar a falácia de que a ameaça externa é o maior desafio para a segurança cibernética, uma vez que, majoritariamente, os ataques se tratam de scans e fraudes, além de que os ataques partem do interior do próprio Brasil e não do exterior, contrariando o argumento defendido nos documentos de defesa e suas instituições (tabela 2 e 3, p. 37-38).

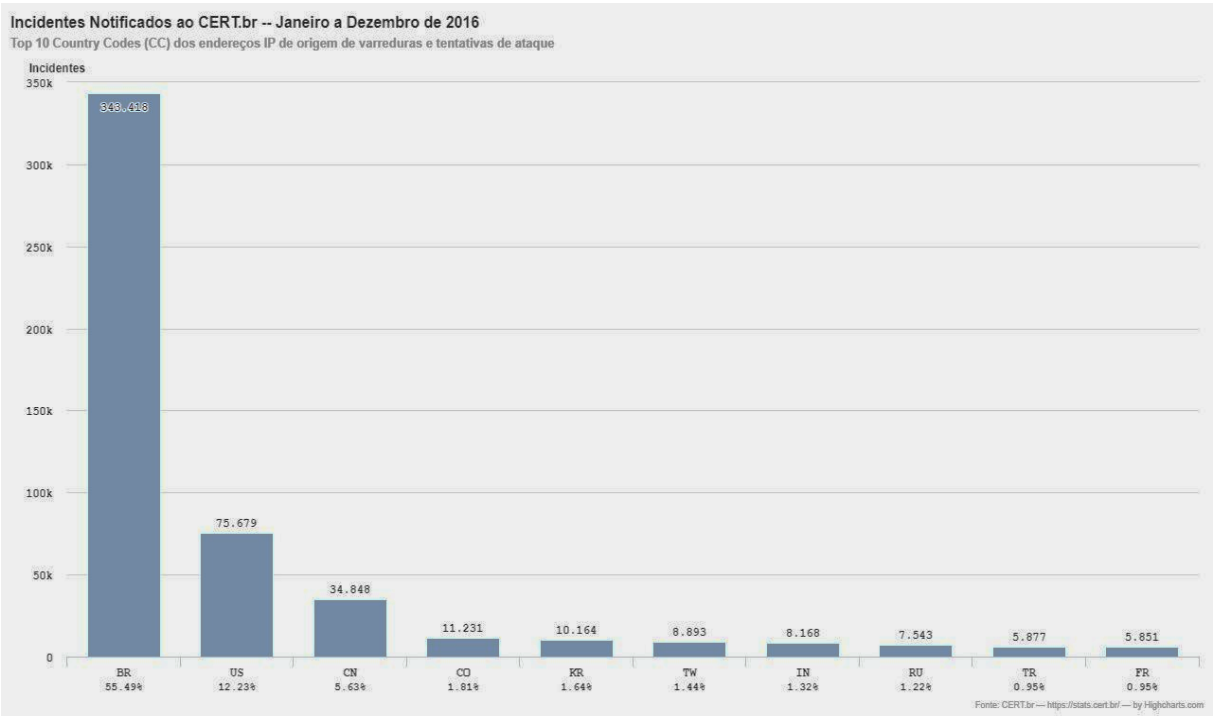
Os dados apresentados nas tabelas 2 e 3 (p. 37-38) reforçam o argumento de Hurel e Lobato (2021) quanto à natureza do risco cibernético no Brasil, em que grande parte das ameaças são de impacto mínimo: fraudes, roubo de dados e etc (Figura 1, p. 32). Bem como substanciam o fenômeno da hipersecuritização no caso brasileiro, visto que se fomenta um imaginário de ameaça cibernética externa com potencial destrutivo massivo, quando na verdade o risco ao qual o Brasil está submetido é oriundo de ataques cibernéticos simples, desordenados e com baixíssimo impacto do ponto de vista da sobrevivência do Estado.

Tabela 2 - Incidentes notificados por categoria ao CERT.br (2016).



Fonte: CERT.br

Tabela 3 - Incidentes Notificados por endereço de IP ao CERT.br (2016).



Fonte: CERT.br

Em 2016, durante o último ano do período dos megaeventos, o Brasil apresentou a atualização da END, PND e LBDN prevista na Lei complementar nº 136 de 2010, a qual entrou em vigor a partir do ano de 2012, e que determina a atualização desses documentos a cada 4 anos (BRASIL, 2010; OLIVEIRA; PORTELA, 2017). Devido à experiência obtida durante os megaeventos, já era esperado que os documentos fossem apresentados com maior nível de detalhamento sobre os objetivos e as medidas que serão aplicadas para alcançar um

fim desejável na pauta de segurança cibernética. De fato houve avanço no detalhamento e o arranjo normativo trouxe maior transparência para essas ações.

Dentre as novidades presentes na END 2016 em comparação a END 2012, podemos ressaltar a aparição do termo “Segurança Cibernética” como não subordinado à Defesa Cibernética e à Segurança da Informação e Comunicações. Enquanto a END de 2012 no mesmo trecho tratava segurança cibernética indiretamente como sendo o mesmo que segurança da informação e comunicações ou como condição para o aprimoramento da defesa cibernética, a nova edição do documento não só traz o termo como também sinaliza a autonomia do conceito, apresentando que segurança da informação e comunicações, segurança cibernética e defesa cibernética atuam em conjunto para se atingir o resultado esperado para o setor cibernético (BRASIL, 2016a).

Essa lógica de reafirmação do tema de segurança cibernética se estendeu para parte do documento que relata as "Estratégias e Ações Estratégicas de Defesa". Como se trata de uma revisão do documento anterior é compreensível que a estrutura dos documentos se repita. No entanto, o trecho que traz os "Objetivos Nacionais de Defesa" (OND) aparece no documento de 2016 com muito mais detalhes do que no documento anterior, apresentando elementos de segurança cibernética necessários à implementação de estratégias específicas para os OND (BRASIL, 2016a) A tabela 4 nos apresenta de forma resumida, os OND e suas respectivas Ações Estratégicas de Defesa.

Tabela 4 - Representação dos Objetivos Nacionais de Defesa e suas Ações Estratégicas de Defesa que o cibernético está inserido como medida estratégica.

Objetivos Nacionais de Defesa (OND)	Ações Estratégicas de Defesa (AED)
Garantir a Soberania, o Patrimônio Nacional e a Integridade Territorial	AED-2 Contribuir para o incremento do nível de segurança das Estruturas Estratégicas (sistema de captação, tratamento e distribuição de água, geração e distribuição de energia elétrica, sistemas de transporte, produção e distribuição de combustíveis, finanças, comunicações e cibernética) AED-10 Incrementar as capacidades de defender e de explorar o espaço cibernético.
Promover a Autonomia Produtiva e Tecnológica na Área de Defesa	AED-69 Promover o desenvolvimento da tecnologia cibernética.

Fonte: Política Nacional de Defesa e Estratégia Nacional de Defesa, 2016

Em relação ao LBDN de 2016, os elementos presentes na END e PND de 2016 são transferidos para esse documento do mesmo modo que ocorreu com os documentos de 2012, conforme pode ser visualizado na tabela 5 (p. 41). Por conta dessa relação, não há inovações que sejam pertinentes ao escopo da nossa análise, principalmente do ponto de vista conceitual, tendo em vista que há um certo tradicionalismo conceitual que atravessa o tempo nos documentos (BRASIL, 2016b; DONADELLI *et al*, 2021). O mesmo acontece com a PND 2016, que infelizmente continua a tratar segurança cibernética de modo raso e indireto, referindo-se a ela por meio de referências à segurança da informação e comunicações, mas principalmente por meio do termo defesa cibernética (BRASIL, 2016a).

Tabela 5 - A abordagem dos Documentos de Defesa sobre Segurança e Defesa Cibernética (2012-2016)[10]

Documentos Oficiais	**Referências a Segurança e Defesa Cibernética**
Estratégia Nacional de Defesa (2012)	-Apresenta a necessidade de se fortalecer o setor cibernético, como eixo estratégico.(p. 49)
	- Define um rol de prioridades para o setor cibernético: fomentar a pesquisa científica voltada para o setor; (p. 93-94)
	- Desenvolver sistemas de defesa computacional; desenvolver tecnologias que permitam o planejamento e a execução da defesa e segurança cibernética no âmbito do Ministério da Defesa; (p. 94)
	- Produzir avanços no emprego dos poderes cibernéticos operacionais e estratégicos, em prol da proteção da infraestrutura estratégica. (p. 94)
Política Nacional de Defesa (2012)	- Apresenta a necessidade de se fortalecer o setor cibernético, como eixo estratégico.(p. 32)
	- Dispõe que para se opor a possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos de suporte de tecnologia da informação e comunicação. (p. 34)
Livro Branco de Defesa Nacional* (2012)	- A proteção do espaço cibernético abrange um grande número de áreas, como a capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional e gestão de pessoal; (p. 69)
	- Compreende, também, a proteção de seus próprios ativos e a capacidade de atuação em

[10] A análise do Livro Branco de Defesa Nacional em suas duas versões (2012 e 2016), esteve centrada na leitura específica dos documentos em seus capítulos voltados para o setor cibernético, é possível que haja alguma outra menção indireta a segurança e defesa cibernética dentre as mais de 400 páginas de ambos os documentos somados.

	rede. (p. 69)
	- Fomentar a base industrial de defesa; induzir a indústria nacional a produzir sistemas inovadores; e produzir componentes críticos nacionais. (p. 69)
	- Objetivos que se espera alcançar com o Centro de Defesa Cibernética (CDCiber): melhoria da capacitação dos recursos humanos; atualização doutrinária; (p. 69)
	- fortalecimento da segurança; respostas a incidentes de redes; incorporação de lições aprendidas; e proteção contra ataques cibernéticos.
Estratégia Nacional de Defesa (2016)	- Define um rol de prioridades para o setor cibernético: Capacitar o setor civil e militar quanto ao setor cibernético; (p. 55-56)
	- Aprimorar a Segurança da Informação e Comunicações e a Segurança Cibernética, em todas as instâncias do Estado, com ênfase na proteção das estruturas estratégicas relacionadas a Tecnologia da Informação; (p. 56)
	- Fomentar a pesquisa e desenvolvimento com foco nas tecnologias, que permitam a execução e planejamento da defesa cibernética e segurança cibernética no âmbito do Ministério da Defesa; (p. 56)
	- Fortalecer a atuação colaborativa entre o setor de defesa e a comunidade acadêmica, os setores públicos e privados e a Base Industiral de Defesa. (p. 56)
Política Nacional de Defesa (2016)	- O amplo espectro de possibilidades no ambiente cibernético requer especial atenção à segurança e à defesa desse espaço virtual. (p. 14)
Livro Branco de Defesa Nacional (2016)*	- Apresenta o mesmo texto do documento anterior (LBDN 2012), porém traz informações relacionadas ao CDCiber e o ComDCiber:
	- O Comando de Defesa Cibernética (ComDCiber), organização militar conjunta, na estrutura organizacional do Comando do Exército, [...] vem somar esforços com as organizações governamentais já existentes; (p. 58)
	- E tem como principais atribuições, dentre outras, planejar, orientar, supervisionar e controlar as atividades operacional, de inteligência, doutrinária, de ciência e tecnologia, bem como de capacitação no Setor Cibernético de Defesa. (p. 58)
	- Os órgãos subordinados ao ComDCiber são o Centro de Defesa Cibernética (CDCiber) e a ENaDCiber, também conjuntos, compostos por servidores das três Forças Singulares.
	- O CDCiber o tem por finalidade a execução das atividades operacional e de inteligência no âmbito do Sistema Militar de Defesa Cibernética;
	- Enquanto a ENaDCiber em tela tem por missão fomentar e disseminar as capacitações necessárias à Defesa Cibernética, no âmbito da Defesa Nacional, nos níveis de sensibilização, conscientização, formação e aperfeiçoamento. (p. 58)
	-A implantação do ComDCiber situa o MD no rol das organizações, nacionais e internacionais, que tratam a Segurança e a Defesa Cibernéticas. (p. 58)

Fonte: Elaborado pelo autor com base nos documentos analisados (2012a; 2012b; 2012c; 2016a; 2016b; 2016c)[11]

A estrutura normativa construída pela tríade END, PND e LBDN de 2008 a 2016 apresenta a constante proeminência dos temas de defesa sobre os temas de segurança. Donadelli et al (2021) afirmam que é recorrente na história do Brasil o envolvimento das Forças Armadas, uma instituição de defesa, em assuntos internos e/ou de segurança. Essa sobreposição institucional dos assuntos de defesa sobre os de segurança já foi vista no período dos megaeventos de forma prática e tem sido reforçada por meio de normativas que sustentaram essa atuação durante todos esses anos (HUREL, 2018).

Sendo assim, o modo como a estrutura institucional de segurança cibernética no Brasil está inserida, reforça e se retroalimenta de discursos securitizantes pautados na determinação da segurança cibernética como um assunto de defesa nacional, que permite ações excepcionais e um ordenamento legal e organizacional baseado na tomada de decisão por parte do Ministério de Defesa, do GSI/PR e das Forças Armadas, os quais controlam a pauta de segurança cibernética nos níveis político, estratégico e operacional. Para alguns autores (LOBATO; KENKEL, 2015) essa concentração da pauta de segurança cibernética na figura do Gabinete da Presidência e órgãos correlatos é uma demonstração de movimento securitizador.

Dado toda a análise e discussão disposta neste capítulo, podemos apontar que no período de 2008 a 2012 ocorreu o surgimento da pauta de segurança cibernética. É nesse recorte temporal que as temáticas de segurança e defesa cibernética aparecem pela primeira vez nos documentos de defesa, considerando o setor cibernético como eixo estratégico e de destaque para os próximos anos. Consequentemente, o período de 2012 a 2016 representou a consolidação de todo o arcabouço e estrutura institucional de segurança e defesa cibernética que havia sido criado até então, em que os megaeventos foram catalisadores e atuaram como um teste para o Brasil, tornando-se o período mais relevante para a compreensão do tema de segurança cibernética no país.

[11] A tabela é uma elaboração própria, baseada na leitura dos documentos de defesa inseridos no recorte temporal de 2012 a 2016. A tabela buscou trazer o modo como o assunto de segurança e defesa cibernética são abordados na íntegra dos documentos oficiais.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa se propôs a responder a pergunta: como se deu a expansão normativa e institucional do Brasil para tratar do tema da segurança cibernética no período dos megaeventos de 2012 a 2016? Para tal, o trabalho perpassou por delimitar e conceituar ontologicamente a área científica em que este debate está inserido, apresentando a segurança cibernética como uma temática relevante para os estudos contemporâneos de segurança internacional, devido especialmente a expansão das temáticas de segurança internacional ocorrida no final do século XX, bem como o sentimento de vigilância que se criou no século XXI para o espaço cibernético.

Além disso, as discussões conceituais e interpretações do campo da segurança cibernética são majoritariamente observadas pela bibliografia a partir da ótica do fenômeno de securitização. Autores como Hansen e Nissembaum (2009) sugerem que partindo da teoria de securitização (BUZAN et al, 1998) a segurança cibernética apresenta condições e características para se firmar como "setor", colocando segurança cibernética no mesmo rol de categorias de análise que os setores militar; econômico; político; social e ambiental, nos termos da teoria da securitização. Em outras palavras, as autoras defendem que a segurança cibernética deve ser analisada como um elemento de análise autônomo, evidenciando a relevância e as particularidades próprias dessa área.

Passado o resgate e delimitação conceitual da segurança cibernética enquanto área científica, partimos para os recortes do objeto, que é o recorte geográfico e temporal, sendo o Brasil durante o período dos megaeventos, de 2012 a 2016. Sendo assim, há a retomada do tema de segurança cibernética no Brasil com base na bibliografia especializada e nos documentos oficiais que tratam do tema. Dado a contextualização do caso brasileiro, voltamos à análise do período dos megaeventos que são tidos como parte importante da consolidação de toda a estrutura institucional e normativa do Brasil, acerca do tema (HUREL, 2018; HUREL; LOBATO, 2021).

Os anos de 2012 a 2016 compreenderam o período em que o Brasil sediou grandes eventos como a Rio +20 e a Copa do Mundo, em que esse cenário de grande fluxo de visitantes e de palco para o Brasil internacionalmente foi visto como um desafio pelas instituições de defesa e segurança cibernética. Foi uma ótima oportunidade de pôr à prova a estrutura institucional do Brasil e sua capacidade de responder às ameaças cibernéticas externas, que se esperava ocorrer devido aos megaeventos.

De fato, houve um crescimento de incidentes cibernéticos durante os megaeventos, especialmente em 2014 (CERT.br). No entanto, esses incidentes foram em sua maioria

ataques cibernéticos voltados para o roubo de dados e fraude financeira em pequena escala, além de que o local de origem desses incidentes se originou majoritariamente no Brasil. Ou seja, toda a estrutura institucional e normativa que foi construída sobre a percepção de que as ameaças externas representam o maior risco para o Brasil se traduziu como uma percepção enganosa.

Conforme a bibliografia, a estrutura institucional do Brasil em segurança cibernética é centrada na percepção errônea de risco elevado vindo de um inimigo externo com capacidade de ameaçar a sobrevivência do Estado. Esse fenômeno é responsável, em parte, pela predominância da pauta de defesa sobre a de segurança, a exemplo das instituições que atuam no planejamento e operacionalização da pauta de segurança, que são majoritariamente órgãos de defesa. Há ainda o agravante de que os documentos oficiais que deveriam delimitar e legitimar os assuntos de segurança, na verdade o fazem de modo que permite a sobreposição pelos assuntos de defesa, ou ainda que os assuntos de segurança sejam transformados em de defesa.

Dessa forma, o caso brasileiro é construído a partir de uma percepção exacerbada de uma ameaça externa no campo cibernético. Essa percepção está enraizada em toda a estrutura institucional e normativa e o período dos megaeventos esclarece todo esse fenômeno, evidenciando que a segurança cibernética brasileira possui diversos elementos de discursos e movimentos securitizadores, a exemplo da percepção exacerbada de um risco que não é real, chamado pela bibliografia de hipersecuritização, um elemento presente nas pautas securitizadas.

Sendo assim, o presente trabalho buscou contribuir para a compreensão das motivações e da natureza do caso brasileiro e sua estrutura de segurança cibernética. Espera-se que essa seja mais uma contribuição que nos leve, enquanto tema de estudo, a desenvolver interpretações e respostas acerca de outros assuntos de segurança cibernética brasileiro. A título de ilustração, o Brasil ainda não possui uma Política Nacional de Segurança Cibernética que é prevista em normativas anteriores, o que nos leva ao questionamento: qual a perspectiva dessa normativa para os próximos anos? O ano de 2023 marca o fim da Estratégia Nacional de Segurança Cibernética (E-Ciber), documento público que apresenta as ações do Governo Federal em segurança cibernética no quadriênio 2018-2023. O que esperar de um novo documento? Maior vinculação do setor civil, militar e acadêmico para o planejamento de segurança cibernética? De fato, há muitas possibilidades a serem exploradas pela comunidade acadêmica que se disponha a compreender o tema de segurança cibernética no Brasil.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Congresso. Senado. Lei Complementar nº 136, de 25 de agosto de 2010. . Brasil, 25 ago. 2010. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp136.htm>. Acesso em: 30 mar. 2023.

_____. Decreto nº 10.222, de 05 de fevereiro de 2020. **Aprova A Estratégia Nacional de Segurança Cibernética.**. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm>. Acesso em: 09 nov. 2022.

_____. Decreto nº 484, de 30 de Junho de 2005 e Lei Complementar nº 136, de 25 de Agosto de 2010. **Política Nacional de Defesa (PND)**. Brasília. Disponível em: <http://bibliotecadigital.economia.gov.br/handle/123456789/461>. Acesso em: 21 mar. 2023.

_____. DOU Diário Oficial da União. Publicado no D.O.U. de 21 de agosto de 2012.

_____. Portaria nº 2.221, de 20 de agosto de 2012c. Disponível em: <https://mdlegis.defesa.gov.br/norma_pdf/?NUM=2221&ANO=2012&SER=A>. Acesso em: 30 mar. 2023.

_____. **Estratégia Nacional de Defesa**. (2008). Presidência da República. Casa Civil. Decreto nº 6.703, de 18 de dezembro de 2008. Brasília, DF. Disponível em: <https://www.gov.br/capes/pt-br/centrais-de-conteudo/estrategia-nacional-de-defesa-pdf>. Acesso em: 09 mar. 2023

_____. Gabinete de Segurança Institucional. (2015). **Estratégia de Segurança da Informação e Comunicações (SIC) e de Segurança Cibernética da Administração Pública Federal (APF)**. Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/noticias/2015/estrategia-de-seguranca-da-informacao-e-comunicacoes-sic-e-de-seguranca-cibernetica-da-administracao-publica-federal-apf>. Acesso em: 19 abril. 2023.

_____. Ministério da Defesa. (2012a). **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf>. Acesso em: 30 mar. 2023.

_____. Ministério da Defesa. (2012b). **Livro Branco de Defesa Nacional**. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 30 mar. 2023

_____. Ministério da Defesa. (2016a). **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/copy_of_pnd_e_end_2016.pdf>. Acesso em: 30 mar. 2023.

_____. Ministério da Defesa. (2016b). **Livro Branco de Defesa Nacional**. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/2017/mes03/livro-branco-de-defesa-nacional-consulta-publica-12122017.pdf/view>. Acesso em: 30 mar. 2023.

BUZAN, Barry; HANSEN, Lene. **A evolução dos estudos de segurança internacional**. São Paulo: Unesp, 2012. 576 p.

BUZAN, Barry; WAEVER, Ole; WILDE, Jaap de. **Security**: a new framework for analysis. London: Lynne Rienner, 1998. 239 p.

CARRION, Alexandre Luckemeyer Machado. **ORGANIZAÇÃO PARA A SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL**. 2022. 46 f. Tese (Doutorado) - Curso de Trabalho de Investigação Individual do Cpog 2021/2022, Instituto Universitário Militar Departamento de Estudos Pós-Graduados, Pedrouços, 2022. Disponível em: <http://hdl.handle.net/10400.26/42480>. Acesso em: 13 mar. 2023.

CEPIK, Marco; CANABARRO, Diego Rafael; BORNE, Thiago. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In **Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século XXI**, SOUZA, André de M.; Nasser,

Reginaldo M.; Moraes, Rodrigo F. eds. Brasília: IPEA, p.161-186, 2014. Disponível em: <http://repositorio.ipea.gov.br/handle/11058/3007>. Acesso em: 02 de nov. de 2022.
CERT.br (org.). **Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil**. Disponível em:< https://cert.br>. Acesso em: 25 mar. 2023.
DOD. **Dictionary of Military and Associated Terms**. U.S. Department of Defense (DOD), Washington, DC, 2021. Disponível em: <https://www.supremecourt.gov/search.aspx?Search=DOD+dictionary&type=Site>. Acesso em: 06 mar. 2023.
DONADELLI, L. .; SAINT-PIERRE, . H. L. .; VITELLI, M. G. Os documentos de defesa do Brasil: aproximações sucessivas à Doutrina de Segurança Nacional. **Revista de Relaciones Internacionales, Estrategia y Seguridad**, *[S. l.]*, v. 16, n. 2, p. 141–156, 2021. DOI: 10.18359/ries.5602. Disponível em: <https://revistas.unimilitar.edu.co/index.php/ries/article/view/5602>. Acesso em: 30 mar. 2023.
ESPAÇO CIBERNÉTICO. *In:* **Glossário de Segurança da Informação**. Brasil: Gabinete de Segurança Institucional, 2023. Disponível em: <https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/glossario-de-seguranca-da-informacao-1>. Acesso em: 09 mar. 2023.
European Union Agency for Cybersecurity (ENISA). **Definition of Cybersecurity - Gaps and overlaps in standardisation**. 2016. Disponível em: <https://www.enisa.europa.eu/publications/definition-of-cybersecurity>. Acesso em: 20 mar. 2023.
FARIA, Iramar Renó. **Vigilância ou militarização da segurança cibernética?** Uma análise entre as mentalidades militar e liberal de segurança e a regulação das ameaças do ciberespaço. 2016. Disponível em: <https://bdm.unb.br/handle/10483/17658>. Acesso em: 02 de nov. de 2022.
GREENWALD, Glenn *et al*. **EUA espionaram milhões de e-mails e ligações de brasileiros**. 2013. Disponível em: <https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>. Acesso em: 20 nov. 2022.
HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. **International Studies Quarterly**, [S.L.], v. 53, n. 4, p. 1155-1175, dez. 2009. Oxford University Press (OUP). http://dx.doi.org/10.1111/j.1468-2478.2009.00572.x. Disponível em: <https://academic.oup.com/isq/article/53/4/1155/1815351?login=false>. Acesso em: 14 nov. 2022.
HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. **INSTITUTO IGARAPÉ**. Disponível em: <https://igarape.org.br/wpcontent/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf>. Acesso em: 14 mar. 2023.
_____. **Securitização e Governança da Segurança Cibernética no Brasil**. 2018. Disponível em: <https://www.researchgate.net/profile/Louise-Marie-Hurel/publication/329973134_Securitizacao_e_Governanca_da_Seguranca_Cibernetica_no_Brasil/links/5d787c6d92851cacdb30dc0a/Securitizacao-e-Governanca-da-Seguranca-Cibernetica-no-Brasil.pdf>. Acesso em: 02 de nov. de 2022.
HUREL, Louise Marie; LOBATO, Luisa Cruz. Cyber Security Governance in Brazil: keeping silos or building bridges?. In: ROMANIUK, Scott N.; MANJIKIAN, Mary. **ROUTLEDGE COMPANION TO GLOBAL CYBER-SECURITY STRATEGY.** Londres e Nova York: Routledge, 2021. p. 504-518. Disponível em: <https://www.researchgate.net/publication/347767051_Routledge_Companion_to_Global_Cy

ber-Security_Strategy>. Acesso em: 08 nov. 2022.
_____. Uma Estratégia para a Governança da Segurança Cibernética no Brasil. **INSTITUTO IGARAPÉ**. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/09/Uma-estratégia-para-a-governança-da-segurança-cibernética-no-Brasil.pdf>. Acesso em: 14 mar. 2023.
INTERNATIONAL TELECOMMUNICATIONS UNION. **Cybersecurity**. 2008. Disponível em: <https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user%27s%20assets.>. Acesso em: 20 mar. 2023.
LANDLER, Mark; MARKOFF, John. **Estônia protagoniza primeira guerra virtual**. 2007. Disponível em: <https://g1.globo.com/Noticias/Tecnologia/0,,MUL45961-6174,00-ESTONIA+PROTAGONIZA+PRIMEIRA+GUERRA+VIRTUAL.html>. Acesso em: 09 maio 2023.
LOBATO, Luisa Cruz; KENKEL, Kai Michael. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional**, v. 58, p. 23-43, 2015. Disponível em: <https://doi.org/10.1590/0034-7329201500202>. Acesso em: 02 nov. 2022.
LOPES, Gils Villar. **Relações internacionais cibernéticas (CiberRI)**: uma defesa acadêmica a partir dos estudos de segurança internacional. 2016. Tese (Doutorado) - Universidade Federal de Pernambuco, Recife/PE, 2016. Disponível em: <https://repositorio.ufpe.br/handle/123456789/20723>. Acesso em: 21 out. 2022.
LVSC. **Livro Verde de Segurança Cibernética**. (2010). GSIPR. DSIC. Brasília, DF. Disponível em: <https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf>. Acesso em: 09 mar. 2023
MAIER, Friedrich. A REVOLUÇÃO DA INFORMAÇÃO E O PODER CIBERNÉTICO: um mapeamento conceitual na obra de joseph s. nye jr. **Revista de Iniciação Científica da Ffc - (Cessada)**, [S.L.], v. 14, n. 1, p. 1-34, 6 jun. 2014. Faculdade de Filosofia e Ciências. Disponível em: <http://dx.doi.org/10.36311/1415-8612.2014.v14n1.6345>. Acesso em: 09 nov. 2022.
MD31-M-07 (2014). Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. MD31-M-07, 1. ed. Brasília, DF. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_ciberneticaa_1a_2014.pdf>. Acesso em: 06 mar. 2023.
MEDEIROS, B. P.; CARVALHO, A. C.; GOLDONI, L. R. F. Uma análise sobre o processo de securitização do ciberespaço. **Coleção Meira Mattos: revista das ciências militares**, v. 13, n. 46, p. 45-66, 10 abr. 2019. Disponível em: <http://ebrevistas.eb.mil.br/RMM/article/view/1889>. Acesso em: 08 nov. 2022.
MORIKAWA, George. Hajime no Ippo. **Weekly Shonen Magazine**. Japão: Kodansha, 1998.
MOTTA, Bárbara Vasconcellos de Carvalho. **Securitização e política de exceção**: o excepcionalismo internacionalista norte-americano na segunda Guerra do Iraque. 2014. 125 f. Dissertação (mestrado) - UNESP/UNICAMP/PUC-SP, Programa San Tiago Dantas, 2014. Disponível em: <http://hdl.handle.net/11449/111154>. Acesso em: 08 de nov. 2022.
NYE, Joseph S.. **Cyber Power**. Cambridge: Belfer Center For Science And International Affairs, 2010. Disponível em: <https://www.belfercenter.org/publication/cyber-power>. Acesso em: 09 nov. 2022.
OLIVEIRA, M. A. G. de; PORTELA, L. S. As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil. **Revista Brasileira de Estudos de Defesa**, *[S. l.]*, v. 4, n. 2, 2017. DOI: 10.26792/rbed.v4n2.2017.75014. Disponível em:

<https://rbed.abedef.org/rbed/article/view/75014>. Acesso em: 9 nov. 2022.
OLIVEIRA, Salvattore Bertini Cavalcanti Siqueira Campos de. **A securitização do cyber space e seus desdobramentos para as relações internacionais**. 2014. 53 f. TCC (Graduação) - Curso de Relações Internacionais, Faculdade Asces, Caruaru, 2014. Disponível em: <http://repositorio.asces.edu.br/handle/123456789/81>. Acesso em: 09 nov. 2022.
PICK, Ulrich. **Stuxnet infecta Irã**. 2010. Disponível em: <https://p.dw.com/p/PN3r>. Acesso em: 09 maio 2023.
SÁ-SILVA, J. R.; ALMEIDA, C. D. de; GUINDANI, J. F. Pesquisa documental: pistas teóricas e metodológicas. **Revista Brasileira de História & Ciências Sociais**, *[S. l.]*, v. 1, n. 1, 2009. Disponível em: <https://periodicos.furg.br/rbhcs/article/view/10351>. Acesso em: 17 abr. 2023.
SAINT-PIERRE, Héctor Luis; VITELLI, Marina Gisela. **Dicionário de Segurança e Defesa**. São Paulo: Unesp, 2018. p. 1038. Disponível em: <https://repositorio.comillas.edu/xmlui/handle/11531/35338>. Acesso em: 14 nov. 2022.
SEGURANÇA CIBERNÉTICA. *In:* **Glossário de Segurança da Informação**. Brasil: Gabinete de Segurança Institucional, 2023. Disponível em: <https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/glossario-de-seguranca-da-informacao-1>. Acesso em: 09 mar. 2023.
SHAKARIAN, Paulo. Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008. **Military Review**, Kansas, v. 6, n. 66, p. 67-74, dez. 2011. Disponível em: <https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Artigos-em-Destaque/2019/Analise-da-Campanha-Cibernetica-da-Russia-Contra-a-Georgia-em-2008/>. Acesso em: 09 maio 2023.
SOUZA, Gills Lopes Macedo. **Reflexos da digitalização da guerra na política internacional do século XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá**. 2013. Dissertação de Mestrado. Universidade Federal de Pernambuco. Disponível em:<https://repositorio.ufpe.br/handle/123456789/12489>. Acesso em: 02 de nov. 2022.
VENTRE, Daniel. O dilema da fronteira virtual: Quando os Estados se tornam construtores de ciberfronteiras. **Dilemas-Revista de Estudos de Conflito e Controle Social**, n. Esp. 3, p. 75-96, 2019. Disponível em: <https://www.redalyc.org/journal/5638/563864592005/html/>. Acesso em: 09 nov. 2022.