UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS ECONÔMICAS
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS

DAFNE ALVES

ATAQUES CIBERNÉTICOS AO BRASIL: LEVANTAMENTO SISTEMÁTICO DOS ÚLTIMOS DEZ ANOS (2010 – 2020)

Porto Alegre

2022

DAFNE ALVES

ATAQUES CIBERNÉTICOS AO BRASIL: LEVANTAMENTO SISTEMÁTICO DOS ÚLTIMOS DEZ ANOS (2010 – 2020)

Trabalho de conclusão submetido ao Curso de Graduação em Relações Internacionais da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título Bacharel em Relações Internacionais.

Orientador: Prof. Dr. Érico Esteves Duarte.

Porto Alegre

2022

CIP - Catalogação na Publicação

Alves, Dafne
ATAQUES CIBERNÉTICOS AO BRASIL: LEVANTAMENTO SISTEMÁTICO DOS ÚLTIMOS DEZ ANOS (2010 - 2020) / Dafne Alves. -- 2022.
85 f.
Orientador: Érico Esteves Duarte.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Curso de Relações Internacionais, Porto Alegre, BR-RS, 2022.

1. Espaço Cibernético. 2. Brasil. 3. Segurança Nacional. 4. Ameaças Cibernéticas. 5. Internet. I. Duarte, Érico Esteves, orient. II. Título.

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

DAFNE ALVES

ATAQUES CIBERNÉTICOS AO BRASIL: LEVANTAMENTO SISTEMÁTICO DOS ÚLTIMOS DEZ ANOS (2010 – 2020)

Trabalho de conclusão submetido ao Curso de Graduação em Relações Internacionais da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título Bacharel em Relações Internacionais.

Aprovada em: Porto Alegre, 04 de maio de 2022.

BANCA EXAMINADORA:

Prof. Dr. Érico Esteves Duarte – Orientador

UFRGS

Prof. Dr. Thiago Borne Ferreira

UFSC

Profa. Dra. Adriana Iop Bellintani

UFRGS

AGRADECIMENTOS

Agradeço, em primeiro lugar, ao Estado brasileiro pela oportunidade de cursar o ensino superior em uma universidade pública, gratuita e de qualidade — em tempos tão difíceis para a educação e a ciência. Agradeço à Universidade Federal do Rio Grande do Sul, com destaque à Faculdade de Ciências Econômicas e a todo o corpo docente e de funcionários, que contribuem diariamente para a construção da instituição.

Agradeço a todos os professores e todas as professoras do curso de Relações Internacionais, cujos ensinamentos foram fundamentais para minha formação acadêmica. Em especial, agradeço ao professor Érico Duarte, por aceitar meu pedido de orientação e confiar em meu potencial, sempre disponível a me ajudar e aconselhar. Seus ensinamentos e suas contribuições ajudaram não só a realizar este trabalho de conclusão do curso, como também a aprimorar minha formação acadêmica e pessoal. Sempre levarei comigo suas palavras de apoio.

Agradeço à minha mãe, que sempre colocou minhas necessidades acima das dela e me deu todo o seu amor. À minha irmã, Ceura Cunha, que está presente em minha vida desde que existo e que é, para mim, um exemplo de mulher.

Agradeço com todas as forças de meu coração ao meu companheiro, Paulo Allem, por estar comigo nos dias bons e nos dias ruins, sempre me apoiando e acreditando em minha inteligência. Seu amor me tornou uma pessoa mais forte. Também agradeço à minha amiga Valquíria Allem, que tem o maior coração do mundo e é uma mulher incrível.

Alguns agradecimentos especiais para as pessoas que me ajudaram durante o processo deste estudo, incentivaram-me e dividiram seus conhecimentos comigo: Eduardo Izycki, Tamiris Santos, Leila Fonseca e Bruna Toso de Alcântara. Obrigada por me escutarem e por me fazerem sentir mais segura com o trabalho.

"Information is power, and modern information technology is spreading information more widely than ever before in history." (NYE, 2004. p. i)

RESUMO

Este trabalho tem como objetivo identificar os ataques cibernéticos ocorridos no Brasil entre os anos de 2010 e 2020. Dessa forma, busca-se analisar as vulnerabilidades do espaço cibernético e as respostas brasileiras aos ataques. O trabalho está dividido em quatro capítulos. O primeiro capítulo trata dos conceitos fundamentais ao entendimento do espaço cibernético, da Internet, da segurança cibernética, de conflitos e de ameaças cibernéticas. Já o segundo capítulo é a aplicação da Teoria da Prática Internacional, uma nova teoria que está criando espaço no âmbito das Relações Internacionais. O terceiro capítulo, por sua vez, consiste em um panorama geral da organização brasileira que trabalha com a segurança e a defesa cibernéticas, panorama que examina o modo como é formado o arcabouço institucional, com vistas a entender quais são as responsabilidades dos atores no espaço cibernético. Assim, procura-se analisar a evolução da estratégia brasileira, a partir dos documentos oficiais e das leis que abordam a segurança de dados. Por seu turno, o quarto capítulo tem como objetivo o levantamento de dados de incidentes notificados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, a fim de apontar quais são as maiores ameaças que o país sofre. Após o levantamento de dados, examina-se a forma como o país responde e se preocupa com o tema. Por fim, a conclusão apresenta os resultados da pesquisa, os quais demonstram que a agenda estratégica de segurança cibernética nacional vem se desenvolvendo ao longo do período analisado, buscando alinhar-se às principais práticas internacionais de segurança no espaço cibernético.

Palavras-chave: Espaço Cibernético. Brasil. Segurança Nacional. Internet. Ameaças Cibernéticas.

ABSTRACT

This paper aims to identify the cyberattacks and vulnerabilities of the Brazilian cyberspace. The research presents an outlook on the cyberattacks in the period 2010 - 2020. It is divided into four parts. The first chapter deals with the basic concepts to understand cyberspace, Internet, cybersecurity, cyber conflicts and threats. The second part focuses on the application of Practical International Theory, a new theory that is gaining ground in the field of International Relations. The third chapter provides an overview of the Brazilian organization that works with cybersecurity and defense, starting from the formation of the institutional framework to the understanding of the responsibilities of the actors in cyberspace. In this way, the evolution of the Brazilian strategy is analyzed with the official documentation and laws that approaches data security. The fourth topic aims to study the data of the incidents reported to the Brazilian Computer Security Incident Response Team, showing the cybersecurity strategy that has been developed and how much the country cares about the issue. In conclusion, the research shows that the strategic cybersecurity agenda has evolved during the period studied and is trying to align with the main international security practices in cyberspace.

Keywords: Cyberspace. Brazil. National Security. Internet. Cyber Threats.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
APF	Administração Pública Federal
ASN	Autonomous System Number
CDCiber	Centro de Defesa Cibernética
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI.br	Comitê Gestor da Internet no Brasil
COMDCiber	Comando de Defesa Cibernética
CREDEN	Câmara de Relações Exteriores e Defesa Nacional
CSIRT	Grupo de Resposta a Incidentes de Segurança
CSN	Conselho de Segurança Nacional
CTIR GOV	Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo
DDoS	Distributed Denial of Service
DoS	Denial Of Service
DSIC	Departamento de Segurança da Informação e Comunicações
E-Ciber	Estratégia Nacional de Segurança Cibernética
END	Estratégia Nacional de Defesa
ENSI	Estratégia de Segurança Nacional da Informação
GSI	Gabinete de Segurança Institucional
IP	Internet Protocol
ITU	International Telecommunication Union
MD	Ministério da Defesa
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
PF	Polícia Federal
PNSI	Política Nacional de Segurança da Informação
WWW	World Wide Web

SUMÁRIO

1 INTRODUÇÃO

O espaço cibernético é um novo ambiente de desafios que não são observados nos domínios tradicionais de terra, mar, ar e espaço. Ao se pensar em espaço físico, países são marcados por fronteiras, pessoas podem ser localizadas por endereços, telefones, cartão social. O espaço cibernético não é um ambiente visível, não havendo nele distinção de fronteiras, do individual, de modo que se torna difícil localizar um ator, assim como as ameaças constantes. A esse respeito, Nye e Scowcroft (2012) apontam que a dinâmica no espaço cibernético é uma das mais complexas ameaças para a segurança nacional.

Os avanços na área de tecnologia da informação e comunicação resultaram em uso intenso do espaço cibernético para as mais diversas atividades. O acesso à internet já é regulamentado por lei como serviço essencial para o Brasil. Na pandemia de Covid-19, foi colocada em vigor a Lei nº 13.979, de 2020[1],; nesse período, como forma de evitar aglomerações, as empresas e as instituições decidiram manter trabalhos e estudos de maneira remota. Dessa forma, há mais pessoas trabalhando em casa, usando mais serviços digitais, como aplicativos de compras e redes sociais, o que aumenta o risco não só individual, mas também o de organizações e companhias.

Nessa direção, o crescimento de conectividade traz consigo uma vasta gama de vulnerabilidades cibernéticas, que podem acarretar prejuízo e impactos, por exemplo, financeiros. Conforme o relatório da McAfee (2020), a economia global sofre um prejuízo de mais de 1 trilhão de dólares devido aos crimes cibernéticos. Além disso, com base no Banco Mundial (2022), de 2019 a 2023, estima-se que o total de perda econômica para ataques cibernéticos será de 5.2 trilhões de dólares, sendo em torno de 10 milhões de prejuízo por mês.

A digitalização tornou a economia global mais eficiente e dinâmica, mas também mais frágil a ataques cibernéticos. Esse cenário leva a um crescente número de investimentos conjuntos por parte dos setores produtivos: estima-se que o mercado de segurança cibernética mundial, no ano de 2020, seja avaliado em 151 bilhões de dólares e que o mercado brasileiro de segurança cibernética movimenta em torno de 2 bilhões de dólares (BRASIL, 2020). O mercado doméstico de tecnologias se encontra bem estabelecido: há uma ampla variedade de produtos de software de segurança cibernética desenvolvidos internamente por empresas públicas e

[1] A lei que dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019.

privadas, sendo algumas dessas tecnologias exportadas e utilizadas por outros países (OEA, 2020).

Portanto, os ataques cibernéticos são um risco especialmente para a economia brasileira. A esse propósito, os dados levantados pelo documento Estratégia Nacional de Segurança Cibernética (E-Ciber) demonstram bem a situação em que o país se encontra no que tange à segurança: apenas 11% dos órgãos federais têm bom nível em governança de tecnologia da informação; em 2017, mais de 70 milhões foram vítimas de crimes cibernéticos; também em 2017, o Brasil foi o segundo país com maior prejuízo decorrentes de ataques cibernéticos; em 2018, 89% dos executivos foram vítimas de fraudes cibernéticas (BRASIL, 2020).

Os ataques cibernéticos se tornaram uma realidade próxima após os ataques de *Stuxnet*[2], nas instalações nucleares do Irã. Esse acontecimento revelou, para os governos e para as sociedades, o quão perigoso e profundo pode ser um ataque cibernético, o que levou à percepção de que o espaço cibernético é um campo de disputas geopolíticas. Nessa conjuntura, países como Singapura, Dinamarca, Austrália, dentre outros, empregaram diplomatas na área de espaço cibernético, os *cyber* diplomatas. Em 2019, o Brasil nomeou Marcelo Câmara como o primeiro *cyber* diplomata. A decisão, inspirada nas atitudes de outros Estados, partiu como resposta a trabalhar com a integridade do espaço cibernético (HUREL, 2022).

Logo, é necessário abrir a discussão acerca do espaço cibernético na área de Relações Internacionais e na diplomacia digital. Nessa perspectiva, diplomacia digital liga-se ao conceito de *soft power*. Segundo Hedling e Bremberg (2021), a maneira mais adequada de diplomacia digital é analisar as práticas dos Estados, mas principalmente como eles agem entre si, como eles podem se juntar para a produção de políticas contra os ataques cibernéticos. Por ser um meio de constante mudança, o trabalho fundamental de um diplomata consiste em acompanhar as transformações do campo, as ações dos atores que lidam com o espaço cibernético e suas influências em outras regiões. A Teoria da Prática Internacional se insere ao mostrar que essa é uma área que está passando por um processo de reconhecimento e conhecimento, adaptando-se à conjuntura e preenchendo lacunas sobre a diplomacia digital que teorias tradicionais não preenchem. Por exemplo, o uso das redes sociais por um diplomata como ferramenta de

[2] Não se sabe quem criou o *worm Stuxnet*; há rumores de que foram a inteligência norte-americana e a israelense. A intenção principal foi de sabotar o programa nuclear iraniano. O *Stuxnet* mais perigoso aconteceu em 2011, na instalação nuclear de Natanz, no Irã, ataque que resultou em um apagão nos sistemas, interrompendo o fornecimento de energia e danificando uma instalação que abriga centrífugas sensíveis. Fonte: DefesaNet, 2011. Disponível em: https://www.defesanet.com.br/nuclear/noticia/40317/STUXNET-2---Ira-diz-que-pane-eletrica-em-usina-atomica-foi-ato-de-%E2%80%98terrorismo-nuclear%E2%80%99/.

divulgação do que se realiza nas políticas e nos modos de proteção às ameaças é uma prática eficiente, que tenta alcançar um maior número de pessoas, criando conexões que ultrapassam o *on-line*.

Explica Radu (2014) que as tecnologias de informações e comunicações mudaram o estilo de vida individual e as interações sociais, mudança que atingiu igualmente os Estados. Assim, o espaço cibernético interfere na economia, no social e nas áreas políticas no campo das Relações Internacionais. Nesse contexto, a arquitetura internacional dá espaço para que os atores tomem iniciativas e cooperações a fim de obterem resultados em um nível estratégico internacional. As práticas de segurança da informação são, nesse cenário, uma estrutura crescente.

O Brasil tem o papel nas agendas internacionais, é visto nos documentos de estratégias de segurança nacional que sempre houve preocupação em alcançar essa posição de participar no cenário internacional. O país já participou duas vezes da *United Nations Group of Governmental Experts of Information Security* (UNGGE): o primeiro encontro foi em 2015 e o segundo, em 2021. Além disso, o Brasil participou do consenso de necessidade de comprometimento dos Estados no que se refere às normas de responsabilidades na área (HUREL, 2022).

A *Convention on Cybercrime*, conhecida como Convenção de Budapeste sobre o Cibercrime, é um tratado internacional elaborado em 2001, com o intuito de combater os crimes cometidos no espaço cibernético, trabalhar com legislações, garantir segurança e tomar medidas através de cooperação internacional. O Brasil, que entrou na Convenção somente em 2021, desfrutará de um quadro com cooperação internacional e assistência técnica eficiente, podendo integrar normas modernas e aproveitar ferramentas processuais igualmente modernas (BELLI, 2022).

Desde 2014, o país também dialoga com a União Europeia (UE) sobre os interesses de políticas cibernéticas. Acerca disso, a UE conta com uma agência especializada em segurança cibernética: a *European Union Agency for Cybersecurity* (ENISA). Tal debate com a UE serve de apoio para o Brasil identificar as áreas mais fracas, os problemas de segurança, o fortalecimento das leis e as estratégias do Estado.

A *International Multilateral Partnership Against Cyber Threats* (IMPACT) é a primeira aliança de segurança cibernética apoiada pela Organização das Nações Unidas desde 2011. É uma plataforma com apoio público e privado que visa juntar atores, indústria e academia para

discutir sobre as capacidades de lidar com as ameaças cibernéticas. Seu principal parceiro é a *International Telecommunication Union* (ITU), com a qual cria estratégias para os Centros de Respostas a Incidentes e que sirvam de influência para os Centros de cada Estado (ITU, 2009).

A ITU é a agência especializada da ONU para lidar com informações e comunicações tecnológicas. Trata-se de uma organização global que inclui 193 atores estatais e mais de 900 entidades entre organizações regionais e universidades. Dentre suas iniciativas, há a cooperação internacional da *Global Cybersecurity Agenda* (GCA), que dispõe de colaborações entre os parceiros para a criação de iniciativas no que diz respeito ao espaço cibernético. Essa agenda consiste em trabalhar em cinco áreas: (a) medidas legais, relacionadas aos modos de lidar com atividades criminais e às respostas apropriadas a estas; (b) área técnica e processual, em que se buscam vulnerabilidades nos *softwares* e nos protocolos; (c)organização estrutural, parte em como cada Estado trabalha com sua infraestrutura de informações; (d) área de capacidade, vinculada às estratégias e aos mecanismos de cada agenda de segurança sobre o espaço cibernético; (e) área de cooperação internacional, a qual incentiva o diálogo e a coordenação de práticas que lidem com as ameaças cibernéticas (Schjølberg, 2008).

O Projeto CyberBRICS é uma iniciativa do grupo BRICS (Brasil, Rússia, Índia, China e África do Sul) e apresenta três objetivos centrais: mapear as regulamentações existentes dos países, identificar as melhores práticas e desenvolvimentos nas áreas de governança de segurança cibernética, política de acesso à internet e estratégias para digitalização das administrações públicas dos países do BRICS (CyberBRICS, 2022). Os países integrantes desse projeto reuniram seus campos de ciência e tecnologia para realizarem uma publicação de segurança cibernética. Tal aproximação resultou no guia CyberBRICS, um conjunto de articulações para lidar com a proteção do espaço cibernético: "Esse livro é um estudo importante e necessário das legislações e políticas relevantes para garantir que as metas do BRICS, no cenário da 4º Revolução Industrial, sejam alcançadas" (MTUZE, 2021 p. viii).

Tendo esse cenário em vista, o presente trabalho pretende analisar os dados de estatísticas dos incidentes de ataque cibernético ocorridos no Brasil. A partir dessa análise, busca-se entender melhor como tem sido estabelecida, no país, a estratégia cibernética enquanto mecanismo de resposta. De forma a acompanhar-se a agenda de segurança, os dados coletados compreendem o período de 2010 a 2020.

Conforme analisa-se os dados de incidentes relatados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), a partir de 2010, acompanha-se

com a primeira publicação de uma estratégia de segurança cibernética, o Livro Verde de Segurança Cibernética até os dados de 2020. Esse recorte contempla o período de formulação da Estratégia Brasileira de Cibersegurança (E-Ciber), a qual prevê medidas até 2023. Portanto, a análise da capacidade brasileira de diagnóstico e análise de ataques permitirá uma avaliação mais fundamentada de tais documentos e ações de cibersegurança brasileiros. Com isso, espera-se entender o caminho percorrido pela segurança nacional, bem como a legislação e a estrutura organizacional das entidades responsáveis por essa segurança. Espera-se, igualmente, apontar quais são as ameaças que aparecem nos dados e compreender quais são as políticas públicas adotadas para a proteção do campo cibernético.

A fim de cumprir os objetivos propostos, o presente trabalho está estruturado em quatro capítulos. Inicia com uma introdução aos principais conceitos de *espaço cibernético*, a origem do termo e suas características. A introdução da internet à sociedade e ao Brasil. Descrevendo o princípio de segurança e defesa, identificando uma tipologia de conflitos cibernéticos e as principais ameaças cibernéticas.

Em seguida, no segundo capítulo, discute-se o modo como têm evoluído os estudos da Teoria da Prática Internacional no âmbito das Relações Internacionais e se é possível colocá-la dentro da segurança do espaço cibernético, aplicando o conceito de *soft power* e promovendo o aumento de atores na atuação da segurança doméstica e da internet.

O terceiro capítulo apresenta uma análise dos principais documentos de estratégia de segurança e defesa nacional, bem como identifica os focos no que se refere à introdução do campo cibernético no país e à atenção do governo ao assunto. Esses documentos têm um impacto institucional progressivo, já que, a partir da formulação deles, foram formadas as estruturas de órgãos brasileiros focados em aumentar a capacidade nacional no setor (BOHN, NOTHEN, 2015). Também explora a legislação que protege as informações da sociedade e garante o direito à privacidade.

O quarto capítulo contempla o levantamento dos dados coletados, a análise das respostas e a posição do Brasil no cenário internacional no que concerne à capacidade de atuação na segurança. Por fim, expõem-se as considerações finais, nas quais se esclarece se a pesquisa atingiu os objetivos estabelecidos.

Quanto à metodologia empregada pelo trabalho, primeiramente, realizou-se uma pesquisa documental dos documentos de segurança estratégica brasileira organizados pelo Estado, quais sejam: *Livro Verde de Segurança Cibernética*, *Estratégia de Segurança da Informação e*

Comunicações e de Segurança Cibernética da Administração Pública Federal e Estratégia Nacional de Segurança Cibernética. A pesquisa documental contemplou, também, as principais leis que garantem privacidade na internet, a saber: o *Marco Civil da Internet* e a *Lei Geral de Proteção de Dados Pessoais*, assim como o Decreto da *Política Nacional de Segurança da Informação*, o qual dispõe sobre a governança da segurança da informação.

Após a consulta dos documentos, a coleta das estatísticas foi feita pelo site CERT.br. Primeiro uma descrição dos números totais dos incidentes, depois examinar os DNS maliciosos, ataques *phishing* e notificações de ataques de negação de serviço. São dados os quais há mais conhecimento empírico acessível. Para agregar a pesquisa foram coletado dados de empresas privadas de segurança digital, tais como: Axur, Kaspersky, AVAST. São dados de relatórios anuais e identificação de ameaças disponíveis nos sites das empresas.

No que se refere localizar o país no cenário internacional de preocupação e ações em segurança cibernética, foi exposto o índice de ações dos países para enfrentar riscos cibernéticos do *International Telecommunication Union*. A métrica da Fundação da Academia de Governança Eletrônica da Estônia que identifica os pontos fortes das estratégias dos Estados, também é analisada. Por último, examinar o Relatório de Revisão da Capacidade de Cibersegurança da República Federativa do Brasil organizado pela Organização dos Estados Americanos.

2 ESPAÇO CIBERNÉTICO

O termo “espaço cibernético” ou “ciberespaço” foi visto, em primeiros momentos, na obra *Burning Chrome*, de 1982, do escritor américo-canadense de ficção especulativa William Gibson, e, em seguida, popularizado em outra obra sua, chamada *Neuromancer*, de 1984. Esse último livro retrata o universo de redes digitais como forma de conflito mundial; a exploração do ciberespaço foi colocada na história com foco em segurança e vazamento de informações, em razão de sua fragilidade. Acredita-se que serviu de primeiros passos para o que viria a ser, contemporaneamente, o termo político (SHELDON, 2019).

Alguns pesquisadores conceituam o espaço cibernético de forma particular. Lévy (1999) já o definia como espaço de comunicação aberto pela interconexão mundial dos computadores e de suas memórias, reunindo um conjunto de redes com essa conectividade, tais como computadores, redes telefônicas e codificação digital. Em *Magna Carta for the Knowledge Age in New Perspective Quarterly*, de 1994, a definição dada por Esther Dyson, George Gilder, Hay Keyworth e Alvin Toffer foi: "é mais um ecossistema que máquinas, o espaço cibernético é ambiente bioeletrônico, literalmente universal: existe em todos os lugares onde há rede telefônica, cabos, linhas de fibra ótica ou ondas eletromagnéticas". As ideias dos autores indicam que o conhecimento era basicamente temporário, pois a velocidade das mudanças e das evoluções da informação deixariam vários assuntos obsoletos.

Nye (2010) analisa espaço cibernético de forma estratégica, baseado em sua nova força de poder – a informação é poderosa e o espaço deve ser respeitado como uma nova fonte de perigo, podendo ser considerado como parte de uma Terceira Revolução Industrial, já que a tecnologia computacional evolui 30 anos a cada 18 meses. O autor descreve o ciberespaço como “um domínio operacional constituído por eletrônicos que expõem informações via sistemas interconectados por suas infraestruturas.” (NYE, 2010, p. 3).

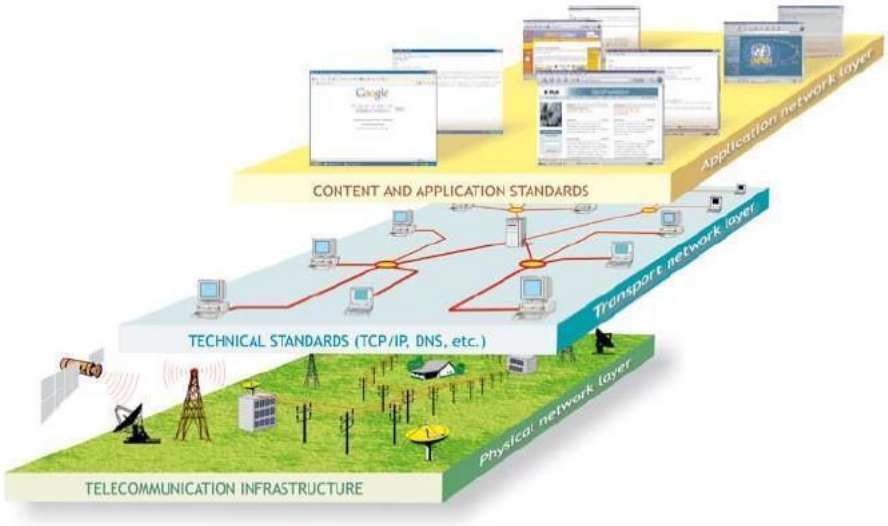
Por ser um domínio relativamente novo, que vai mudando conforme o desenvolvimento de tecnologias, há a dificuldade em se chegar a um consenso. No entanto, com algumas visões complementares, pesquisadores chegaram a uma estrutura organizacional para o espaço cibernético, podendo haver alguns espectros que essa estrutura traz para a discussão. A arquitetura em três camadas (figura 1), definida por Kurbalija (2010) e também discutida por Libicki (2007), é composta da seguinte forma:

- A camada física compreende os elementos palpáveis para funcionamento, como os *hardwares*, cabos, satélites, roteadores.

- A sintática compreende as informações, o *software* que contém os códigos. É todo o conteúdo.
- A semântica compreende as relações humanas com o ciberespaço e a linguagem usada para transferir esse conhecimento e utilizá-lo.

O controle de uma das camadas é independente das outras; ou seja, o ator pode ter poder sobre uma camada, porém não necessariamente controla as anteriores (Libicki, 2007).

Figura 1 - Rede de Camadas



Fonte: Kurbalija (2010)

Zimet e Skoudis (2009) ainda adicionam uma quarta camada, que seria retratada como domínio de dinâmicas sociais:

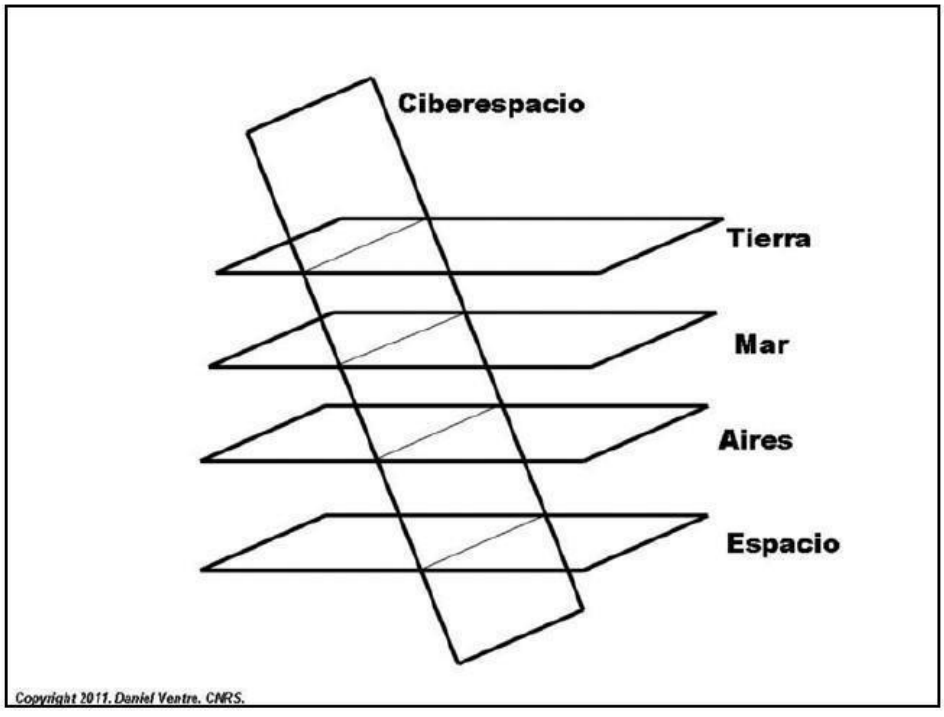
> "O espaço cibernético é uma produção humana, criada para acesso à informação e compartilhamento dela entre máquinas e pessoas. Com o aumento da presença do espaço cibernético na vida moderna, o domínio do sistema, dos conteúdos e das aplicações dá origem a um novo grupo social de pessoas que criam comunidades. Existem vários tipos de comunidades online, usados por pessoas do mundo inteiro, que têm possibilidade de compartilhar interesses pessoais, de negócios, políticos e outros." (ZIMET, SKOUDIS. 2009, p.110).

Independente do propósito, o espaço cibernético tem aproximado pessoas, o que as torna um importante elemento para as camadas. A comunidade *online* se junta para discutir e compartilhar conhecimento sobre diversas áreas que serão usadas por grupos, criando elementos de realidade virtual. Ou seja, é necessário abordar a figura dos usuários como componentes importantes do encontro entre físico e virtual que o espaço oferece.

Adiciona Sheldon (2019) outras características particulares do espaço cibernético: há disponibilidade de atuação de vários atores, o domínio é de relativo baixo custo e há amplas oportunidades estratégicas. Outras vantagens são a constância, a aptidão de mudanças, os reparos e as manipulações no espaço: “Em sua grande parte, nada é final no espaço cibernético.” (SHELDON, 2019, p. 297). É um ambiente instantâneo, em que as informações ultrapassam tempo e espaço. A velocidade do processo de propagação das informações não é vista em outros domínios.

Dessa forma, reforça-se que espaço cibernético não é algo natural, mas sim criado por mãos humanas, diferentemente de dimensões tradicionais como espaço, terra, ar e mar. Essa característica de ultrapassar dimensões é chamada de transversalidade, de modo que o espaço transpassa outros domínios e ainda interage entre eles, como é possível verificar na figura 2 (VENTRE, 2011).

Figura 2 – Transversalidade do Espaço Cibernético



Fonte: Ventre (2011)

2. 1 INTERNET

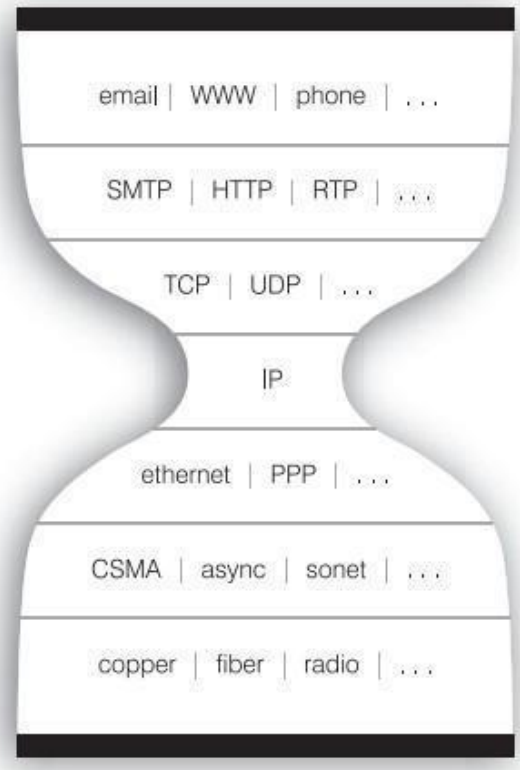
Ciberespaço e internet são coisas distintas. O ciberespaço é um domínio que exige o uso da eletrônica e do espectro eletromagnético, tecnologias já presentes em telégrafos, radioamador,

telefonia fixa e televisão via satélite (CEPIK, CANABARRO, BORNE, 2014, p.162). O espaço cibernético já funcionava de forma independente da internet; com o surgimento dela, o domínio foi se fortalecendo e se criou uma forte ligação.

Em 1969, em plena Guerra Fria, com a intenção de fortalecer o domínio de conexão, o Departamento de Defesa dos Estados Unidos (DoD) montou uma rede de comunicação com pesquisadores trabalhando junto a computadores do *Massachussets Institute of Technology* (MIT), da Universidade da Califórnia, do *Stanford Research Institute* e da Universidade de Utah. O resultado dos trabalhos levou ao primeiro protótipo da internet: uma rede de comunicações nomeada de ArpaNET – *Advanced Research Projects Agency Network.* Protocolos provieram das pesquisas, entre eles o TCP e o IP – *Transmission Control Protocol* e *Internet Procotol* – dois protocolos únicos e centrais que definem a internet. Outro que veio a incorporar a comunicação foi o HTTP – *Hypertext Transfer Protoco*l –, que permitiu a criação do WWW – *World Wide Web* –, uma aplicação que funciona como uma janela de entrada, a partir da qual há o acesso a outros locais da internet (CEPIK, CANABARRO, BORNE, 2014, p.163).

Assim como o espaço cibernético, a internet também possui uma arquitetura em camadas. A camada inferior é o local dos elementos físicos, que servem de base para a conectividade: cabos, antenas, satélites, linhas. A camada intermediária é onde funcionam os padrões técnicos e lógicos que levam a informação decodificada, de leitura e acesso simples, para a camada superior, que, por fim, transmite a informação para os usuários (CEPIK, CANABARRO, BORNE, 2014). Zittrain (2008) discute que há ainda uma outra camada a ser localizada, a social, onde há as relações humanas que usufruem o conteúdo final e criam uma comunidade. Essa arquitetura pode ser descrita em forma de ampulheta (figura 3):

Figura 3 – Ampulheta da Internet



Fonte: Zittrain (2008)

A internet é desenhada em camadas para entender os limites entre elas, sua divisão aos olhos e o trabalho posto em cada uma. "Trabalhadores podem agir em uma camada sem necessariamente entender algo sobre as outras, não precisa haver relação ou coordenação entre trabalhadores de uma camada a outra." (ZITTRAIN, 2008. p. 68). Desse modo, um usuário da camada de superfície pode interagir na comunidade sem ter a noção do que acontece em camadas técnicas e de codificação.

No cenário brasileiro, na década de 1980, houve a introdução de serviços de comunicação de dados, uma estratégia ligada a segurança e pesquisa nacional, com interesses econômicos para desenvolvimento do Brasil Potência (LUCERO, 2011). Assim, até os anos de 1990, o controle das redes de comunicações estava nas mãos do Estado, pela Telebrás.

Por necessidade de uso não comercial das redes, principalmente para o meio acadêmico, criou-se uma rede remota chamada BITNET – *Because It´s Time Network* – pela empresa privada IBM. Seu protocolo assemelhava-se com o funcionamento do TCP/IP, mas não era compatível com esses protocolos, muito menos com o modelo ISO – *International Organization for Standardization* –, entidade internacional para a padronização de camadas e

funções das redes[3]. Por esses motivos, a BITNET não era apta a nenhum financiamento público (LUCERO, 2011). Lucero (2011) explica que apenas quando a Embratel modernizou o RENPAC, rede de computação por pacotes em que a tecnologia não é feita por circuitos e o usuário paga pelo uso dos serviços[4], houve mudança do cenário comercial brasileiro, começando a se tornar mais acessível a todos o uso de redes.

2.2 SEGURANÇA CIBERNÉTICA

Antes de tudo, é necessário distinguir segurança e defesa no contexto do espaço cibernético. Segurança cibernética, definida pela Secretaria de Assuntos Estratégicos (2011), são, em suma, as interações com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais. O princípio é proteger e garantir a ação dos ativos de informações estratégicas. Já a defesa cibernética são ações realizadas no espaço cibernético no contexto de um planejamento nacional, coordenado e integrado pelo Ministério da Defesa (BRASIL, 2019).

Conforme Deibert (2012), as grandes mudanças de comunicação na última década têm sido rápidas demais, pois o espaço não possui barreiras e não há limites demográficos. Cada vez mais nos tornamos dependentes dele, essencialmente da internet, sendo inevitável colocá-lo como problema de segurança nacional e internacional, inclusive porque os Estados maximizam poder e procuram tomar posição no cenário internacional. Faltar com estratégia de segurança cibernética os coloca atrás de países que de fato investem nisso. Um exemplo é o Canadá, que, desde 2010, coloca o ciberespaço como prioridade na agenda de segurança em cooperação com empresas privadas, resultando em organizações como *Public Safety Canada*, *Communications Security Establishment* (CSE),[5] entre outras.

Deibert (2012) defende que a concepção da agenda de segurança cibernética está, cada vez mais, dando lugar para a ação de vários atores:

> "No começo da história da internet, era normal assumir que os governos tinham dificuldade em controlar a internet, isso traria muitas mudanças na forma autoritária de governar. Com o tempo, essas suposições tornaram-se questionáveis pelos governos, frequentemente trabalhando em cooperação com empresas privadas. Foram construídos vários controles de informações, não somente na internet, mas em outras plataformas também. É justo agora dizer que é crescente a ordem de filtrar informações na internet, porém, implementar esse planejamento varia entre países." (DEIBERT, 2012, p. 7).

[3] GOOGLE. Disponível em: https://sites.google.com/site/profsuzano/redes/modelo-iso-osi

[4] UFRGS. Disponível em: http://penta2.ufrgs.br/Eduardo/renpac.html

[5] PUBLICSAFETY. Disponível em: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-en.aspx

Para Radu (2014), na conjuntura internacional, não é vantajoso que os Estados se isolarem ou que apenas um número pequeno trabalhe com a segurança em sua agenda política. A expansão da internet dá oportunidade ao crescimento de instituições transnacionais, tais quais *Internet Corporation for Assigned Names and Numbers* (ICANN) e *Internet Governance Forum*.

Goldsmith (2010) identifica que as redes de internet e os computadores, por si sós, já são uma cadeia de insegurança, e, desse modo, algum lado já possui vantagens. É muito rápido a disseminação de acesso às informações, e o caso do ataque chinês ao Google, o maior site de busca do mundo[6], é um exemplo. Em 2009, operadores chineses conseguiram acessar páginas da *web*, programaram mensagens para os funcionários da empresa, que, ao abri-las, eram encaminhados para um link aparentemente confiável, em que perdiam controle dos seus computadores. Essa prática comum é chamada de *trapdoor*.

As ameaças no espaço cibernético não acontecem na nossa frente; as evidências são de formas remotas, sem fator físico, isso atrapalha o discernimento para tomada de decisões. Porém, para evitar os riscos, os Estados precisam agir para mitiga-las. Mesmo com uma segurança cibernética efetiva, não há como impedir que todos os ataques aconteçam, sendo necessário diminuir os efeitos e as vítimas que são afetadas no espaço (SHELDON, 2019).

Ainda, destaca-se que a complexidade dos sistemas de computadores oferece gradualmente acidentes, erros e falhas (GOLDSMITH, 2010). Esses só acontecem quando há a falta de poder de dissuasão dos Estados: “criminosos cibernéticos podem agir globalmente, mas se escondem na jurisdição local, onde essas atividades podem ser toleradas ou falta capacidade de policiamento.” (DEIBERT, 2012, p. 12).

2.3 CONFLITOS CIBERNÉTICOS

Segundo Canabarro e Borne (2013), as diferenças entre os tipos de ameaças cibernéticas contemporâneas importam, pois, dependendo do quadro, a estratégia política será diferente, e isso dá liberdade para que Estados e entidades possam se organizar e responder adequadamente. "E jogar diferentes categorias de atores embaixo de um mesmo guarda-chuva coloca em risco as liberdades civis, direitos políticos e individuais em todo o mundo, tanto em uma democracia quanto em um regime autocrático." (CANABARRO, BORNE, 2013. p. 14).

[6] Google, 23 anos: 10 coisas que você talvez não saiba sobre o buscador. Disponível em: https://g1.globo.com/tecnologia/noticia/2021/09/27/google-23-anos-10-coisas-que-voce-talvez-nao-saiba-sobre-o-buscador.ghtml

O que pode ser identificado na tipografia dos conflitos cibernéticos:

Guerra Cibernética: uso de computadores para prejudicar as redes de uma nação inimiga. Essa atividade é de cunho político, de uso em escala e períodos específicos e obtém vantagem operacional militar significativa (BRASIL, 2019).

Terrorismo Cibernético: ataques contra redes de comunicação, sistemas operacionais e computadores, com a intenção de intimidar ou coagir um governo ou sociedade a favor de ideais político-sociais (CAVELTY, 2012).

Sabotagem Cibernética: trabalho de distúrbio e empecilhos no funcionamento do espaço cibernético.

Espionagem Cibernética: envolve ataques com finalidade de adquirir informações confidenciais, não viola explicitamente leis internacionais (NYE, 2010). A espionagem é o método mais antigo da história da humanidade, ainda mais comparando aos outros métodos citados.

Crime Cibernético: "atividade criminal usando computadores e internet". (CAVELTY, 2012. p. 116).

Hacktivismo: atividades de *hackers*, indivíduos com habilidades de entrar em sistemas de computador (SENHORAS *et al*., 2015), contra sites e operações específicas.

A figura 4 montada por Cavelty (2012), mostra as probabilidades de cada conflito acontecer, sendo, em sua visão, o terrorismo e a guerra cibernética os limites, ao mesmo tempo em que são menos prováveis de acontecer. Essa questão mostra que crimes não se enquadram facilmente em níveis avançados, pois isso exigiria conhecimento excessivo, técnica e operações custosas.

Figura 4 – Tipografia dos Conflitos Cibernéticos

Fonte: Cavelty (2012)

2.4 AMEAÇAS CIBERNÉTICAS

Categorizar os tipos de ataques cibernéticos é uma maneira de organizar as evidências para ter uma resposta apropriada. Em um espaço onde as características principais são crescente mutação e vulnerabilidade, os ataques entram em categorias entre complexos e mais simples. Comentam Diniz, Muggah e Glenny (2014) que ignorância ou má interpretação podem resultar em falhas de segurança cibernética e retrocesso em conhecimento; não se deve desconsiderar que a falha reflita nas informações que são passadas aos usuários, e isso afetaria os riscos online.

Assim, a análise feita por Diniz, Muggah e Glenny (2014) define três categorias de ameaças que atingem o Brasil. As mais convencionais são: intercepção de dados, pornografia infantil, crimes de ódio, fraude, roubo de identidade, danos a direitos autorais, *cracking*. O

Cracking é uma técnica comum usada para violar software de computador ou um sistema de segurança de computador, usada de forma estritamente criminosa (AVAST, 2022). No geral, esses crimes tem intenções econômicas ou ideológicas, e são combatidos com respaldo em leis.

As ameaças que possuem abordagem mais complexa são: terrorismo, *hacktivismo*, espionagem e ataques a infraestruturas e sistemas. Nesses casos, as respostas dependem do nível de complexidade, variando o uso da inteligência, com base em leis ou por poder militar.

A última categoria são os ataques emergentes, contra direitos humanos, e que envolvem crime organizado e violência. Tradicionalmente realizados por grupos criminosos, gangues, crime organizado e lavagem de dinheiro. São os mais difíceis de combater, a preocupação é crescente e proporcional ao desenvolvimento rápido do aperfeiçoamento das técnicas.

Ademais ameaças são relatadas pela Cartilha de Segurança para Internet, uma iniciativa no início dos anos 2000, tomada pelo CERT.br e grupos de pesquisa, com objetivo de identificar os principais códigos maliciosos que prejudicam a maior parte dos cidadãos. A intenção era passar informação de forma acessível e organizar os ataques para futuros acessos. O documento destaca os principais códigos maliciosos, dentre estes (CERT.br, 2012):

- Vírus: um programa ou parte de um programa que insere copias de si em outros programas, infestando arquivos e o sistema.
- *Ransomware*: um código que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e exige pagamento de resgate para liberar o acesso ao usuário. As principais formas de propagação ocorrem através de e-mails com arquivos e links que induzem o usuário a clicar. Os dois tipos de *ransomware* que atacam o país são: os *ransomware locker*, impedem que o usuário acesse o equipamento, e o *ronsomware crypto*, que usa a criptografia para acessar, além do equipamento, dados armazenados.
- *Worm*: semelhante ao vírus, ele é programado para se propagar de forma acelerada pelas redes, explorando vulnerabilidades nos programas já instalados nos equipamentos,
- *Backdoor*: é uma porta de acesso para o retorno de um antigo invasor no sistema.
- *Bot*: é um programa que executa as tarefas de modo remoto, o invasor vai funcionar dentro do sistema como um robô. Quando centenas de programas se

juntam para essa finalidade, fazendo os equipamentos funcionarem a distância, é chamado de *botnet*.

- *Spyware*: é um programa destinado a coletar dados de um computador ou dispositivo e encaminhá-los a terceiros, também trabalha com um rastreamento de hábitos do usuário (KASPERSKY, 2022).

Dos golpes da internet, quando há fraude de dados, servidores, instituições bancárias ou comerciais, dois mencionados pela Cartilha:

- *Phishing*: é o tipo de fraude em que o golpista obtém dados pessoas e financeiros por meio de uma combinação de meios técnicos e engenharia social. Primeiro, através de mensagens eletrônicas, atrai a atenção do usuário, passando-se por uma instituição conhecida, informa procedimentos e induz os usuários a fornecerem dados pessoais e financeiros.

- *Pharming*: é derivado da ameaça anterior, porém, trabalha especificamente em encaminhar a navegação do usuário para um site falso, por meio de alterações no serviço de DNS (*Domain Name System* ou Sistema de Nomes de Domínio).

Deve-se ter em vista que qualquer equipamento que tenha acesso à internet são fáceis alvos para ataques. Os atacantes possuem várias maneiras de usar suas técnicas para os ataques; uma delas é explorando as vulnerabilidades: "exemplos de vulnerabilidade são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede. (CERT.br, 2012. p. 18).

Existem varreduras em rede, chamadas de *Scan*, uma técnica que consiste em realizar buscas em redes procurando identificar computadores ativos, assim, "com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados" (CERT.br, 2012. p. 18). Por isso é tão importante dedicar-se a melhorias em vulnerabilidades, para que estas não sejam objeto de ataque.

Por fim, à medida que cresce a dependência da sociedade em relação a sistemas informáticos e computacionais, mais se diversificam as possibilidades de novas aplicações das tecnologias para fins maliciosos. É preciso compreender que todas as redes estão propensas a sofrer ameaças. Os perigos que acontecem na internet são reais e os riscos diários são similares àqueles que ocorrem na rua (CERT.br, 2012).

3 A TEORIA DA PRÁTICA INTERNACIONAL

O campo de estudo de Relações Internacionais é predominante estudado por três correntes teóricas: realismo, liberalismo e construtivismo. Para o objetivo desse estudo, será colocado uma nova teoria que tem em sua base introduzir concepções que observam as atitudes tomadas pelos Estados em frente as novas tecnologias e globalizações. Nem sempre as teorias tradicionais possuem respostas condizentes com novas realidades, ambientes e contextos.

Será visto nesse capítulo a posição que a Teoria da Prática Internacional (*International Practice Theory*) traz sobre as teorias tradicionais e como pode se compreender conceitos complexos por uma nova percepção. As abordagens práticas possuem uma visão diferente do habitual sobre o sistema internacional. Enquanto se distanciam de estruturas calculadas, de normas e regras, as abordagens continuam concordando com conceitos tradicionais de cultura, critica, construtivismo. Há uma compreensão melhor das dinâmicas quando se entende que o mundo funciona em movimento. (BUEGER, GARDINER, 2015)

3.1 A TEORIA DA PRÁTICA NAS RELAÇÕES INTERNACIONAIS

A Teoria da Prática é uma reflexão que começou a surgir nos anos 1990 com a introdução de pensamentos construtivistas. Dentro das ciências sociais havia tentativas de incluir a ideia de prática nos debates. Sociólogos analisavam conceitos de organizações, aprendizado e estratégias pelas lentes da prática. Outra área da sociologia que apresentava a prática era nos dos estudos de comportamentos do consumidor, como são as relações de consumo e sua influência nas pessoas.

Por ser uma teoria que acompanha o construtivismo e as ciências sociais, suas primeiras definições não são fáceis de datar. Escreve Bueger[7] e Gadinger (2017) que a antropóloga Sherry Ortner, em 1984, foi uma das primeiras a considerar a noção de teoria da prática e a perceber como um novo símbolo para orientações teóricas, seus estudos se basearam no trabalho do sociólogo Pierre Bourdieu. Anteriormente, foi presenciado o uso da prática em pontos levantados por Karl Marx sobre como a prática é uma categoria fundamental para a vida humana

[7] Christian Bueger é um professor de Relações Internacionais e sua área de pesquisa atualmente é nas respostas políticas para a insegurança marítima, principalmente no que se refere a pirataria. Pesquisa a Teoria da Prática Internacional e em como implementar esse viés nas práticas das organizações internacionais em lidar com o problema da pirataria. Sua pesquisa é um exemplo de como aplicar essa teoria em assuntos que se transformam durante os anos e desdobram a novas problemáticas. Mais sobre sua pesquisa e também a discussão teórica da Teoria da Prática Internacional em seu site: http://www.safeseas.net/

e que toda sociedade é, em sua essência, o funcionamento de várias práticas. Por esse pensamento, o fato de teorizar já é uma prática. (BUEGER, 2018)

Dentro das ciências sociais há várias definições de prática, porém a maior parte das pesquisas chegam aos mesmos conceitos, Bueger (2018) expõe: práticas são compostas por *bodily movements*, que são as ações e falas; o conhecimento prático e os objetos - que são a parte material. O autor cria um exemplo que pode servir como um desenho para entender melhor a junção dos três elementos: na culinária avançada, sempre há um time de cozinheiros e chefes que se comunicam (movimentos e mensagens) e ensinam as receitas (conhecimento prático). Para cozinhar são necessários ingredientes e produtos (objetos). E por último a ação de cozinhar (prática) (BUEGER, 2018).

Não há um campo unificado nem consenso, porém a maioria dos teoristas, segundo Schatzki (2001) usam o conceito de *field of practices* para juntar todos os componentes da prática: conhecimento, ideais, atividades, ciência, poder, interações sociais, linguagem e transformações históricos. Vendo assim, a Teoria da Prática Internacional tem o propósito de ser plural e compreender todas as atividades.

No campo de estudo das relações internacionais, os teoristas práticos colocam-se opostos a outras teorias, tais como Intelectualismo, Representacionismo, Individualismo, Estruturalismo, Teoria de Sistemas, Semiótica. Também se posiciona delineando diferenças com Racionalismo e vários tipos de Construtivismo, de uma maneira que a teoria se encaixe de forma única:

> "A intenção é de mostrar como o núcleo do fenômeno de Relações Internacionais, incluindo poder, comportamento dos Estados, identidade, organizações internacionais, multinacionais, normas e regras, guerra e paz, podem ser estudados de maneiras diferentes. Assim, Teoria da Prática Internacional contribui para o estudo das relações internacionais e a política global estudando as áreas problemáticas de cada tema." (BUEGER, GADINGER. 2017. p. 15)

Segundo Bueger e Gadinger (2017), o cientista político Neumann, em 2002, já levantava questões sobre entender os movimentos dos atores políticos no ambiente internacional usando a Teoria da Prática Internacional. A teoria tem o propósito de colocar as ações com a mesma importância dos resultados finais. Para estudos políticos, a percepção das práticas e atividades dos atores é tão significativo quanto chegar ao resultado esperado.

Ao contrário de compreender a ordem social como um arranjo de normas e regras, as abordagens da Teoria da Prática Internacional tentam entender, em primeiro lugar, o que faz o ator acreditar naquilo que ele faz. Teorias tradicionais que se empenham a usar somente a

racionalidade como se fosse uma variável fixa, acabam limitando o papel da ordem social e da comunidade (BURGER, GADINGER. 2015). Por isso a teoria se afasta dos modelos que focam em cálculos de interesse ou em validar normas e se aproxima em investigar e compreender as dinâmicas. O conceito de prática busca ser vista como ação orgânica.

> "Seria errado ver o conceito de prática como somente sinônimo de ação. Teoria da Prática integra os atores e seus objetivos, os valores, as crenças, recursos, ambiente externo, todos colocados em um sistema de atividades em que o individual, o social e o material são interdependentes" (HAJER, WAGENAAR, 2003, p.20)

Pouliot (2008) concorda que diplomacia é uma área que a Teoria da Prática Internacional se adequa perfeitamente. A maioria das teorias de relações internacionais coloca a diplomacia como "[...] antes de tudo, sobre ações estratégicas, racionalidade instrumental e cálculos de custo benefício." (POULIOT, 2008 p. 258). Porém, o cientista prefere perceber a diplomacia de uma forma mais natural, que não é puramente ações calculadas. Dessa forma, não é uma ciência exata, sua base parte de julgamentos, habilidades humanas e conhecimento.

A imagem de conhecimento vai além do que a palavra indica, aqui ela funciona em conexão com aprendizado prático. Por exemplo, o conhecimento teórico não é suficiente para entender como a diplomacia funciona, pois, não requer só observar, como também aprender, adaptar e se tornar ativo no ambiente. Bueger e Gadinger (2017) explica como escrever um discurso diplomático não é uma ação isolada de um indivíduo sozinho, por trás há um processo cheio de pessoas, etapas, momentos. O conhecimento é aprendido com experiência e muitas vezes com coisas não ditas, considerando, antes de tudo, o contexto e o ambiente. É mais sobre *"knowing how"* do que *"knowing that".*

Essa ideia de conhecimento prático acompanha a história há tempos, como na expressão grega *métis*, segundo Scott (1998) e Pouliot (2008) sua tradução para a atualidade seria: "um conhecimento rudimentar que só pode ser adquirido na prática e quase não pode ser transmitido na forma escrita ou oral, apenas na prática real". (POULIOT, 2008. p. 270). Esse exato tipo de conhecimento é fundamental na política, visto que, é esta e não a burocracia, que acompanham o dia a dia da sociedade.

A questão central da Teoria da Prática Internacional é: os tempos mudam. Não parece viável explicar eventos atuais com teorias que explicavam fenômenos de 50 anos atrás. O estudo da teoria vai tentar preencher as lacunas que surgem com a modernização e o aparecimento de novas problemáticas. Citando o caso do Brasil, em 2009, com Decreto Ministerial nº 14/2009 de Integração e Coordenação dos Setores Estratégicos da Defesa, o espaço cibernético entrou

no rol de estratégias para segurança nacional. O que indica que, a segurança nacional, pela primeira vez, trabalhará com novas dimensões. A tecnologia de modo intrínseco é uma atualização do cenário político. Então, reforça Pouliot (2008), o que está faltando no Realismo e no Construtivismo são as conexões com a modernidade, algo que a Teoria da Prática Internacional pretende acompanhar.

3.2 INTERNET E SEGURANÇA

A Teoria da Prática Internacional é aplicada no estudo da diplomacia digital, termo usado por teoristas ao se tratar de instrumentos de tecnologia e internet, com base no processo de explorar interações e hábitos que são influenciados por novas tecnologias. É um idioma que abrange aspectos tanto de um grande fenômeno, a internet, quanto de aspectos cotidianos, troca de e-mails e redes sociais. Os atores devem estar sempre atentos ao caminho da digitalização e os riscos do desconhecido. (HEDLING, BREMBERG, 2021)

Nessa perspectiva, as pesquisas associam a teoria com efeitos de *soft power* e *strategic communication*. O *soft power* é uma visão adotada para que as políticas insistam em mostrar os tributos culturais e valores de um país. *Strategic communication* é uma perspectiva de compreender por que certas estratégias funcionam melhores que outras e, tentar aprimorá-las para cada nação. É visto também que a transparência das ações resulta em maior participação dos espectadores, aqui encaixa as pessoas que não participam diretamente da diplomacia adotada (HEDLING, BREMBERG. 2021). Isso significa que tem espaço de atuação para todos atores dentro da diplomacia digital.

O choque moderno da inclusão da internet na diplomacia, aumentou a necessidade de entender a estrutura dessa nova mídia. A desinformação ou a plantação de informações falsas confunde os planos estratégicos das instituições. “O aumento da desinformação digital e ameaças à segurança cibernética obriga Estados e organizações internacionais repensarem sobre o papel da diplomacia digital” (HEDLING, BREMBERG. 2021. p. 9) Atualmente, as instituições estão passando por um processo de adaptação a tecnologias e novos desafios e é necessário a discussão da era digital. Perigos *online* resultam em danos *offline*.

É citado por Adler-Nissen, Drieschova (2019) que o uso das tecnologias abre espaço para pessoas fazerem coisas que não fariam em outros meios. A acessibilidade permite que as ameaças e ataques tenham espaço.

> "Nós debatemos que a diplomacia digital é uma abordagem prática interessante dentro das Relações Internacionais, porque envolve práticas que podem

> ser observadas melhor que outras práticas do campo. Isso está ligado com a transparência da internet, onde por exemplo, as práticas de comunicações são visíveis, assim como a relativa ou observada neutralidade da tecnologia comparada a outros elementos de diplomacia." (HEDLING, BREMBERG. 2021. p. 11)

Na análise da tecnologia é importante, separar as conexões da internet entre o espaço e o material, para que assim haja compreensão melhor de cada área. As conexões são as redes e os canais, enquanto o material é o uso da tecnologia como estratégia política. Afirma Hedling, e Bremberg (2021) que o jeito que a internet é usada, os algoritmos, conexões e o *software* é o que influencia na disseminação da informação. O mau uso das funções da internet resulta em ameaças cibernéticas. A teoria pondera a contextualização dessas informações e do uso da internet, cabe avaliar a conjuntura *offline*.

Dessa forma, a área de prática na diplomacia no que tange a tecnologia é a forma de validar as conexões entre atores e internet. A internet é uma dimensão importante nas políticas contemporâneas e a digitalização está influenciando as relações e se tornando fundamental para agenda estratégica dentro do Estado.

Introduzindo a segurança, Abrahamsen e Williams (2011) defendem que nos últimos séculos está muito enraizado a ideia do monopólio legitimo da violência e da segurança nas mãos do Estado (público), dominados pelos militares. E esse pensamento ignora as organizações privadas de segurança e a modernidade política. Discute-se que as instituições privadas ocupam papel global e local. Segundo a Teoria da Prática Internacional há uma nova relação de articulação entre relações público e privado, global e local.

O aumento de atores do setor privado de segurança não deve ser visto como uma diminuição do poder estatal. A melhor maneira de incluir o setor privado nessa estrutura é o colocando como uma terceira via, acompanhando ao lado de políticas estatais. Como resultado, deve ser reconhecido que a segurança privada tem o papel de oferecer uma segurança que pode ser comprada no livre mercado, o que não só influência positivamente nas capacidades econômicas, como também é uma forma a mais de oferecer segurança para quem tem capital de comprar.

Quanto mais atores trabalharem em identificar riscos, que nem sempre são sinônimos de perigos imediatos, há a vantagem de poder lidar com uma resposta eficácia. A troca de conhecimentos e dados entre os atores é o que daria controle em lidar com ambiente inseguro e é uma estratégia calculada (ABRAHAMSEN, WILLIAMS. 2011). Deve-se fortalecer a ideia

de que a segurança acompanha a globalização e surgimento de novas tecnologias que abre espaço para necessidades novas de proteção.

As práticas de segurança, especialmente a segurança internacional, tem sido tratada tradicionalmente como um campo dominado por poder material, coerção e centralização estatal. Todas as variáveis embora importantes, não são únicas, Abrahamsen e Williams (2011) apontam que, para entender a dinâmica é preciso ver como a segurança funciona em prática. Deve-se incluir os conceitos levantados por Bourdieu de capital cultural (conhecimentos, atitudes, habilidades praticadas pela sociedade) e capital simbólico (status, reconhecimento, privilégios do indivíduo) para compreender o cenário de necessidade da sociedade.

> "A aquisição de capital cultura e simbólico está no centro do reconhecimento das competências dos atores de segurança privada, um status conectado a práticas sociais maiores como a comercialização e tecnificação de segurança, que está se distanciando de uma visão pública de segurança, agora fazendo disso um "serviço" ou uma mercadoria que pode ser comprada e introduzida em mercados competitivos." (ABRAHAMSEN, WILLIAMS. 2011. p. 314)

Posto isso, incluir atores privados na dinâmica proveria uma escala maior de segurança dependendo do que a individuo precisa. "[...] a criação de parceria e redes de apoio garante compartilhar recursos e dilui a responsabilidade, fazendo com que, riscos se tornem mais fáceis de lidar." (DUPONT, 2004 p. 78). A inclusão não seria visando somente o bem estar social, mas a união do privado e público, assim como do global e local, resultarão em um plano estratégico para combater as ameaças.

Portanto, a segurança é um campo de eternas mudanças. Acentuado por Pouliot (2008) segurança não simplesmente está lá, ela cresce e desenvolve conforme as necessidades da realidade. Com o surgimento de novos riscos há o aumento crescente de segurança privada, porque a sociedade e os atores desejam garantir segurança dentro de todas as áreas, assim como no espaço cibernético. Essa conexão é natural da modernização. Essa é uma dificuldade que as teorias tradicionais resistem, em parar de colocar o papel da segurança nas mãos dos militares (ABRAHAMSEN, WILLIAMS. 2011).

4 ESTRATÉGIA CIBERNÉTICA DO BRASIL

A segurança cibernética é uma coleção de vários componentes: políticas, conceitos de segurança, proteções, agendas, documentos, avaliação de riscos, atuação, treinamento, garantias, capacidade humana e tecnologias. As organizações devem compreender o ritmo das mudanças e repensar em novas maneiras de proteção dos sistemas e das redes de acesso, planejando ações capazes de mitigar as necessidades de segurança. Um Estado que trabalha com todas as variáveis terá um ambiente de espaço cibernético confiável, integral e de boa reputação (ITU, 2008).

O Brasil possui, em sua esfera governamental, várias normativas que abordam o tema e documentos que vêm evoluindo e absorvendo mais a necessidade de estabelecer diretrizes, ações e iniciativas para as vulnerabilidades que o espaço cibernético oferece. Conforme Fonseca (2020), a cibersegurança não pode ser compreendida e nem estruturada de forma isolada; o país vem avançando desde 2008, com a premissa de criar estratégias e juntar os órgãos para que esse cenário seja mais seguro.

Nesse capítulo será abordado o arcabouço institucional, que envolve os principais órgãos que atuam no campo cibernético no país, em seguida verificar como tem percorrido o caminho das estratégias na segurança cibernética. Ao final, conclui-se que o último documento estratégico, a E-Ciber, que está em vigor até o ano de 2023, trabalha em constante para consolidar a atuação brasileira, domesticamente e internacionalmente.

4.1 ARCABOUÇO INSTITUCIONAL

A estratégia de segurança cibernética atua para proteger a disponibilidade, integridade, confiabilidade e autenticidade das informações de aspectos de segurança institucional, assim como da sociedade (BRASIL, 2020). O Estado, ao promover esses princípios, busca constituir uma estrutura organizacional que funcione com eles.

Aponta Cruz Jr. (2013) que o desenvolvimento de segurança e defesa cibernética são duas áreas recente no Brasil, de maneira que as instituições estão se adaptando à nova realidade e acompanhando o desenvolvimento da internet. A organização do sistema brasileiro funciona com diversas entidades, instituições públicas desde o nível estratégico até o operacional. A estrutura do setor cibernético possui uma ordem para tomada de decisão hierárquica que parte da Presidência da República, no topo, até que se encontre no último, o nível operacional.

Na área governamental, o tema foi tratado inicialmente com o desenvolvimento da Segurança da Informação (BRASIL, 2014), que se caracterizou consequentemente na criação do Gabinete de Segurança Institucional (GSI-PR). Os deveres do Gabinete, apresentados no Decreto Nº 9.668 de 2019, incluem coordenar as atividades de segurança da informação e das comunicações e supervisionar a atividade da Segurança da Informação no âmbito da Administração Pública Federal, inserida nessa a segurança cibernética. Assessora o Presidente da República no que se refere à segurança.

Dentro do Gabinete de Segurança Institucional, o Departamento de Segurança da Informação e Comunicações (DSIC), possui, como atribuição operacional, as atividades de segurança da informação e da comunicação na Administração Pública Federal (BRASIL, 2008). O que compete a sua função, descrito no Decreto Nº 10.363 de 2020, é planejar, coordenar e supervisionar a atividade nacional de segurança da informação, incluindo, assim, segurança cibernética, bem como gestão de incidentes computacionais, proteção de dados, credenciamento de segurança, tratamento de informações sigilosas e elaboração de normativos e requisitos metodológicos das atividades nacionais de segurança da informação. No site do governo destinado ao Gabinete de Segurança da Informação, os boletins normativos são publicados mensalmente desde janeiro de 2020. Os boletins informam sobre ameaças cibernéticas e orientações para evitá-las.

Um dos serviços que cabe ao Departamento é manter a Central de Tratamento e Resposta a Incidentes Cibernéticos do governo. O Centro de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos do Governo (CTIR Gov) consiste na disponibilização das estatísticas resultantes do trabalho de detecção, triagem, análise e respostas a incidentes cibernéticos.

Outras instituições que operam no campo de segurança cibernética incluem a Polícia Federal, com o Serviço de Repressão a Crimes Cibernéticos (SRCC), que parte da Diretoria de Investigação e Combate ao Crime Organizado (Dicor). Também, a Agência Brasileira de Inteligência (ABIN), que, em uma de suas funções, desenvolve competências criptográficas para proteger instituições públicas conduzidas pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (DINIZ, MUGGAH, GLENNY. 2014).

No que se refere aos níveis estratégico, operacional e tático, fica a critério do Ministério da Defesa. desde a Estratégia Nacional de Defesa (END) de 2008, quando o setor cibernético entrou para a estratégia de defesa nacional, que como prescrito, deu início à consolidação do

setor cibernético no âmbito da defesa (BRASIL, 2008). Com o Centro de Defesa Cibernética (CDCiber), criado em 2010, e o Comando de Defesa Cibernética (ComDCiber), em 2012, o Ministério da Defesa e as Forças Armadas começaram a participar de atividades coordenadas pelo Gabinete de Segurança Institucional no que tange ao espaço cibernético. Desse modo, todos os órgãos mencionados acima podem assegurar a capacidade de atuar em rede.

Entre os propósitos do CDCiber, estão a criação de um simulador de guerra cibernética, a elaboração de antivírus nacional, o desenvolvimento de sistemas de criptografias e a capacitação de militares para situações críticas. O apoio da iniciativa privada nacional para atingir os objetivos é fundamental (CRUZ JR. 2013).

Desta forma, o papel de organizações privadas, em cooperação com atores estatais:

> "Além do setor público, ainda existem as organizações privadas que atuam proporcionando segurança na rede, proteção de dados, sistemas de criptografia, antivírus etc. Este setor é um braço forte e mais eficiente em termos operacionais e produtivos em relação ao setor público. Percebendo isso, o Exército Brasileiro tem se utilizado da capacidade da indústria nacional para desenvolver ferramentas estratégicas para o programa de segurança nacional." (CRUZ JR, 2013 p. 26)

Como assinalado anteriormente, a segurança cibernética é um assunto transversal, multidisciplinar e multissetorial. A área é abordada em diversas normativas no Brasil. A fio, serão divididos os pontos dos campos de segurança e defesa, que, ao se completarem, sucedem à realização das estratégias de segurança cibernética nacional.

4.2 SEGURANÇA CIBERNÉTICA

A discussão de preocupação com a segurança cibernética teve como um dos marcos, segundo Canongia e Mandarino (2009), a reunião da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), em 2009, sobre a Sociedade da Informação, que levantou importantes pontos que serviriam de benefício para as nações. Era notável que surgiriam cada vez mais pautas sobre o tema, devido ao aumento do acesso à internet, aos avanços cada vez mais rápidos da tecnologia da informação e comunicação, ao crescimento das ameaças e vulnerabilidades e às constantes mudanças no ambiente.

Cada parte envolvida tem papel significativo na segurança de sistema e redes. A preocupação e responsabilidade deve integrar todos os atores, tanto público quanto privado; consequentemente, os resultados serão de ordem doméstica e internacional (CANONGIA, MANDARINO, 2009).

Como resultado da reunião, foi feita a proposta de princípios estratégicos que são recomendações para as políticas públicas dos atores, tais como posição de alerta, controle sobre os riscos, interconectividade e interpendências de sistemas de rede e informação. É possível citar também: ter responsabilidade para estar habitualmente avaliando e atualizando procedimentos de segurança; estar preparado para responder no momento de detecção de incidentes; respeitar a democracia e seguir mantendo valores fundamentais do regime político, como privacidade; minimizar as ameaças e vulnerabilidades por meio de ações que avaliam os riscos e que englobam fatores internos e externos, dando importância, também, a fatores humanos, físicos e políticos (CANONGIA, MANDARINO, 2009).

No âmbito do Brasil, a Sociedade de Informação já era assunto implementado nesse período. Em 2008, foi publicada a Instrução Normativa IN GSIPR º 01/2008, que tinha como objetivo disciplinar a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal. De forma que seus principais propósitos eram: disponibilidade de tornar a informação acessível de forma integra; confidencialidade de informações pessoais; autenticidade e confiabilidade. Sem quebra de segurança, o tratamento da informação ocorre de forma que recepciona, produz, utiliza, transporta, transmite, distribui, elimina e controla, inclusive as informações sigilosas, baseado no princípio de que seja respeitada a privacidade destas. O artigo 6º, que trata do inciso VI do art. 5º, define:

> I - assessorar na implementação das ações de segurança da informação e comunicações;
>
> II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;
>
> III - propor alterações na Política de Segurança da Informação e Comunicações; e
>
> IV - propor normas relativas à segurança da informação e comunicações.
>
> (BRASIL, 2008)

Em 2013, aconteceu um episódio de exposição de espionagem cibernética realizado pelos Estados Unidos da América contra sociedades e nações. Veio a ser a divisa entre relações diplomáticas e ferimento da segurança cibernética. Esse acontecimento foi nomeado de *Arquivos Snowden*. Edward Snowden é um técnico em redes de comunicação que já trabalhou para a Central Intelligence Agency (CIA), mas foi trabalhando para a National Security Agency (NSA) que ele expôs documentos de espionagem americana. Os dados foram passados para o jornalista norte-americano Glenn Greenwald, que começou a publicar no jornal britânico The Guardian as primeiras partes do que viria a ser o escândalo. “O mundo já tinha visto ou ouvido falar de algumas formas de vigilância online no passado, mas, desta vez, isso se tornou público

por um país que sempre quis aparecer como um guardião da liberdade pessoal e da democracia, enquanto, na verdade, coletava secretamente dados pessoas de milhões de cidadãos de vários países, incluindo a comunicação de governos estrangeiros." (OPPERMANN, 2014. p. 148),

O Brasil foi o país mais afetado da América Latina, o único da estação no mapa descritivo das operações norte-americanas de espionagem por satélites estrangeiros. Ficou em segundo lugar, após os Estados Unidos, em dados interseccionados, com 2,3 bilhões de telefonemas e mensagens. Três softwares funcionaram na espionagem contra o Brasil: *Highland*, que coletava direta de dados e sinais digitais; *Vagrant*, que copiava telas de computadores; e *Lifesaver*, que acessava cópias dos discos rígidos, onde eram armazenadas as memórias das máquinas (GLOBO, 2013). EUA e seus aliados definiam as espionagens conforme suas percepções de radicalismo; os radicais eram Irã, Cuba, China, Síria, Egito e Rússia. O Brasil ficava na posição moderada, junto com Índia, México, África do Sul e outros (CANABARRO, FERREIRA, 2015).

Dentre os dados brasileiros revelados, é possível citar informações de armazenamentos do sistema da Petrobrás, em que a tecnologia envolvendo exploração em alta profundidade da camada do pré-sal teria sido o alvo. A Petrobrás nunca teve interesse de se posicionar (BBC, 2013). Também espionaram *e-mails* e comunicações telefônicas da Presidenta Dilma Rousseff, até mesmo seu telefone via satélite do avião presidencial. O número pessoal de seu assessor, Anderson Dornelles, e o do general José Elito Carvalho Siqueira, na época diretor do Gabinete de Segurança, vazaram. Há, ainda, indicações de espionagem ao Banco Central (BRASIL, 2015).

A primeira atitude tomada pela presidenta foi cancelar a visita presidencial a Washington, em outubro, uma forma de demonstrar repúdio aos acontecimentos. A mídia começou a especular que a falta da presença da presidenta seria um choque para as relações entre Brasil e EUA (HUFFPOST, 2013). Contudo, Dilma Rousseff foi uma das líderes mundiais a tomar uma frente rígida sobre o assunto (CANABARRO, FERREIRA, 2014). Em seu discurso na 68º Assembleia Geral da Organização das Nações Unidas em Nova Iorque, estabeleceu o posicionamento do país:

> "O Brasil, Senhor Presidente [Barack Obama], redobrará os esforços para dotar-se de legislação, tecnologias e mecanismos que nos protejam da interceptação ilegal de comunicações de dados. Meu governo fará tudo que tiver ao seu alcance para defender os direitos humanos de todos brasileiros e todos cidadãos do mundo, proteger os frutos da engenhosidade, os trabalhadores e as empresas brasileiras. O problema, porém, transcende o relacionamento bilateral de dois países e afeta a própria comunidade internacional que dela exige resposta. As tecnologias de telecomunicação e

> informação não podem ser novo campo de batalha entre os estados, esse é o momento de criar novas condições para evitar que o espaço cibernético seja instrumentalizado como arma de guerra por meio da espionagem, a sabotagem e os ataques contra sistema e infraestrutura de outros países." (ROUSSEFF, 2013).

Rousseff comentou também que o Brasil faria de tudo para respeitar a privacidade dos cidadãos, pois a internet faz parte de uma democracia saudável, e que a proposta do Marco Civil da Internet teria medidas que garantem efetiva proteção dos dados, porém, por mais que o país implemente leis, a segurança da internet é uma preocupação que deve ser lidada de forma multilateral. Ao se falar de liberdade de expressão, privacidade e direitos humanos, é mais adequado que os Estados os priorizem na agenda internacional de segurança cibernética.

A lei com o propósito de proteger a internet foi nomeada de Marco Civil da Internet e definida por Arnaudo (2017) como Constituição da Internet Brasileira, por ser importante componente da estrutura política do país. Anteriormente, já havia se discutido um delineamento do que viria a ser a lei. Duas leis de segurança cibernética que a antecedem são: Lei Azeredo, lei Nº 12.375 de 2010, e Lei Carolina Dieckmann, lei Nº 12.737 de 2012. A formulação da lei foi tanto um marco doméstico, como um episódio internacional, já que foi uma das primeiras a tratar sobre privacidade da internet no mundo (DINIZ, MUGGAH E GLENNY, 2014). Antes de oficializá-la, houve a criação de um debate virtual em busca da participação dos cidadãos, dando direito a opiniões e abertura de debates. A comunidade funcionava com voto dos cidadãos e uma área de fórum aberta, onde as pessoas poderiam se conhecer e trocar informações, tornando a realização participativa e informativa.

O Marco Civil da Internet foi sancionado na NETmundial, Encontro Multissetorial Global Sobre o Futuro da Governança da Internet, que aconteceu em abril de 2014 em São Paulo. Foi organizado em parceria com CGI.br, Comitê Gestor da Internet no Brasil, e 1Net, plataforma online de coordenação e cooperação que reúne entidades internacionais.

A lei tem como fundamento o respeito à liberdade de expressão, aos direitos humanos, à pluralidade e à diversidade. Em seu Art. 4º, defende os princípios do acesso à internet: deve ser um direito de todos; já em seu Art. 8º, protege a liberdade de expressão e o exercício pleno do usuário. A internet é um ambiente que fornece informação, conhecimento, participação em assuntos de políticas públicas e de comunidades culturais. Define, assim, que a internet é, atualmente, essencial para o exercício da cidadania, sendo necessário criar uma rede de proteção para um ambiente livre. O Art. 7º define garantias que o usuário possui:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; (BRASIL, 2014)

Outras providências da Lei se referem à conexão da internet, pela disponibilização de acesso seguro, confiável e de qualidade para os cidadãos. O provedor deve preservar a honra, imagem e intimidade de cada usuário, e o conteúdo acessado e informações privadas só devem ser disponibilizados mediante ordem judicial. As medidas fornecidas de segurança e sigilo devem ser descritas de modo claro para que sejam de linguagem fácil para os cidadãos. De modo que o acesso à internet, além de ser seguro, deve ser inclusivo – fomentando a produção e circulação de conteúdo nacional.

Outro pilar da Governança da Internet Brasileira, segundo Canabarro e Ferreira (2015), é o Comitê Gestor da Internet do Brasil (CGI.br), que foi criado em 1995 pelo Ministério das Comunicações com a Portaria Interministerial Nº 147. O comitê tem como atribuições acompanhar e disponibilizar serviços de internet no país, estabelecer recomendações relativas a estratégia de implantação e interconexão de redes, analisar e selecionar opções tecnológicas, recomendar padrões, procedimentos técnicos e operacionais junto a um código de ética de uso para todos os serviços de internet no Brasil (CGI.br, 2022).

Em 2003, foi assinado o Decreto Nº 4.829, que define outras providências para o Comitê Gestor da Internet no Brasil, acrescentando mais atividades e introduzindo representantes de variados órgãos do governo. Neste decreto, foi atribuído pelo Art. 1º:

> III - propor programas de pesquisa e desenvolvimento relacionados à Internet, que permitam a manutenção do nível de qualidade técnica e inovação no uso, bem como estimular a sua disseminação em todo o território nacional, buscando oportunidades constantes de agregação de valor aos bens e serviços a ela vinculados;
>
> IV - promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade;
>
> V - articular as ações relativas à proposição de normas e procedimentos relativos à regulamentação das atividades inerentes à Internet;
>
> VI - ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;
>
> VII - adotar os procedimentos administrativos e operacionais necessários para que a gestão da Internet no Brasil se dê segundo os padrões internacionais aceitos pelos órgãos de cúpula da Internet, podendo, para tanto, celebrar acordo, convênio, ajuste ou instrumento congênere; (BRASIL, 2003)

Em 2018, pelo Decreto Nº 9.637, foi instituída a Política Nacional de Segurança da Informação, uma afirmação do Brasil em demonstrar preocupação em garantir os três pilares da Segurança da Informação: confidencialidade, integridade e autenticidade (LAGINESTRA, OLIVEIRA, BRAREN, FREITAS, 2021).

Segundo o Art. 2º, a segurança da informação abrange:

> Art. 2º Para os fins do disposto neste Decreto, a segurança da informação abrange:
>
> I - a segurança cibernética;
>
> II - a defesa cibernética;
>
> III - a segurança física e a proteção de dados organizacionais; e
>
> IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. (BRASIL, 2018)

Estabelecer um nível estratégico com uma política nacional de segurança da informação é de importante proporção para alinhar o normativo e estratégico das ações do Estado; espera-se que, com ela, a organização e estrutura da Segurança da Informação no país melhore. Colocada de forma apropriada, fomentaria investimentos internos, aumento da confiança dos cidadãos nas atividades públicas e, junto a isto, aumento de cultura da segurança de informação (SABBAT, 2018).

Em suas competências, pelo Art. 12º, fica a responsabilidade de aprovar diretrizes, estratégias, normas e recomendações, acompanhar a evolução doutrinária e tecnológica, tanto em âmbito doméstico quanto internacional. Apoia a elaboração dos planos nacionais vinculados às estratégias nacionais de segurança, o trabalho com os centros de prevenção, o tratamento e respostas a incidentes cibernéticos e a combinação de apoio para articular-se com entidades de prevenção de outros países. Dessa forma, a Política Nacional de Segurança estabelece as diretrizes no nível estratégico. Observa-se melhor na figura 5 a seguir:

Figura 5 – Política Nacional de Segurança

Fonte: Fonseca, 2020

4.3 DEFESA CIBERNÉTICA

A defesa nacional desempenha a função de proteção do Estado frente a ameaças e perigos à soberania. Cruz Jr. (2013) localiza o funcionamento da defesa dentro do espaço cibernético por assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos ativos de informações. Apesar de, como já visto no capítulo anterior, o cenário de guerra declarada não ser, na conjuntura atual, iminente, o interesse da defesa é fundamental para os ataques em geral e o fator humano. “O ambiente cibernético não existe por si só: sua dinâmica de funcionamento depende de conjunturas e interesses não virtuais” (CRUZ JR., 2013. p. 10).

A defesa cibernética fica sob a responsabilidade das Forças Armadas (FA), consideradas parte da Defesa Nacional. A Estratégia Nacional de Defesa (END) já havia, em 2008, considerado o espaço cibernético como setor estratégico, assim como o nuclear e o espacial. A consolidação do Setor Cibernético no Ministério da Defesa foi firmada com a Diretriz Ministerial nº 14/2009 Integração e Coordenação dos Setores Estratégicos da Defesa, em 2009. O documento reconhece:

> "Nesse contexto, é imperiosa a necessidade de que haja irrestrita coordenação e integração na definição e desenvolvimento dos programas e ações que digam respeito, particularmente, aos setores nuclear, cibernético e espacial, definidos como estratégicos pela END, que ficarão sob responsabilidade, respectivamente, da Marinha, do Exército e da Aeronáutica." (BRASIL, 2009)

O documento, por fim, prevê a necessidade de definir as ações de cada estratégia e limitar um ambiente especializado, capacitação de profissionais, tecnologia e pesquisa que

sirvam de base para cada área. Em 2010, cumprindo essa diretriz, foi ativado o Núcleo do Centro de Defesa Cibernética.

Em 2012, com a Portaria Nº 3.028-MD, foi atribuída ao Centro de Defesa Cibernética (CDCiber) a responsabilidade e integração das atividades de defesa cibernética, de forma que deve servir para proteção militar e governamental das redes de acesso de ataques internos ou externos, protegendo a integridade nacional (DINIZ, MUGGAH, GLENNY, 2014). Duas atribuições na íntegra dos artigos:

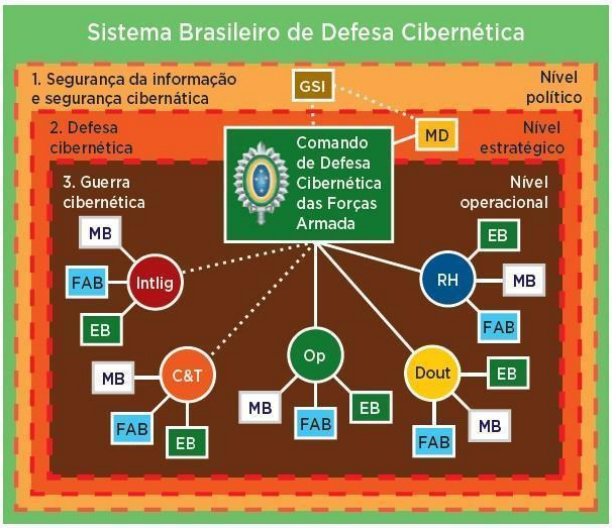
> Art. 1º Atribuir ao Centro de Defesa Cibernética (CDCiber), do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de defesa cibernética, no âmbito do Ministério da Defesa (MD), consoante o disposto no Decreto nº 6.703, de 18 de dezembro de 2008.
>
> Art. 2º O Estado-Maior Conjunto das Forças Armadas (EMCFA) deverá realizar as coordenações necessárias para a adequação da estrutura organizacional do CDCiber às atribuições previstas no art. 1º desta Portaria. (BRASIL, 2020)

No mesmo ano, a Portaria Normativa Nº 3.389/MD criou a Política Cibernética de Defesa, com a finalidade de orientar as decisões em nível estratégico, assegurar o uso efetivo do espaço cibernético pelas Forças Armadas, capacitar e investir em recursos humanos e atividades ao setor cibernético, contribuir para a segurança dos ativos de informação da Administração Pública Federal (APF) no que se refere à Segurança Cibernética.

Desse modo, a inclusão do espaço cibernético na agenda militar terá respostas parecidas dos outros meios: “[...] o poder cibernético envolve a capacidade de responder aos ataques cibernéticos da mesma forma que respondemos a qualquer outro ataque, utilizando-se os recursos considerados mais convenientes ao fim, inclusive por meio de ações cibernéticas ofensivas.” (BRANDÃO, IZYCKI, 2019. p. 244).

A figura 6 mostra a organização do Sistema Militar de Defesa Cibernética (SMDC):

Figura 6 – Sistema Militar de Defesa Cibernética



Fonte: Carvalho, 2011

As decisões da organização, como descrito na Doutrina Militar de Defesa Cibernética (2014), ocorrem em quatro níveis: o nível político, em que os principais atores ficam na responsabilidade da Presidência da República e do Comitê Gestor da Internet no Brasil; o nível estratégico, que trata das ações de Defesa Cibernética, a cargo da Defesa Cibernética, dos Centros de Tratamento de Incidentes de Redes (CTIR) e da Administração Pública Federal (APF); o nível operacional, que lida com ações de Guerra Cibernética, a cargo dos Comandos Operacionais; por fim, o nível tático, quando ativado a Guerra Cibernética e fica a cargo das Forças Componentes.

O emprego da Defesa Cibernética tem sustentação em quatro princípios: No princípio do efeito, as ações tomadas no espaço cibernético devem resultar em efeitos estratégicos, operacionais ou táticos que afetam o mundo real, mesmo que estes não sejam cinéticos, ou seja, resultados físicos. No princípio da dissimulação, há as medidas ativas que devem ser aplicadas para dissimular no espaço cibernético, o que tornará as ações ofensivas e explanatórias difíceis de rastrear. No princípio da rastreabilidade, há as medidas que são necessárias para detectar as ações cibernéticas ofensivas e explanatórias. E no quarto elemento, o princípio de adaptabilidade, a defesa deve acompanhar a evolução da tecnologia e as mudanças do espaço cibernético.

O que a Defesa Cibernética não alcança, conforme citado na Doutrina Militar de Defesa Cibernética (2014):

a) limitada capacidade de identificação da origem de ataques cibernéticos;

b) existência de vulnerabilidades nos sistemas computacionais;

c) dificuldade de identificação de talentos humanos;

d) grande vulnerabilidade a ações de oponentes com poder assimétrico;

e) dificuldade de acompanhamento da evolução tecnológica na área cibernética; e

f) possibilidade de ser surpreendido com base nas vulnerabilidades dos próprios sistemas de informação.

4.4 EVOLUÇÃO DAS ESTRATÉGIAS BRASILEIRAS

Organizando os principais acontecimentos da agenda brasileira abordados no capítulo, para uma visualização melhor, a figura 7 indica uma linha do tempo do período retratado:

Figura 7 – Linha do Tempo

Fonte: Elaboração própria com base no site do Igarapé[8]

As estratégias nacionais de segurança cibernética são planos de ação desenhados para melhorar e assegurar a segurança de infraestruturas, serviços e cidadãos (IGARAPÉ, 2011). São estruturadas a partir de objetivos principais, prioridades e princípios a serem seguidos nos anos seguintes.

Anteriormente aos documentos de estratégia, que começaram a incluir o conceito de espaço cibernético, a preocupação brasileira era a proteção de dados e informações. Por exemplo, por meio do Decreto Nº 3.505/2000, que institucionalizou o Comitê Gestor da

[8] IGARAPÉ. Instituto. Disponível em: https://igarape.org.br/sobre-o-igarape/

Segurança da Informação (CGSI). “Esse processo vai culminar com a inclusão da área cibernética como estratégica na END, dando então espaço para o desenvolvimento de novos elementos de defesa nesse campo” (PAGLIARI, PINTO, VIGGIANO, 2020, p. 158).

Com o Decreto Nº 6.703/2008, foi aprovada a Estratégia Nacional de Defesa (END), que possui, em sua dimensão, questões referentes a tecnologias para gestão de capacitações, orçamentos e projetos, sob o nome de Segurança das Informações. É importante registrar esse significativo passo no caminho que o país está percorrendo com a segurança e defesa cibernética, pois a estratégia serviu de auxílio para incorporar o termo cibertecnologia na agenda (CANONGIA, MANDARINO, 2009).

A Estratégia Nacional de Defesa propunha fortalecer os três setores inclusos agora na agenda: nuclear, espacial e cibernético. "Como decorrência de sua própria natureza, esses setores transcendem a divisão entre desenvolvimento e defesa, entre o civil e o militar." (BRASIL, 2008). Em seu texto, propunha a construção de uma organização encarregada em desenvolver a capacitação cibernética nos campos industrial e militar.

Como visto anteriormente, o espaço cibernético contorna outros campos, e, pela END, entendia-se que seria de grande importância o domínio cibernético para outras áreas. Em um primeiro momento, era apenas um instrumento para assegurar comunicações entre os monitores espaciais, aéreos e a força terrestre, mas seu uso tem mudado conforme os anos. Segundo Cruz Jr. (2013), foi criada, dessa forma, uma multiplicidade de lideranças dentro do próprio Ministério da Defesa, e o novo setor acaba por ser representado nas três Forças, cada unidade possuindo seu próprio núcleo de proteção cibernética.

A Estratégia Nacional de Defesa foi revista em 2012 e novamente em 2016, cuja versão é a última e está em vigor atualmente. Nesta, o Setor Cibernético possui mais planejamento e intenção de unir vários atores do Setor de Defesa, comunidade acadêmica, setores públicos e privados, tendo em vista também intensificar parcerias estratégias com as Forças Armadas de outros países.

Ademais, em campo de âmbito nacional, reforça, novamente, a ligação entre o espaço cibernético e os sistemas de informações brasileiros:

> “2.2.16. Adicionalmente, requerem especial atenção a segurança e a defesa do espaço cibernético brasileiro, essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional.” (BRASIL, 2016)

Raphael Mandarino Junior e Claudia Canongia foram os organizadores do Livro Verde Segurança Cibernética no Brasil, em 2010. Visava começar um debate social, econômico, político e técnico-científico sobre a Segurança Cibernética, reconhecendo que "[...] ainda há muito a ser alcançado, pois estamos dando os primeiros passos para criar condições necessárias de segurança cibernética[...]" (BRASIL, 2010). Menciona como suas fronteiras não são claramente definidas, uma discussão que tem sido conduzida desde os primeiros conceitos sobre o campo e na estratégia anterior, e ainda impacta o dia a dia.

O que, comparado à Estratégia Nacional de Defesa, ainda se observa é a preocupação de desenvolver um conjunto de ações colaborativas entre os órgãos públicos, setores privados, academia e sociedade. O papel social tem sido conduzido de forma a incluir todos na segurança cibernética. Uma das prioridades é a manutenção e o reforço da preocupação nas infraestruturas críticas, como energia, transporte, telecomunicações, água, finanças e informação.

O Brasil era considerado um dos protagonistas em se posicionar estrategicamente em iniciativas e fóruns. Uma das reconhecidas participações em fóruns aconteceu entre 2009 e 2010, no evento promovido pela Organização para Cooperação e Desenvolvimento Econômico (OCDE), em que o país apresentou uma proposta de estratégia nacional de segurança cibernética. A proposta foi bem vista e aprovada: "O que realça a competência articuladora, de gestão, e técnica do país no tema" (BRASIL, 2010). Por concepção de vários Estados, a Convenção de Budapeste, elaborada pelo Comitê Europeu para os Problemas Criminais como o primeiro tratado internacional sobre os chamados cibercrimes, não estava atendendo às exigências dos crimes cibernéticos e avanços tecnológicos. O Brasil tomou atitude, emitindo uma declaração em 2010, consensada pelos países sobre tal aspecto, abrindo uma oportunidade de o país se posicionar com sua preocupação perante os crimes cibernéticos, além de iniciar debate sobre as dificuldades de lidar com espaço cibernético.

No mesmo ano, houve a criação do CDCiber, a primeira unidade militar dedicada ao espaço cibernético da América Latina, de forma que o país tem começado a investir na área, tentando uma posição de jogador no sistema internacional (DINIZ, MUGGAH, GLENNY, 2014). Um dos fatores considerados como vantagem para continuar investindo é o baixo custo comparado a expandir militarmente em outras áreas, como a terrestre.

No Livro Verde estavam pontuadas as expectativas do campo estratégico para o ano de 2020; a ideia dos autores era que no período futuro haveria aumento na penetração da banda larga de alta velocidade e das redes sem fio, e que essas chegariam ao alcance da maior parte

da sociedade. Isso leva a outro ponto: seria maior o número de pessoas conectadas, por isso haveria mais compartilhamento de dados confidenciais. Continuando nesse raciocínio, haveria necessidade de classificar as informações. O futuro das finanças iria depender dos serviços e comércios online e já exigiria mais regulamentações e normas severas.

Dentre os desafios que se destacavam, continuava a preocupação com a falta de uma estrutura firme para o que diz respeito à segurança cibernética. O avanço na área tem aumentado, comparado aos anos anteriores, alcançando 1,3% do PIB, embora continuem persistindo estas dificuldades:

> "Carência de programa, em nível nacional, que promova sistematicamente o desenvolvimento tecnológico e prospecção em temas como inteligência de sinais e de imagens, recursos criptográficos, segurança na computação em nuvem, desenvolvimento seguro de software, segurança cibernética, e segurança das infraestruturas críticas;
> Carência de conhecimento, mapeamento, e prospecção de tecnologias que apoiem a segurança cibernética do país, minimizando tanto suas vulnerabilidades quanto suas dependências tecnológicas externas e hiatos tecnológicos;" (BRASIL, 2010)

Por fim, no Livro Verde está apontada a ausência de legislação nacional e internacional específica para segurança e crimes cibernéticos, no que, durante a última década, o país tem evoluído. Como citado anteriormente, a exemplo do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais.

De forma a atender as necessidades de uma governança efetiva da segurança de informações, o Gabinete de Segurança Institucional publicou em 2015 o livro de Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal. A estratégia foi planejada para os anos de 2015 a 2018.

A Estratégia foi escrita após os acontecimentos do Caso Snowden, e a Comissão Parlamentar de Inquérito, nominada CPI da Espionagem, apontou as fragilidades do país perante os incidentes de espionagem. Logo em seguida, a preocupação foi reforçada no estudo realizado pela Agência Brasileira de Desenvolvimento Industrial (ABDI), em 2014. O estudo, denominado de Mapeamento de Fornecedores Nacionais de Tecnologia da Informação e Comunicação (TIC) para Redes Elétricas Inteligentes (REI), colocou como frágil a segurança cibernética, "identificada como uma das principais preocupações das concessionárias, empresas fornecedoras de TIC e centros de pesquisa voltados para o setor." (BRASIL, 2015, p. 15).

Nesse cenário de crescentes ameaças cibernéticas, o governo reforça as relações de Segurança da Informação e Comunicação e Segurança Cibernética na agenda estratégica. Ao colocar em prática o previsto no documento, no futuro terá sido estabelecida a Governança Sistemática nesse campo.

Uma grande parte dos objetivos levantados na estratégia são iguais aos anteriores; na educação, por exemplo, continua discutindo sobre fortalecer pesquisas sobre segurança cibernética no âmbito da academia; investir em desenvolvimento e inovação nesse campo, principalmente porque suplementaria a reputação do país:

> "[...] para que o Estado brasileiro seja reconhecido mundialmente, como ator de destaque no cenário internacional, sendo respeitado por resultados tecnológicos relevantes, de forma a atender a necessidade de assegurar a soberania da Nação e, associado a isso, a privacidade de seus cidadãos no espaço cibernético." (BRASIL, 2015 p. 45)

Cita também a importância de profissionais que lidem com identificação de vulnerabilidades, reconhecimento de artefatos maliciosos e outras ferramentas cibernéticas que surgem. Entende-se que um ecossistema de segurança precisa harmonizar especificações de bens e serviços, o que necessita de uma gama maior de profissionais, um dos objetivos da agenda de segurança: investir em capacidade humana.

É reconhecido no livro que a segurança cibernética e de informações ainda não é de alta prioridade na agenda de governo. "Urge, então, aumentar gradativa e prioritariamente o nível de maturidade e estabelecer a Governança Sistêmica de SIC e SegCiber [...]" (BRASIL, 2015. p. 52). Caso falte atenção na segurança nas infraestruturas críticas, a sociedade será prejudicada, e a missão do Estado é prover a segurança da sociedade. É fundamental que cada instituição planeje e invista em recursos para fortalecer a segurança cibernética.

A conjuntura nacional, aos poucos, foi ampliando a visão das políticas e estratégias. Em 2014, já havia sido criada a Doutrina Militar de Defesa Cibernética, e, em 2015, houve atualização do Glossário das Forças Armadas (GFA):

> “Será somente o Glossário das Forças Armadas (GFA) de 2007 (4ª edição) e o de 2015 (5ª edição), que irão problematizar de forma mais efetiva o termo cibernético. A partir de 2007, passa a existir uma diferenciação entre o termo eletrônico e o termo cibernético, que irá se consolidar no documento de 2015 e abrirá espaço para a execução de medidas práticas para institucionalização de procedimentos ligados à defesa cibernética.” (PAGLIARI, PINTO, VIGGIANO, 2020, p. 159).

É importante notar, segundo Diniz, Muggah e Glenny DINIZ, G. MUGGAH, R. GLENNY (2014), que, durante os anos 2010, o Brasil investiu gradativamente nas capacidades

cibernéticas, como, por exemplo, normativos como o Marco Civil, em 2013, e os documentos da segurança cibernética. Em 2018, foi instituída a Política Nacional de Segurança da Informação, que reflete recomendações previamente ressaltadas nos documentos estratégicos desde 2010. Logo, há uma carência de uma nova agenda estratégica, atualizando e ressaltando pontos importantes e que sejam de concordância com a Política Nacional de Segurança da Informação.

A nova estratégia, que viria a se chamar Estratégia Nacional de Segurança Cibernética (E-Ciber), resultou de sete meses de trabalho, três grupos temáticos, 30 dias de reuniões fechadas e 20 dias de consultas públicas, em 2019. A atitude de liberar consultas públicas é um passo importante de transparência das ações dos órgãos públicos e inserção da sociedade no que tange à segurança cibernética. Após as diversas contribuições recebidas, pelo Decreto Nº 10.222, de fevereiro de 2020, foi aprovada a estratégia para o período de 2020 a 2023.

A E-Ciber veio a preencher a lacuna no arcabouço normativo nacional sobre segurança cibernética, e levanta três pontos de dificuldades pelas quais a área ainda passa: a fragmentação das iniciativas de segurança, fragilizando os esforços no setor; a falta de alinhamentos normativo, estratégico e operacional que trabalhem juntos; por último, a diferença dos níveis de maturidade da sociedade em relação à importância do tema.

O documento apresenta, em 10 tópicos, as ações que são abordadas e seus objetivos, sendo estes:

1. Fortalecer as ações de governança cibernética.

2. Estabelecer um modelo centralizado de governança no âmbito nacional.

3. Promover ambiente participativo, colaborativo, confiável e seguro entre setor público, setor privado e sociedade.

4. Elevar o nível de proteção do governo.

5. Elevar o nível de proteção das Infraestruturas Críticas Nacionais.

6. Aprimorar o arcabouço legal sobre segurança cibernética.

7. Incentivar a concepção de soluções inovadoras em segurança cibernética.

8. Ampliar a cooperação internacional do Brasil em Segurança cibernética.

9. Ampliar parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade.

10. Elevar nível de maturidade em segurança cibernética.

É reforçado, novamente, o interesse do Brasil em se destacar no ambiente internacional, ampliando as cooperações de segurança cibernética. Há interesse também em incentivar a participação do país nos fóruns e grupos internacionais, ampliar acordos e se posicionar ao combate aos crimes cibernéticos. Ademais, expandir as relações com os países da América Latina, sendo o Brasil um importante condutor regional (BRASIL, 2020). As recomendações descritas abrem espaço para uma visão mais robusta sobre o futuro da ciberdiplomacia, ao reconhecer a cooperação internacional nessa área e a demanda por profissionais que atuem diretamente representando o país (HUREL, 2021).

Há grande preocupação com as infraestruturas críticas, um dos pontos que exige a colaboração entre os setores públicos e privados, dado que, como escrito no documento, grande parte das infraestruturas críticas estão sob responsabilidade do setor privado. São propósitos comuns. Dessa maneira, uma das propostas seria a criação de canais de comunicação a que as instituições tivessem acesso para comunicarem entre si. O planejamento é que o maior número de atores da sociedade coopere para implementar as políticas públicas de segurança cibernética.

> "Portanto, como a segurança cibernética é de extrema importância para o poder público e para as instituições privadas, entende-se como relevante a criação de um mecanismo de compartilhamento de informações sobre riscos cibernéticos, com o fim de contribuir para a identificação, o gerenciamento e a mitigação de riscos. Essa contínua troca de conhecimento irá auxiliar organizações a evitar, a avaliar e a gerenciar riscos corretamente, além de viabilizar uma abordagem coordenada mais eficaz e eficiente. " (BRASIL, 2020)

Alguns procedimentos são necessários para seguir ações conjuntas entre o Governo e instituições, para proteger o espaço cibernético, como: criação de uma estrutura de governança de segurança cibernética nas empresas de infraestruturas críticas com regras, diretrizes, procedimentos e tratamentos de incidentes; criação de Grupos de Resposta a Incidentes de Segurança que, de alguma forma, tenham mecanismos de troca de informações; e incentivo a notificações ao CTIR Gov sobre ocorrências de incidentes cibernéticos. Dessa forma, pode haver uma melhor elaboração de planos de respostas a incidentes e recuperação dos ambientes afetados (BRASIL, 2020).

É de grande importância o destaque em fortalecer o papel do Centro de Tratamento e Resposta a Incidentes Cibernéticos, com propósito de sempre mantê-lo atualizado em pessoal

e material e que possa emitir consistentemente alertas e recomendações. Uma das formas de aperfeiçoar o sistema é estabelecendo mecanismos que permitam a interação e o compartilhamento de informações em diferentes níveis, entre eles o compartilhamento de informações sobre incidentes e vulnerabilidades cibernéticas (BRASIL, 2020).

5 LEVANTAMENTO DE DADOS DE INCIDENTES E ATAQUES CIBERNÉTICOS AO BRASIL

Uma das estratégias para manter o espaço cibernético seguro é dar atenção as estatísticas de incidentes e ataques às redes brasileiras. Por isso é tão importante o trabalho feito pelos Grupos de Segurança e Resposta a Incidentes (CSIRT).[9] O Brasil possui mais de 30 grupos ativos reconhecidos pelo CERT.br. Para que um grupo de Segurança e Resposta a Incidentes seja reconhecido, precisa atender aos requisitos disponibilizados no site do CERT.br, tais quais: estar trabalhando há pelo menos 6 meses, ser reconhecido por sua organização ou público alvo, preencher um formulário de solicitação de inclusão, identificar seus times de profissionais e responder periodicamente os testes de reação enviados para seus *e-mails* de contato.

Esse capítulo apresenta as estatísticas de incidentes reportados ao CERT.br entre os anos de 2010 a 2020. Dentro desses dados analisados, uma leitura das notificações de DNS maliciosos e ataques de negação a serviços. Para acrescentar às informações disponíveis do CERT.br, também há levantamento de dados de empresas privadas: Axur, Cloudflare, Avast, Kapersky. A combinação das pesquisas dos setores privados e públicos tem o intuito de enriquecer a análise dos números dos ataques cibernéticos. Também, fortalece o princípio visto no capítulo teórico e a descrição dos documentos estratégicos que esse encontro entre setores favorecem o fortalecimento da segurança cibernética.

Por último, uma contextualização das pesquisas de segurança cibernética no cenário internacional e como o Brasil é posicionado nos estudos. Será visto dois índices e um relatório significativos para discussão do espaço cibernético: Global Security Index da International Telecommunication Union e National Cyber Security Index pela Fundação da Academia de Governança Eletrônica da Estônia, e o Relatório de Revisão da Capacidade de Cibersegurança do Brasil, realizado pela Organização dos Estados Americanos.

5.1 CENTRO DE ESTUDO, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) foi criado em 1997 por iniciativa do Comitê Gestor da Internet no Brasil (CGI.br),

[9] Cabe apontar que o CTIR Gov é um CSIRT que age em âmbito nacional, executa as mesmas atividades para a Administração Pública Federal, com suas diretrizes, estratégias e papéis sobre o que se refere à resposta a incidentes e em seu site há alertas e recomendações.

que tinha, no período, o nome de NIC BR Security Office Brazilian Computer Emergency Response Team (NBSO/Brazilian CERT). O Centro é um Grupo de Resposta a Incidentes de Segurança (CSIRT) Nacional de Último Recurso; isso significa que ele é de responsabilidade nacional.

Os incidentes de segurança reportados no país estavam dobrando a cada ano: em 1999, o número era de 3.107 e, em 2003, já estava em 54.607 incidentes. O que chamou a atenção do Comitê foi a associação dos incidentes a fraudes financeiras; a porcentagem tendia a aumentar mais de 75% em cada semestre (NIC.br, 2004).

Dessa maneira, houve a necessidade do governo tomar uma atitude perante o crescente número de ameaças à internet:

> "Para responder de maneira rápida e efetiva a essas ameaças é necessário que as instituições conectadas à Internet desenvolvam meios de reconhecer, analisar e responder a incidentes que venham a ocorrer, minimizando prejuízos e reduzindo custos de recuperação. Esses objetivos, em geral, são atingidos pelos Grupos de Resposta a Incidentes de Segurança em Computadores (do inglês CSIRTs - Computer Security Incident Response Teams), cujo relacionamento com outras organizações de segurança pode facilitar o compartilhamento de estratégias de resposta e a geração de alertas para potenciais problemas." (NIC.br, 2004).

Os deveres do CERT.br auxiliam no cumprimento do Decreto Nº 4.829, de 2003, que dispõe da criação do CGI.br. Entre eles, estão: estabelecer as diretrizes estratégicas relacionadas ao uso da internet no país, promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para que seja garantida a segurança da internet e que essa seja vista pela sociedade. O CERT.br também representa a internet brasileira nos fóruns técnicos nacionais e internacionais (CERT.br, 2022).

As atividades têm como objetivo, segundo o Estatuto do NIC.br (2014), atender aos requisitos de segurança e emergências na internet brasileira, assim como promover ou colaborar na realização de cursos, conferências e congressos com a intenção de contribuir para o desenvolvimento na área de ensino para a segurança da internet.

O trabalho do CERT.br está de acordo com o padrão FIRST CSIRT Services Framework, um documento que detalha os serviços que os Centros de Segurança e Resposta a incidentes devem fornecer. O documento é amplo e de escopo global, de forma que tenta guiar e servir de apoio para o desenvolvimento de segurança ao espaço cibernético. Funciona como base para 99 países, e há 615 Centros em funcionamento. No Brasil funcionam 6 centros, entre eles o próprio CERT.br, o CTIR Gov-BR e o CSIRT da Petrobrás (FIRST.org, 2019).

O CERT.br presta serviços em três áreas, com base no documento: Gestão de Incidentes (*Information Security Incident Management*), Consciência Situacional (*Situational Awareness*) e Transferência de Conhecimento (*Knowledge Transfer*). Gestão de Incidentes consiste em

identificar, detectar e monitorar informações de incidentes, baseado em entender os eventos e contextos dos dados de análise (FIRST.org, 2019). Ele atua, então, como um ponto de contato nacional para notificação de incidentes de segurança e facilitar a comunicação entre profissionais, especialistas e outras equipes. Desempenha o papel de localizar e coordenar as atividades com CSIRTs e Grupos de Segurança das organizações envolvidas.

O CERT.br desempenha a função de analisar potenciais incidentes para que suas características sirvam de informações de segurança, descobrindo ameaças reais e alarmes falsos. Outras funções dele são:

> Coordenação: auxiliar a comunicação e resolução do incidente através de um trabalho colaborativo com outras entidades como CSIRTs, empresas, universidades, provedores de acesso e serviços Internet, sistemas autônomos e operadores da justiça;
> Análise Técnica: dar suporte ao processo de análise de atividades maliciosas e de sistemas comprometidos;
> Suporte à Mitigação e Recuperação: dar suporte ao processo de mitigação de danos causados por um incidente e de recuperação de sistemas comprometidos. (CERT.br, 2022).

No que se refere às informações recebidas, são tratadas de forma confidencial. Quando é necessária a organização de resolução do incidente, elas podem ser compartilhadas, mas somente com outros times. O CERT.br tem a política de não comentar nem emitir opiniões sobre essas informações, com o objetivo de não interferir em considerações sobre os incidentes.

O processo de coleta das informações de dados é obtido por 4 fontes principais. Dois são projetos próprios, sendo o primeiro deles o Projeto *Honeypots* Distribuídos. *Honeypot* é um recurso computacional de segurança dedicado a ser sondado; são ferramentas que emulam sistemas operacionais e serviços com os quais os atacantes irão interagir, ou seja, são próprios para obter dados de ataque, já que sua função é atrair o atacante. Esses sensores são distribuídos por redes nacionais. O outro se chama Projeto *Spampots*; são redes de *honeypot*, porém, serve para obter dados sobre abuso da infraestrutura de redes conectadas à internet para envio de spam, e esse projeto possui sensores distribuído por diversos países (CERT.br, 2022).

Também há os *Threat Feeds*, em que os parceiros globais enviam acesso a dados de ameaças relacionadas aos Número de Sistema Autônomo (ASNs). É uma rede administrada por uma mesma organização, alocada no Brasil. E, por último, existem as notificações de incidentes informados ao CERT.br (CERT.br, 2022).

As informações coletadas e processadas são compartilhadas com a sociedade, de forma confidencial, como já visto, classificadas dependendo da natureza da informação. As Estatísticas Públicas são um conjunto de métricas públicas de notificações voluntárias de incidentes, são dados que podem ser facilmente acessados pelo site do CERT.br. As

Notificações para Sistema Autônomos são os dados analisados recebidos dos parceiros com o objetivo de identificar sistemas mal configurados e vulneráveis. Os dados são enviados semanalmente para os responsáveis, contendo as informações analisadas. Por fim, o compartilhamento é feito via Open Source Threat Intelligence Platform (MISP), uma plataforma de software livre para compartilhar os dados de inteligência de ameaças, aberta, gratuita e amplamente utilizada pela comunidade internacional (CERT.br, 2022).

5.2 ESTATÍSTICA DE INCIDENTES

No documento estratégico E-Ciber, já há uma vasta discussão sobre a importância de detecção, triagem, análise e respostas a incidentes cibernéticos. Para haver uma resposta correspondente ao alcance de um ataque cibernético, o primeiro passo é detecta-lo com rapidez para minimizar a perda e a destruição que podem causar. É previsto na estratégia que toda organização tenha sua equipe de tratamento para que nenhum setor seja excluído.

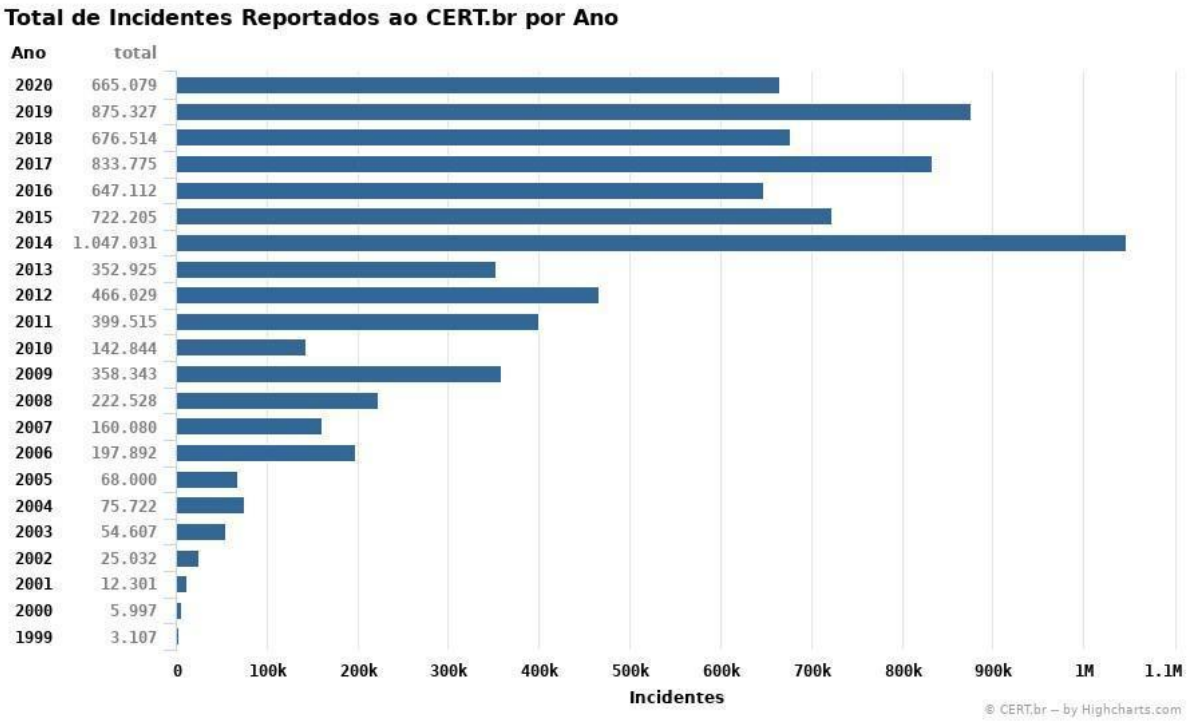
O próprio CERT.br incentiva a notificação de incidentes de segurança e aponta o quão necessárias são elas. A partir delas que a detecção melhora com o tempo, e as instituições conseguem trabalhar em seus pontos comprometidos. Contribui para a segurança geral da internet; o processo de mitigar o ataque é difícil, porém, o fato de levantar os incidentes facilita a solução do problema e ajuda a conter danos e prejuízos. E, por fim, permite gerar estatísticas, correlacionar dados e identificar tendências (CERT.br, 2022).

O incidente de segurança pode aparecer de diversas formas e são todas situações que prejudicam à segurança de sistemas de computação ou de redes de computadores. Alguns exemplos de incidentes apontados pelo CERT.br são:

- tentativas de ganhar acesso não autorizado a sistemas ou dados;
- ataques de negação de serviço;
- uso ou acesso não autorizado a um sistema;
- modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;
- desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso. (CERT.br, 2022).

Em 2019, o CERT.br recebeu o total de 875.327 notificações voluntárias de incidentes para seu endereço de *e-mail*, totalizando 4.086.406 *e-mails* (NIC.br, 2019). Segue as estatísticas totais desde 1999:

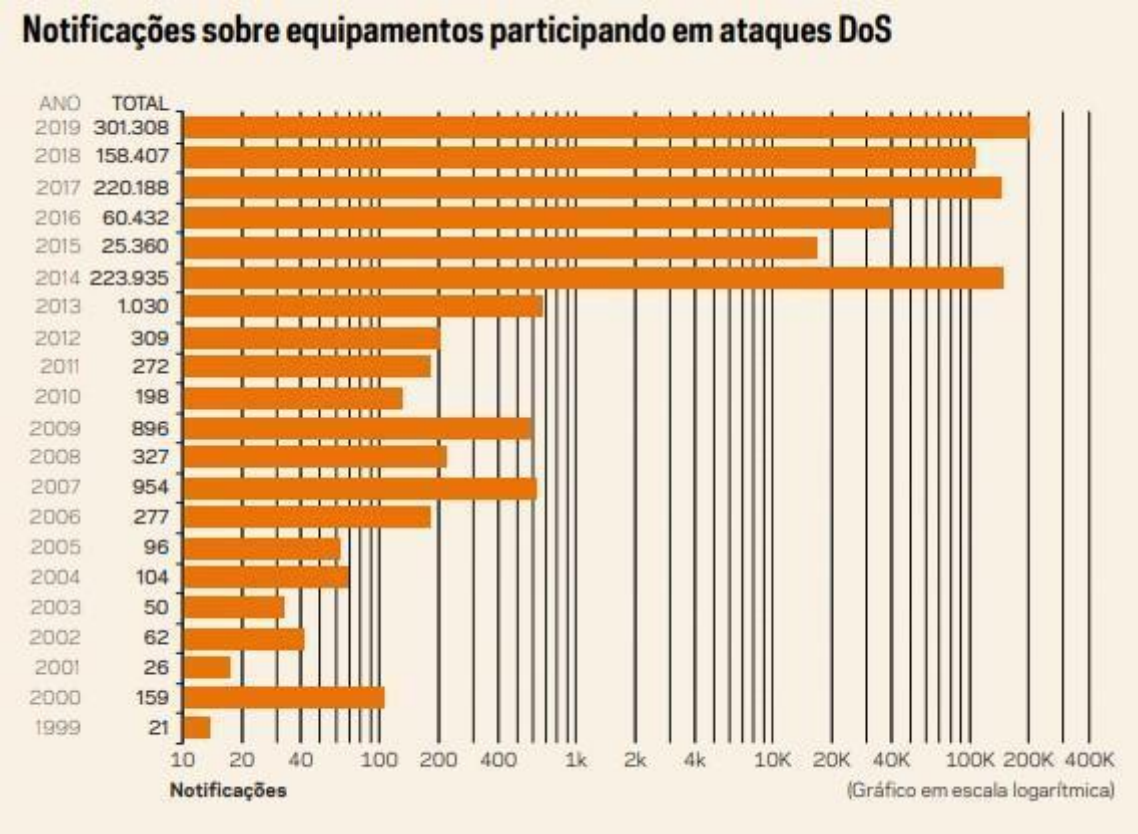
Figura 8 - Total de incidentes reportados ao CERT.br



Fonte: CERT.br, 2022

O núcleo NIC.br destaca o abrupto aumento de ataques de negação de serviços, os DoS. Em 2019, chegaram a 301.308 notificações, o maior número desde 1999, sendo 90% maior que as notificações recebidas no ano anterior. A figura 9 mostra o número de notificações dos ataques DoS:

Figura 9 - Notificações DoS



Fonte: NIC.br, 2019

Quaisquer redes, equipamentos ou sistema conectados à internet são alvos dos ataques de Negação de Serviço, tanto os que ocorrem com um atacante ou com um conjunto de equipamentos, os DDoS. Os alvos, como visto anteriormente, sofrerão indisponibilidade de acesso a serviços e recursos; como consequências, terão perdas financeiras, de credibilidade, danos a imagens, problemas com backups, armazenamento ou nuvem. Os setores alvos e as motivações são vários, podendo ser originados em qualquer circunstância, mas, como levantado pelas estatísticas do CERT.br, podem-se identificar alguns grupos:

- Ganho econômico ou financeiro: esses ataques ocorrem diretamente à empresa que o atacante tem em vista, de forma que há alguma perda econômica para essa, pois a ideia é extorquir dinheiro.
- Vingança, crença ideológica ou política: esses ataques partem de algo particular do atacante e costumam estar associados à prática do *hacktivismo*.

- Distração: esses ataques são realizados com objetivo de desfocar equipes de redes e segurança para que algum outro ataque aconteça e resulta em dificuldades das empresas de mitigar os ataques.

A empresa privada de segurança cibernética Cloudflare relatou os ataques DDoS pelo mundo e, em 2021, a maior parte do tráfego tinha origem brasileira. As estatísticas levantaram que, combinando Brasil, Indonésia e Índia, o percentual de ataques é de 17%. A resposta da empresa foi usar uma ferramenta própria para atuar dentro do servidor e do centro de dados. Somente após analisar os dados, é possível detectar os ataques e agir sem prejuízo para o usuário. É um exemplo de como as instituições privadas respondem aos ataques, geralmente com sistemas próprios e estatísticas para localizar vulnerabilidade para quem os contrata (YOACHIMIK, 2021).

Segundo o relatório anual do NIC.br (2019), para reduzir o número de redes brasileiras vulneráveis, o CERT.br notifica administradores de sistemas autônomos, cujas redes possuam sistemas mal configurados, com indicação do problema e solicitação para que sejam tomadas medidas necessárias. Alguns serviços que são regularmente notificados são: *Domain Name System* (DNS), *Simple Network Management Protocol* (SNMP*), Network Time Protocol* (NTP), *Simple Network Management Protocol* (SNMP), entre outros. Esses serviços são protocolos de redes que estão mal configuradas e seus abusos vão prejudicar a rede em si.

Ao final de 2017, as organizações do CGI.br e do NIC.br criaram o Programa por uma Internet mais Segura (BCP), com apoio do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel, Celular e Pessoal (SindiTelebrasil), associação das operadoras de telecomunicações, da Associação Brasileira de Internet (ABRANET) e da Associação Brasileira de Provedores de Internet e Telecomunicações (ABRINT), associações de provedores de acesso à internet e à InternetSociety. O programa tem como objetivo apoiar a comunidade técnica da internet para a redução de ataques DDoS originados no Brasil e as vulnerabilidades que decorrem deles (CGI.br, NIC.br, 2022).

O programa identifica como um dos principais ataques das infraestruturas de rede as negações de serviços e os ataques de sequestro de prefixos e vazamento de rotas. Para reduzir o impacto, deve-se tomar cuidado nas escolhas adequadas de configurações padrão de fábrica, além das atualizações automáticas de software para corrigir problemas. O plano de ação do programa para melhorar esse cenário é promover palestras, cursos, treinamento e materiais didáticos para que todos possam ter acesso ao que se refere a administração das redes e configurações. Visa, também, a se inteirar com associações de provedores e afiliados para a disseminação da cultura de segurança e mitigação dos problemas existentes.

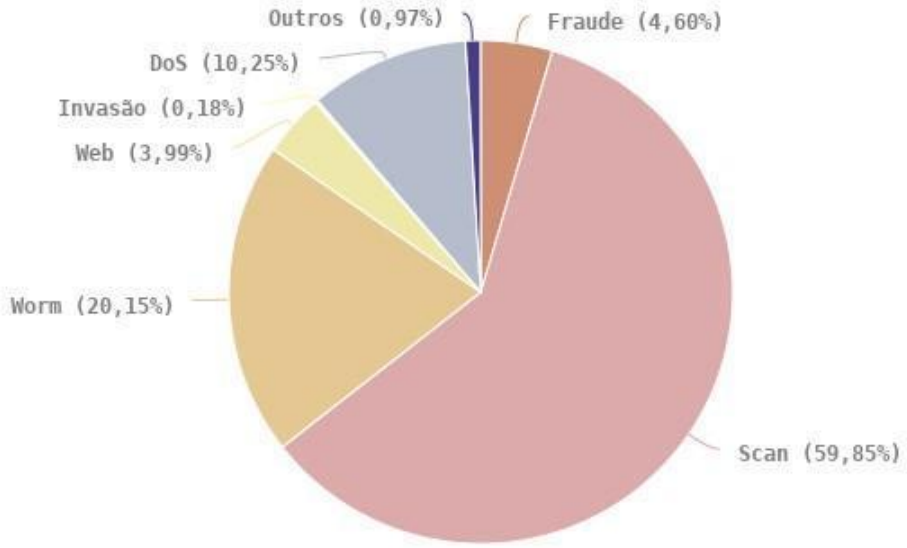
É apresentado pelo CERT.br que é importante ter um pessoal preparado para atuar frente ao problema e políticas claras de comunicação, como forma de preparação para os ataques de negação de sistemas. Dentro do grupo de respostas a incidentes, deve haver canal de comunicação efetivo entre os usuários, clientes e administradores e deve ser estabelecido também contato com outros grupos de segurança. O fator humano que há por trás da internet aparenta ser essencial. É necessário estar preparado para fazer relatórios, lidar com entrevistas e declarações públicas, ter responsáveis pelos sistemas e serviços e um atendimento prático de central de atendimento.

No que se refere a levantar as estatísticas entre 2010 a 2020, as figuras 10 e 11 mostram quais foram os aumentos das ameaças notificadas:

Figura 10 - Incidentes do ano de 2010

Fonte: CERT.br

Figura 11 - Incidentes do ano de 2020



Fonte: CERT.br

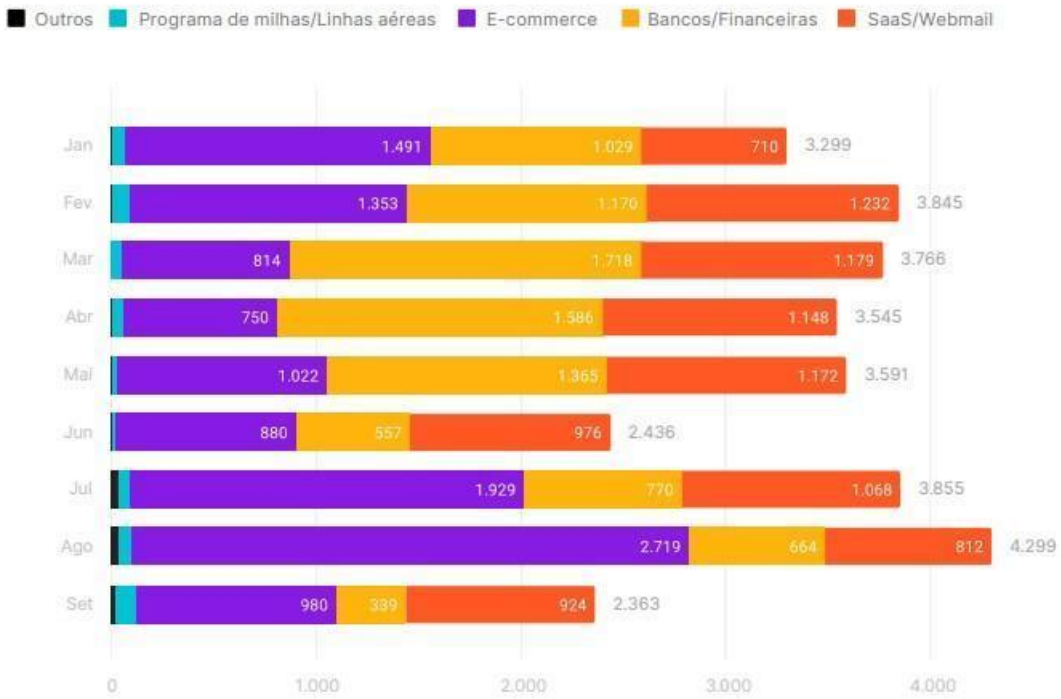
Vale evidenciar que o *scan*, com a letra n, é diferente do *scam*, o termo utilizado para golpes e ações fraudulentas via internet e nas estatísticas entre como fraude. O *scan* não é exatamente um ataque, já que é uma notificação de varredura nas redes usada pelo atacante. Dentro dos incidentes, há os ataques de invasão, quando há um acesso não autorizado a um computador ou rede. O *web* é um caso particular de ataques, visando especificamente ao comprometimento de servidores web ou à interferência na estrutura de páginas na internet.

As notificações de fraude em 2020 diminuíram 22% comparado a 2019 e, dentro desse número, percebe-se que, em relação a páginas de banco e sites de comércio, o *phishing* clássico diminuiu 24% e as notificações que não envolvem fator de comércio aumentaram em 35%. Os casos de *phishing* nesse ano, como é levantado pelo CERT.br, são de temas relacionados com a COVID-19, como nos casos de auxílio emergencial oferecido pelo Governo. Segundo o Instituto Histórico Cultural da Aeronáutica, os atacantes aproveitaram da fragilidade da pandemia para atacar especialmente os sistemas informáticos de hospitais. Ainda, há relatos de propagação de *ransomware* enviado por e-mail com o título *CORONAVIRUS_CONVID-19.vbs*. O próprio centro de tratamento de incidentes das Forças Aéreas publicou alertas e orientações para a proteção das redes (CTIR.FAB, 2020).

A empresa privada Axur fez seu próprio levantamento de estatísticas e, no terceiro trimestre de 2020, 53,5% dos ataques *phishing* eram direcionados ao E-commerce, e 16,9%,

direcionados a bancos e financeiro. Na figura 12 estão os casos dos ataques detectados por setores:

Figura 12 - Casos de *phishing* detectados por mês em 2020



Fonte: AXUR, 2020

Em 2010, foi comunicado pelo NIC.br que os ataques *phishing* eram as fraudes mais usadas da internet brasileira. As notificações desse ataque representavam 49,4% dos incidentes totais reportados. Os relatos dos Cavalos de Troia, um programa malicioso, estavam em segundo lugar (NIC.br, 2010). Na figura 13, aparece a estatística dos incidentes de *phishing* reportados ao CERT.br no ano de 2020, sendo que o setor financeiro foi, também, identificado como o mais atacado, e o Cavalo de Troia não chega a 5% do total.

Figura 13 - incidentes de fraude em 2020

Fonte: CERT.br

O CERT.br, em conjunto com NIC.br e CGI.br, realizaram uma palestra que se transformou em uma cartilha sobre os modos de prevenção e mitigação desses ataques. Desenhado em forma de triângulo virado, até chegar em um plano de ação, primeiro devem-se filtrar os *e-mails*, fazendo o possível para que tenha um controle dos *spoofing*, quando o atacante finge ser uma marca, usando um outro IP que não seja dele. Deve-se ter um treinamento, política institucional e pessoal das divulgações de informações e normas para reportar incidentes, no momento que são identificados. Algumas formas de mitigar os danos são autenticação em duas etapas, segurança dos equipamentos e ferramentas locais de segurança (ZUBEN, 2021).

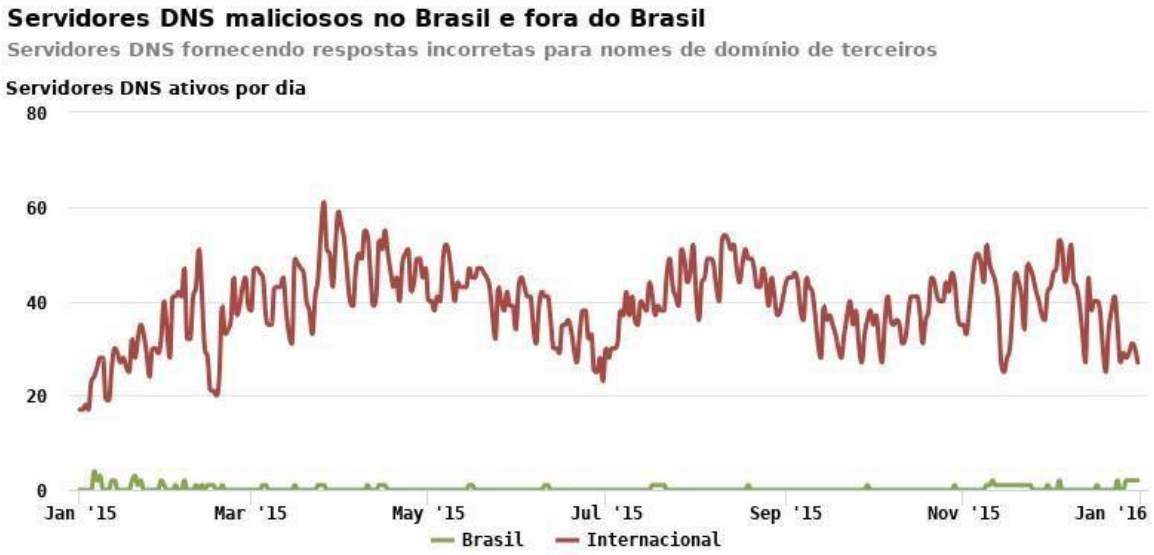
Desde 2015, o CERT.br tem feito um levantamento de estatística de notificações de servidores DNS maliciosos. Um servidor DNS malicioso é aquele que está fornecendo respostas incorretas:

> "Um servidor DNS malicioso é um servidor que está fornecendo respostas incorretas para nome(s) de domínio(s) de instituições vítima, em geral instituições financeiras, de comércio eletrônico, redes sociais e/ou domínios bastante conhecidos. O propósito de um servidor DNS malicioso é direcionar os usuários para sites falsos, como parte de ataques de *pharming*. Em sua maioria estes servidores são instalados pelo próprio atacante, contratando serviços de hospedagem ou de nuvem." (CERT.br, 2020).

Assim, os servidores DNS maliciosos fornecem respostas incorretas para domínios populares, tais como instituições financeiras, comércio eletrônicos e redes sociais. O protocolo

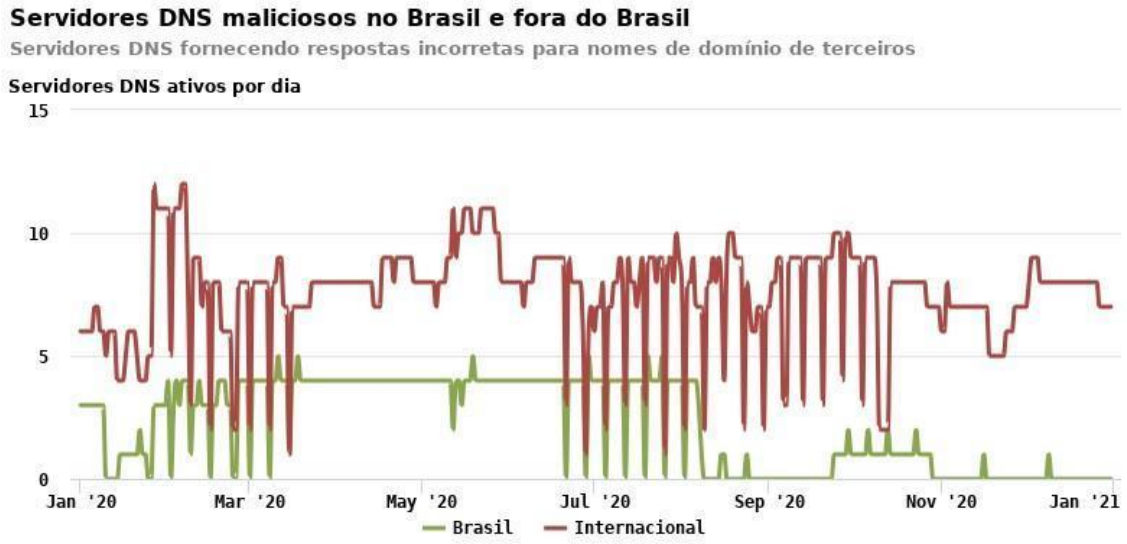
DNS normal é a tradução do endereço de páginas da internet para um IP, desse modo não há necessidade de usar os números do IP para acessar um site. A diferença das notificações entre 2015 (figura 14) a 2020 (figura 15) mostra que houve um grande aumento nos números e que o Brasil tem alcançado números internacionais.

Figura 14 - DNS maliciosos no Brasil e fora do Brasil em 2015



Fonte: CERT.br

Figura 15 - DNS maliciosos no Brasil e fora do Brasil em 2020



Fonte: CERT.br

O ataque *pharming* é exemplo de um DNS malicioso, em que direciona o tráfego de um site legítimo para um site falso, e este é igual ao site verdadeiro. Há o DNS *poisoning*, que tem

como um dos principais alvos operadores de telefonia, por causa do grande número de vítimas. Esse retém os servidores e logo direciona o tráfego para servidores maliciosos (MAGANHATI JR. 2020). Ainda há o Rogue DNS, que é um servidor DNS falso. Se esse ataque for bem sucedido, levará a vítima para páginas de *phishing*, em que é aberto um site de banco e o atacante consegue ter acesso aos dados.

A empresa Avast, em 2019, realizou uma pesquisa mostrando que bloqueou mais de 4,6 milhões de ataques em usuários de sites maliciosos; a maior parte desse tráfico ocorreu nos sites de banco e uma grande parte no serviço de transmissão online Netflix:

> "Dados do Avast mostram os sites das organizações ativas no Brasil que mais sofrem sequestro:
> - Santander (24%)
> - Bradesco (19%)
> - Banco do Brasil (13%)
> - Itau BBA (13%)
> - Netflix (11%)
> - Caixa (10%)
> - Serasa Experian (10%)" (AVAST, 2019)

A empresa acrescenta sobre a dificuldade que é evitar o *phishing*. O que se pode fazer é alertar os usuários e seguir as recomendações das informações que eles fornecem, já que a maioria dos sites de *phishing* são fora dos domínios brasileiros (AVAST, 2019).

O CERT.br regularmente realiza workshops e palestras com intuito de prestar serviço à comunidade sobre proteção dos ataques e a melhor maneira de responder. Em 2021, foi realizado um evento para a proteção de invasões e vazamentos de dados por *phishing* e DNS maliciosos. O Centro aponta que mais de 80% dos incidentes seriam evitados se todas as correções fossem aplicadas, se houvesse mais atenção a erros e configurações, se todos os serviços possuíssem mais de um fator de autenticação e, por último, se os padrões de aumento a segurança fossem mais modernos. Devem-se modernizar os padrões de autenticação com múltiplos fatores, possuir uma criptografia forte, segurança de DNS e *e-mail*, protocolos IP para dar mais estabilidade menor complexidade e segurança de roteamento (HOEPERS, STEDING-JESSEN, 2021).

Com o objetivo de identificar se a internet está seguindo padrões técnicos internacionais modernos, o NIC.br criou a ferramenta TOP, um site que realiza testes para ver se as conexões de internet, site e *e-mail* possuem padrões técnicos mais modernos e confiáveis. A ferramenta foi inspirada em uma iniciativa holandesa chamada *Internet Standards Platform*. Segundo a TOP, o Brasil ainda usa padrões técnicos ultrapassados, mesmo sendo um país com intenso uso da internet. Os padrões mais antigos, que ainda estão amarrados aos padrões datados nas décadas de 70 e 80, tornam um ambiente frágil para os atacantes. Se há alguma implementação

incorreta dos padrões, o site produz relatório detalhado com indicações para corrigir esses problemas (TOP.nic.br, 2022).

Dentro das iniciativas criadas para estratégia de segurança, o NIC.br criou o Portal Internet Segura, com o propósito de levar informação e educação sobre a internet para o maior número possível de pessoas. O Portal possui cartilhas, slides, fascículos, dicas e explicações sobre ameaças e segurança de uma forma acessível, há um espaço destinado a crianças e outro a idosos (maiores de 60 anos).

As iniciativas que participam do portal possuem grande apoio de empresas, como a SaferNet Brasil, que disponibiliza material voltado a educadores e adolescentes. MP On, programa do Ministério Público do Rio Grande do Sul voltado à educação digital, apoia com a promoção de educação digital a respeito do uso seguro da internet e das redes sociais. A operadora de telefonia Vivo colabora com a iniciativa Dialogando, um espaço que discute conteúdos de privacidade às redes.

No que diz respeito à capacitação humana, o CGI.br e o NIC.br organizam eventos, a maioria das vezes de forma gratuita, para a sociedade, de maneira a incentivar a produção e o compartilhamento do conhecimento. Inclusive, realizações de conferências na América Latina, como por exemplo a Conferência *Latin America Web* (LA-Web), que aconteceu em conjunto com a *The Web Conference* 2019, realizada em San Francisco sobre dados na web, mineração de dados, e outros assuntos.

O CERT.br ministra cursos de Treinamento em Tratamento de Incidentes de Segurança licenciados do *Software Engineering Institute*, da *Carnegie Mellon University*. Em 2019 foram realizados 5 cursos e participaram quase 60 organizações, tal como Banrisul, Caixa Econômica Federal, Dell Technologies, Logical IT, Latin Tech, Porto Seguro, Marinha do Brasil, Telefônica Vivo.

Aponta Getschko (2020) que o componente mais importante para buscar soluções e respostas para os incidentes é educar os usuários da rede. Por isso há uma demanda por capacitar profissionais da área. A estabilidade, segurança e funcionalidade das redes devem ser preservadas de forma ativa, por meio de medidas técnicas compatíveis com padrões internacionais, porém, não se deve ignorar que a maior parte da internet envolve fator humano.

> "Dessa forma, precisamos observar os impactos dos diferentes tipos de ameaças digitais, para que possamos desenvolver uma cultura da segurança que enfrente esses riscos. Embora, por exemplo, o uso de criptografia na camada de aplicações seja uma forma de a tecnologia tornar a comunicação via rede mais segura, ela não é suficiente: muitos incidentes de segurança têm origem em uma “engenharia social” que explora vulnerabilidades do comportamento humano." (GETSCHKO, 2020. p. 14)

5.3 O BRASIL NO CENÁRIO INTERNACIONAL

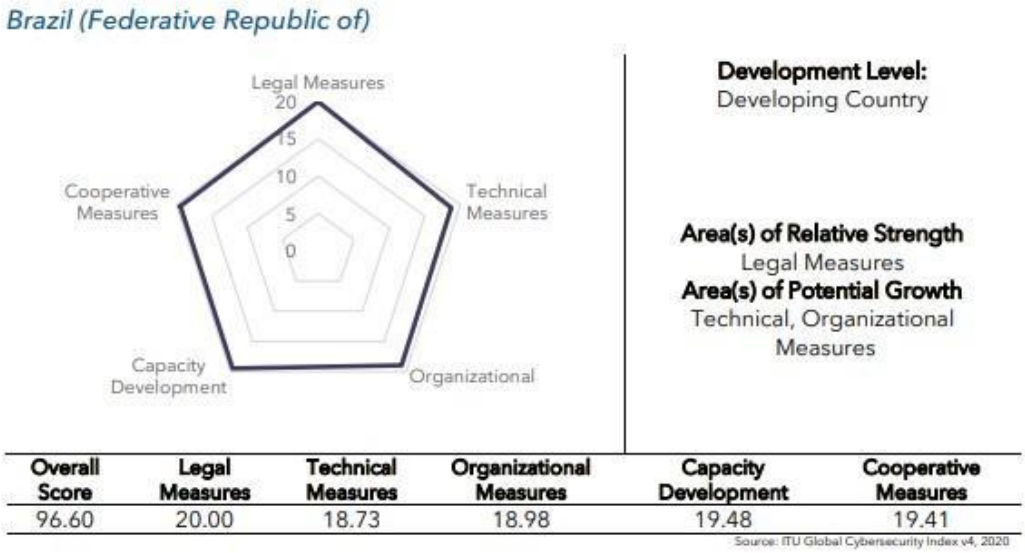
O Brasil é visto como um dos maiores alvos de ataques cibernéticos no cenário internacional. Empresas de segurança digital fazem anualmente levantamentos sobre incidentes com objetivo de relatar as ameaças, classificar e identificar os países mais frágeis nessa área. Segundo a Kaspersky, os brasileiros são os principais alvos de ataques *phishing* no mundo, em 2020 um a cada cinco brasileiros sofreram ao menos uma tentativa de ataque. O índice de alvos fica em torno de 20% e está acima da média mundial de 13%. (KASPERSKY, 2020)

O relatório feito pela NSFOCUS coloca o Brasil em 4º lugar de países que mais sofreram ataques DDoS em 2020. Segundos dados do Fortinet nesse mesmo ano, o Brasil sofreu mais de 3.4 bilhões de tentativas de ataques, um dos maiores aconteceu aos sistemas do Tribunal Regional Federal da 1ª Região e Superior Tribunal de Justíca. Os sistemas do TRF-1 foram paralisados e colocados em modo restrito, as consultas processuais e as emissões de certidões online ficaram indisponíveis por um tempo. (ORTIZ, 2020) A rede de tecnologia do STJ também sofreu ataques e tiveram atividades paralisadas durante dias. As sessões de julgamento por videoconferência e audiências foram suspensas, sistema de telefonia e internet ficaram fora do ar. (VALENTE, VITAL, 2020)

No que refere a observar a posição brasileira na conjuntura internacional, analisar a *Global Cybersecurity Index*, índice criado pela International Telecommunication Union (ITU) é importante, pois essa é referência global para os Estados. O índice mede as ações dos países para enfrentar os riscos cibernéticos, avaliando por cinco pontos: medidas jurídicas, técnicas cooperativas, organizacionais e de capacitação. O objetivo é identificar os pontos fortes e as áreas que necessitam de atenção de cada estado.

Em 2020, o Brasil passou da 71º posição para o 18º no índice global. Em primeiro lugar está o Estados Unidos. Conforme a figura 16 mostra, as notas atribuídas ao Brasil, a área mais forte são as de medidas legais. A parte técnica e organizacional estão marcadas com potencial de crescimento.

Figura 16 - *Global Cybersecurity Index*



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.60	20.00	18.73	18.98	19.48	19.41

Source: ITU Global Cybersecurity Index v4, 2020

(Fonte: ITU, 2020)

Observando outra métrica, o *National Cyber Security Index* desenvolvido pela Fundação da Academia de Governança Eletrônica da Estônia é um índice global que mede a preparação dos países para prevenirem ameaças cibernéticas e gerirem os incidentes cibernéticos. O índice identifica quais as ameaças cibernéticas predominante no país, qual a maneira que o país responde e quais indicadores ele trabalha. Também, avalia, a legislação, a organização, o formato de cooperação, as tecnologias, programas e tudo aquilo que influencia a capacidade de tomar decisão em relação à segurança.

Desde 2019, última atualização de levantamento de dados, o Brasil está com 46.75 pontos de 100. Essa avaliação é com base de mais de 12 aspectos, os pontos mais fortes do país são as capacidades militares, as análises e informações das ameaças cibernéticas e a estratégia de segurança. Os pontos que estão abaixo da média são as proteções de dado, os serviços essenciais de proteção, a proteção de dados pessoais, planos de gerenciamento contra ameaças cibernética e outros. (NCSI, 2019)

Por último, o Relatório de Revisão da Capacidade de Cibersegurança da República Federativa do Brasil organizado pela Organização dos Estados Americanos (OEA), O Centro

de Capacidade Global de Segurança Cibernética da Universidade de Oxford, o Departamento de Segurança da Informação e outras instituições brasileiras, realiza uma análise da capacidade de segurança cibernética do país, o último foi preparado entre 2018 a 2020.

As maturidades de capacidade das instituições de proteger a infraestrutura crítica varia entre o público e o privado. As instituições públicas são obrigadas a fazer a avaliação interna de riscos, que são atualizadas anualmente com base nas lições aprendidas de grandes incidentes. Os procedimentos são seguidos com base nas informações disponíveis pela ferramenta nacional de conhecimento situacional da CERT.br. O acesso a essas informações é cedido à Polícia Federal e aos serviços de inteligência, com o objetivo de aumentar a cooperação e o gerenciamento de incidente entre as organizações. Os protocolos, procedimentos e avaliações de risco são examinados todos os anos por um grupo específico de trabalho de defesa cibernética. As lições que são aprendidas com grandes incidentes servem de base para ajudar a aperfeiçoar os protocolos atuais. As instituições privadas não são obrigadas a relatar o Governo sobre um incidente grave, tendo assim que desenvolver suas próprias avaliações internas de risco e políticas de segurança. (OEA, 2020)

O exemplo exposto no Relatório em relação a qualidade de gerenciamento de crise aconteceu na Copa do Mundo de 2014. Duas situações preocupantes que aconteceram foram: múltiplos ataques de DDoS que variaram de 300GB por segundo a 1TB por segundo e um incidente de sabotagem que destruiu o gabo que garantia acesso à internet na rede da FIFA. A resposta aos ataques fora eficiente e o retorno à atividade normal foi rápida. Havia protocolos transparentes sobre como divulgar a informação e relatar incidentes à instancias superiores. A segurança cibernética na Copa do Mundo, assim como acontece em grandes eventos, ficou pela responsabilidade das Forças Armadas.

Segundo Beer (2014), alguns ataques que aconteceram durante o evento:

> "Do que já foi divulgado, foram registrados spear-phishing (tipo de ataque que usa e-mails falsos direcionados), de mais de 600 e-mails do Ministério de Relações Exteriores; ataques do tipo DDoS que tirou do ar o website do Ministério do Trabalho e Emprega (mte.gov.br), o website do Ministério dos Esportes; entre outras organizações como o Banco do Brasil (bb.com.br), a Universal Music (universalmusic.com.br), bem como outros como patrocinadores da Copa; havendo ainda vazamento de dados de órgãos como a Polícia Militar do Estado do Rio de Janeiro, e da Agência Nacional Reguladora dos Planos de Saúde (ANS), só para citar alguns exemplos." (BEER, 2014)

A carência de profissionais na área de segurança cibernética prejudica na proteção de sistemas, dados e respostas eficientes para os ataques. A organização *Cybersecurity and IT Security Certifications and Training* (ISC²) realizou um relatório com pesquisa sobre a falta de

profissionais pelo mundo. "Em uma era de vazamento de dados de grande importância e alto número de ataques cibernéticos, a segurança cibernética impacta no individual e em todas organizações." ((ISC²), 2019. p. 3) A lacuna de profissionais deve ser preenchida mundialmente em torno de 65%, em números a defasagem chega a ser de 2,7 e somente no Brasil mais de 400 mil, segundo os dados do relatório do ano de 2021.

Na figura 17 observa-se a comparação da falta de profissionais na área de segurança entre o Brasil e outras regiões estudadas.

Figura 17 - Defasagem de profissionais de segurança cibernética por país

Fonte: ISC², 2021

Assim sendo, o Brasil destaca-se por ser um alvo potencial de ataques cibernéticos, e visto nas figuras anteriores, há muito ainda o que trabalhar para estabelecer uma segurança forte na área cibernética. Apesar disso, o país não aflige sozinho das dificuldades, todos os atores do cenário internacional ainda estão aprendendo a lidar com as novas ameaças que o espaço cibernético trouxe. A agenda de segurança é um processo contínuo e a troca de informações e dados ajudam a construção diária da estratégia doméstica e internacional.

6 CONSIDERAÇÕES FINAIS

Tendo em vista a crescente preocupação de inserir a segurança cibernética nas agendas estratégicas estatais, o Brasil vem aumentando, desde 2010, o grau de atenção quanto a essa problemática. O objetivo deste trabalho foi analisar a evolução das estratégias brasileiras relativamente ao cenário de ataques cibernéticos, de modo a entender as respostas brasileiras aos ataques.

A partir do primeiro capítulo, dedicado à contextualização do espaço cibernético, foi possível apresentar diferenças existentes entre este e a internet. É fundamental abordar os termos para não haver má compreensão ou confusão, ainda mais no que tange a conflitos e ataques cibernéticos. No senso comum, as discussões parecem levar à crença de que tudo é vírus e de que todos são *hackers*, principalmente quando o assunto são as falhas nos sistemas conectados à internet. Nesse contexto, a preocupação de distinguir os *malwares* ajuda a lidar adequadamente com as vulnerabilidades e com o cuidado *on-line*.

O Brasil apresenta dois documentos que tratam sobre conceitos do ciberespaço. O *Glossário de Segurança da Informação* de 2019 e o *Glossário das Forças Armadas* de 2015 serviram de fonte para a realização do presente trabalho e foram escritos para uso mais profissional e acadêmico, enquanto a *Cartilha de Segurança da Internet* tem foco mais popular. A Cartilha, encontrada no site do CERT.br, dispõe de fascículos, guias de internet segura voltada a crianças, explicações de forma acessível sobre os *malware*, segurança de dados, dicas para usuários identificarem ataques, dentre outras informações. O material disponível pode ser usado em forma de *slides* para o computador ou em campanhas de impressão. É importante que esse assunto consiga alcançar o maior número possível de pessoas de todas as faixas etárias, ainda mais por envolver termos em língua estrangeira e um ambiente perigoso como pode ser a internet.

O capítulo seguinte abordou a Teoria da Prática Internacional, com a finalidade de conectar essa teoria relativamente nova à temática do trabalho, que necessita de perspectivas que acompanhem seu rápido progresso. A intenção ao abordar a Teoria da Prática Internacional não é de obter respostas do cenário brasileiro, sim de servir de apoio a levantar a discussão do espaço cibernético.

Quando a internet foi criada há mais de 40 anos, seu uso se restringia a comunidades pequenas, em que a maioria das pessoas se conheciam. Já a internet usada hoje, de forma comercial, tem apenas 20 anos. Os usuários eram, em 1990, em torno de 10 milhões, mas, atualmente, já são mais de 2 bilhões.

Nesse cenário, pesquisadores ainda não têm certeza das ações de defesa, segurança, normas, escalas ou como juntar todos os significados para uma estratégia nacional (NYE JR, 2012). Por isso, as decisões sobre segurança cibernética são difíceis de serem tomadas sozinhas.

A esse respeito, um ponto importante consiste na complexa relação entre atores de segurança pública e segurança privada. Nesse cenário, não há só as relações entre o global e o regional, o público e o privado: a relação entre tais atores também se encontram na área da segurança. Bueger e Gadinger (2018) pontuam que o crescente aumento de atores de segurança privada não é necessariamente algo ruim, mas inevitável para a mercadorização e a tecnificação da segurança. Precisa-se ter noção de que o espaço cibernético é um campo enorme: empresas, pessoas, governos, entidades trabalham com internet, de maneira que nenhum sistema sozinho conseguiria garantir segurança a todas as redes. No Brasil, empresas privadas como Axur, Fortinet, Kaspersky realizam relatórios anuais sobre incidentes de ataques cibernéticos e localização de setores atacados, fornecendo recomendações à sociedade acerca de como lidar com os perigos.

Diante disso, a Teoria da Prática Internacional é vantajosa por estudar os processos, o conhecimento prático, a coletividade, o desempenho dos atores e o material. A prática mencionada na teoria, funciona tanto com o individual quanto com o trabalho em grupo; o resultado das ações pode gerar interações entre grupos que favorecerão a ampliação de conhecimento.

Este trabalho buscou oferecer um panorama das respostas brasileiras a crimes cibernéticos. Embora tenha sido relativamente fácil encontrar os documentos analisados durante a pesquisa, não se pode dizer o mesmo em relação ao entendimento da arquitetura do Estado no que concerne à segurança cibernética. Alguns autores apresentados no trabalho criticam a grande quantidade de entidades que lidam com o espaço cibernético. Dentre tais estudiosos, está Diniz (2014), segundo o qual a maioria das organizações estão focadas na gestão de sistemas, no desenvolvimento técnico e em ferramentas de atualização, havendo pouco espaço para tratar da área de segurança. A parte política fica a cargo do GSI, que responde à Presidência da República. Já a parte estratégica e operacional fica a cargo do Ministério da

Defesa e Forças Armadas; porém, a defesa opera basicamente em casos de guerra cibernética. A Polícia Federal, por sua vez, é responsável pelos crimes cibernéticos, como pedofilia e organizações criminosas.

Então, fica a critério do CERT.br lidar com os tratamentos de incidente e levantamento de dados. O ponto fraco é que, à exceção dos projetos próprios à detecção de vulnerabilidades, o Centro só recebe dados de forma voluntária. Nem todos têm o conhecimento de que essa ferramenta é importante para o funcionamento de todas as redes brasileiras. As empresas privadas não têm obrigação de relatarem seus incidentes, embora, como visto anteriormente, façam relatórios e levantamentos próprios, cabendo ao pesquisador reunir todos os dados e fazer uma análise. Uma grande parte das informações se enquadram à área técnica, como, dentre outras, os números de IPs, *scans* por porta, a origem de ataque ANS. Ao proceder à análise, busquei ler as informações de uma maneira que ultrapasse o escopo da informática e pudesse ser colocada nos campos de Segurança Nacional e Relações Internacionais.

Por fim, a E-Ciber é um documento brasileiro que discute a troca de informações e a cooperação entre empresas privadas de segurança cibernética e o setor público. Quanto ao compartilhamento de informações, esta é uma forma de evidenciar a parceria estratégica, potencializar o levantamento de dados para que as respostas sejam cada vez mais eficientes e auxiliar na mitigação de riscos. O ideal para o país seria o compartilhamento, entre os órgãos privados, de pesquisas e informações, enquanto os órgãos públicos trabalhassem com as condições relacionadas ao *status* da segurança nacional. Essa ligação, na prática, não parece acontecer. As informações de ambas as entidades estão disponíveis na internet, porém é difícil encontrar algum projeto conjunto, embora o fato de a E-Ciber tratar desse assunto já seja um grande passo no que diz respeito ao reconhecimento da necessidade de aproximação.

Acerca das estatísticas de incidentes, coletei mais informações sobre as ameaças que apareceram repetidamente. Em primeiro lugar destacaram-se os ataques de negação de serviços, os quais, no ano de 2019, atingiram um pico com mais de 300 mil notificações. Um relatório de uma empresa privada identificou que a maioria do tráfego de ataques DDoS, no mundo, partia do Brasil.

Em segundo lugar, ressaltaram-se os ataques *phishing*, que aumentaram no período da pandemia de Covid-19. Contudo, desde 2010 já eram identificados pelo NIC.br como as ameaças mais usadas da internet, principalmente as que são direcionadas ao E-commerce.

Em terceiro lugar, levantei as estatísticas dos números de servidores DNS maliciosos. O CERT.br, desde 2015, vem notificando regularmente os usuários que hospedam esses servidores solicitando que sejam aplicadas as políticas adequadas para que o serviço seja retirado do ar. Esses servidores que fornecem respostas incorretas têm como alvos as instituições financeiras, o comércio e as redes sociais.

Ressalto cinco planos de ação que constatei como respostas brasileira aos ataques cibernéticos:

(1) Programas de apoio para a comunidade técnica com vistas à redução de ataques.
(2) Notificação de administradores de sistemas autônomos, cujas redes apresentem sistemas mal configurados, notificação a partir da qual o procedimento devido pode ser tomado.
(3) Verificação se a internet segue padrões técnicos internacionais modernos.
(4) Atualização constante do *Portal Internet Segura*, de forma que o assunto seja acessível e de fácil compreensão.
(5) Capacitação humana, pois é essencial uma linha de frente profissional capacitada para lidar com vulnerabilidades.

O campo de Segurança Cibernética tem sido completado por profissionais da área de Ciência da Computação e técnicos em Informática. Atualmente, já se discute a falta de capacitação de profissionais que analisem os dados e que possam identificar ameaças em contexto tanto doméstico quanto internacional. De certa maneira, faltam pessoas que "leiam" os números e os transformem em informações e estudos.

No âmbito da academia, muitos pontos podem ser aprofundados em pesquisas futuras. A evolução das estratégias nacionais de segurança e defesa cibernética podem ser analisadas de forma minuciosa e com o acompanhamento do contexto histórico. Pesquisas precisam acompanhar de perto as mudanças diárias dos incidentes, dos tratamentos e das respostas, na medida em que a internet está em constante mudança e que as ameaças se tornam cada vez mais perigosas. Há um espaço ainda a ser preenchido com leitura teórica, possibilitando pesquisas à luz de teorias tradicionais e, mesmo, pesquisas que aprofundem o diálogo com a Teoria da Prática Internacional.

Por fim, segundo o relatório do *World Economic Forum* de 2020[10], as ameaças cibernéticas e o comprometimento de infraestruturas de informação estão entre os dez maiores

[10] World Economic Forum. Global Risks Report. 2020. Disponível em: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. Acesso em: 19 abr. 2022.

riscos globais em termos de impacto. Ou seja, nenhuma prática de segurança é totalmente eficiente. Muitas vezes, vulnerabilidades passam despercebidas e, apenas após os danos, as empresas conseguem as identificar. Desse modo, a única coisa certa é que as entidades precisam estar preparadas para conter os dados.

REFERÊNCIAS BIBLIOGRÁFICAS

ABRAHAMSEN, R., WILLIAMS, M. C. **Privatization in Practice: Power and Capital in the Field of Global Security.** *In*: POULIOT, V., ADLER, E. (Orgs) International Practices. Cambridge Studies in International Relations. Cambridge: United Kingdom. 2011.

ADLER-NISSEN, R., DRIESCHOVAM A. **Track-Change Diplomacy: Technology, Affordances, and the Practice of International Negotiations.** International Studies Quarterly. Vol. 63, 2019. p. 531-545. Disponível em: https://academic.oup.com/isq/article/63/3/531/5521928 Acesso em: 25 de março de 2022.

Avast blocks millions of attempts in Brazil to send users to malicious websites. **AVAST Security News Team**. 2019. Disponível em: https://blog.avast.com/avast-blocks-dns-hijacking-in-brazil Acesso em: 05 de abril de 2022.

BEER, W. **Segurança cibernética nos grandes eventos: lições para os próximos.** TI INSIDE Online. 2014. Disponível em: https://tiinside.com.br/24/07/2014/187751/ Acesso em: 09 de abril de 2022.

BELLI, L. **O Brasil Aderiu À Convenção Sobre O Cibercrime: O Que Isso Significa?** 2022. Disponível em: https://cyberbrics.info/o-brasil-aderiu-a-convencao-sobre-o-cibercrime-o-que-isso-significa/ Acesso em: 18 de abril de 2022.

BRASIL. **Decreto Nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm Acesso em 15 de março de 2022.

BRASIL. **Decreto Nº 4.829 de 3 de setembro de 2003.** Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências. Brasília, DF. 2003. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm. Acesso em 20 de fev. de 2022.

BRASIL. **Decreto Nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa. Brasília, DF. 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm Acesso em: 10 de março de 2022.

BRASIL. **Decreto Nº 9.637 de 26 de dezembro de 2018.** Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o

Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24,caput,inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF. 2018. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/56970098/do1-2018-12-27-decreto-n-9-637-de-26-de-dezembro-de-2018-56969938. Acesso em 27 de fev. de 2022.

BRASIL. **Diretriz Ministerial Nº 0014/2009**. Integração e Coordenação dos Setores Estratégicos da Defesa. Brasília, DF. 2009. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/File/legislacao/emcfa/portarias/0014a_2009.pdf. Acesso em 20 de fev. 2022.

BRASIL. **Instrução Normativa GSI/PR Nº 1 de 13 de junho de 2008.** Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Brasília, DF. 2008. Disponível em: https://www.gov.br/governodigital/pt-br/legislacao/14_IN_01_gsidsic.pdf. Acesso em: 27 fev. 2022.

BRASIL. **Lei nº 12.965 de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. 2014. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 27 de fev. de 2022.

BRASIL. **Portaria Nº 93, de 26 de setembro de 2019**. Aprova o Glossário de Segurança da Informação. Brasília, DF. 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663 Acesso em: 27 de fev. de 2022

BRASIL. **Portaria Normativa Nº 3.010/MD, de 18 de Novembro de 2014** Aprova a Doutrina Militar de Defesa Cibernética. Brasília, DF. 2014. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em 20 de fev. de 2022.

BRASIL. Presidência da República. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018**. Versão 1.0. Brasília, DF. 2015. Disponível em: https://www.gov.br/gsi/pt-br/arquivos/4_estrategia_de_sic.pdf Acesso em: 10 de março de 2022.

BRASIL. Presidência da República. **Livro Verde Segurança Cibernética no Brasil**. Brasília, DF. 2010. Disponível em:

http://livroaberto.ibict.br/bitstream/1/639/4/Livro%20verde%20seguran%c3%a7a%20cibern%c3%a9tica%20no%20Brasil.pdf Acesso em: 10 de março de 2022.

BRASIL. Presidência da República. **Política Nacional de Defesa**. Estratégia Nacional de Defesa. 2016. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf Acesso em: 15 de março de 2022.

BRASIL. Secretaria de Assuntos Estratégicos. **Desafios Estratégicos para a Segurança e Defesa Cibernética**. 1º Ed. Brasília, DF. 2011 Disponível em: https://livroaberto.ibict.br/bitstream/1/612/2/Desafios%20estrat%c3%a9gicos%20para%20seguran%c3%a7a%20e%20defesa%20cibern%c3%a9tica.pdf Acesso em: 10 de março de 2022.

BRASIL. Senado Federal. **EUA grampearam telefone do avião de Dilma.** 2015. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/513286/noticia.html?sequence=1. Acesso em: 31 jan. 2022.

Brazilian President Cancels U.S. Trip Over NSA Spying Claims. **HuffPost**. 2017. Disponível em: <https://www.huffpost.com/entry/rouseff-cancels-us-trip_n_3941973>. Acesso em: 2 fev. 2022.

BUEGER, C. GADINGER, F. **International Practice Theory**. Second Edition. Palgrave Mcmillan: Springer Nature. Switzerland. 2017

BUEGER, C. GADINGER, F. **The Play of International Practice: Minimalism, Pragmatism and Critical Theory**. International Studies Quarterly. Vol. 59, 2015. p. 449-460. Disponível em: https://academic.oup.com/isq/article/59/3/449/2963252 Acesso em: 25 de março de 2022.

BUEGER, C. **Security as Practice**. *In:* CAVELTY, D. M., BALZACQ, T. (Org) Routledge Handbook of Security Studies. Routledge, 2018.

CANABARRO, D. R., BORNE, T. B. **Reflections on The Fog of (Cyber) War**. NCDG Policy Working Paper. Nº13-001. 2013.

CANABARRO. D. R., FERREIRA, T. B. **The Brazilian Reactions to the Snowden Affairs: Implications for the Study of International Relations in an Interconnected** World. Revista Conjuntura Austral. Porto Alegre. V. 6, n. 30. p.50-74.

CANONGIA, C. MANDARINO, R. J. **Segurança Cibernética: o desafio da nova Sociedade da Informação**. *In*: Parcerias Estratégicas. 2009 Brasília: Distrito Federal. v.14 n.29. p 21-46

CARVALHO, P. S. M. **Conferência de Abertura.** *In*: Desafios Estratégicos para a Segurança e Defesa Cibernética. Presidência da República. Secretaria de Assuntos Estratégicos. 2011.

CAVELTY, M. D**. The Militarisation of Cyber Security as a Source of Global Tension**. *In:* MOCKLI, D. Strategic Trends 2012: Key Developments in Global Affairs. Switzerland: Center of Security Studies. 2012. p. 103-124

CEPIK, M., CANABARRO, D. R., BORNE, T. B. **A Securitização do Ciberespaço e o Terrorismo: uma abordagem crítica.** *In*: SOUZA, A. M., NASSER, R. M., MORAES R. F. Do 11 de Setembro de 2001 à Guerra ao Terror: reflexões sobre o terrorismo no século XXI. Brasília: Instituto de Pesquisa Econômica Aplicada - IPEA, 2014. p. 161-186

CERT.br. Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança Para Internet**. Versão 4.0. São Paulo. 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf Acesso em: 04 de abril de 2022.

CERT.br. Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. 2022. Disponível em: https://www.cert.br/sobre Acesso em: 04 de abril de 2022.

CERT.br. Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. **Recomendações para Notificações de Incidentes de Segurança.** 2022. Disponível em: https://www.cert.br/docs/whitepapers/notificacoes/#1 Acesso em: 04 de abril de 2022.

CERT.br. Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. **Incidentes Reportados ao CERT.br.** 2020. Disponível em: https://www.cert.br/stats/incidentes/2020-jan-dec/tipos-ataque.html Acesso em 05 de abril de 2022.

CGI.br. Comitê Gestor da Internet no Brasil. **CGI.br - Comitê Gestor da Internet no Brasil**. Disponível em: https://cgi.br Acesso em: 27 fev. 2022.

CRUZ JR., S. C. **A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Russia e Índia para o Espaço Virtual**. IPEA. Governo Federal. Brasília. 2013.

CTIR GOV. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. Disponível em: https://www.gov.br/ctir/pt-br Acesso em: 10 de março de 2022.

CTIR.FAB. Força Aérea Brasileira. **Phishing relacionado ao COVID-19**. 2020 Disponível em: https://www2.fab.mil.br/incaer/index.php/slideshow?start=30 Acesso em: 04 de abril de 2022.

CyberBRICS. 2022. Disponível em: https://cyberbrics.info/ Acesso em: 18 de abril de 2022.

DEIBERT, R. **Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace**. Toronto: Canadian Defence & Foreign Affairs Institute. 2012

DINIZ, G. MUGGAH, R. GLENNY, M. **Desconstructing Cyber Security in Brazil: threats and responses**. Strategic Paper 11: Instituto Igarapé. 2014. Disponível em: https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf Acesso em: 20 de março de 2022.

DUPONT, B. **Security in the Age of Networks**. Policing & Society. Vol 14, nº 1, 2004. p. 76-91. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/1043946042000181575 Acesso em: 25 de março de 2022.

DYSON, E., GILDER, G.., KEYWORTH, G., TOFFLER, A. **Cyberspace and the American Dream: A Magna Carta for the Knowledge Age**. *In:* The Progress & Freedom Foundation. 1994, Washington. Disponível em: http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html. Acesso em: 5 jan. 2022.

Espionagem dos EUA se espalhou pela América Latina. **O Globo.** 2013. Disponível em: https://oglobo.globo.com/mundo/espionagem-dos-eua-se-espalhou-pela-america-latina-8966619. Acesso em: 2 fev. 2022.

EUA espionaram Petrobras, dizem papéis vazados por Snowden. **BBC News Brasil.** 2013. Disponível em: https://www.bbc.com/portuguese/noticias/2013/09/130908_eua_snowden_petrobras_dilma_mm. Acesso em: 31 jan. 2022.

FIRST.org. Computer Security Incident Response Team (CSIRT) Services Framework. **Forum of Incidente Response and Security Teams.** 2019. Disponível em: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1 Acesso em: 04 de abril de 2022

FONSECA, L. O. **A Evolução das Políticas e Estratégias de Segurança do Espaço Cibernético Brasileiro.** Revista Relações Exteriores. 2020. Disponível em: https://relacoesexteriores.com.br/a-evolucao-das-politicas-e-estrategias-de-seguranca-do-espaco-cibernetico-brasileiro/. Acesso em 20 de fev. de 2022.

GETSCHKO, D. **Apresentação.** *In*: Segurança Digital: Uma Análise de Gestão de Risco em Empresas Brasileiras. Núcleo de Informação e Coordenação do Ponto BR. Nic.br. 2020. p. 13-19

GOLDSMITH, J. **The New Vulnerability**. The New Republic, 2010. Disponível em: https://newrepublic.com/article/75262/the-new-vulnerability. Acesso em: 15 jan. 2022.

HEDLING, E., BREMBERG, N. **Practice Approaches to the Digital Transformations of Diplomacy: Toward a New Research Agenda.** International Studies Review. Vol. 23, 2021. p. 1595-1618. Disponível em: https://academic.oup.com/isr/article/23/4/1595/6309155 Acesso em: 25 de março de 2022.

HOEPERS, C., STEDING-JESSEN, K. **Padrões Modernos para Segurança e Estabilidade dos Serviços**. Workshop CKN. CERT.br, NIC.br, CGI.br. 2021. Disponível em: https://www.cert.br/docs/palestras/certbr-ckn2021-1.pdf Acesso em: 05 de abril de 2022.

HUREL, M. L. A **Conversation With Brazil's Cyber Diplomat**. Digital IR in the Information Age. LSE Ideas. 2022. Disponível em: https://www.lse.ac.uk/ideas/Assets/Documents/project-docs/digital-ir/commentary/LSE-IDEAS-Cyber-Diplomat.pdf Acesso em 18 de abril de 2022.

HUREL. L. M. **Cibersegurança no Brasil: Uma Análise da Estratégia Nacional**. Artigo Estratégico. Instituto Igarapé. 2021. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf Acesso em: 10 de março de 2022.

IGARAPÉ. Instituto. 2011. Disponível em: https://igarape.org.br/ Acesso em 10 de março de 2022.

International Telecommunication Union. **Global Cybersecurity Index**. ITU Publications. 2020. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf Acesso em: 08 de abril de 2022.

International Telecommunication Union. **Recommendation ITU-T X.1205- Overview of cybersecurity**. Genebra: ITU, 2008. Disponível em: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136. Acesso em 15 de março de 2022.

KURBALIJA, J. **An Introduction to Internet Governance.** 4 Ed. Malta: DiploFoundation, 2010

LÉVY, P. **Cibercultura**. 2 Ed. São Paulo: Editora 34. 1999.

LIBICKI, M. C. **Conquest in Cyberspace: National Security and Information Warfare.** New York: Cambridge University Press. 2007.

LUCERO, E. **Governança da Internet: Aspectos da Formação de um Regime Global e Oportunidades para a Ação Diplomática.** Brasília: Fundação Alexandre de Gusmão, 2011.

MAGANHATI JR, R. **Ataques de pharming: a verdade está lá fora.** Axur. 2020. Disponível em: https://blog.axur.com/pt/ataques-de-pharming-a-verdade-esta-la-fora Acesso em: 05 de abril de 2022.

National Cyber Security Index. **NCSI**. Disponível em: https://ncsi.ega.ee/country/br/?allData=1 Acesso em: 09 de abril de 2022.

NIC.br **Relatórios de Atividade 2019** Disponível em: https://www.nic.br/media/docs/publicacoes/9/20201223162744/RA_CGI_NIC_2019_livro_eletronico.pdf Acesso em: 05 de abril de 2022.

NIC.br. **CGI.br - Comitê Gestor da Internet no Brasil**. CGI.br - Comitê Gestor da Internet no Brasil. Disponível em: <https://www.cgi.br/noticia/netmundial/393>. Acesso em: 2 fev. 2022.

NIC.br. Comitê Gestor da Internet no Brasil. **Estatuto NIC.br.** 2014. Disponível em: https://nic.br/pagina/estaturo-nic-br/160 Acesso em: 04 de abril de 2022

NIC.br. Comitê Gestor da Internet no Brasil. **NBSO Trata Incidentes de Segurança na Internet Nacional.** 2004. Disponível em: https://www.nic.br/noticia/na-midia/nbso-trata-incidentes-de-seguranca-na-internet-nacional/ Acesso em: 04 de abril de 2022

NIC.br. Comitê Gestor da Internet no Brasil. **Phishing, a fraude mais usada no Brasil.** 2010. Disponível em: https://www.nic.br/noticia/na-midia/phishing-a-fraude-mais-usada-no-brasil/ Acesso em: 06 de abril de 2022.

NSA e CIA mantiveram em Brasília equipe para coleta de dados filtrados de satélite. **O Globo.** 2013. Disponível em: https://oglobo.globo.com/mundo/nsa-cia-mantiveram-em-brasilia-equipe-para-coleta-de-dados-filtrados-de-satelite-8949723. Acesso em: 31 jan. 2022.

NYE JR. **Soft Power**. The Means to Success in World Politics. PublicAffairs: New York. 2004.

NYE, J. S. JR. **Cyber Power**. Cambridge: Belfer Center for Science and International Affairs, 2010.

NYE, J. S. JR. **The Third Annual Ernest May Memorial Lecture: Nuclear Lessons for Cybersecurity?** *In*: NYE JR, J. S., SCOWCROFT, B. Securing Cyberspace: A New Domain for National Security. The Aspen Institute: Washington. 2012

NYE, J. S. JR., SCOWCROFT, B. **Securing Cyberspace. A New Domain for National Security**. The Aspen Institute: Washington. 2012.

O que é cracking? É hacking, mas do mal. **AVAST Security News Team**. 2022. Disponível em: https://www.avast.com/pt-br/c-cracking. Acesso em: 27 fev. 2022.

O que é spyware? - Definição. **Karpersky**. Disponível em: https://www.kaspersky.com.br/resource-center/threats/spyware. Acesso em: 27 fev. 2022.

OPPERMANN, D. **O Cenário de Cibersegurança Depois de Snowden e consequências no Brasil.** Conjuntura Internacional. O Estado do Estado: Metamorfoses da violência. Janus: anuário de relações exteriores. Lisboa: Universade Autónoma de Lisboa. 2014

PAGLIARI, G. C., PINTO. D. J. A., VIGGIANO J. **Mobilização Nacional, Ameaças Cibernéticas e Redes de Interação num Modelo de Tríplice Hélice Estratégica: Um Estudo Prospectivo**. *In*: OLIVEIRA, M. A. G. (Org.) Defesa Cibernética e Mobilização Nacional. Editora UFPE: Recife. 2020. pgs. 153-175

POULIOT, V. **The Logic of Practicality: A Theory of Practice of Security Communities. International Organization.** Vol. 62, 2008. p. 257-288. Disponível em: https://www.cambridge.org/core/journals/international-organization/article/abs/logic-of-practicality-a-theory-of-practice-of-security-communities/63A65E80B53BEC54E705AAE179CCD723 Acesso em: 25 de março de 2022.

RADU, R. **Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace**. *In*: KREMER, J. F., MÜLLER, B. Cyberspace and International Relations: Theory, Prospects and Challenges. [New York]: Springer, 2014. p. 03-20

ROUSSEFF, D. **Discurso de Abertura da Assembleia Geral da Organização das Nações Unidas**. Canal TV BrasilGov. 2013. Disponível em: https://www.youtube.com/watch?v=whoTgyTNk-w&ab_channel=TVBrasilGov. Acesso em 20 fev. 2022.

SABBAT, A. P. **O Brasil Precisa de uma Política Nacional de Segurança da Informação?** Disponível em https://www.linkedin.com/pulse/o-brasil-precisa-de-uma-pol%C3%ADtica-nacional-seguran%C3%A7a-da-sabbat/?originalSubdomain=pt. Acesso em 27 de fev. de 2022.

SCHATZKI, T. R. **Practice Mind-ed Orders**. *In*: SCHATZKI, T. R., CETINA, K. K., SAVIGNY, E. (Org) The Practice Turn in Contemporany Theory. Routledge: New York. 2001.

SCHJøLBERG, S. Report of The Chairman of HLEG. ITU **Global Cybersecurity Agenda**. 2008 Disponível em: https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf Acesso em: 18 de abril de 2022.

SCOTT. J. C. **Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed**. Yale University Press: New Have. 1998.

SENHORAS, M. E. et al. **Conflitos Cibernéticos como Ameaça Multidimensional**. Anais do XII Congresso Acadêmico de Defesa Nacional. Pirassununga: AFA. 2015

SHELDON, J. **The Rise of Cyberpower.** *In*: BAYLIS, J, WIRTZ, J. J., GRAY, C. S. Strategy in the Contemporary World. 6 Ed. United Kingdom: Oxford University Press, 2019. p. 291-306

The Hidden Costs of Cybercrime. **McAfee.** 2020. Disponível em: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf Acesso em: 10 de abril de 2022.

The World Bank. Overview. 2022. Disponível em: https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview Acesso em: 13 de abril de 2022.

TOP. Teste os Padrões. 2022. Disponível em: https://top.nic.br/ Acesso em: 07 de abril de 2022.

VENTRE, D. **Ciberguerra**. *In*: Seguridad global y potencias emergentes em um mundo multipolar. XIX Curso Internacional de Defensa. Espanha: Academia General Militar. Universidad Zaragoza. 2012. p. 31-47

YOACHIMIK, O. Cloudflare thwarts 17.2M rps **DDoS attack — the largest ever reported.** Cloudflare. 2021. Disponível em: https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/ Acesso em: 05 de abril de 2022.

ZIMET, E., SKOUDIS, E**. A Graphical Introduction to the Structural Elements of Cyberspace** *In*: KRAMER, F. D., STARR, S. H., WENTZ, L. K. Cyberpower and National Security.Washington: Potomac Books, 2009. p. 91-113

ZITTRAIN, J. L. **The Future of the Internet and How to Stop It.** London: Yale University Press. 2008.

ZUBEN, M. **Dicas de Como se Proteger Contra Phishing.** Tarde de Conscientização em Segurança Cibernética. CERT.br, NIC.br, CGI.br. 2021. Disponível em: https://www.cert.br/docs/palestras/certbr-anatel2021.pdf Acesso em: 06 de abril de 2022.