UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL
DA LUSOFONIA AFRO-BRASILEIRA
INSTITUTO DE HUMANIDADE E LETRAS DOS MALÊS
BACHARELADO EM RELAÇÕES INTERNACIONAIS

NILTON LOPES DA SILVA GOMES

VULNERABILIDADE CIBERNÉTICA E AS ESTRATÉGIAS DE SEGURANÇA CIBERNÉTICA INTERNACIONAL DO ESTADO BRASILEIRO

SÃO FRANCISCO DO CONDE
2020

NILTON LOPES DA SILVA GOMES

VULNERABILIDADE CIBERNÉTICA E AS ESTRATÉGIAS DE SEGURANÇA CIBERNÉTICA INTERNACIONAL DO ESTADO BRASILEIRO

Trabalho de Conclusão de Curso submetido ao Bacharelado em Relações Internacionais da Universidade da Lusofonia Afro-Brasileira como parte dos requisitos necessários para a obtenção do título de Bacharel.

Orientador: Prof. Dr. Enzo Lenine Nunes Batista Oliveira Lima.

SÃO FRANCISCO DO CONDE

2020

Universidade da Integração Internacional da Lusofonia Afro-Brasileira
Sistema de Bibliotecas da Unilab
Catalogação de Publicação na Fonte

G615v

Gomes, Nilton Lopes da Silva.
Vulnerabilidade cibernética e as estratégias de segurança cibernética internacional do Estado brasileiro / Nilton Lopes da Silva Gomes. - 2020.
62 f. : il. mapas, color.

Monografia (graduação) - Instituto de Humanidades e Letras dos Malês, Universidade da Integração Internacional da Lusofonia Afro-Brasileira, 2020.
Orientador: Prof. Dr. Enzo Lenine Nunes Batista Oliveira Lima.

1. Cibernética - Medidas de segurança - Brasil. 2. Hackers - Brasil. 3. Proteção de dados - Brasil. 4. Segurança internacional. I. Título.

BA/UF/SEBI CDD 003.5081

Ficha catalográfica elaborada por Bruno Batista dos Anjos, CRB-5/1693

NILTON LOPES DA SILVA GOMES

VULNERABILIDADE CIBERNÉTICA E AS ESTRATÉGIAS DE SEGURANÇA CIBERNÉTICA INTERNACIONAL DO ESTADO BRASILEIRO

Trabalho de Conclusão de Curso submetido ao Bacharelado em Relações Internacionais da Universidade da Lusofonia Afro-Brasileira como parte dos requisitos necessários para a obtenção do título de Bacharel.

Data de aprovação: 06/02/2020.

BANCA EXAMINADORA

Prof. Dr. Enzo Lenine Nunes Batista Oliveira Lima (Orientador)
Universidade da Integração Internacional da Lusofonia Afro-Brasileira - UNILAB

Prof.ª Dr.ª Cinthia Regina Campos Ricardo da Silva
Universidade da Integração Internacional da Lusofonia Afro-Brasileira - UNILAB

Prof.ª Dr.ª Mariana Preta Oliveira de Lyra
Universidade da Integração Internacional da Lusofonia Afro-Brasileira - UNILAB

Aos meus pais Vera da Silva e Luís Gomes, minha avó Virginia Moniz, meu amado tio José Lino Moniz, irmãos e a toda família que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa da minha vida.

AGRADECIMENTOS

Primeiramente a Deus, maior cientista universal, Senhor dos senhores, pelo dom da vida, proteção, permissão deste acontecimento e, sobretudo pelo conhecimento que certamente contribuiu para desenvolvimento deste trabalho.

Ao meu pai pelo incansável esforço na minha criação e educação, da mesma forma expresso meu reconhecimento a minha mãe. A minha melhor amiga/companheira, Evelene Patrícia Alves Robalo (Nha Best) pelo apoio motivacional em todo momento.

Aos meus irmãos Janilson e Gilson, as minhas irmãs Mônica e Verônica inclusive minha sobrinha Juceila, pela inspiração em apreender e puder compartilhar aprendizado com eles.

Ao meu tio José Lino pela força e coragem na minha formação pessoal e acadêmica, pelos momentos embaraçosos de desesperos no qual sempre esteve presente com possíveis soluções para continuar a caminhada e concretizar o sonho de formar numa universidade. Aos meus primos/as, tios/as e a todas as famílias que participaram direta ou indireta na assistência dessa trajetória.

A todos os amigos, especialmente membros de *M7, Web-104 e AP-B* por mostrarem sempre disponíveis por o que der e vier, por compartilharem quase tudo desde sempre e se fizeram presente nos momentos difíceis e nos momentos alegres.

A Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB), seu corpo docente, em especial a todos/as os/as professores/as de Relações Internacionais, direção e administração, técnicos, funcionário/as, sobretudo os que compõem Instituto de Humanidades e Letras – Malês (IHL), que de uma forma ou outra, contribuíram neste processo e viabilizaram oportunidade de enxergar nitidamente um horizonte superior.

Ao orientador, prof. Dr. Enzo Lenine, por ter aceitado o convite de me orientar neste Trabalho de Conclusão de Curso (TCC), pela confiança na minha capacidade de desenvolver este tema, ele que sempre esteve presente para auxiliar da melhor forma possível.

A toda comunidade acadêmica especificamente estudantes provenientes de diversas regiões brasileiras e de países africano (Angola, Cabo Verde, Guiné-Bissau e São Tomé e Príncipe), pela integração que permitiu trocar de experiências e

convivências inesquecíveis. A todos que direta ou indiretamente fizeram parte da minha formação, meu muito obrigado.

O maior risco é não arriscar. Em um mundo que muda muito rápido, a única estratégia em que a falha é garantida é de não arriscar.

Mark Zuckerberg.

RESUMO

A inovação tecnológica mediante ferramentas digitais e aparelhos eletrônicos tem influenciado a mudança na interação entre os Estados no cenário internacional e na interação social em diversas sociedades. Atualmente várias atividades são realizadas por meio da internet, o que gera preocupações quanto às vulnerabilidades dos sistemas de segurança. Estes estão submetidos a constantes ameaças, o que demandam uma atenção tanto para defesa quanto para ataque, constituindo o campo que se denomina de segurança cibernética. Nesse contexto, os Estados vêem desenvolvendo estratégias para lidar com as vulnerabilidades de um mundo cada vez mais integrado computacionalmente e dependente das internets. Nesse sentido, o presente trabalho visa a compreender as vulnerabilidades cibernéticas e as estratégias de segurança cibernética do Brasil a partir da política nacional. Utiliza-se a análise de conteúdo para caracterizar a estratégia de defesa cibernética brasileira nos documentos oficiais sobre a temática. Diante disso, verifica-se que a vulnerabilidade cibernética brasileira versa na disponibilidade, a integridade, a confidencialidade e a autenticidade da informação, o que estabelece a constatação de que o Brasil assume um caráter defensivo e orientado para prevenção e remediação da SegCiber.

Palavra-chave: Cibernética - Medidas de segurança - Brasil. Hackers - Brasil. Proteção de dados - Brasil. Segurança internacional.

ABSTRACT

Technological innovation through digital tools and electronic devices has influenced the change in the interaction between the States in the international scenario and in the social interaction in several societies. Currently several activities are carried out through the Internet, which generates concerns about the vulnerabilities of security systems. These are subjected to constant threats, which demand attention both for defense and for attack, constituting the field that is called cybersecurity. In this context, States have been developing strategies to deal with the vulnerabilities of an increasingly computer-integrated and Internets-dependent world. In this sense, the present work aims to understand the cyber vulnerabilities and cyber security strategies of Brazil from the national policy. The content analysis is used to characterize the Brazilian cyber defense strategy in the official documents on the subject. Therefore, it is verified that the Brazilian cyber vulnerability relates to the availability, integrity, confidentiality and authenticity of the information, This establishes the observation that Brazil is defensive and oriented towards the prevention and remediation of SegCiber.

Keyword: Cybernetics - Security measures - Brazil. Data protection - Brazil. Hackers - Brazil. International security.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABC - Agência Brasileira de Cooperação

ABIN - Agência Brasileira de Inteligência

ABNT - Associação Brasileira de Normas Técnicas

ADF - Administração Pública Federal

ADURGS - Associação das Universidades do Rio Grande do Sul

ARPA - *Advanced Research Projects Agency*

ARPANET - *Advanced Research Projects Agency Network*

CDCIBER – Centro de Defesa Cibernética

COPRI - *Copenhagen Peace Research Institute*

CSIS - Centro de Estudo Estratégico e Internacional

DARPA - *Defense Advanced Research Projects Agency*

END – Estratégia Nacional de Defesa

HTTP - *Hypertext Transfer Protocol*

IHL - Instituto de Humanidades e Letras – Malês

IBGE – Instituto Brasileiro de Geografia e Estatística

ISO - *International Organization for Standardization*

LAN - *Local Area Network*

MCT - Ministério da Ciência e Tecnologia

OEA – Organização dos Estados Americanos

OI – Organizações Internacionais

ONU – Organização das Nações Unidas

OTAN – Organização do Tratado do Atlântico Norte

PNUD - Programa das Nações Unidas para o Desenvolvimento

RI - Relações Internacionais

RNP – Rede Nacional de Pesquisa

RST – Rede Sul de Teleprocessamento

SI - Segurança Internacional

SECOM - Secretaria de Comunicação Social da Presidência da República

SEGCIBER – Segurança Cibernética

TCC - Trabalho de Conclusão do Curso

TCP/IP - *Transmission Control Protocol/Internet Protocol*

TIC – Tecnologia de Informação e Comunicação

UNILAB - Universidade da Integração da Lusofonia Afro-Brasileira

UCLA - Universidade da Califórnia em Los Angeles

URL - *Uniform Resource Locator*

XBT - Bitcoin

WAN - *Wide Area Network*

WWW – *World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

Os avanços científicos das tecnologias de informação têm sido alcançados rapidamente em diversas sociedades contemporâneas, de modo a viabilizar melhoria na comunicação e na interação entre diferentes atores, tais como Estados, instituições públicas e privadas, organizações e povos. O acesso à internet, além de conectar as pessoas, atualmente possibilita a conexão entre objetos como carros, eletrodomésticos (frigorífico, micro-ondas, máquina de lavar) dentre outros aparelhos/dispositivos utilizados por diversas empresas. Nesse contexto, o desenvolvimento tecnológico e o seu envolvimento com a humanidade demonstram-se profundamente intrincados.

Por outro lado, observa-se uma dependência tecnológica e informacional sem precedentes, que além de oferecer as vantagens citadas anteriormente, se coloca como ameaça para a segurança nacional dos Estados (KREIBICH, 2016). Na medida em que os avanços tecnológicos apresentam vantagens em relação à inclusão social, eliminação das fronteiras – em que maiores partes das atividades podem ser realizadas em tempo real independentemente do espaço geográfico –, também demostra suas fragilidades como, por exemplo, a privacidade, anonimato e/ou ilegalidade onde utilizadores não se identificam de modo que consigam alcançar seus objetivos usando ferramentas tecnológicas num viés criminal. Por essas razões, atualmente no ambiente virtual encontram-se tecnologias ofensivas que são designadas por ataques/crimes cibernéticos utilizados para adquirir informações secretas ou para exclusão das mesmas, assim como para alterações tendenciosas em determinado sistema. No entanto, existem tecnologias defensivas, nomeadamente as de segurança/defesa cibernética, nos quais são desenvolvidos mecanismos estratégicos para proteção de dados ou sistemas conectados às redes (BRASIL, 2010; LEAL, 2015). Em outros termos, a Segurança Cibernética é compreendida como um conjunto de ferramentas e políticas que aborda a gestão de risco, treinamentos, ações, práticas seguras das tecnologias utilizadas para proteger o usuário e as propriedades, que inclui dispositivos de computadores conectados (serviços, aplicativos, infraestruturas, informações armazenadas ou transmitidas) no ambiente cibernético (KREIBICH; LOPES, 2016).

Os ataques cibernéticos ocorrem constantemente no espaço cibernético, o que demanda estratégias de defesa cibernética. Essas relações de ataque e defesa são

definidas na literatura como guerra cibernética (LIBATO; KENKEL, 2015; SANDRONI, 2013). Nessa perspectiva, vale mencionar exemplos de recentes casos referentes à temática em territórios distintos, de forma a se compreender a premência do tema.

No Reino Unido, em 2017, cerca de 16 hospitais sofreram um ataque cibernético, bloqueando sistemas e criptografando arquivos. Este ataque gerou uma desordem laboral dificultando acesso aos registros médicos. No entanto, os dados no sistema não sofreram alterações tendo em conta o objetivo de obter recursos financeiros. Neste caso, foi solicitado cerca de 300 dólares americanos em bitcoin (XBT). Geralmente os ataques pelo acesso às informações têm essa finalidade: ameaçar os arquivos de um usuário ou o acesso ao computador em troca de um resgate. Brandon (2017) afirma que cerca de 45.000 computadores em 74 países já sofreram este tipo de ataque.

A República do Equador anunciou em abril de 2019 ter sofrido um ataque cibernético após a prisão do fundador de *Wikileaks* – Julian Assange – sem que estes tenham afetado portais do governo central. O presidente Lenin Moreno considera que Assange converteu a Embaixada do Equador em Londres em um centro de espionagem, havendo falhado o compromisso com os protocolos de convivência, que especificam a não interferência nos assuntos de outros Estados, como os Estados Unidos da América, o Vaticano, a Espanha e o próprio Equador (EQUADOR, 2019). Nessa perspectiva, o presidente aponta que o país já recebeu cerca de 40 milhões de ataques cibernéticos de equipes ligadas a ele, as identidades estatais, financeiros e governamentais. Ainda no mesmo exemplo de ataque cibernético, verificou-se que hackers russos próximos a Julian Assange estariam envolvidos em um plano para desestabilizar o presidente equatoriano.

Estes exemplos demonstram que as mudanças tecnológicas e ataques cibernéticos estão afetando o mundo no século XXI. Não por acaso, o Centro Internacional de Estudos Estratégicos (CSIS, em inglês) dos Estados Unidos analisa esses fenômenos que abordam as questões da inteligência, vigilância, criptografia, privacidade, tecnologia militar, espaço cibernético, crimes econômicos e entre outros, apresentando e atualizando listas de incidentes cibernéticos significativos desde 2006. Os Estados Unidos investem muito no desenvolvimento tecnológico e busca

manter o controle do mesmo por meio de agentes especializados.[1] A relação dos Estados tem gerado alerta de segurança referente ao avanço tecnológico utilizado para espionagem.

Neste novo contexto, não é surpresa que o Brasil não esteja livre de ataques cibernéticos. A Symantec (2019) apresentou relatório em que o Estado brasileiro está classificado como terceiro país em ranking de ataques cibernéticos, recebendo principalmente ameaças em dispositivos conectados à internet. A empresa de segurança cibernética informou em relatório global que 9,8% dos ataques cibernéticos ocorreram no Brasil, sendo a China em primeiro lugar com 24%, seguida dos Estados Unidos com 10,1%. Em linhas gerais, o Brasil registra séries de ataques realizados de forma automática, ou seja, por robôs, em *ransomware* (confisco de dados pessoais), *crypto jacking* (roubo de processamento usado para mineração de *criptomoedas*), *phishing* por e-mail (acontece quando o usuário é induzido a baixar um programa ou a clicar em um link) e *malware* (por meio de vírus virtuais). Segundo a Symantec, o *form jacking* (roubo de informações de cartões de crédito executado enquanto a vítima preenche formulários para realizar compras na internet) teve destaque em 2018 no país.

Nesse sentido, e sendo o espaço cibernético composto por ferramentas técnicas no espaço físico e ferramentas lógicas no espaço virtual, evidencia-se que há vulnerabilidade cibernética que ameaça à segurança humana e institucional, nomeadamente no que tange às informações sigilosas dos Estados (LEAL, 2015; KREIBICH, 2016; VINHAS, 2014; SANTOS 2017). Diante deste cenário virtual, e considerando o caso específico do Brasil, visa-se a responder a seguinte questão: Como se caracterizam as estratégias de segurança cibernética do Brasil em seus documentos oficiais para lidar com suas vulnerabilidades cibernéticas? Por meio dessa questão, pretende-se enfatizar três níveis desta pergunta, quais sejam: 1. Quais os tipos de vulnerabilidades reconhecidas pelo governo brasileiro; 2. Quais são os princípios norteadores de SegCiber definidos pelo Brasil; e 3. Quais são as estratégias desenvolvidas pelo Estado brasileiro para lidar com as vulnerabilidades reconhecidas pelo País, tanto em termos de normatização técnica e jurídica como remediação. Pretende-se alcançar o objetivo principal e responder à questão supracitada,

[1] Em fevereiro de 2019 “foi revelado por Centro Internacional de Estudos Estratégicos que ex-funcionários da inteligência dos Estados Unidos trabalhavam para ajudar o país a invadir os telefones de ativistas, diplomatas e funcionários do governo estrangeiro” (CSIS, 2019).

buscando identificar as estratégias políticas do Estado brasileiro que operacionalizam a segurança cibernética no âmbito nacional e internacional.

2 HISTÓRIA DA INTERNET

A Internet tem sido um dos instrumentos mais eficazes não só para a comunicação entre as pessoas, mas também para a conexão entre aparelhos eletrônicos. Embora tenha surgido com o intuito de estabelecer comunicação, verificam-se no mundo atual milhões de usuários da Internet para realizações de serviços de entretenimento, comercialização de produtos, criação dos materiais tecnológicos e demais fins. Neste capítulo, apresenta-se uma abordagem histórica da internet, primeiramente, com ênfase no contexto da Guerra Fria, e, em seguida, detalho a implementação da Internet no Brasil em perspectiva contextual.

2.1 INTERNET NO CONTEXTO DA GUERRA FRIA

Muitos historiadores defendem que o lançamento da bomba atômica sobre Hiroshima e Nagasaki durante a Segunda Guerra Mundial em 1945 como marco inicial da Guerra Fria. Após esse período, as duas grandes potências, os Estado Unidos e a União Soviética, estabeleceram um conflito ideológico que consistia em sobrepor para o mundo as suas formas de dominação. Nesse período, não houve uma guerra direta entre as superpotências devido à arma nuclear adquirida por ambos os lados, a qual podia causar grandes danos para o mundo, inclusive a extinção da vida na face da Terra. Enquanto os Estados Unidos buscavam expandir a sua influência política (sistema democrático), econômica (mercado, propriedade privada) e militar caracterizada pelo sistema capitalista, a União Soviética procurava disputar a hegemonia pela igualdade social, economia planificada, partido único (Partido Comunista) caracterizados por influência socialista. Os estudos apontam que o mundo bipolar era viável para a segurança mundial, todavia, as estratégias da dominação continuaram a ser implementadas (SARAIVA 2007; GONÇALVES, 2016). Nesse sentido, a corrida armamentista foi vista como forma de defender-se do outro sem adentrar nas vias de fato de uma guerra de larga escala. Os dois países investiram

em tecnologia para fabricação de armas (foguetes, mísseis satélites e outros artefatos espaciais) que serviria de possível defesa e ataque.

Considera-se, portanto, esses investimentos tecnológicos uma arte da guerra para empregar técnicas em combate com os meios que lhe forem atribuídos. Em outras palavras, a arte da guerra são as formas de conduzir conflito por meio das atividades que existem por sua causa, tais como a formação das forças combatentes, o seu recrutamento, armamento, equipamento e adestramento (CLAUSEWITZ, 1996; SUN TZU, 2014). Nessa perspectiva, podemos classificar a Internet como uma das invenções tecnológicas estratégicas no contexto da Guerra Fria.

Na década de 1960, houve uma necessidade de estabelecer linhas de comunicação entre militares e cientistas estadunidenses para articularem suas estratégias de ataque e defesa, mesmo em caso de eventual bombardeio no conflito com a União Soviética. Em 1969 foi criado um mecanismo estratégico no Departamento de Defesa dos Estados Unidos, por meio de um projeto da agência militar de pesquisa conhecida na época por *Advanced Research Projects* Agency (ARPA). Os militares norte-americanos desenvolviam diversos programas de mísseis balísticos e outras experiências de pesquisa básica de longo prazo dentro da agência, com vinculação a universidades que colaboravam sem fazer parte do projeto. A ARPA propunha pesquisa nas áreas de processamento, análise e tomada de decisões sobre um grande volume de informação, com o intuito de aumentar a eficiência nos campos de batalha da guerra nuclear.

Dada a importância cientifica das universidades, o nome da agência passou a ser *Defense Research Projects Agency* (DARPA) (CARVALHO, 2006; GONÇALVES, 2016). O processo resultou em pesquisa mais avançada em computação. Nessa fase, se projetava a interligação entre diferentes computadores. Posteriormente, o projeto teve seu avanço no qual ligava redes tecnológicas e foi designado por *Advanced Research Projects Agency Network* (ARPANET), que inicialmente tinha uma função de conectar laboratórios de pesquisa e garantir a comunicação através de um conjunto de protocolo. A força aérea estadunidense, também, necessitava de um projeto de comunicação mínima essencial, cujo objetivo era de manter uma estrutura que pudesse em algum momento ter articulação de ataque bélico contra o inimigo, permitindo, deste modo, alguma comunicação que viabilizasse o disparo de uma operação de contra-ataque.

Essa comunicação seria distribuída em um conjunto de mensagem formada em pequenos blocos e chamada de pacotes. Ou seja, a ideia era de uma rede de pontos automáticos (não comandados), pela qual passariam os pacotes, de um ponto para outro, até que chegassem ao seu destino final. Por essa razão, a criação de pequenas redes local – *Local Area Network* (LAN) – era posicionada nos lugares estratégicos do país e conectada através de telecomunicação geográfica *Wide Area Network* (WAN). Na eventualidade de uma cidade vir a ser destruída por um ataque nuclear, esse conjunto de redes conexas – internet, isto é, *Inter networking*, literalmente, coligação entre redes locais distantes – garantiria a comunicação entre as remanescentes cidades coligadas (NETO; GUIMARÃES, 2003). Além disso, Lins acrescenta:

> A vantagem desse sistema era a de que cada pacote iria trafegar na rede de modo independente, buscando seu próprio caminho até o destino. Desse modo, a rede resistiria a interrupções ou ataques, pois a queda de parte dos computadores não comprometeria a rede: os pacotes seguiriam seu caminho pelas conexões restantes. (LINS, 2013, p.16)

Logo após instalação do sistema, a rede começou a funcionar no ano em que surgiu a DARP (1969), quando a primeira ligação foi efetuada entre a Universidade de Stanford e a Universidade da Califórnia em Los Angeles (UCLA). Inicialmente, a rede era utilizada restritamente no seio acadêmico nos Estados Unidos.

Várias redes locais que anteriormente se encontravam isoladas de um nível mundial maior, as *Local Area Networks* (LANs), com a Internet e especialmente o protocolo TCP/IP (que padroniza a forma como essas redes se comunicarão), passam a integrar uma rede muito maior, sendo seu fluxo de informações mediado por roteadores, responsáveis por redirecionar a mensagem enviada ao destinatário. Com o avanço do projeto de pesquisa na década de 1970, foi registrado o Protocolo de Controle de Transmissão/Protocolo Internet (Protocolo TCP/IP) em 1973 pelo Vinton Cerf, responsável pelo projeto do Departamento de Pesquisa avançada da Universidade da Califórnia (NETO; GUIMARÃES, 2003). Esse protocolo interligava diversas redes incompatíveis por meio de códigos, programas e sistemas de comunicação entre si. Desta forma, na década de 1980 ocorreu uma expansão da conexão da rede: além do ambiente acadêmico, isto é, o uso da ARPANET se expandiu para outros países do Ocidente como Dinamarca, Holanda, Noruega, Reino Unido e Suécia. É importante realçar que a expansão da ARPANET passou a ser reconhecida mundialmente por INTERNET e permitiu a comunicação e interação entre

os computadores com larga capacidade de transmitir informações à longa distância e em curto período de tempo.

No final da década de 1980 foi criado pelo Tim Berners-Lee e Robert Cailliau a *World Wide Web* (WWW) no Laboratório Europeu de Física de Altas Energias. A WWW ficou reconhecida como rede mundial. Esse sistema tinha por objetivo distribuir a rede composta por hipertextos, de modo que documentos, imagens e sons tivessem uma interligação entre outros recursos do gênero. Porém, em determinado momento, "[a] WWW ultrapassou largamente o âmbito para qual foi originalmente desenhada - partilha de documentos científicos". (NUNES, 2012, p.12). Durante décadas a rede mundial de computadores foi utilizada nos Estados Unidos somente no meio acadêmico e científico para colocar informações ao alcance de usuário. No início da década de 1990, a rede foi liberada para uso comercial, permitindo o surgimento de diversas empresas provedoras de acesso à internet. Deste modo, ocorreu a expansão da rede em larga medida com mais de dois bilhões de usuários no qual se verifica mais de 250 milhões de sítios web em funcionamento.

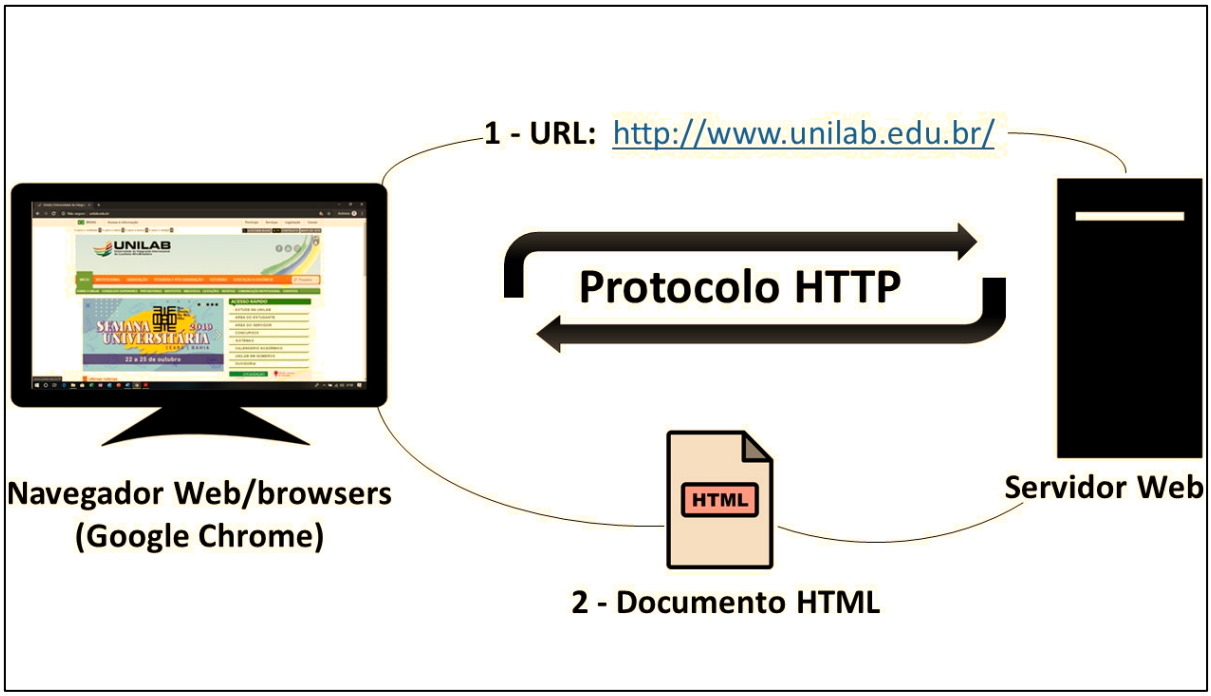
Dados da Mashabe[2] (2012) apontam que mais de 144,8 bilhões de e-mails são enviados por dia no mundo todo, e cerca de 90% dos usuários de Internet estão localizados nos países industrializados como a Alemanha, Canadá, Estados Unidos, França, entre outros países desenvolvidos. Destes 144,8 bilhões, 89 bilhões são profissionais e 55,8 bi são pessoais. Além do tráfego mundial de e-mails, a *World Wide Web* possibilitou o compartilhamento de diversos dados em formato de documentos, imagens, vídeos etc. Através de endereçamento – *Uniform Resource Locator* (URL) – , cada documento ou recurso existente na web tem um endereço único. Os URL são usados para identificar de forma única cada documento ou recurso. Por meio da Transferência - *Hypertext Transfer Protocol* (HTTP), os documentos são transferidos entre o servidor web e o navegador web. A forma como se processa esta transferência é definida pelo protocolo HTTP, pertencente à família TCP/IP.

Por fim, através da representação - *Hypertext Markup Language* (HTML). Os documentos seguem uma estrutura padrão definida (NUNES, 2012; LINS, 2013). Por exemplo, o nome de domínio de um provedor de acesso conhecido no Brasil poderia ser www.unilab.edu.br, onde "br" delimita o espaço dos endereços situados no Brasil,

[2] Mashabe é uma empresa global de mídia e entretenimento multiplataforma. Alimentado por sua própria tecnologia proprietária, o Mashable é a fonte de conteúdo de tecnologia, cultura digital e entretenimento para seu público dedicado e influente em todo o mundo.

“edu” as entidades comerciais/institucionais dentro do espaço brasileiro e “unilab” o provedor propriamente dito. Após essa abordagem, segue **figura 1** abaixo ilustrando o funcionamento das ferramentas da rede.

Figura 1 - Representação da função *World Wide Web*



Fonte: Autoria própria.

Consoante à figura 1, o número 1 representa a URL que identifica o protocolo HTTP, servidor e documento; enquanto que o número 2 retrata o documento em formato HTML devolvido ao usuário, ou seja, o protocolo estabelece a comunicação entre o navegador web e o servidor web. A denominação HTML refere-se a uma linguagem de marcação ou codificação fundamentada em marca (tags/código fonte) por meio das quais se elabora todo o conteúdo das páginas (texto, imagens, vídeos, links, tabelas, etc.), conferindo acesso à informação.

A *World Wide Web* foi uma das criações tecnológicas que viabilizou acesso Internet e, por conseguinte, a transferência de dados a nível mundial. Em 1993, Marc Andreessen e Rob McCool inventou o primeiro navegador livre e gráfico, o Mosaic. O navegador Mosaic foi o principal meio de explorar a Internet fora das universidades e centros de pesquisa. O objetivo da dupla McCool e Andreessen era transformar a Internet em algo prático também para outros usuários. Nesse sentido, em 1994 nasce o Netscape, primeiro navegador comercial da Internet. A partir disso surgiram outros

browsers como Internet Explorer, Mozilla, Opera Safari, Firefox, Google Chrome e entre outros em diferentes momentos.

2.2 IMPLEMENTAÇÃO DA INTERNET NO BRASIL

Neste tópico apresenta-se os marcos históricos de desenvolvimento e implementação da Internet no Brasil. O Brasil, sendo o maior país da América do Sul e da América Latina, possui vários pontos para investimento no acesso à Internet em todo território. No período da Guerra Fria as influências ideológicas da União Soviética e dos Estados Unidos expandiram pelo mundo, sobretudo, no Sul Global, onde o Estado brasileiro se alinhou ao bloco capitalista, ou seja, o Brasil se aproximou dos Estados Unidos no conflito entre as superpotências. Tendo em vista o surgimento da Internet no território estadunidense e a sua liberação para uso comercial em outros países, estudos apontam que, na década de 1970, já havia no Brasil um projeto da Rede Sul de Teleprocessamento (RST), criada pela Associação das Universidades do Rio Grande do Sul (ADURGS). Esse projeto objetivava compartilhar os recursos das instituições que possuíam computadores, de modo que permitisse o acesso das outras instituições mesmo sem computadores via terminais remotos. Entretanto, esse projeto não teve êxito na sua implementação devido ao alto custo de conectar à ARPANET/Internet mundial. Ao longo do tempo, foram pensadas diversas formas de desenvolver as ferramentas técnicas que permitissem a conexão da Internet no país, mas todos os projetos criados tiveram dificuldades na sua implementação pelo fato de haver inicialmente poucos recursos investidos na área. De todo modo, havia uma intenção por parte do Governo Brasileiro de desenvolver a sua própria rede. Sendo assim:

> No final do ano de 1979, foi criado o Laboratório Nacional de Redes de Computadores (LARC) III uma entidade “virtual” que visava integrar os esforços institucionais na área de redes de computadores, gerar um know-how de âmbito nacional nesta área, promover o intercâmbio de software e informação científica, através da integração de laboratórios de computação das instituições participantes. Alguns dos trabalhos mais importantes realizados por seus membros foram na área de redes locais de alto desempenho, especialmente na UFRJ e na PUC/RJ. (CARVALHO, 2006, p.74)

Já na década de 1980, a Internet ganhou estrutura no território brasileiro, mais concretamente em 1989 por meio de *backbone*[3] da Rede Nacional de Pesquisa (RNP) criada pelo Ministério da Ciência e Tecnologia (MCT). Seu objetivo era construir uma infraestrutura nacional de rede de Internet também no âmbito acadêmico. A RNP tinha função de disseminar o uso de redes no país. Em 1992 a rede foi complementada a custo dos recursos das fundações estaduais de amparo à pesquisa (LINS, 2013). Posteriormente, a sua estrutura básica teve apoio financeiro do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP).

A RNP contou com apoio da Embratel na construção da sua estrutura básica de tráfego de dados, que de certo modo configuraria a espinha dorsal da Internet brasileira. A rede começou a funcionar com um desempenho muito baixo entre capitais dos Estados do Brasil. Conforme atestam Lins e Carvalho:

> A partir dessa rede, três pontos de acesso ao exterior, mantidos pela Fapesp em São Paulo, pelo Laboratório Nacional de Computação Científica – LNCC no Rio de Janeiro e pela Universidade Federal do Rio Grande do Sul, este último de menor capacidade, garantiam a interconexão com provedores internacionais de tráfego (LINS, 2013, p.20).
>
> Inicialmente com circuitos de 9,6 Kbps interligando onze capitais e quatro circuitos de 64 Kbps entre São Paulo, Rio de Janeiro e também ao Rio Grande do Sul, o qual visava compartilhar o acesso ao primeiro Centro Nacional de Supercomputação, instalado na UFRGS. Assim como acontecera com a NSFNET nos Estados Unidos, os supercomputadores também reforçaram a importância de implantação de rede acadêmica nacional (CARVALHO, 2006, p.102).

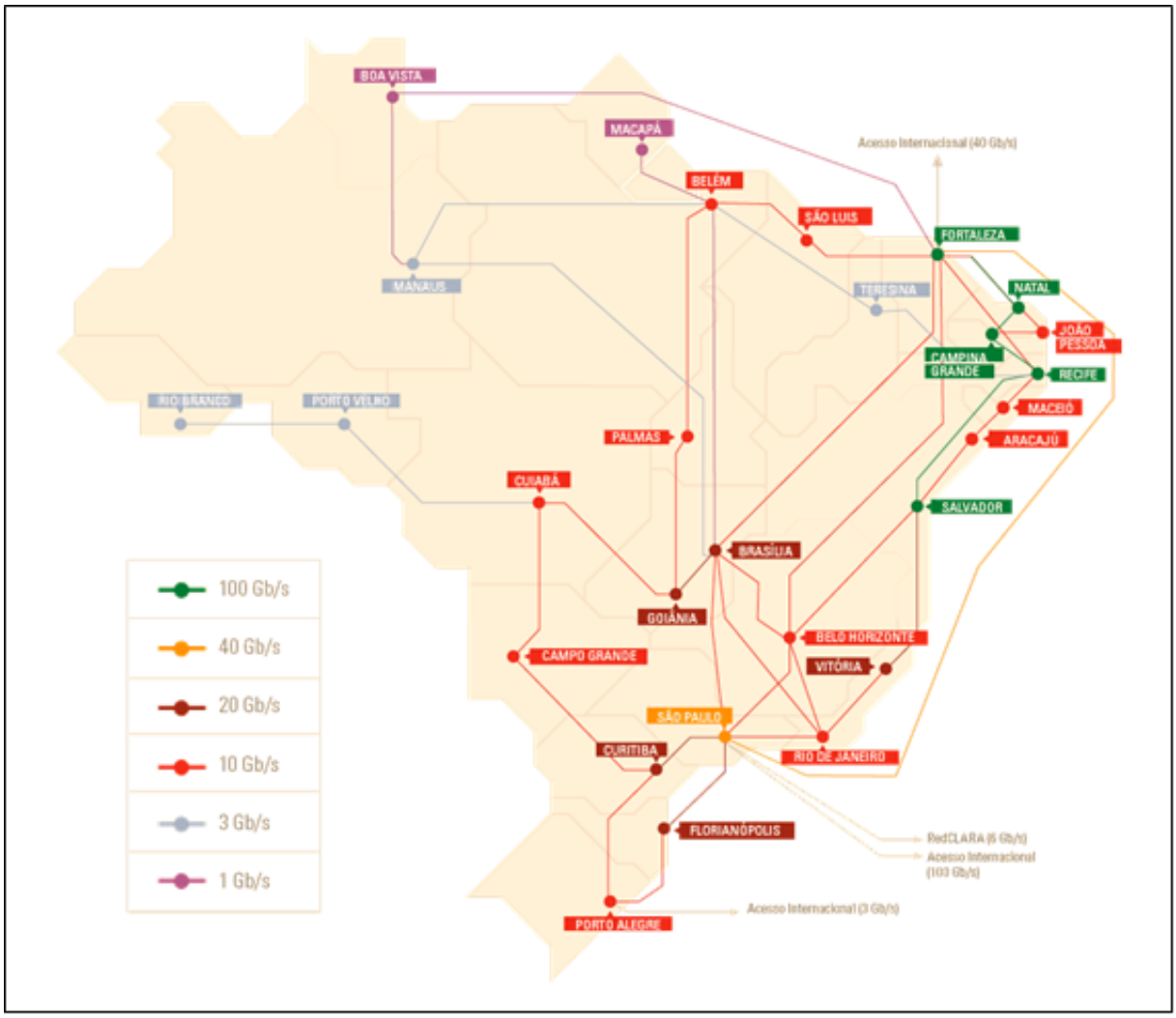
As capacidades da rede foram testadas nas universidades e correspondeu à expectativa. No entanto, a comunidade acadêmica sentiu a necessidade de avançar no tráfego de dados. Para alcançar tal objetivo, foi necessário adquirir supercomputadores com capacidade para processar operações que atendessem às demandas da época. Esse investimento serviria, ademais, de estímulo ao fomento das pesquisas a nível nacional e internacional a partir de grandes centros de processamento de dados remotos. Em 1993, a RNP ganhou um impulso com o acordo

[3] *Backbone* é uma palavra de origem inglesa que significa espinha dorsal. Nesse contexto se refere à espinha dorsal da Internet por ter a função de identificar a rede por onde passa os dados de cada usuário e possibilitar o envio e recebimento das informações de um servidor para o outro. Ou seja, todo acesso é encaminhado para a central da rede a fim de receber um aval do conteúdo solicitado. Grosso modo, *backbone* além da referida função, serve para manter o controle dos sites. Mais informações disponíveis em: https://www.rnp.br/sobre/nossa-historia.

de cooperação técnica e tecnológica assinado pelo CNPq, a Agência Brasileira de Cooperação (ABC) e o Programa das Nações Unidas para o Desenvolvimento (PNUD). Essas três instituições tiveram aporte financeiro de 27 milhões de dólares num convênio que durou oito anos. Com a garantia de suporte financeiro, a RNP ampliou o desenvolvimento nos anos seguintes (CARVALHO, 2006; LINS, 2013). Da mesma maneira que nos Estados Unidos, a Internet passou a ser utilizada para fins comerciais, expandindo seu alcance a partir de 1994, deixando de ser utilizada somente para propósitos acadêmicos. A partir do momento em que a rede foi liberada para o uso comercial, começaram a surgir outros *backbones* privados que permitem enviar e receber tráfego da rede nacional.

Em virtude dos dados analisados, é importante frisar que a RNP continua desenvolvendo mecanismos para o avanço tecnológico no Brasil por meio de aprimoramento da rede. Atualmente, a Rede Nacional de Ensino e Pesquisa possui um ecossistema que conecta 800 organizações, com mais de quatro milhões de usuários, 50 redes comunitárias e mais de 100GB/s, isto é, uma velocidade muito avançada nas transmissões de dados em relação ao anterior. Outrossim, diversas instituições tais como instituições de educação superior e pesquisa, agências de fomento à pesquisa, museus e instituições culturais, empresas inovadoras, estabelecimentos de saúde com ensino e pesquisa e ambientes promotores de inovação (parques e polos tecnológicos) estão conectados à rede (RNP, 2019). **A figura 2** ilustra o avanço da rede nacional.

Figura 2 - Rede Ipê[4], conexão 2019



Fonte: RNP (Rede Nacional de Pesquisa), 2019.

Considerando a velocidade da Internet utilizada em 1992, quando os dados eram transmitidos a 64kbps/s em algumas partes do território nacional, atualmente verifica-se o aumento de pontos de acesso com maior capacidade agregada em todo país. Além dessas conexões nacionais, foram criadas estratégias para conexões internacionais, com destaque para duas redes que permitem o avanço das pesquisas: 1. A Cooperação Latino Americano de Redes (RedCLARA) dentro da rede Ipê de modo que o Brasil conecta os demais países da região; e a rede Géant, ampliando a sua conexão com os países europeus. Particularmente, a Rede Nacional de Pesquisa

[4] A Rede Ipê é uma rede acadêmica brasileira que fornece acesso à internet em todo território brasileiro. Segundo RNP (2019), a infraestrutura da rede Ipê engloba 27 Pontos de Presença (PoPs), um em cada unidade da federação, além de ramificações para atender 1522 campi e unidades de instituições de ensino, pesquisa e saúde em todo o país, beneficiando mais de 3,5 milhões de usuários.

na cooperação com *Amlight*[5] e a *Academic Network at São Paulo*[6] (ANSP) responde pela conectividade internacional entre Brasil e os Estados Unidos. As conexões ocorrem por meio de acesso às redes acadêmicas estadunidenses, sobretudo, à internet2, a outras redes acadêmicas internacionais e à Internet comercial mundial. As conexões entre os referidos países transmitem cerca de 240GB/s (RNP, 2019).

2.3 A SOCIEDADE DA INFORMAÇÃO NO BRASIL NO SÉCULO XXI

Os meios de comunicação e equipamentos eletrônicos criados nas décadas passadas transmitiam informações limitadas, restringindo acessibilidade. No Brasil, a sociedade da informação ganhou impulso na sua formação com a chegada da Internet na década de 1990 e, na medida em que novas tecnologias foram desenvolvidas, a sociedade passou a produzir e adquirir mais informação. No século XXI, verificam-se diversos pontos de acesso à internet no país possibilitando comunicação social, institucional e empresarial em tempo real. Hoje há uma dependência da internet bastante considerável a nível nacional e fomenta cada vez mais o uso da mesma na sociedade.

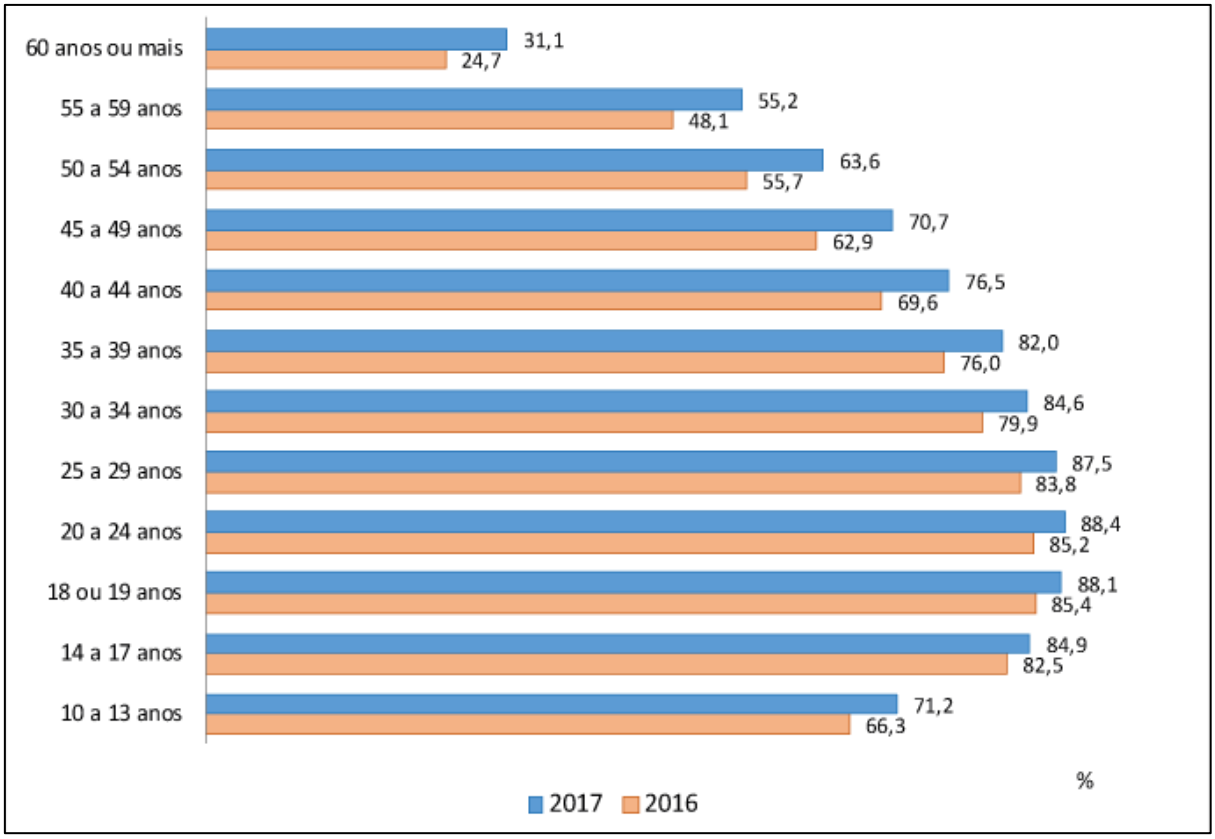
Segundo a última informação da Pesquisa Nacional por Amostra de Domicílios contínua (PNAD) sobre Tecnologia de Informação e Comunicação (TIC) (IBGE, 2018), demostra que o acesso à internet, à televisão e posse de telefone móvel celular para uso pessoal aumentou de 69,3% para 74,9% entre 2016 e 2017. A proporção de domicílios com telefone fixo caiu de 33,6% para 31,5%, enquanto a presença do celular aumentou, passando de 92,6% para 93,2% dos domicílios (IBGE, 2018). O **gráfico 1** representa uso da Internet por faixa etária no ano 2016 e 2017.

---

[5] O *LightPaths Express e Protect das Américas* (AmLight ExP) é um projeto de redes de Internet norte-americana que tem por objetivo desenvolver conexão de pesquisa e educação entre povo das Américas. A empresa fornece conectividade de cabo submarino entre Miami, FL e Fortaleza e São Paulo, Brasil, além de Santiago, Chile, para fins de pesquisa e educação. Desde abril de 2016 o *LightPaths* procurou manter a conectividade para promover seus objetivos educacionais e de pesquisa, para promover o desenvolvimento de aplicativos, conteúdos e serviços avançados de rede entre os EUA e a América Latina. A equipe de rede desenvolveu pesquisa na ativação de um segundo link 100G, passando pela rota do Pacífico. Depois disso, a equipe estabelecerá um link 100G com Fortaleza, Brasil.

[6] É um Projeto de apoio à pesquisa no Estado de São Paulo que pretende fornece conectividade de rede de computadores de última geração à comunidade acadêmica. O projeto foi criado junto a Conselho de Administração da FAPESP desde 1988. A ANSP é responsável pelo acesso das instituições de educação e pesquisa paulistas à Internet. De acordo com seu objetivo principal, os pesquisadores de universidade e centros de pesquisa do Estado de São Paulo necessita de um provedor de conectividade que possa oferecer serviço de qualidade nas diversas áreas de pesquisa.

Gráfico 1 - Utilização de Internet por pessoas, ano 2016 e 2017



Fonte: IBGE (2018).

O gráfico 1 representa percentagem de usuário de internet no Brasil por idade compreendida entre 10 a 60 ou mais no ano de 2016 e 2017. Consoante o IBGE (2018), entre 181,1 milhões de pessoas com 10 anos ou mais de idade no Brasil, 69,8% acessaram a internet pelo menos uma vez nos três meses anteriores à pesquisa. Em números absolutos, esse contingente passou de 116,1 milhões para 126,3 milhões, no período. O maior percentual foi no grupo etário de 20 a 24 anos (88,4%). Já a proporção dos idosos (60 anos ou mais) que acessaram a Internet subiu de 24,7% (2016) para 31,1% (2017) e mostrou o maior aumento proporcional (25,9%) entre os grupos etários analisados pela pesquisa.

Além do uso da Internet por pessoa, várias instituições brasileiras dependem e utilizam desse meio para execução das atividades do quotidiano. Consequentemente, tornam-se comuns diversos serviços das instituições políticas ficarem indisponíveis quando ocorrem falhas na conexão da internet, inviabilizando a oferta de serviços.

No que tange à dimensão política, os recursos digitais aumentam a potencialidade de comunicação nos Estados democráticos, tendo em vista a aquisição de diferentes plataformas digitais disponíveis para atendimento das demandas públicas. Nesse

sentido, vale mencionar alguns dos marcos no contexto brasileiro, nomeadamente no âmbito do Poder Executivo. A primeira versão do Portal da Presidência da República Federativa do Brasil foi lançada em 1998, ainda no primeiro mandato do presidente Fernando Henrique Cardoso (FHC), oferecendo aos usuários a oportunidade de acessarem o conjunto de sites e páginas dos órgãos oficiais e que compõem a estrutura institucional sobre administração direta do chefe do Poder executivo Federal (MARQUES, 2010). Atualmente, a Secretaria de Comunicação Social da Presidência da República (SECOM) conta com 23 sites dos órgãos do governo federal (Casa Civil, Ministério da Justiça e Segurança Pública, Ministério da Defesa, Ministério das Relações Exteriores, Ministério da Economia, Ministério da Infraestrutura, Ministério da Agricultura, Pecuária e Abastecimento, Ministério da Educação, Ministério da Cidadania, Ministério da Saúde, Ministério de Minas e Energia, Ministério da Ciência, Tecnologia, Inovações e Comunicações, Ministério do Meio Ambiente, Ministério do Turismo, Ministério do Desenvolvimento Regional, Controladoria-Geral da União, Ministério da Mulher, da Família e dos Direitos Humanos, Secretária-geral, Secretaria de Governo, Gabinete de Segurança Institucional, Advocacia-Geral da União, Banco Central do Brasil e Planalto), cada um deles voltado para o provimento de notícias e de informações sobre atribuições, competências e mecanismo de contato atinente às referidas entidades (BRASIL, 2019). Vale apontar que esses sites contêm suas ramificações conforme a dinâmica dos setores.

Por outro lado, o Portal Governo do Brasil possui um projeto de unificação dos canais digitais do governo federal com intuito de estabelecer a relação do cidadão com o Estado. No entanto, este projeto busca atualizar uma nova versão (versão beta) do site gov.br até dezembro de 2020 para reunir serviços e informações de todas as áreas de atuação do governo (BRASIL, 2019).

Ademais, diversos setores econômicos apresentam ampla dependência da Internet. Diversas empresas no Brasil prestam serviços por meio de plataforma digital, sendo os setores comerciais e financeiros altamente dependentes da internet. Por exemplo, os bancos desenvolvem aplicativos para dispositivos móveis nos quais oferecem vários serviços ligados à web. Da mesma forma as empresas de transportes (ônibus, Uber, companhia áreas e etc.) estão cada vez mais dependentes da internet para seus funcionamentos. Há ainda o marketing das lojas virtuais nas redes sociais, responsável pela troca de informação frequentemente. Finalmente, a criação dos sites de compras e vendas também demostra dependência da Internet.

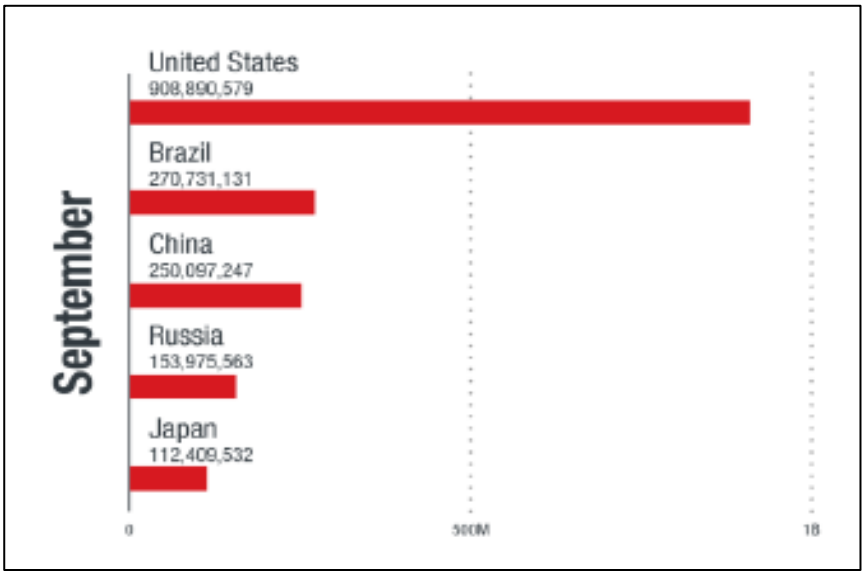
Neste cenário, a sociedade da informação no Brasil no século XXI tende a crescer, haja vista inúmeras atividades desenvolvidas por meio de novas tecnologias. Na medida em que avanços das TICs procedem, emergem vários fenômenos, tais como: (a) elevada convergência tecnológica; (b) aumento significativo de sistemas e redes de informação, como a interconexão e interdependência dos mesmos; (c) aumento crescente e bastante substantivo de acesso à Internet e das redes sociais; (d) ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças (BRASIL, 2010).

Da mesma forma que estas possibilidades de uso da internet e a complexidade dos espaços virtuais se aprofundam e operam para melhorar a vida da população, desenvolvem-se, outrossim, formas de ameaça à informação, os chamados ataques cibernéticos. A nível mundial, a sociedade da informação enfrenta novos desafios relacionados à segurança cibernética: a integridade, a confidencialidade e a autenticidade da informação (CANONGIA; MANDARINO, 2009).

Pelos eventos ocorridos no país a respeito de ataques cibernéticos no presente século, especialmente no âmbito do amplo espectro de competências da administração pública federal, encontra-se um dos casos mais recentes da Lava Jato no qual envolve vazamento de áudio do atual Ministro da Justiça e Segurança Pública, Sérgio Fernando Moro com jurista Deltan Martinazzo Dallagnol. Os celulares deles e demais autoridades foram hackeados com objetivo de verificar suposta parcialidade no julgamento do ex-presidente Luiz Inácio Lula da Silva acusado de praticar crime de corrupção. O ataque digital foi realizado por meio do *Telegram* e denominado pela Policia Federal de operação *spoofing*, para referenciar a uma técnica de ataque cibernético comum que frauda a identidade de um aparelho ou conta, usada, por exemplo, para interceptar dados bancários ou mensagens pessoais (PIMENTEL, 2019). O chamado "*caller ID spoofing*" funciona com um chip qualquer onde um usuário consegue simular ter o celular da vítima. É uma espécie de imitação da linha telefônica, não é exatamente uma invasão ao aparelho ou aos servidores do *Telegram*. Da forma análoga, os celulares do presidente Jair Messias Bolsonaro, também, foram supostamente atacados por mesmo grupo de hackers acusado de cometer crimes cibernéticos contra as autoridades supracitadas. Esses atentados a agentes estatais na obtenção das informações sigilosas do Estado brasileiro demostram vulnerabilidade no sistema de informação e ameaça à segurança nacional (BERTONI, 2019).

Ademais, o Brasil é classificado como segundo país com maior número de ameaça de e-mail em setembro de 2018. Segundo o **gráfico 2** da Trend Micro[7] mais de 270 milhões de e-mail bloqueados. (TREND MICRO, 2018).

Gráfico 2 - Relatório da Trend Micro, setembro, 2018



Fonte: Trend Micro, 2018.

Nesse contexto, percebe-se a necessidade de se pensarem as estratégias para lidar com as vulnerabilidades e ameaças crescentes na sociedade da informação brasileira, visto que elas colocam em xeque a segurança nacional (LEAL, 2015). Em função do gradativo crescimento das relações econômicas e com o incremento da globalização, uma nova espécie de crime se despontou como sendo um ilícito sem fronteiras geográficas e que estava fora do domínio legislativo do Estado. Emerge, portanto, o campo da segurança cibernética, sobre o qual me debruço no capítulo seguinte.

[7] A Trend Micro "*Smart Protection Network*" é uma empresa multinacional japonesa de segurança cibernética Co-fundada por Steve Chang, Jennyg Chang e Eva Chen em 1988. A principal função da empresa é desenvolver softwares antivírus para defesa de rede das pequenas empresas. Além de oferecer segurança de nuvem hibrida, a Treand Micro analisa comportamento do usuário por meio da infraestrutura de TI, de troca de informações digitais inovadoras.

3 VULNERABILIDADE E ESTRATÉGIA DE SEGURANÇA CIBERNÉTICA

O mundo virtual apresenta-se como um cenário crítico em relação às vulnerabilidades dos sistemas cibernéticos. Essas vulnerabilidades dependem dos *hardwares* e *softwares* utilizados para o desenvolvimento das atividades das organizações governamentais e não-governamentais; dos serviços das empresas ou das instituições, tanto públicas como privadas; e até mesmo pela navegação do usuário comum que esteja conectado a uma rede de internet. Nesse sentido, ainda que sejam desenvolvidas diversas ferramentas para proteger os dados armazenados no sistema, atualmente, verificam-se diversos casos de acesso a conjuntos de informações que por vezes são resultado de falhas de segurança. Além das entidades mencionadas, as indústrias são bastante prejudicadas com ataques cibernéticos, por possuírem informações que contêm alto valor no mercado, seja ele legal ou ilegal. Nesse capítulo, abordo os conceitos fundamentais associados à vulnerabilidade cibernética, apontando as discussões referentes à dimensão política da informação no Brasil, assim como às novas tecnologias de segurança cibernética.

3.1 CONCEITOS FUNDAMENTAIS

O acesso universal da Internet produziu um novo léxico conceitual para tratar dos desenvolvimentos tecnológicos. Inicialmente, na década de 1940, o matemático Norbert Wiener publicou livros sobre o controle e a comunicação entre animais e máquinas. Essas publicações resultaram de pesquisa intensa que envolvia estudiosos de diversas áreas científicas e Wiener denominou esses estudos matemáticos de cibernética (KIM, 2004). Nesse sentido, Masaro argumenta:

> Pode-se chamar de cibernética uma determinada “ciência” – um conjunto de conceitos e fórmulas matemáticas – elaborada por um grupo de cientistas norte-americanos de especialidades diversas durante os anos 40 e primeira metade dos anos 50 [do século XX]. Duas espécies de conexões uniam estas pessoas – cuja formação de origem era a mais variada possível para a época, contando com representantes das três grandes “áreas” (ciências exatas, humanas e biológicas): a intuição de que descobertas recentes estavam provocando profundas mudanças nas bases da ciência ocidental, e um lugar no topo do complexo industrial-militar acadêmico norte-americano (seja na academia, seja em instituições privadas, filantrópicas ou empresariais, seja em órgãos governamentais civis e militares – ou, mais frequentemente, em trânsito por estas três formas de organização). (MASARO, 2010, P.32)

Nessa perspectiva, a cibernética é compreendida como a teoria das mensagens que ocorre pelas funções de controle e de processamento de informação de igual modo em máquinas e seres vivos, e certamente no mundo atual, a troca de mensagens e o processamento de informação ocorre com mais intensidade nas sociedades (KIM, 2004). No âmbito tecnológico, diversas máquinas – como computadores, celulares e entre outros – possuem linguagem que estabelece conexão entre si. O fluxo de informação que circula no sistema tecnológico apresenta duas formas principais de funcionamento. A primeira se encontra relacionada ao equipamento físico ligado à energia, permitindo funcionamento do circuito interno dos aparelhos, o que possibilita a segunda forma de trabalhar. Essa segunda etapa se refere ao funcionamento lógico do sistema, ou seja, à forma como os computadores "pensam", emitem informação, processam dados do sistema e realizam operações. Todo esse conhecimento denominado de cibernética foi desenvolvido como forma de compreender e controlar sistemas animados e inanimados (MASARO, 2010). Por essa razão, existem ferramentas que descrevem a linguagem técnica das máquinas proporcionando informação ao sistema. Finalmente, os estudos cibernéticos surgem na academia como meio de analisar informações emitidas pelos aparelhos tecnológicos. O mesmo busca manter o controle das informações geradas pelos usuários. É importante notar que, por um lado, a cibernética se consolidou no plano científico como área de estudos e influenciou de forma determinante a cultura moderna com resíduos de seus modelos explicativos, engendrando, junto com outros resíduos que são incessantemente produzidos pela tecnologia e ciência, o que poderíamos chamar hoje de "*cibercultura*" (KIM, 2004).

Tendo em vista a vulnerabilidade desses sistemas, a inquietação emerge no âmbito do controle das máquinas triviais que podem gerar ou permitir fluxos de informação não programados ou mal-intencionados. Devido à amplitude tecnológica, o estudo cibernético proporcionou novos conceitos com diferentes especificidades. A "*cibercultura*" apresenta certas noções provenientes do discurso técnico e científico que possibilita a interação de um mundo sem fronteira no que diz respeito às informações. Além do conceito supracitado, atualmente verificam-se diversos outros conceitos relacionados à cibernética. Nesse sentido, Massaro argumenta que:

> Não somente a cibernética penetrou nossa linguagem – e continua a orientar a forma de vocábulos novos – como penetrou no imaginário de nossas sociedades capitalistas. Assim, a literatura e o cinema vivenciaram, a partir

> dos anos 40, uma explosão de cyber-temáticas e de cyber-criaturas, como a ameaça das máquinas inteligentes (HAL- 9000) e dos *ciborgues*, organismos cibernéticos feitos da fusão de corpo animal e máquina. (MASARO, 2010, p.29)

Diante dessa afirmação, encontram-se nomenclaturas tais como: cybercafé, *cyberarte*, ciberespaço, cyber-terrorismo, crimes eletrônicos designados de *cybercrimes, cyber-squatting* (registro de domínio na internet), *cyberpunk, ciborgue* (*cyberg – cybernetic* organismo) dinheiro eletrônico (*cybercash*)*, cyber-bullying* (comunicação de um indivíduo ou um grupo através de acesso remoto via internet, celulares, computadores) *feedback, loop,* controle, *cyberataque*, cyber defesa, *cybersegurança* e entre outros conceitos relacionados à temática (ALCÂNTARA, 2018; MASARO, 2010; KREIBICH, 2016, VINHA 2014). Pode-se afirmar que o espaço cibernético ou ciberespaço impulsionou a difusão dos demais conceitos como a SegCiber, dado a formação desse novo campo, os Estados buscam manter o domínio de modo que efetive seus poderes.

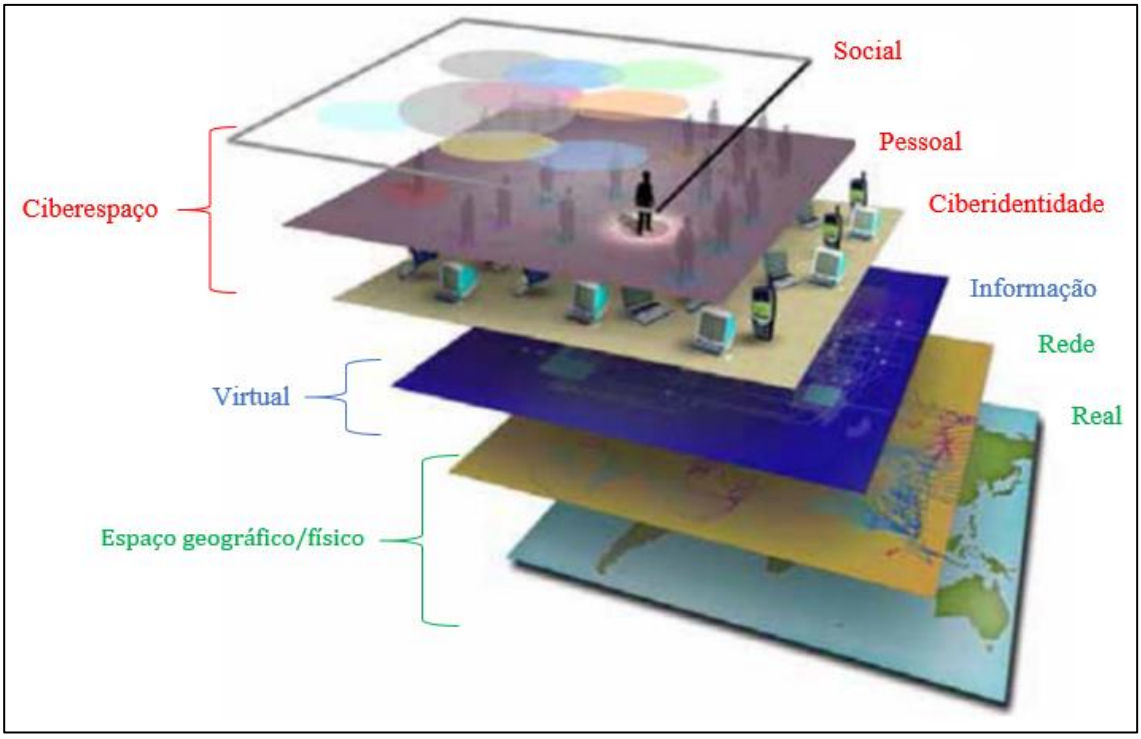
A literatura apresenta diferentes conceitos de ciberespaço, porém, nota-se conexão entre si e torna nítida a compreensão sobre o termo. Em primeiro lugar, ciberespaço está intimamente ligado a um conjunto de redes de informação e equipamentos físicos, assim formando comunidades imaginadas[8] que atravessam o meio geográfico. Outras partes do ciberespaço são redes transacionais que realizam diversas operações, como enviar dados sobre fluxos de dinheiro, negociações na bolsa e transações com cartão de crédito. Algumas redes são sistemas de controle que apenas permitem que as máquinas se comuniquem com outras, como painéis de controle conversando com bombas, elevadores e geradores (CLARKE; KNAKE, 2010; VINHAS, 2014). Por outro lado, ciberespaço (ou espaço cibernético) é considerado como a metáfora que descreve o espaço não físico criado por redes de computador, notadamente a internet, onde as pessoas podem se comunicar de diferentes maneiras, como mensagens eletrônicas, salas de bate-papo, grupos de discussão, dentre outros (CANONGIA; MANDARINO, 2009, p. 25).

De modo genérico, ciberespaço é conceituado como mundo virtual, pelo fato de pessoas estarem sempre presente nele. Contudo há grande debate na literatura sobre

[8] As Comunidades imaginadas, aqui, se referem a um conjunto de endereços eletrônicos que forma sociedade virtual no ciberespaço. No contexto internacional é um fenômeno do nacionalismo que ultrapassa a comunidade real, ou seja, a delimitação geográfica é imaginada. Ver Benedict Anderson (2008).

o assunto devido a sua invisibilidade física, ou seja, é um espaço desterritorializado geograficamente e bastante complexo de delimitar nos tratados internacionais como algo de pertencimento para cada Estado. Apesar desta limitação intrínseca, no sistema penal internacional existe cooperação no combate a crimes cibernéticos, inclusive com punições transnacionais (LOPES, 2016). No ambiente doméstico, cada país, em sua estrutura política, determina sua compreensão do ciberespaço. Como forma de visualizar a complexidade deste espaço tão idiossincrático, a **figura 3** ilustra a forma do funcionamento do ciberespaço a nível global.

Figura 3 - Estrutura do ciberespaço



Fonte: Adaptado de Santos (2017, p. 16).

Essa representação do ciberespaço em seis camadas é dependente entre si, o espaço geográfico/físico é de suma importância para o desenvolvimento das outras camadas. Nele são montados os equipamentos materiais que permitem o avanço para os demais processos. A rede funciona a parte da instalação dos equipamentos no espaço físico movido pela internet, desse modo, gerando a outra fase que é o espaço virtual no qual circula informação. Por fim, o ciberespaço abarca a ciberidentidade – identidade virtual tanto dos aparelhos como celulares e computadores e dentre outros – como dos usuários denominados na estrutura por pessoas. Nesse sentido, forma a

camada social que contempla diversas atividades como um todo. Por essa razão, percebe-se a presença humana em todas as esferas cibernéticas.

Por ser um espaço onde circulam várias informações de interesse individual, coletivo e estatal, os Estados buscam manter o domínio do ciberespaço. Hoje em dia diversas pautas dos debates sobre segurança nacional, SegCiber, estudos estratégicos encontram-se mesclados ao conceito de ciberespaço. Isso inclui a Internet, além de muitas outras redes de computadores que não deveriam estar acessíveis pela Internet. Algumas dessas redes privadas se parecem com a Internet, mas são, pelo menos teoricamente, separadas (CLARKE; KNAKE, 2010). Todavia, nasce o termo SegCiber que permite construir mecanismos de controle da infraestrutura crítica de cada Estado, proteção dos usuários, das empresas públicas e privadas.

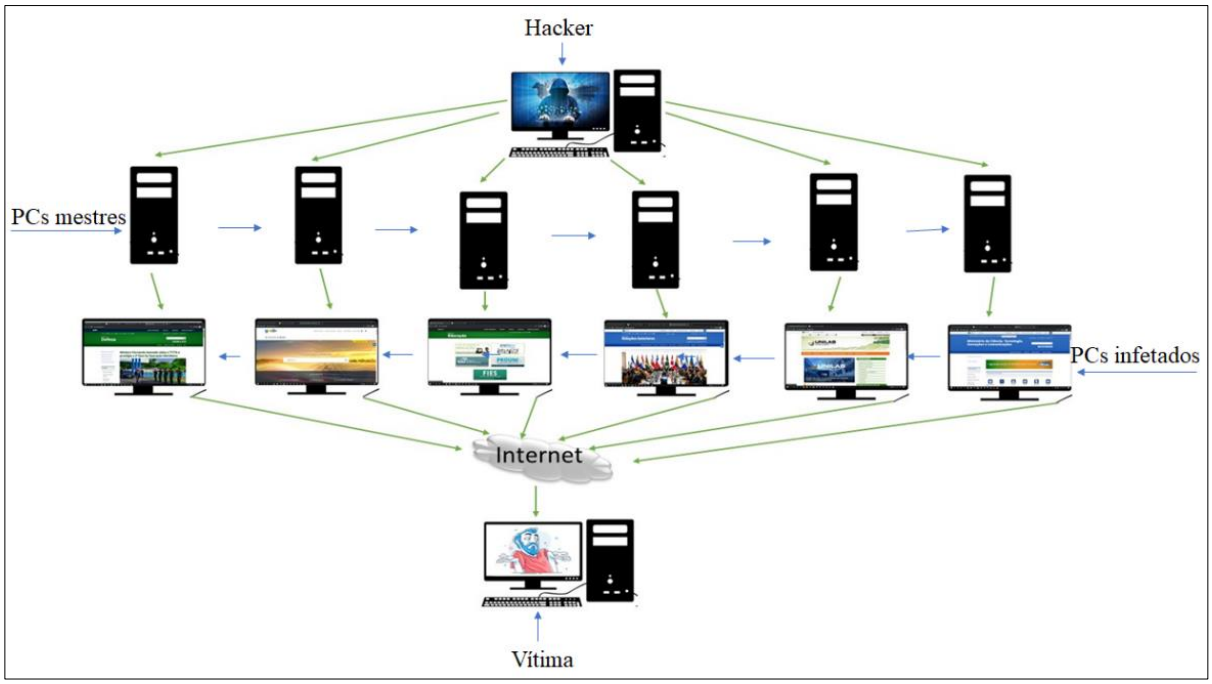
A SegCiber (ou cibersegurança ou, ainda, *cyber security*) e defesa cibernética (ou ciberdefesa, ou ainda, *cyber defense*) foram termos que ganharam destaque ao longo da trajetória da Internet como transporte da informação (SOUZA; MEDEIROS, 2011). Contudo, o termo segurança cibernético é preferencialmente utilizado ao longo desse estudo. No contexto da segurança online, a SegCiber pode ser uma forma simples de proteção privada contra spam ou outros *malwares* distribuídos na Internet. Também poderia significar a proteção dos membros da família (por exemplo, crianças) de acessar conteúdo da web indesejado (OPPERMANN, 2010). Apesar de o conceito estar associado à segurança de informação, percebe-se uma difusão conceitual em relação a diversos órgãos internacionais. Por essa razão, a SegCiber na perspectiva da União Internacional das Comunicações (ITU - sigla inglês) da Organização das Nações Unidas (ONU), envolve questões estratégicas, técnicas, legais, políticas e de segurança que englobam ações, treinamentos para proteção da propriedade dos usuários, quanto à propriedade das organizações, inclusive dispositivos de computadores conectados, aplicativos, serviços etc. (ITU, 2019). Deste modo, o ambiente cibernético torna-se cada vez mais difuso devido à amplitude das ameaças e riscos, sobretudo nas questões da economia mundial.

No cenário brasileiro a segurança cibernética é definida pela Administração Pública Federal (APF) como “a arte de assegurar a existência e a continuidade da sociedade da informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas” (BRASIL, 2015). Vale salientar que existem tipos de segurança considerados positivos – quando há

oportunidade de articular as ameaças com outros atores e a capacidade de determinar meios de finalizar, mitigar ou adaptar-se a esses riscos e ameaças, seja de maneira individual ou em coletivo – e por outro lado, a segurança vista de forma negativa – quando indivíduos e/ou múltiplos atores têm liberdade de identificar riscos e ameaças a seu bem-estar e valores (GURJOV, 2012). Outros conceitos associados a temática de segurança cibernética brasileira encontram-se na diferença entre o termo segurança e defesa. Do ponto de vista do Brasil (2010), a diferença entre segurança e defesa cibernética é que o primeiro termo compreende aspectos e atitudes, tanto de prevenção quanto de repressão, e o segundo termo abrange ações operacionais de combates ofensivos. Portanto, entende-se por SegCiber uso de ferramentas técnicas, políticas ofensivas e defensivas de informações e de sistemas de informações para negar, explorar, corromper ou destruir valores do adversário, baseado em informações, sistemas de informações e redes de computadores (JUNIOR, 2013).

Diante desses fatos, vale mencionar exemplos dos tipos de ataque ou crimes cibernéticos reconhecidos e que impulsionam a estratégia de SegCiber. Em primeiro lugar, menciono os ataques de negação de serviço tributada *Distributed Denial of Service* (DDoS). Esse ataque, além de acessar informações em computadores, tem por objetivo dificultar o fluxo de informações na rede a ponto de sobrecarregar a máquina, de modo que determinado sistema permanece desativado temporariamente. Essa fragmentação, porém, não é considerada uma invasão, vez que é controlada por um atacante ou hacker via computadores mestres que comandam milhares de computadores fantasmas ou afetados com funcionamento submisso, assim como elucida a **figura 4** abaixo.

Figura 4 - Demonstração de ataque DDOS



Fonte: Autoria própria.

Nesse caso, *hacker* é o sujeito atacante ou pessoa que quer acessar o sistema. Geralmente, este começa por realizar solicitações falsas de acesso a um computador ou a um servidor (PCs mestres) que gerenciam e controlam PCs fantasmas ou infectados para realizar ataques à vítima. Dentre essas solicitações estão às verdadeiras, realizada por usuários que almejam consumir conteúdo oferecido pelo site. Por outro lado, o sistema acaba sendo afetado por ações tendenciosas do *hacker*. Ademais, verifica-se o ataque conhecido por *botnet*, que consiste no controle de uma única autoridade sobre vários computadores. Esse ataque ocorre a partir da configuração de uma máquina de modo automático e autônomo no controle de vários computadores conectados à rede. Nas palavras de Oppermann (2010):

> Esse tipo de ataque DDoS baseado em *bot* redes são ataques virtuais comuns e podem ser executados por uma única pessoa. As redes de *bots* são oferecidas para contratar cibercriminosos. Criminais, ciberterroristas ou qualquer indivíduo a Internet. O contato entre fornecedor e locatário pode ser feito em vários fóruns na Internet. Os preços diferem de US $ 50 por dia para uma pequena *botnet* de até milhares de dólares para redes mais complexas. (OPPERMANN, 2010, p. 14)

É importante salientar que todas essas ações só são possíveis de serem executadas por procedimentos de um conjunto de máquinas conectadas entre si via

internet. Assim sendo, outro tipo de ataque a ser destacado é o *Stuxnet*. Em 2010 os Sistemas SCADA da Siemens recebeu um ataque cibernético com intuito de controlar e monitorar um processo industrial, e *Stuxnet* foi o nome dado ao *worm*, uma espécie de vírus (KREIBICH, 2016). Esse vírus foi desenhado para atingir um tipo de programa usado por um software (WinCC/PCS 7 SCADA) de controle da infraestrutura industrial da Siemens (ALCÂNTARA, 2018). Esse *worm* foi identificado pelos pesquisadores do *VirusBlokAda* (SANDRONI, 2013), porém a sua origem é desconhecida. O *Stuxnet* foi espalhado por diversos computadores do mundo, mas que operou apenas nas usinas nucleares do Irã (JÚNIOR, 2013). Evidencia-se a compra de uma centrifuga pelos Estados Unidos em 2003 semelhantes à iraniana, em 2008 foi desenvolvida uma atividade junto a Laboratório Nacional de Idaho e a Siemens para detectar a vulnerabilidade na instalação de sistemas de controle industriais (LEAL, 2015). Grosso modo, o *Stuxnet* permite reconhecimento de assinaturas digitais com chaves privadas das companhias e dos usuários comuns, além de poder operar em qualquer sistema operativo (Windows, Mac OS X). Como característica fundamental, esse *worm* tem a função de alterar e apagar dados nos sistemas. No caso da usina do Irã, o *Stuxnet* foi usado para gerenciamento das máquinas físicas, ou seja, alterou o funcionamento das centrífugas – forçando mudança de velocidade de rotação –, que causou destruição nos mesmos em Natanz. No entanto, vale apontar que as centrífugas são programadas pelos sistemas operacionais que podem ser afetados por vírus sem que estejam conectados à internet. Estudos apontam que *Stuxnet* invadiu por meio de um drive USB, assim, prejudicando os esforços nucleares iranianos.

Esses exemplos diferenciados de ataques cibernéticos demonstram a premência de se pensarem estratégias de SegCiber por parte dos Estados individualmente; e do sistema internacional em sua coletividade. Ademais, por se tratar de um risco à segurança nacional, é natural que os Estados “escondam” suas vulnerabilidades, bem como tornem confidenciais as informações sobre os instrumentos tecnológicos utilizados para enfrentar as ameaças cibernéticas. Diante deste novo cenário, faz-se mister compreender como as teorias de Relações Internacionais – nomeadamente, as da vertente realista – compreendem esses fenômenos.

3.2 TEORIAS DE RI E SEGCIBER

Após Segunda Grande Guerra Mundial, surgiram diversas teorias nos estudos de Relações Internacionais (RI) para explicar a segurança e a paz mundial, dentre elas, encontra-se a teoria realista, colocando o Estado no centro das discussões, ou seja, o Estado é o ator principal nos debates internacionais. Para os realistas, esse Estado deve ter poder absoluto que garanta a sua sobrevivência no sistema internacional. Diferentemente do poder coercitivo no cenário doméstico, na arena internacional os Estados buscam estratégias de segurança para impossibilitar ameaça a sua soberania (supremacia do poder, domínio da população, território e independência). “Num sistema internacional anárquico no qual prevalecem as relações de poder, a insegurança é um caractere perene e cada ator sofre ameaças em variáveis graus advindos do nível sistêmico” (ÁCACIO; SOUZA, 2012, p. 8). Nesse sentido, os realistas observam o tema de segurança com bastante relevante para manutenção do poder que permite seu reconhecimento como ator internacional.

O mundo bipolar da Guerra Fria foi marcado pela disputa de poder entre a União Soviética e Estados Unidos, em que essas superpotências realizaram corrida armamentista por meio do desenvolvimento tecnológico para produção de armas nucleares. Essa bipolaridade, defendida pelos neorrealistas, especialmente Kenneth Waltz (1979), encerrou-se com o colapso da superpotência soviética no começo dos anos 1990, inaugurando uma nova ordem internacional. Como consequência, a virada do século XX para XXI impulsionou novos debates sobre Segurança Internacional, especialmente ante a emergência de uma multipolaridade, com novos atores influentes nas tomadas de decisões global. Ademais, a agenda de segurança diversificou-se em termos temáticos e teóricos, frente ao desenvolvimento das potências regionais; as ameaças contemporâneas que excedem armamento; segurança militar que pelo responde conflito bélico; segurança econômica, ambiental, humana e, para os interesses deste trabalho, SegCiber (TANNO, 2003; ÁCACIO; SOUZA, 2012).

A agenda de Segurança Internacional (SI) moderna estabelece níveis de segurança que pode ser de alta ou baixa intensidade. Nesse sentido, a literatura define *hard security* como o aparelho militar para combater ameaças, enquanto que *soft security* corresponde aos aparatos utilizados pelos Estados para enfrentar as ameaças alternativas, ou seja, contra eventos de menores impacto (ÁVILA; SILVA,

2011) como por exemplo, imigração, identidades nacionais etc. Em relação ao evento cibernético, Ávila e Silva (2011) evidenciam a importância do tema no debate de *hard security*, tendo em vista sua potencialidade a nível mundial envolvendo diversos assuntos nacionais e internacionais de interesse estatal.

Dando importância à invenção da internet como estratégias de segurança utilizada durante a Guerra Fria na proteção das possíveis ameaças do outro, observa-se a sua sofisticação que gerou uma nova área de interesse dos Estados, isto é, o ciberespaço. Uma nova fase no sistema internacional de constante conflito desenvolve-se em torno da guerra cibernética (LEAL, 2015; JÚNIOR; LOPES; FREITAS, 2017; OPPERMANN, 2010). Espionagem, sabotagem e as guerras de informação são feitas a distância, sem a presença humana e com grandes danos para os Estados. Na medida em que novos avanços tecnológicos ocorrem, modificam o modo de interação entre usuários. As vulnerabilidades dos sistemas digitais geram preocupação com possíveis ameaças, sobretudo, nos estudos das Relações Internacionais quando se trata da responsabilidade dos Estados. Por essa razão, os conflitos cibernéticos e até mesmo a guerra cibernética tendem a produzir impactos com danos de grandes dimensões.

O tema de segurança tornou-se ainda mais relevante nos estudos de Relações Internacionais devido ao advento das novas ameaças. O medo de ser atacado incentiva a criação de mecanismos de defesa e ataque cibernético, e o acesso súbito do fluxo de informação no contexto da globalização mediante recursos tecnológicos reforça o estudo de segurança nas RI. Valeriano e Maness (2017) buscam compreender a importância de SegCiber como questão emergente no domínio da segurança, ou seja, como as tecnologias estão sendo aprimoradas pelos atores e como isto tem mudado as relações entre os Estados que almejam manter o domínio cibernético para manter outros Estados dependentes ou dominados. Embora alguns Estados criem políticas que regulamentam o uso da internet nos seus territórios, todos estão conectados na internet global, expondo, em dado grau, a infraestrutura crítica nacional. Não é por acaso que alguns países vêm desenvolvendo formas de se proteger desta exposição, como demonstram os exemplos da Rússia no

desenvolvimento da *RuNet*[9], da China ao criar *Great Firewall*[10] e, por fim, do Irã após sofrer o ataque *Stuxnet* criando meios de SegCiber.

Essas medidas de proteção adotadas pelos Estados no presente século ocorrem em função da segurança nacional. A vertente realista defende que no sistema anárquico cada Estado necessita de vigiar a sua própria segurança, isto é, adotar medidas políticas de defesa voltadas a seus interesses (ÁCACIO; SOUZA, 2012). Por outro lado, consoante a percepção realista, os países supracitados adquiriram domínio mediante desenvolvimento tecnológico que fomenta o equilíbrio de poder na questão cibernética a nível internacional. A premissa neorrealista busca complementar o argumento da teoria tradicional – qual seja, o realismo–, que focaliza no poder como fator mais importante nas relações entre os Estados. No debate ensejado a partir do neorrealismo, duas perspectivas realistas foram desenvolvidas no que tange às estratégias para lidar com o dilema de segurança dos Estados a nível estrutural: realismo ofensivo e realismo defensivo. O realismo ofensivo é apresentado por John Mearsheimer na sua obra intitulada *The Tragedy of Great Power Politics* (A Tragédia da Política das Grandes Potências) como teoria básica para explicar o comportamento do Estado: os Estados buscam estratégias ou táticas ofensivas de maximizar poder a ponto de alcançar hegemonia (MEARSHEIMER, 2001). De outro lado, o realismo defensivo é explicado por Kenneth Waltz na sua obra *Theory of International Politics* (Teoria Política Interacional), alegando que o mundo multipolar oferece várias possibilidades de risco e ameaças. O autor (Waltz, 1979) defende que os Estados mais fortes estão satisfeitos com o status quo. A acumulação de poder é um meio e não um fim, consequentemente, o Estado busca segurança para proteger sua economia, recursos tecnológicos e população; e para aumentar seu poderio e garantir a sua sobrevivência externa (WALTZ, 1979). Desse modo, enquadra-se SegCiber no dilema de segurança precisamente por existir falta de confiança no sistema internacional (SOUZA; ALMEIDA, 2016). Além dos Estados desenvolverem

[9]A *RuNet* é projeto de SegCiber russa aprovado pelo governo em maio de 2019 com objetivo de reforçar a segurança nacional de eventuais riscos e ameaça que fere infraestrutura crítica do País. Em dezembro do referido ano, a Rússia realizou teste bem-sucedida da Internet soberana no qual possui a função de: manter funcionamento de sites russos sem ligação a servidor exterior, ou seja, desconectado do *World Wide Web*; controlar conteúdos acessados pelos usuários no seu território e etc. Por outro lado, a *RuNet* foi preparada para identificar e responder possíveis ataques cibernética.

[10] *Great Firewall* é sistema de SegCiber chinesa que impede usuários de acessar sites não aprovados pelo governo. A denominação *Great Firewall* faz-se referência a Grande Muralha da China construída para proteger o País das invasões. Desse modo, o gigante asiático busca bloquear software e hardware que coloca em risco ou ameaça sua soberania.

suas capacidades autônomas de assegurar seus territórios, necessitam de poder que os mantenham equilibrados em relação a outros Estados. Quando se trata de SegCiber no sistema multipolar, há maior risco de advir conflito cibernético devido à complexidade deste fenômeno envolvendo novos atores nos debates de Relações Internacionais.

A Escola de Copenhague ou *Copenhagen Peace Research Institute* (COPRI) aborda temáticas na área de Segurança Internacional no pós-Guerra Fria tencionando debates acadêmicos para se pensar a paz no mundo (TANNO, 2003). No entanto, sem descartar as premissas do realismo tradicional, a escola desempenha papel importante ao delinear novas perspectiva da SI a partir de conceitos contextualizados. Autores como Barry Buzan e Waever propõem o desenvolvimento teórico no estudo de segurança para abarcar as ameaças oriundas dos principais setores (economico, político, social, ambiental, militar etc.) do Estado. Assim, pode-se considerar a SegCiber um tema relevante na abordagem da Escola Copenhague devido as suas características multifacedas. Nas palavras de Acácio e Souza (2012),

> O tema do ciberespaço não é, em específico, abordado por Buzan et alii (1998), mas deve-se ressaltar que, Nissenbaum (2005), Hansen e Nissenbaum (2009) e Hart (2011), bem como alguns outros autores na literatura internacional aplicam a teoria desenvolvida pela Escola de Copenhague ao setor cibernético, propondo, inclusive, que, dada a relevância que o tema segurança cibernética adquiriu na agenda de segurança internacional, a adoção de um Setor Cibernético, com próprias Unidades de Análise em Segurança e dinâmica própria de funcionamento, demonstrando que a literatura também caminha para a aplicação do instrumental da Escola de Copenhague à questão da segurança cibernética (ACÁCIO; SOUZA, 2012, p. 16).

Do ponto de vista desses teóricos, a temática SegCiber explica-se nas premissas da referida Escola, sobretudo no processo de securitização interpelado pelos discursos proferidos por atores empenhados em estabelecer as agendas de segurança. É importante frisar que esse processo passa, primeiramente, pela identificação ou reconhecimento social das ameaças à segurança, ou seja, por uma iniciativa da sociedade vinculada ao esforço dos agentes estatais a ser politizado. A politização ocorre quando o assunto é discutido como parte da política pública na seara doméstica do Estado. Comumente, a criação de leis voltadas ao tema emergencial simboliza outra faceta da politização conhecida por securitização. O **Quadro 1** abaixo ilustra as três categorias da teoria da Escola Copenhague. O processo de securitização divide-se em: não politizado, politizado e Securitizado.

Quadro 1 - Categorias da teoria da escola Compenhague

Categorias	Não politizado	Politizado	Securitizado
Caraterísticas	• Estado não lida com o tema; • Não há debate público; • Não tem decisão política.	• Contém política Pública; • Há decisões do governo sobre o tema; • Aplicação dos recursos.	• Existência de ameaça medidas de emergênci • Politização avançada; • Justificação de ações e enquadramento na agenda Política.

Fonte: Adaptado de Acácio; Souza, (2012, p16).

A securitização dos setores ocorre quando esses apresentam níveis avançados de risco ou ameaça à soberania do Estado. Por essa razão, o setor militar ganha destaque imprescindível com maior investimento para garantir a segurança tanto a nível nacional quanto internacional, precisamente por meio da força quando necessário (TANNO, 2003), assim como defende a premissa teórica realista. Nessa perspectiva, ao abordar a questão cibernética, frente às constantes ameaças cibernéticas, entende-se que a SegCiber contém relevância primordial para configurar no processo de securitização, conforme o qual os Estados desenvolvem políticas específicas de segurança. A teoria de securitização possui caraterística de inserção da SegCiber na análise da Segurança Internacional pela relação integrativa com diversos atores e setores estruturados por riscos e ameaças cibernéticas de interesse político (ALCÂNTARA, 2018; TANNO, 2003; VALERIANO; MANESS,2017). Desse modo, fomenta o debate da política internacional dando importância à natureza crítica da guerra cibernética, o que pode levar a cabo a securitização, por exemplo, da internet. Nesse sentido, o argumento dos autores da Escola de Copenhague (BUZAN; WAEVER; WILDE, 1998) mostra que todo tema de interesse público pode ser politizado ou não para securitização. Não obstante, atualmente vários Estados criam políticas de SegCiber pelo entendimento das vulnerabilidades existentes no ciberespaço, securitizando, por conseguinte, o espaço cibernético.

Destarte, o campo de SegCiber apresenta mudanças contínuas, interpondo desafios pertinentes aos estudos de RI. Sendo o ciberespaço um ambiente propício ao domínio de poder, os Estados buscam afirmar-se cada vez mais nesse espaço de múltiplas possibilidades de controle na esfera global. O poder tem sido um dos elementos primordiais no sentido de manter a sobrevivência dos Estados, todavia, as correntes teóricas, como realismo e Escola de Copenhague apoderam-se desse elemento para explicar as ações dos atores autônomos nas suas relações internacionais. Hoje em dia, o avanço tecnológico apresenta novos incitações elucidadas pelas rápidas mudanças, incluindo rupturas das fronteiras econômicas que potencializam ainda mais o envolvimento estratégico no domínio cibernético. Embora, nessa discussão a teoria realista e a contribuição da Escola de Copenhague corroborarem o ciberespaço como lugar de disputa de poder, a estratégia de SegCiber dispõe a tendência de constante análises nos estudos de Relações Internacionais, Política Internacional, especialmente, Estudo Estratégico da Segurança Internacional.

4 METODOLOGIA DE PESQUISA

A metodologia de pesquisa conduz o pesquisador na realização da investigação pretendida. Nesse caso, por meio de métodos científicos são demostrados procedimentos metodológicos descritivos em relação aos objetivos, à natureza da pesquisa, à escolha do objeto de estudo, à técnica de coleta e à técnica de análise de dados. Na perspectiva de Lakatos e Marconi (2003), o método é o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo da pesquisa, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista. Consoante os autores mencionados, o conhecimento científico se forma por meio da razão e de maneira metodologicamente rigorosa buscando excluir, do seu contexto, as emoções, as crenças religiosas e os desejos do homem. Por outras palavras, Gil (2008) define método como o caminho para se chegar a determinado fim e método científico como o conjunto de procedimentos intelectuais e técnicos adotados para se atingir o conhecimento. Vários outros autores conceituam método em diferentes pontos de vista, de modo a seguir o mesmo caminho (GERHARDT; SILVEIRA, 2009; GUERRA, 2014; MORESI, 2003; OLIVEIRA, 2011).

A escolha metodológica foi feita com base na categoria de classificação apresentada por Oliveira (2011), desse modo, a metodologia para este trabalho se encontra classificada da seguinte maneira:

- Referente ao objetivo trata-se de uma pesquisa descritiva;
- Quanto à natureza, zela pela pesquisa quantitativa;
- Em relação à escolha de objeto, sustenta-se no estudo de caso único;
- No que tange à técnica de coleta de dados, o estudo apoia-se na pesquisa documental;
- No que se refere à técnica de análise de dados, conta com a análise de conteúdo.

As categorias escolhidas demostram sua pertinência para este trabalho. Nesse sentido, importa detalhar a relevância das classificações mencionadas que contribuíram para o alcance da resposta da pesquisa.

A pesquisa descritiva é importante para responder os objetivos deste trabalho. Ela busca descrever um fenômeno ou situação em detalhe sem interferência do pesquisador. As frequências com que o fenômeno ocorre devem abranger as características que opera o processo ou a realidade (GIL, 2002).

A pesquisa quantitativa demostra caracterização da quantificação, ou seja, tudo que pode ser quantificável ou transformado em números tanto nas modalidades de coletas de informações quanto no tratamento de recursos (SILVA; MENEZES, 2005). Por essa razão, a pesquisa é de natureza quantitativa por requer o uso de estatística descritiva.

O estudo de caso único, na percepção de Yin, (2001) é uma investigação empírica investiga um fenômeno contemporâneo dentro de seu contexto da vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos. Desse modo, trata-se de um estudo de caso quando envolve o estudo profundo e exaustivo de um ou poucos objetos de maneira que se permita o seu amplo e detalhado conhecimento (GIL, 2002). A pesquisa documental possibilita uma coleta de dados em fontes primárias para análise (LAKATOS; MARCONI, 2003) quando elaborada a partir de materiais que não receberam tratamento analítico. Exemplo desses materiais são documentos oficiais escritos que pertencem aos arquivos públicos, arquivos particulares de instituições.

Por fim, não menos importante, a análise de conteúdo, consiste em desmontar a estrutura e os elementos de conteúdo para esclarecer suas diferentes características

e extrair sua significação. Essa técnica de análise permite enriquecer a leitura e ultrapassar as incertezas, extraindo conteúdos por trás da mensagem analisada (BARDIN, 1977). Além disso, seus principais objetivos são: descrever tendências no contexto das comunicações; comparar mensagens, níveis e meios de comunicação; medir a clareza das mensagens; identificar intenções, características e apelos de comunicadores. A análise de conteúdo abarca três etapas fundamentais para compreender os dados. A primeira é coletar e organizar os materiais para uma pré-análise. A segunda busca aprofundar no estudo do material e definir categorias que devem ser exaustivas e mutuamente excludentes, propondo uma descrição analítica. A terceira procura criar quadros de referências, ou seja, os conteúdos em torno da finalidade do estudo mediante interpretação inferencial (MARTINS; THEÓPHILO, 2009).

As três etapas fundamentais (pré-análise, descrição analítica e interpretação inferencial) foram aplicadas conforme a necessidade da pesquisa. Em relação à primeira etapa, foram organizados os materiais, selecionados três documentos oficiais (Livro Verde da Segurança Cibernética no Brasil, Estratégia de Segurança da Informação e Comunicações e de Ssegurança Cibernética da Administração Pública Federal e Guia Básico de Orientações ao Gestor em Segurança da Informação e Comunicações) a serem analisados para responder a pergunta de partida.

Na segunda etapa foi realizada a exploração minunciosa dos materiais e definida a unidade de análise relevante para este trabalho. Nessa perspectiva, foi escolhida “estratégias de SegCiber” como unidade de análise. Conforme Martins e Theóphilo (2009), a escolha das unidades de análises pode ser a palavra, o tema, a frase os símbolos e entre outros. Com base nesse argumento foram definidas categorias delineadas no **quadro 2** abaixa.

Quadro 2 - Catergoria e definição

Categoria	Definição
Vulnerabilidades Cibernéticas	Conjunto de um incidente indesejado, que resulta em risco para um sistema.
Normatização Técnica e Jurídica da SegCiber	Ação política que estabelece normas padrões de segurança cibernética.
Estratégias de Remediação	Técnica para restaurar ou neutralizar eventuais lacunas em determinado sistema.

Fonte: elaboração propria.

Neste trabalho utilizou-se a frequência das categorias como medida de contagem de aparição da unidade de análise. Martins e Theóphilo (2009) considera categorização um processo de tipo estruturalista que envolve duas etapas: o inventário (isolamento das unidades de análise) e a classificação das unidades comuns que releva as categorias de acordo com assunto ou tema em análises. Na mesma perspectiva, Bardin (1977) complementa a ideia de categorização sendo agrupamento em razão de caracteres comuns dos elementos (unidade de análise) sob um título geral.

Na terceira e última etapa, criaram-se quadros de referência que consistem na interpretação em função do propósito do estudo. Nesta etapa, a análise de conteúdo adquiriu força e valor mediante o apoio de referências teóricas (apresentadas no capítulo 3) que permitiram a construção das categorias de análise (MARTINS; THEÓPHILO, 2009). Conforme o propósito da análise de conteúdo, o trabalho buscou inferências confiáveis do contexto. As informações extraídas para o objetivo da referida análise evidenciaram não somente dados disponíveis como ampliou detalhes do contexto. Portanto, além da discrição dos conteúdos, as interpretações interpõem-se à inferência. O **quadro 3** demostra um exemplo de caracterização das Estratégias de SegCiber esquematizado por Código Doc. 1, 2 e 3 (Documentos oficiais abordados), Descrição, (Dados descritivos de análise) e categorias (Vulnerabilidades Cibernéticas, Normatização técnica e jurídica da SegCiber e Estratégias de remediação).

Quadro 3 - Exemplo de Estrat

Código	Descrição	Categorias
Doc1	Ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças.	Vulnerabilidades cibernéticas
Doc2	Regulamentação do Marco Civil da Internet, processo de regulamentação da Lei nº 12.965/2014, em andamento por meio de consultas públicas pelo Comitê Gestor da Internet e pelo Ministério da Justiça.	Normatização técnica e jurídica da SegCiber
Doc3	Identificar os cenários de riscos para os quais os planos de continuidade específicos devem ser desenvolvidos.	Estratégias de remediação

Fonte: Elaboração própria

A criação de quadro auxilia na análise e interpretação dos dados (BURDIN, 1977), contudo, no próximo capitulo apresenta-se, os dados absolutos das inferências que proporciona a interpretação e a estatística descritiva.

5 CARACTERIZAÇÃO DA ESTRATÉGIA DE SEGURANÇA CIBERNÉTICA DO BRASIL

Os Estados são caracterizados como atores soberanos no cenário doméstico, assim como no sistema internacional. A questão de segurança é fundamental para sobrevivência de qualquer Estado, e a carta da Organização das Nações Unidas (ONU) no artigo II, parágrafo I, reconhece igualdade soberana de todos Estados membros (ONU, 1948). Porém, existem diversos fatores que diferenciam os níveis do poder. Desse modo, Estados desenvolvem as suas estratégias de segurança em diferentes campos, sobretudo quando verifica ameaça de outro. Nesse contexto, busco caracterizar a estratégia de SegCiber brasileira a partir da estrutura de segurança nacional.

A estrutura do Brasil no setor da informática iniciou desde 1982, na altura em que foi criada a Agência Brasileira de Inteligência (ABIN) com o intuito de sanar as deficiências de segurança do país no que tange à garantia do sigilo dos canais de

comunicação, mormente dos órgãos estratégicos da Administração Pública Federal (BRASIL, 2015). Na década de 2000, o número de usuários começou a aumentar gradualmente, e desde essa época, o país busca criar mecanismos estratégicos para solucionar a ruptura de segurança da informação e comunicações com base em algoritmos criptográficos de Estado. Assim sendo, os temas relacionados a SegCiber foram reconhecidos por vários atores do Governo Federal, tais como o Ministério de Defesa, Indústria de Defesa, Ministério da Ciência e Tecnologia, Ministério de Educação e Forças Armadas. Nesse sentido, o Estado brasileiro tem demostrado interesse em desenvolver trabalhos de pesquisa sobre estratégias na área de SegCiber. À vista disso, encontram-se alguns marcos normativos pela importância concedido ao tema marcado pela complexidade e diversidade de atores.

A imprescindibilidade do avanço tecnológico e as novas configurações do sistema mundial geraram setores estratégicos para a defesa nacional. Desta feita, a Estratégia Nacional de Defesa (END) optou por desenvolver três setores prioritários – nuclear, espacial e cibernético – para atualizar a estrutura nacional de defesa. A gerência do programa nucelar encontra-se sob tutela da Marinha do Brasil; o programa espacial localiza-se sob responsabilidade da Forma Aérea; e, por fim, não menos importante, a defesa cibernética em território nacional está sob responsabilidade do Exército Brasileiro (BRASIL, 2019). Para responder as demandas do setor cibernético reconhecido como área importante no desenvolvimento de um Estado, o Exército criou, em 2011, o Centro de Defesa Cibernética (CDCiber), o qual fortalece a estratégia de proteger informações sigilosas do Estado e a suas infraestruturas críticas. Por outro lado, o ambiente cibernético brasileiro busca conferir sua importância em quatro eixo crucias, sendo: confidencialidade, disponibilidade, integridade e autenticidade envolvendo tráfico nas redes de comunicação, nos computadores e nos sistemas informatizados.

Feita esta introdução, faz-se mister apresentar e analisar os resultados da aplicação da análise de conteúdo aos três documentos que versam sobre as estratégias de SegCiber do Brasil. O objetivo fundamental desta análise consiste em caracterizar, por meio das três categorias estabelecidas no capítulo anterior, os entendimentos e as prioridades do conjunto de políticas e estratégias nessa área da segurança.

5.1 ANÁLISES DOS RESULTADOS

A realização de coleta de dados nos documentos oficiais teve por finalidade verificar como ocorrem as abordagens das questões cibernéticas no Brasil. De igual modo, objetiva extrair conteúdos que permitam responder à pergunta de pesquisa norteadora deste trabalho. Inicialmente, pretende-se aqui, apresentar os resultados dos dados coletados e em seguida, realizar uma relação desses resultados com o problema de pesquisa.

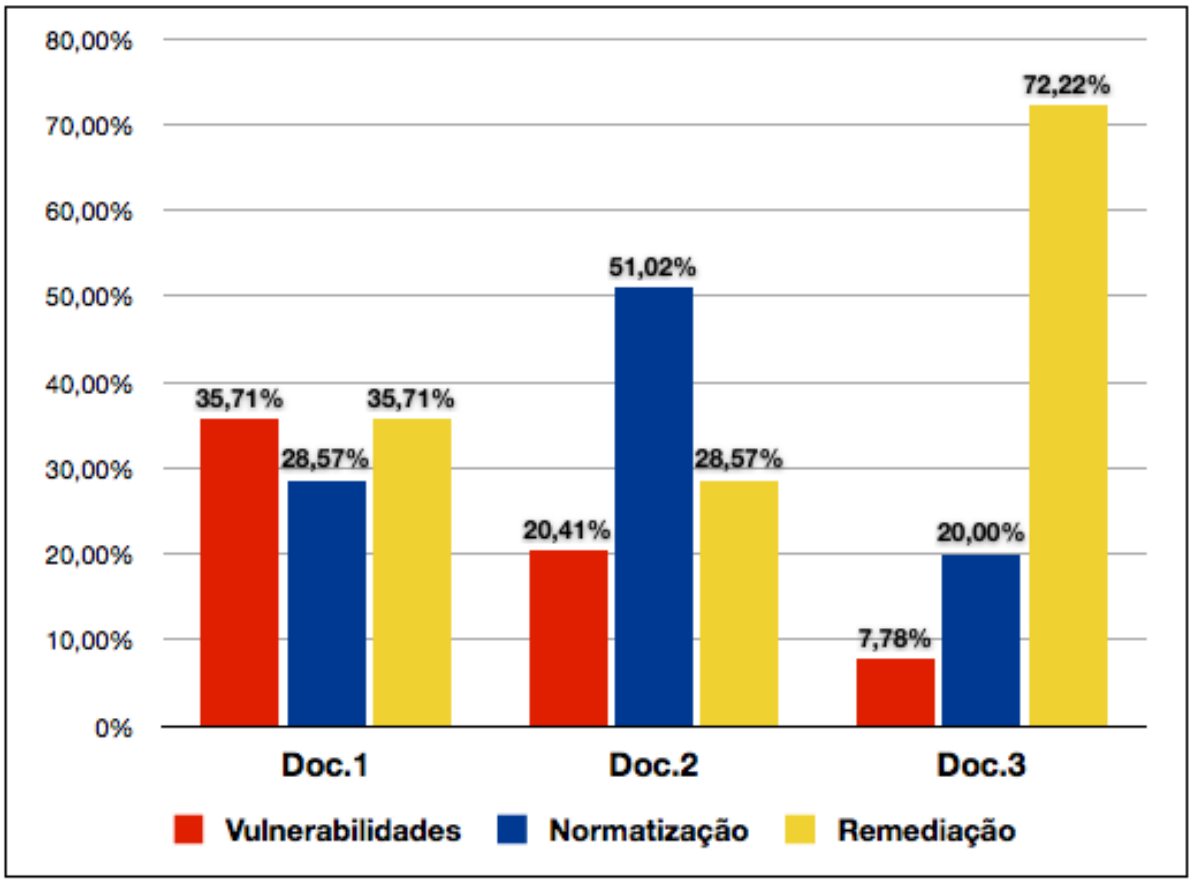
Primeiramente, apresenta-se na **tabela 1** os quantitativos absolutos das ocorrências de cada categoria nos três documentos. Para efeitos da análise, o total para cada documento representa a soma das categorias utilizadas neste trabalho, permitindo, assim, que se calculem as proporções vis-à-vis cada categoria.

Tabela 1 - Número absoluto de ocorrências das categorias

Categoria	Doc1	Doc2	Doc3
Vulnerabilidades cibernéticas	10	10	7
Normatização Técnica e Jurídica	8	25	18
Estratégias de Remediação	10	14	65
Total	28	49	90

Fonte: Elaboração própria. Observação: Doc1 = Livro Verde da Segurança Cibernética; Doc2 = Guia Básico de Orientações ao Gestor em Segurança da Informação e Comunicações; Doc3 =Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal.

Gráfico 3 - Número de ocorrência por DOC



Fonte: Elaboração própria.

O gráfico 3 representa número de ocorrência das categorias (vulnerabilidade, normatização e remediação) nos Doc. 1, 2 e 3. Desta forma, os dados analisados no Doc1 demostram a categoria vulnerabilidade com 35,71% de ocorrência, enquanto que a normatização aparece com 28,57% e a remediação com 35,71%. Nesse sentido, o Doc1 apresenta maior preocupação com SegCiber dando especial atenção à vulnerabilidade cibernética, em geral, a predominância da categoria demostra a identificação dos primeiros passos na abordagem do tema. As categorias normatização e remediação apresentaram menor ocorrência. Portanto, entende-se que inicialmente a vulnerabilidade necessita de métodos para identificação dos possíveis ataques e resolução de ruptura no sistema. Sob outra perspectiva, o Doc2 apresenta a vulnerabilidade com menor ocorrência, 20,41%, não só na análise interna, como também em relação aos outros Doc. A normatização foi marcada com maior número de ocorrência com 51,02%. Finalmente, no que tange ainda ao Doc2, a importância dada à categoria remediação parte dos planos estratégicos para sanar

possíveis ameaças, com 28,57%. Referente ao Doc3 a categoria vulnerabilidade apresentou 7,78%, correspondendo não só ao menor número no documento como também em relação aos demais. Já a categoria normatização representou 20,00% das ocorrências, e, por fim, a categoria remediação demostrou 71,22% de ocorrências, assim sendo, mais relevante nas estratégias de SegCiber no Doc3.

Diante dos resultados observados, percebe-se no Doc1 a inquietação voltada à vulnerabilidade cibernética, visto que esta se justifica como marco inicial da construção das estratégias de SegCiber e como consequência da nova conformação da Sociedade da Informação configurada pelo aumento crescente de acesso à Internet e das redes sociais, elevada interdependência de sistemas e redes de informação e aumento das ameaças e das vulnerabilidades de segurança cibernética (SYMANTEC, 2019). Dessa maneira, vale realçar que a prioridade dessa categoria, correspondendo a 35,71% das ocorrências no Doc1, deriva dos primeiros passos da SegCiber brasileira. No entanto, entende-se que, na medida em que as vulnerabilidades foram identificadas, demandaram-se planos estratégicos definidos pelas políticas e normas específicas, o que passa a ser reconhecido as altas esferas do governo e, por conseguinte, refletindo-se nos documentos subsequentes. Nesse sentido, os Doc2 e Doc3 buscam rever sistematicamente as políticas, normas e respectivo(s) marco(s) legal(is), com especial atenção às ameaças e vulnerabilidades das infraestruturas críticas da informação do País, buscando minimizar riscos e desenvolver novos instrumentos e/ou mecanismos de segurança da informação e comunicações.

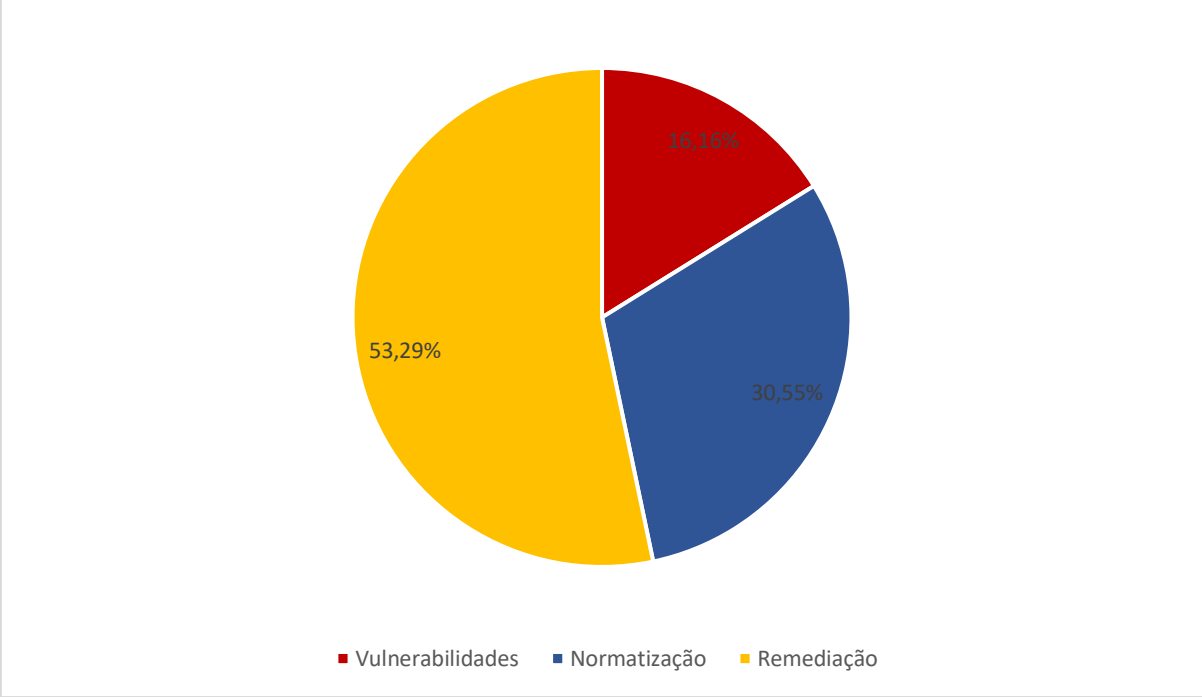
Esse achado converge com o fato de que o Doc2 apresenta resultado diferente no que concerne à prioridade das categorias. Deste modo, a categoria Vulnerabilidade Cibernética foi abordada com menor frequência, enquanto que as demais apresentaram significante crescimento em relação ao Doc1. A leitura desse dado, posta em perspectiva, permite compreender o andamento do processo político de formulação da estratégia de SegCiber: primeiramente foi apresentado o Doc1, com mais ênfase na identificação das vulnerabilidades e ameaças cibernéticas; e após cinco anos surge o Doc2, dando mais importância às demais categorias. Nesse sentido, a categoria normatização técnica e jurídica de SegCiber alcança pouco mais de metade da atenção, correspondendo a 51,02% da discussão devido ao avanço que se teve para garantir o domínio da SegCiber. É importante salientar que o Doc2 busca

de antemão, priorizar a categoria com maior percentagem para adequar-se aos decretos da SegCiber reconhecidos desde os anos 2000 a 2015.

Por fim, o Doc3 consolida o enfoque em remediação. Entende-se que a predominância da categoria Estratégia de Remediação ocorre pela importância do envolvimento de órgãos governamentais no incremento das políticas de segurança de informação do Governo Federal. Sob essa perspectiva, a DPF buscou, por meio do decreto Nº 3.505, de 13 de junho de 2000, adotar instrumentos jurídicos, normativos e organizacionais que asseguram a confidencialidade, a integridade, a autenticidade e a disponibilidade dos dados e informações considerados sensíveis ou sigilosos, ao passo que busca promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação, consequentemente em SegCiber. Essa estratégia política demanda a interdependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação.

Nesse sentido, e de forma a conformar a caracterização da SegCiber brasileira nos documentos analisados, o **gráfico 4** apresenta a totalidade das ocorrências por categoria identificada nos três documentos.

Gráfico 4 - Proporção total de ocorrência



Fonte: Elaboração própria.

Entre as ocorrências verificadas nos documentos, nota-se a categoria vulnerabilidade com 16,16%, normatização com 30,55% e por fim, remediação com 53,29%, está assumindo prioridade na estratégia de SegCiber brasileira.

Os resultados permitem, então, responder à questão de pesquisa: **Como se caracterizam as estratégias de segurança cibernética do Brasil em seus documentos oficiais para lidar com suas vulnerabilidades cibernéticas?** Consoante a análise dos dados, observa-se que a categoria Vulnerabilidades Cibernéticas inicialmente desencadeou a importância na caraterização das Estratégias de SegCiber brasileira, porém, devido à confidencialidade das informações, seu detalhamento é escasso. Todavia, do ponto de vista tecnológico e considerando os avanços científicos e a utilização das ferramentas técnicas, verificou-se que, para lidar com as vulnerabilidades cibernéticas, o Estado Brasileiro demostra ser vulnerável em quatro eixos relacionados à proteção de dados e informações sigilosas, quais sejam: confidencialidade, integridade, autenticidade e disponibilidade. Por outro lado, a categoria Normatização Técnica e Jurídica de SegCiber caracteriza as medidas tomadas para lidar com as vulnerabilidades. Nesse sentido, essa estratégia foi desenvolvida pelo Estado por intermédio de planos políticos da Segurança cibernética de cada órgão e entidade da APF, promovendo e motivando a criação de uma cultura de segurança da informação, buscando, nesse sentido, incrementar e manter os controles de segurança adequados a serem reconhecidos na agenda estratégica do país.

O processo de construção da estratégia de SegCiber, como apontado, seguiu um curso evolutivo, culminando com a priorização mais recente das estratégias de remediação. Isto demostra que os documentos analisados dialogam mais diretamente com o realismo defensivo e a Escola de Copenhague. Quanto ao primeiro, a estratégia de SegCiber preocupa-se primariamente com a identificação das vulnerabilidades, prevenção de ataques e remediação dos mesmos. Já quanto à segunda, o tema de SegCiber é politizado e consolidado em documentos que não se restringem somente à pasta de Defesa, como também a toda administração federal. Nesse sentido, conclui-se que o espaço cibernético no Brasil se apresenta como espaço securitizado e politizado – e, portanto, um lócus de atuação das forças militares e segurança -, porém, assumindo um caráter defensivo e orientado para prevenção e remediação.

6 CONSIDERAÇÕES FINAIS

A pesquisa se propôs caracterizar a estratégia de SegCiber do Estado brasileiro a partir de suas políticas oficiais. Foram analisados três documentos que permitiram verificar o desenvolvimento do debate sobre SegCiber no País. Verificou-se que o Brasil prioriza, atualmente, as estratégias de remediação, após haver consolidados discussões com maior ênfase, em um primeiro momento, nas vulnerabilidades e normatização técnica e jurídica.

A contextualização da temática com o avanço tecnológico possibilitou o enquadramento da evolução das ferramentas técnicas que emergiram ao passar do tempo. Desse modo, entende-se que a internet foi um dos mecanismos cruciais no desenvolvimento da SegCiber, sendo àquela criada inicialmente como estratégia de guerra entre as duas grandes potências – Estados Unido e União Soviética – no período da Guerra Fria. A expansão da internet para uso comercial alargou possibilidades a fim de países desenvolverem as suas políticas, indústrias e economias, a ponto de criar interesse em manter o domínio do espaço cibernético. No caso do Brasil, especificamente, constata-se o esforço do mesmo desde a década de 1970, quando começou a ser pautado o desenvolvimento de linhas de comunicação. Nesse sentido, com o aumento do consumo da internet e novos aparelhos no país, demostrou-se a importância dos conceitos cibernéticos, tendo em vista os riscos e ameaças às infraestruturas críticas e as informações confidenciais do Estado.

Nesse contexto, observa-se a relevância do realismo defensivo na explicação desses fenômenos. Cada Estado é responsável pela sua proteção e desenvolvimento de estratégias de segurança para assegurar sua soberania, e, no caso em tela, assumiram proeminência as estratégias de prevenção e remediação de ataques. Ademais, a Escola de Copenhague teve importante contribuição para a compreensão dos processos políticos que culminaram na securitização do espaço cibernético e no seu enquadramento como dinâmica própria na SegCiber brasileira, tendo em conta, as abordagens da mesma como tema fundamental para se pensar nas práticas de Defesa Nacional.

Inicialmente, para alcançar entendimento desse fenômeno, foram traçadas três questões complementares: 1. Quais os tipos de vulnerabilidades reconhecidas pelo governo brasileiro; 2. Quais são os princípios norteadores de SegCiber definidos pelo Brasil; e 3. Quais são as estratégias desenvolvidas pelo Estado brasileiro para lidar

com as vulnerabilidades reconhecidas pelo País, tanto em termos de normatização técnica e jurídica como remediação. Evidenciou-se que o espaço cibernético é composto por ferramentas técnicas no espaço físico e ferramentas lógicas no espaço virtual, formado por vulnerabilidades cibernéticas que ameaçam a segurança humana e institucional, sobretudo, as informações sigilosas dos Estados. O processo metodológico da análise de conteúdo permitiu compreender como o Estado brasileiro constrói seus entendimentos sobre e, fundamentalmente, suas estratégias para lidar com a SegCiber. Além do mais, a técnica de pesquisa permitiu a classificação das categorias e quantificação das ocorrências nos documentos oficiais que serviram de base para caracterizar o conjunto de políticas de SegCiber do País.

Destarte, o tema das vulnerabilidades cibernéticas e as estratégias de SegCiber apresentam importância no aprimoramento do conhecimento informático conectado a diversas áreas, tanto para melhor funcionamento das sociedades e organizações quanto das instituições públicas e privadas. Nos estudos de Relações Internacionais, esta temática chama especial atenção por envolver interesses dos Estado na atualização tecnológica a fim de garantir a segurança nacional no espaço cibernético. Ainda que este trabalhado tenha focado no estudo de caso do Estado brasileiro, abrem-se novas agendas para debates desse novo fenômeno internacional nos demais países do Sul Global, especificamente, nos países africanos. Nesse sentido, a pesquisa apresenta conceito fundamentais que potencializa continuidade dos estudos em outras dimensões e localidades.

REFERÊNCIAS

ÁVILA Rafael Oliveira de. SILVA, Rafael Pinto da. **Brasil informacional: a segurança cibernética como desafio à segurança nacional**. XII ENANCIB, Brasília, DF, out. 2011.

ACÁCIO, Igor Daniel; SOUZA, Gills Lopes M. **Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço?** 36º Encontro Anual da Anpocs., 2012.

ALCÂNTARA, Bruna Toso. **Internet, terror e ciberterrorismo: uma análise comparativa.** Universidade Federal do Rio Grande do Sul, Porto Alegre, 2018.

BARDIN, Laurence. **Análise de conteúdo.** Ed. 70, press universitaires de France, 1977.

BERTONI, Estêvão. **O que diz a lei quando o celular atacado pertence ao presidente.** Disponível em: <https://www.nexojornal.com.br/expresso/2019/07/25/O-que-diz-a-lei-quando-o-celular-atacado-pertence-ao-presidente>. Acessado em 09 de nov. 2019.

BRANDOM, Russell. **Hospitais do Reino Unido atingem um enorme ataque de ransomware.** The Verge, publicado 12 de maio. De 2017. Disponível em: <https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin>. Acesso em: 21 de maio de 2019.

BRASIL. **Presidência da República. Gabinete de Segurança Institucional. Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018:** versão 1.0 / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. – Brasília: Presidência da República, 2015.

_____. **Presidência da República. Casa Militar. Departamento de Segurança da Informação e Comunicações. Guia básico de orientações ao gestor em segurança da informação e comunicações:** versão 2.0 / Casa Militar, Departamento de Segurança da Informação e Comunicações; organizadores Danielle Rocha da Costa, José Ney de Oliveira Lima. – Brasília: Presidência da República, 2016.

_____. **Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Livro verde: segurança cibernética no Brasil** / Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010.

_____. **Secretaria de Comunicação Social da Presidência da República (SECOM).** Disponível em: <https://www.gov.br/pt-br>. Acesso em 05 de nov. 2019.

_____. **Ministério da Defesa. Setores estratégicos para a Defesa**. Disponível em: <https://www.gov.br/defesa/pt-br>. Acesso em 07 de nov. 2019.

BRITO, G. F. De; CHOI, V. P.; DE ALMEIDA, A. **Manuel ABNT: Regras Gerais de Estilo e formatação de trabalhos acadêmicos.** FECAP. 4ª ed. São Paulo-SP, 2014.

BUZAN, Barry; WAEVER, Ole; WILDE, Jaap de. **Security: a new framework for analysis.** Boulder: Lynne Reinner, 1998.

CANONGIA, Claudia; MANDARINO, Junior Raphael. **Livro Verde: segurança cibernética no Brasil.** Brasília, 2010.

_____. S**egurança cibernética: o desafio da nova Sociedade da Informação.** Parc. Estrat, Brasília-DF, v. 14, n, 29, p. 21-46, Jul/Dez, 2009.

_____. **Relações Exteriores.** Disponível em: <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/20235-visita-oficial-a-israel-de-sua-excelencia-o-presidente-da-republica-federativa-do-brasil-jair-bolsonaro>. Acesso em 26 de dez. 2019.

CLARKE, Richard A; KNAKE, Robert K. **Cyber War: the next threat to national security and what to do about it.** New York: HarperCollins, 2010.

CLAUSEWITZ, Carl Von. **Da Guerra.** São Paulo: Martins Fontes, 1996.

CARVALHO, M. S. R. Menezes. **A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança.** Rio de Janeiro, 2006.

CSIS. **Lista de incidentes cibernética significativa desde 2016**. Disponível em: <https://www.csis.org/>. Acesso em: 31 de maio de 2019.

EQUADOR, notícia. **Presidente Lenin Moreno disse que Julian Assange se tornou Embaixada do Equador em Londres em um centro de espionagem.** Publicado 15 de abril de 2019. Disponível em: <https://www.presidencia.gob.ec/?s=ataques+cibern%C3%A9ticos>. Acesso em: 21 de maio de 2019.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de pesquisa**. SEAD/UFRGS. – Porto Alegre: Editora da UFRGS, 2009.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social.** – 6. Ed. – São Paulo: Atlas, 2008.

_____. A. C. **Como elaborar projeto de pesquisa.** 4. Ed. São Paulo: Atlas, 2002.

GUERRA, Elaine Linhares de Assis. **Manual Pesquisa Qualitativa.** Centro Universitário UNA. Belo Horizonte, 2014.

GJORV, G.H (2012). **Security by any other name: negative security, positive security, and a multiactor security approach.** Review of International Studies, 38, PP 835-859.

IBGE. **PNAD Contínua TIC 2017: Internet chega a três em cada quatro domicílios do país.** Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais>. Acesso em: 05 de nov. 2019.

ITU, (org.). **Programa de segurança cibernética.** Disponível em: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx>. Acesso em: 18 de nov. 2019.

JUNIOR, Alcyon Ferreira de Souza. **Segurança cibernética: política brasileira e a experiência internacional**. 120f. 2013. Dissertação (Mestrado em Gestão do Conhecimento e tecnologia da Informação). Universidade de Brasília, Brasília, 2013.

JÚNIOR, Augusto W. M. Teixeira; LOPES, Gills Vilar; FREITAS, Marco Túlio Delgobbo. **As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica.** Rev. Carta Inter, Belo Horizonte, v. 12, n. 3, p. 30-53, 2017.

JÚNIOR, Samuel César da Cruz. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual.** Texto para discussão/ instituto de pesquisa econômica aplicada, Brasília, julho de 2013.

KREIBICH, Eduardo. Ciberespaço brasileiro: **caracterização, organização e políticas.** Universidade Federal do Rio Grande do Sul, Porto Alegre, 2016.

KIM, Joon Ho. **Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural.** Horizontes Antropológicos, Porto Alegre, ano 10, n. 21, p. 199-219, jan./jun. 2004.

LAKATOS, Eva Maria; MARCONI, Mariana de Andrade. **Fundamentos de metodologia científica.** – 5. Ed. – São Paulo: Atlas 2003.

LEAL, Marcelo Mesquita. **Guerra e ciberespaço: uma análise a partir do meio físico.** Universidade Federal do Rio Grande do Sul, Porto Alegre, 2015.

LINS, Bernardo Felipe Estellita. **A evolução da Internet: uma perspectiva histórica.** Cadernos ASLEGIS, 48. Jan/Abr. 2013.

LIBATO, Luísa Cruz; KENKEL, Kai Michael. **Discourses of cyberspace securitization in Brazil and in the United States.** Rev. Bras. Polít. Int. 58 (2): 23-43, 2015.

LOPES, Jéssica Rodrigues. **Mecanismos de cooperação internacional de repressão e combate dos crimes cibernéticos**, 2016.

MATTOS, Antônio Carlos M.; VASCONCELLOS, Heraldo. **Reserva de mercado de informática o Estado da arte.** Revista de Administração de Empresas São Paulo, set. 1988.

MARTINS, Gilberto de Andrade; THEÓPHILO, Carlos Renato. **Metodologia da investigação científica para ciências sociais aplicadas.** – 2. Ed. – São Paulo: Atlas, 2009.

MARQUES, Francisco Paulo Jamil Almeida. **Participação, instituições políticas e Internet: um exame dos canais participativos nos portais da câmara e da Presidência do Brasil.** Intercom – Revista Brasileira de Ciências da Comunicação São Paulo, v.33, n.1, p. 53-79, jan./jun. 2010.

MASARO, Leandro. **Cibernética: ciência e técnica.** Campinas, SP: [s. N.], 2010.

MEARSHEIMER, John. **A Tragédia da Política das Grandes Potências** – 2001.

MORESI, Eduardo**. Metodologia da Pesquisa.** Brasília-DF, Universidade Católica de Brasília – UCB, 2003.

NETO, M. F.; GUIMARÃES, J. A. C. **Crimes na internet: elementos para uma reflexão sobre a ética informacional.** Revista CEJ, n. 20. Brasília, 2003.

NUNES, Sérgio. **Comunicações Digitais e Internet Ciências da Comunicação.** U. Porto 2012.

OLIVEIRA, Maxwell Ferreira de. **Metodologia científica: um manual para a realização de pesquisas em Administração**. Catalão, Universidade Federal de Goiás, 2011.

ONU (Org.). **A carta das Nações Unidas e Estatutos da corte internacional de justiça.** Departamento de Informações Públicas Lake Success. N. Y. 1948.

OPPERMANN, Daniel. **Virtual attacks and the problem of responsibility: the case of China and Rússia.** Carta Internacional. Dez. 2010.

PCS, Departamento de Engenharia da Computação e Sistemas Digitais. **História**. Disponível em: <https://pcs.usp.br/departamento/historia/>. Acesso em: 05 de dez. 2019.

PIMENTEL, Matheus. **A prisão dos suspeitos de hackear o celular de Moro.** Disponível em: <https://www.nexojornal.com.br/expresso/2019/07/24/A-pris%C3%A3o-dos-suspeitos-de-hackear-o-celular-de-Moro>. Acesso 09 de nov. 2019.

RNP. **Rede Ipê.** Disponível em: <https://www.rnp.br/sistema-rnp/rede-ipe>. Acesso em 05 de nov. 2019.

SANDRONI, Gabriela A. **Prevenção da guerra no espaço cibernético.** IV Simpósio de Pós-Graduação em relações Internacionais do Programa “San Tiago Dantas” (UNICAMP e PUC/SP) de 05 a 08 de novembro de 2013.

SANTOS, Cor. Tm. Luís Filipe Camelo Duarte. **Contributos para uma estratégia nacional de ciberdefesa.** Instituto Universitário Militar Departamento de Estudos Pós-graduados, Pedrouços, 2017.

SILVA, E. L. Da. MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação.** 4. Ed. Rev. Atual. Florianópolis: UFSC, 2005.

SILVA, Thales do Nascimento Da. **Uma arquitetura para descoberta de conhecimento a partir de bases textuais.** Universidade federal de Santa Catarina, Tecnologias da Informação e Comunicação. Araranguá, 10 de junho de 2012.

SOUZA, Eduardo André Araujo de; ALMEIDA, Nival Nunes de. **A questão da segurança e defesa do espaço cibernético brasileiro, e o esforço político-administrativo do estado.** R. Esc Guerra Naval, Rio de Janeiro, v.22 n.2, p. 381 – 410, mai./ago. 2016.

SOUZA, Gills Lopes Macêdo; MEDEIROS, Marcelo de Almeida. **Da cibersegurança à ciberdefesa Americana: a diplomacia da internet como instrumento de proteção e de integração dos estados da OEA.** 3° Encontro Nacional ABRI 2011, 2011.

SYMANTEC. **Sobre a Symantec.** Disponível em: <https://www.symantec.com/about>. Accesso me: 20 de junco de 2019.

_____. **Adapting to the new reality of evolving cloud threats.** Vol. 1, Jun. 2019.
TREND MICRO. **Trend Micro: Brasil é o 2°país com o maior número de ameaças de e-mail.** Disponível em: <https://www.trendmicro.com/pt_br/about/newsroom/press-releases/2018/fast-facts.html>. Acesso em 05 de nov. 2019.

VALERIANO, Brandon; MANESS, Ryan C. **International Relations Theory and CyberSecurity Threat, Conflict, and Ethics in an Emergent Domain.** OUP uncorrected proof – firstproofs, Fri Oct 13, NEWGEN, 2017

VINHAS, Bernardo Lobo. **O ciberespaço e a dinâmica internacional: a inserção Brasileira e seus obstáculos.** Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

WALTZ, Kenneth N. **Theory of International Politics**. New York: McGraw Hill, 1979.

WIKILEAKS. **O que é Wikileaks?** Publicado 03 de novembro de 2015. Disponível em: <https://wikileaks.org/What-is-WikiLeaks.html>. Acesso em: 17 de maio de 2019.

YIN, R. K. **Estudo de caso:** planejamento e método. 2. Ed. Porto Alegre: Bookman, 2001.