**UNIVERSIDADE FEDERAL DE UBERLÂNDIA**
**INSTITUTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS**
**CURSO DE RELAÇÕES INTERNACIONAIS**

JOÃO VITOR FERNANDES CAETANO

# CIBERESPAÇO, CIBERSEGURANÇA E OS DESAFIOS DA IMPLANTAÇÃO DA TECNOLOGIA 5G NO BRASIL

UBERLÂNDIA
2023

JOÃO VITOR FERNANDES CAETANO

# CIBERESPAÇO, CIBERSEGURANÇA E OS DESAFIOS DA IMPLANTAÇÃO DA TECNOLOGIA 5G NO BRASIL

Trabalho de Conclusão de Curso apresentado ao Instituto de Economia e Relações Internacionais da Universidade Federal de Uberlândia como requisito parcial para a obtenção do título de bacharel em Relações Internacionais.

Orientador: Prof. Erwin Pádua Xavier.

UBERLÂNDIA

2023

JOÃO VITOR FERNANDES CAETANO

# CIBERESPAÇO, CIBERSEGURANÇA E OS DESAFIOS DA IMPLANTAÇÃO DA TECNOLOGIA 5G NO BRASIL

Trabalho de Conclusão de Curso apresentado ao Instituto de Economia e Relações Internacionais da Universidade Federal de Uberlândia como requisito parcial para a obtenção do título de Bacharel em Relações Internacionais.

Orientador: Prof. Erwin Pádua Xavier.

Uberlândia, 26 de janeiro de 2022

Banca Examinadora:

_____

Prof. Erwin Pádua Xavier – Orientador (UFU)

_____

Prof. Edson Jose Neves Junior – Examinador (UFU)

_____

Prof. Armando Gallo Yahn Filho – Examinador (UFU)

## AGRADECIMENTOS

Ter a oportunidade de cursar uma graduação em uma universidade pública é, sem dúvidas, algo que eu nunca imaginei na minha vida. Criado de forma humilde em um lar, de certa forma, conturbado, sempre fui aquela criança inquieta. Quando entrei na UFU, fui um dos poucos da minha família a conseguir tal feito, o que me deixou sempre orgulhoso dessa conquista. Em algum momento ouvi a frase: "Você carrega um pouco de cada um que já passou pela sua vida" e, chegar ao fim desse ciclo que se iniciou em 2018, me faz olhar para trás e relembrar de cada um que, mesmo minimamente, fez parte de toda essa jornada.

Por isso, gostaria de começar agradecendo a minha família, meu pai, Nelson, por propiciar a minha vinda para Uberlândia e dar todo o suporte para que eu me mantivesse na cidade durante a graduação; a minha mãe, Rivany, por ter me criado e nunca ter desistido da minha capacidade, sempre me fazendo lembrar que "Eu posso, eu quero, eu consigo", um lema que me fez seguir mesmo em tempos difíceis; e, por fim, a meu irmão, por ser um exemplo de homem e pai para mim e que, mesmo abdicando de seus estudos aos 19 anos para ir trabalhar quando estávamos passando por dificuldades, não tendo a mesma oportunidade que eu tive, sempre me apoiou e me incentivou em todos os momento. Te amo muito, você é um herói para mim e o Miguelito, nosso príncipe.

Agradeço ao meu grupo de amigos durante toda a graduação, denominado "Puleiro", composto por Max, Neto, Cantarino, Marcelo, Fogolin, Pedrinho, Christian e outros que se juntaram ao longo dos anos. Saibam que sem vocês essa fase não teria sido a mesma, juntos passamos por momentos inesquecíveis que ficarão marcados na minha memória por toda a vida. Agradeço aos meus amigos Marcelo e Leandro por serem meus "irmãos mais velhos" quando mudei para a cidade, sem vocês não conseguiria me adaptar. Agradeço a minha amiga Mikaelle que me mostrou muitos caminhos que me mudaram profundamente, mesmo não tendo consciência disso. Para aqueles que não consegui citar, saibam que estão gravados em minha memória e meu coração de alguma forma!

Agradeço a minha namorada, Sarinha, que é a minha maior parceira, que compra todas as brigas comigo, que me incentiva a ser uma pessoa melhor todos os dias. Sou grato por construirmos uma vida juntos. Agradeço também ao meu mais antigo amigo, Teteus, que há mais de 10 anos me apoia e me faz perceber o valor da verdadeira amizade.

Por fim, agradeço minha avó Maria Aparecida que foi meu maior suporte familiar durante a graduação e que sinto muita saudade. Onde quer que a senhora esteja, saiba que te amo muito e que seu neto só terminou um ciclo, mas que ainda vai voar muito!

O futuro pertencerá a quem investir na indústria do conhecimento, que será objeto de uma estratégia nacional, planejada em diálogo com o setor produtivo, centros de pesquisa e universidades, junto com o Ministério de Ciência, Tecnologia e Inovação, os bancos públicos, estatais e agências de fomento à pesquisa.

Luiz Inácio “Lula” da Silva, 2023

## LISTA DE FIGURAS

## LISTA DE QUADROS

**SUMÁRIO**

## 1. INTRODUÇÃO

Ao longo da história do Estado moderno e contemporâneo, a tecnologia tem assumido um dos papéis fundamentais, assim como capacidade militar, economia e alianças, em termos de poder e influência dentro do Sistema Internacional. Aliada ao crescente fluxo de dados entre as mais diversas sociedades, além da evolução mundial transformando o mundo em um local quase sem fronteiras, ela apresenta possíveis problemas e vulnerabilidades em termos de segurança. Uma vez que, através da internet, o usuário é capaz de acessar diferentes redes e sites, não restrito a seu país, mas a todo o mundo, há de ressaltar os perigos deste tipo de acesso ao usuário comum, além de, principalmente, para organizações e instituições, tanto privadas quanto públicas.

Desse modo, surge, em meados da década final do século XX, o termo ciberespaço, utilizado para definir todo o conjunto de redes de internet, o qual interliga usuários, sites, servidores, organizações, etc. Juntamente com ele, surgem diversas variações a fim de denominar seus diferentes âmbitos, necessidades e consequências, como, por exemplo, a segurança cibernética e as gerações da internet, as quais vão ser discutidas nesta monografia. Nesse contexto, o ministro das Relações Exteriores da França, Jean-Yves Le Drian, na 72ª Assembleia Geral das Nações Unidas, afirmou, em setembro de 2017, a importância que ciberespaço assumiu na nossa sociedade, além de alertar para alguns efeitos e riscos do ciberespaço. Segundo ele:

> O mundo digital enfrenta também novas vulnerabilidades, as quais são suscetíveis a colocar em questão os princípios de abertura e de liberdade que são base do ciberespaço; elas têm também consequências nefastas sobre as oportunidades econômicas oferecidas pela revolução digital. Na verdade, nós assistimos a uma proliferação das ameaças no ciberespaço: esse fenômeno representa um desafio fundamental que está apenas em seu início; ele se intensificará durante os próximos anos, disso não há dúvida (LE DRIAN, 2017, s/p[1]).

Com a elevada difusão tecnológica, surge naturalmente a necessidade de interligar os distintos aspectos das sociedades, transcendendo o aspecto meramente nacional e contribuindo para a consolidação de uma estrutura informacional transfronteiriça extremamente importante para as relações e o jogo de poder entre os Estados modernos. Nessa estrutura, as relações estatais adquirem novas dimensões quando perpassam o ciberespaço, entendido como uma "rede interdependente de infraestruturas de Tecnologia da

[1] Referência retirada de site HTML, portanto, não possui paginação determinada. Ao longo do trabalho, quando houver a utilização do termo "s/p" em citações diretas, terá essa mesma conclusão.

Informação e Comunicações (TIC) e de dados, incluindo a internet, redes de telecomunicações, sistemas de computador, processadores embarcados e controladores" (BRASIL, 2017, s/p).

Trazendo para uma perspectiva interna brasileira, a segurança cibernética pode ser localizada como pauta tanto de segurança e defesa brasileira, quanto também em âmbito da ciência e do desenvolvimento tecnológico. Fazendo um paralelo de dois diferentes momentos, pode ser notada a importância notada ao tema, quando o presidente eleito em 2022 e já empossado Luiz Inácio "Lula" da Silva, cita, em seu discurso de posse que "caberá ao Estado articular a transição digital e trazer a indústria brasileira para o Século XXI, com uma política industrial que apoie a inovação, estimule a cooperação público-privada, fortaleça a ciência e a tecnologia e garanta acesso a financiamentos com custos adequados" (G1, 2023, s/p). O segundo momento, está presente no primeiro documento brasileiro que cita segurança cibernética, a Estratégia Nacional de Defesa (END) de 2008, coincidentemente lançada pelo governo do então presidente Lula, durante seu segundo mandato, ressaltando que a estratégia atuaria no forte desenvolvimento nacional, a fim de buscar a "independência nacional, alcançada pela capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear. Não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento" (BRASIL, 2008, s/p).

Desse modo, esta monografia tem como objetivo responder à seguinte pergunta de pesquisa, que deverá ser respondida ao longo do trabalho: *Em que medida o Brasil tem se preparado, tecnológica e institucionalmente, para garantir sua cibersegurança, implantar e enfrentar os desafios que a tecnologia 5G apresenta?* Partindo de uma abordagem metodológica quantitativa e qualitativa de estudo de caso, sob hipótese de que a capacidade nacional brasileira em termos de segurança cibernética e desenvolvimento tecnológico se mostra inferior ao necessário, além de gerar uma dependência externa quase completa, durante este século XXI.

Tendo em vista a importância do ciberespaço, da cibersegurança, além do advento da inovação tecnológica acerca da internet chamado 5G, o presente trabalho será dividido em três capítulos principais: o primeiro trata do o próprio ciberespaço, suas características, oportunidades e ameaças; o segundo disserta sobre a segurança cibernética, analisando quais as reais capacidades brasileiras neste campo; e, por fim, o último bloco levanta as

possibilidades da tecnologia 5G, seus desafios, capacidades e como o Brasil vem se preparando para sua implementação.

Dentro da dinâmica do ciberespaço, é fundamental que as nações possuam capacidades internas para se projetarem com tecnologias próprias e mão de obra qualificada. Dessa forma, o Brasil ainda se mantém como um país em segundo plano, com histórico não favorável ao incentivo ao desenvolvimento da tecnologia e ciência, partindo de iniciativas mais pontuais e temporárias, sem efeitos concretos. Além disso, considerando toda a capacidade tecnológica do 5G na intensificação das conexões móveis, maior integração entre pessoas e coisas, maior abertura para más práticas sofridas pela sociedade (como hackerismo), dependência tecnológica, relações de influência entre qual empresa se despontará como aquela precursora na implantação do 5G, assim como a ampliação da capacidade de processamento de dados de pessoas, empresas, governos e coisas, o Brasil precisa de um olhar mais cuidadoso e atencioso para o setor, de forma urgente.

## 2. CIBERESPAÇO E A EMERGÊNCIA DOS DESAFIOS NO MUNDO VIRTUAL

Durante o último quarto do século XX, ocorreram revoluções tecnológicas e informacionais que resultaram em uma maior velocidade de propagação e o progressivo menor custo das informações. Essa revolução mudou a forma pela qual organizamos o mundo e nos relacionamos, logo, tornando-se cada vez mais um assunto importante. Um grande tema central relativo a essa mudança de organização e relação, proporcionada pelo ciberespaço, é que ele já se tornou parte da estrutura financeira e social contemporânea de uma maneira em que dependemos dela para nossa manutenção como sociedade e nosso desenvolvimento.

Ao se fazer um resgate mental ou até mesmo dos livros de história, a ideia mais clara que se tem da relação entre tecnologia e guerra é que esta catalisou, ao longo dos tempos, o desenvolvimento tecnológico, direta ou indiretamente. O professor da Faculdade de Filosofia, Letras e Ciências Humanas da USP e diretor do Centro de História da Ciência, Shozo Motoyama, em uma entrevista para o site Com Ciência (2002), afirma que essa dualidade seria quase uma força paralela entre guerra e tecnologia.

Algumas áreas do conhecimento tiveram seus avanços propiciados por grandes conflitos militares, mas Motoyama destaca dois âmbitos, o da indústria química, o qual "poderíamos pensar numa série de produtos e melhoramentos", mas visivelmente o desenvolvimento de aviões no fim da Primeira Guerra e após, o qual tivera uma utilidade fundamental na Segunda Guerra e, principalmente, na aviação civil dos dias atuais (MOTOYAMA, 2002). Apesar disso, o professor afirma também que

> Se olharmos um pouco a questão da segunda metade do século XX, a grande revolução computacional e a da biologia molecular ou da engenharia genética são desenvolvimentos alheios à guerra. A mesma coisa pode ser falada com relação à revolução informática que vai se observar, porque é claro que houve um financiamento dos militares mas, do ponto de vista do desenvolvimento propriamente dito, não houve um envolvimento direto com a guerra. Nesse sentido, acho que o desenvolvimento da ciência propriamente dita prescinde da guerra para se desenvolver (MOTOYAMA, 2002, s/p).

Desse modo, o desenvolvimento tecnológico pode ser atrelado à guerra, mas nem sempre houve ou precisa haver tal envolvimento direto, sendo a ciência uma área alheia à guerra para o seu desenvolvimento. Mesmo se voltarmos na primeira criação de um computador, o chamado ENIAC (*Eletronical Numerical Integrator and Computer*), que foi construído por uma parceria entre a Universidade da Pennsylvania (UPenn) e a Eletronic Control Company sob encomenda do Exército dos Estados Unidos, em fevereiro de 1946, seu

objetivo era de ser utilizado para realização de cálculos complexos dos laboratórios de testes de balística da instituição (CNN, 2021).

Nesse contexto de evolução tecnológica, o contexto de Guerra Fria, envolvendo as duas superpotências da época, Estados Unidos e União Soviética, a corrida armamentista e tecnológica propiciou um acelerado desenvolvimento, o qual beneficiou os âmbitos político, militar e econômico de cada nação. Foi nesse período que o tema de segurança cibernética surgiu, se tornando pauta consistente ao longo das décadas, adquirindo uma importância fundamental para a política internacional atual, tanto para a tomada de decisão quanto para as relações inter-estatais. Sendo assim, entender o ciberespaço, os problemas gerados por sua existência e a segurança cibernética é fundamental.

### 2.1 - O Ciberespaço

Assemelhando-se bastante ao ambiente anárquico das relações internacionais, o ciberespaço é um termo relativamente novo, não só nas Relações Internacionais, mas em debates na sociedade por todo o mundo. O termo espaço cibernético ou ciberespaço, que será aquele predominantemente a ser usado neste trabalho, teve sua primeira aparição na ficção científica de William Gibson, em 1982, se popularizando em 1984 com sua obra *Neuromancer* (MANDARINO JR, 2010 apud CASTRO, 2020). Direcionando tais definições para autores de campos de estudos que margeiam o campo das relações internacionais, destacam-se dois autores que seguiram uma linha de pensamento congruente ao tema desta monografia, que são Ventre (2012a) e Mandarino Jr. (2010).

Ventre (2012a) salienta a ideia de que o espaço cibernético não seria somente um simples sinônimo de “internet”, mas um aglomerado de “satélites, os drones, os sistemas de identificação por rádio frequência, os computadores - conectados ou não -, e os sistemas industriais informatizados” (VENTRE, 2012a, p. 34 apud CASTRO, 2020, p. 21). Ainda, o mesmo destaca três possíveis camadas para o ciberespaço: “uma camada inferior, de caráter físico, material, formado pela infraestrutura (hardware, redes); uma camada intermediária, representada pelos softwares e pelas aplicações; e uma camada superior, de caráter cognitivo” (VENTRE, 2012a, p. 34 apud CASTRO, 2020, p. 21). Por óbvio, a comunicação entre estas camadas, assim como a futura inserção da segurança cibernética brasileira e a tecnologia 5G, serão os principais temas a serem tratados aqui.

Já Mandarino Jr. (2010) apresenta a proposição que o ciberespaço seria um complexo virtual formado pela infraestrutura da informação. Tal infraestrutura, ligada à segurança cibernética e comunicações, abarca softwares, hardwares e, por exemplo, dispositivos conectados por meio de fibras óticas; locais de processamento, armazenamento e transmissão de dados (como servidores); e, por fim, a interação entre as pessoas e a infraestrutura informacional (MANDARINO JR., 2010 apud CASTRO, 2020, p 22). Desse modo, ambos os autores se complementam em suas análises sobre o ciberespaço, sendo que o primeiro deles cita a presença de três camadas - a de hardware, software, e cognitiva - e o último, adiciona a camada chamada de peopleware.

A partir de tal análise, a emergência da internet e, assim, o consequente ciberespaço atual, ocorreu na década de 1960, a partir da atuação de pesquisadores do Massachusetts Institute of Technology (MIT), da Universidade de Stanford e da Universidade da Califórnia, financiados pela DARPA (Agência de Projetos e Pesquisas Avançadas do Departamento de Defesa dos Estados Unidos), que criaram a ARPANET, uma rede para comunicação entre computadores dessas universidades e, também, para o Departamento de Defesa, com sua primeira transmissão efetiva em 1969 (CLARKE; KNAKE, 2015, p. 60).

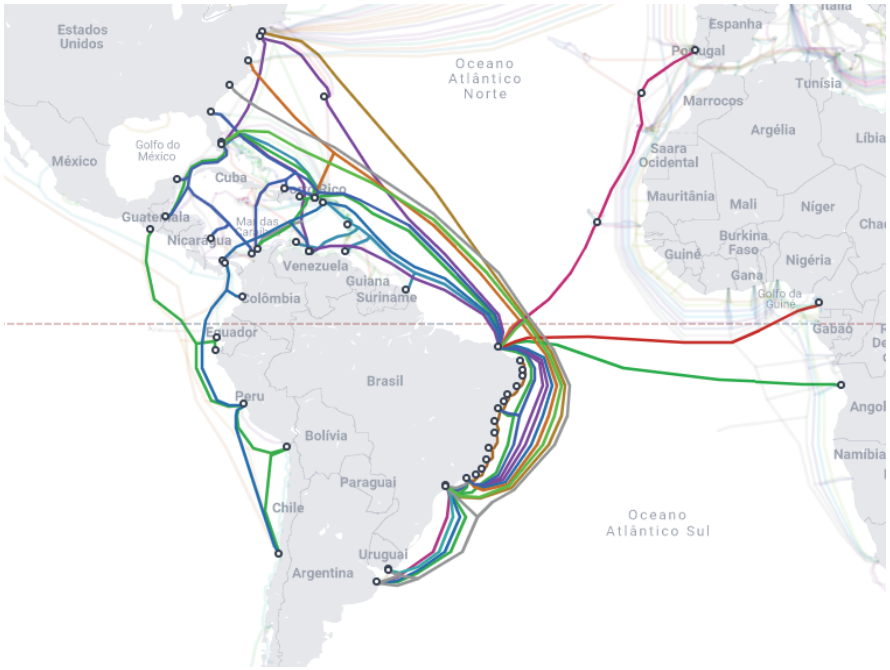
Ainda, na década de 70, foi decidido que o projeto ARPANET seria expandido para o setor espacial, conectando satélites a uma rede comum. Com isso, ao fim da década, o projeto possuía três redes em funcionamento, a ARPANET (via cabos), a PRNET (via radio) e a SATNET (via satélite) (RYAN, 2010 apud RÊ, 2019). Porém, para que tal rede seja considerada a internet como conhecemos hoje e, por consequência, formando o ciberespaço, foi somente ao fim da década de 1980, quando a rede deixou de pertencer com exclusividade ao Exército dos Estados Unidos e criou-se a NSFNET (*National Science Foundation*), uma agência governamental norte americana de pesquisa científica (RYAN, 2010 apud RÊ, 2019).

A mesma foi conectada ao ARPANET utilizando um protocolo TCP/IP, dando início a transição da rede de militares para civis, a qual se espalhou com rapidez pelo território norte-americano. “Em outubro de 1991 cerca de 620 mil computadores estavam online e dois anos depois, em outubro de 1993, mais de dois milhões de computadores estavam conectados à internet” (RYAN, 2010, p. 94 apud RÊ, 2019, p. 18).

A evolução da internet e do ciberespaço criado tem se expandido de forma brusca e deve ser entendido como um ambiente não puramente virtual, mas que também possui sua

contraparte no mundo físico, já que ele engloba as máquinas que armazenam os dados, a infraestrutura que possibilita o fluxo desses dados e até as pessoas que estão por trás e operam os computadores e demais dispositivos conectados ao ciberespaço (SINGER; FRIEDMAN, 2014 apud MESQUITA, 2019). A fim de comprovar tais fatos, estima-se que, em 1996, o ciberespaço possuía cerca de 36 milhões de usuários (cerca de apenas 1% da população mundial naquele momento); já em 2017, havia 3,7 bilhões de usuários, cerca de metade da população mundial (MESQUITA, 2019, p. 7).

**Figura 1 -** Mapa de conexões entre o Brasil a outros países realizadas através de cabos submarinos




Fonte: Telegeography, 2022, s/p

Não diferentemente dos quatro principais domínios físicos dos estudos de defesa - ar, água, terra e espaço sideral - o ciberespaço se configura como um ambiente operacional onde seres humanos, empresas, governos e grupos atuam com um propósito específico, seja ele maléfico ou benéfico (KUEHL, 2009). Ainda, em relação à estrutura física, Willet (2019) argumenta que seria um mito a caracterização do ciberespaço unicamente como um ambiente virtual, citando como exemplo a estruturação dos cabos de fibra ótica (o qual pode ser checado na figura 1, em âmbito brasileiro) e os satélites de comunicação como ferramentas fundamentais para sua infraestrutura.

Todo o fluxo de informação transmitido pela rede precisa, necessariamente, ser hospedado em algum lugar físico. Este local pode ser chamado de servidor ou *data center*,

que seria um complexo físico composto por diversos computadores em que são armazenadas as informações de tráfego da internet (CISCO, 2022). Desse modo, todo site possui um servidor localizado em algum lugar do mundo onde se armazena as informações de acesso. O maior data center do mundo se chama *350 E. Cermak*, possuindo mais de 300 mil metros quadrados, está localizado em Chicago e é de propriedade da Digital Realty, uma multinacional americana do mercado de investimentos imobiliários (DIGITAL REALTY, 2022).

Com a elevada difusão tecnológica, surge naturalmente a necessidade de interligar os distintos aspectos das sociedades, transcendendo o aspecto meramente nacional e contribuindo para a consolidação de uma estrutura informacional transfronteiriça extremamente importante para o jogo de poder entre os Estados modernos. Nessa estrutura, as relações estatais adquirem novas dimensões quando perpassam o ciberespaço, entendido como uma "rede interdependente de infraestruturas de Tecnologia da Informação e Comunicações (TIC) e de dados, incluindo a internet, redes de telecomunicações, sistemas de computador, processadores embarcados e controladores" (BRASIL, 2017).

Segundo Rodrigues (2016, p. 15), as TICs podem ser definidas como "o conjunto total de tecnologias que permitem a produção, o acesso e a propagação de informações, assim como tecnologias que permitem a comunicação entre pessoas". Desse modo, o principal objetivo torna-se fornecer o acesso à informação e comunicação, por meio de dispositivos, incluindo hardwares e softwares de modo geral, mas também outras ferramentas como TV digital, Bluetooth, infravermelho, NFC, QR Code, realidade aumentada e inteligência artificial (RODRIGUES, 2016). As TICs estão presentes em diversos âmbitos da sociedade, na indústria, no comércio, na saúde, no setor bancário, na educação, entre outros. Segundo a Agência Brasil (2021), este último setor, principalmente, sofreu bastante impacto durante a pandemia (2020 a 2021), sendo que, uma ação de caráter emergencial fez com que todos ficassem em casa e toda uma estrutura tecnológica composta por computadores, softwares, internet e celulares teve de ser usada para o funcionamento das atividades educativas, afetando, de início, o desempenho dos estudantes. Apesar disso, a pesquisa destaca que a adaptação dos alunos e professores ao uso das TICs e inserção ao EAD (modelo de ensino à distância) funcionou bem e atendeu as necessidades como uma solução imediata (AGÊNCIA BRASIL, 2021).

Ainda em seu texto, Rodrigues (2016) destaca que a tendência global é a adoção das TICs em larga escala, com automatização da ação humana em todas as áreas da sociedade, sendo a comunicação a grande responsável por tais avanços, devido à troca de informações por meio da tecnologia. Em termos de evolução, podemos destacar desde a TV digital, passando por infravermelho, bluetooth, radiofrequência, realidade aumentada, QR Code, inteligência artificial, computação quântica, etc (RODRIGUES, 2016). Porém, algo que pode unir todos esses dispositivos é a internet móvel e suas gerações e, por isso, mais adiante será apresentada a tecnologia 5G, como ela promete ser 100 vezes mais rápida do que a 4G, sua antecessora e os seus impactos no ciberespaço e no peopleware[2].

Com isso, fazendo uma síntese geral, a classificação do ciberespaço como "domínio global" por parte do Departamento de Defesa dos Estados Unidos (GALOYAN, 2019), ele é entendido como um espaço anárquico em que nações, grupos e civis se relacionam sem leis supranacionais, dando espaço para a preponderância de países como os Estados Unidos, detendo as principais empresas da área e TICs. O país norte-americano detém capacidades de moldar o conceito de ciberespaço, despertando o interesse em outras nações, como China e Rússia, da inserção também no ciberespaço, gerando disputas macroeconômicas e, até mesmo, políticas (EL PAÍS, 2020) - com destaque para a nação chinesa, que disputa com o país norte-americano pelo pioneirismo e supremacia na corrida de implantação do 5G no mundo (G1, 2021a). Desse modo, como em outras arenas de guerra e conflitos, tais como o mar, o ar e a terra, o ciberespaço surge e se estabelece como um espaço, ou mesmo instrumento, de exercício e projeção de poder do Estado.

A esse ponto, entendemos o ciberespaço como uma grande arena geopolítica com diversas possibilidades, tanto para civis, quanto para empresas, grupos e Estados. Dito isso, o conceito de segurança cibernética torna-se fundamental para o entendimento do funcionamento e proteção do ciberespaço, considerando a infinidade de possibilidades de riscos, crimes e ataques por via cibernética que podem ser praticados e, em grande parte dos casos, sem conseguirem ser identificados. O domínio de informações, assim como a quantidade de dados compartilhados na internet, tornou-se um ponto-chave para os perigos cibernéticos ao combinar os riscos e fraquezas do ciberespaço, aumentando consideravelmente as vulnerabilidades contidas em toda a infraestrutura da informação. Dessa

[2] Como apresentado anteriormente, "o peopleware refere-se à camada superior do espaço cibernético, a qual se refere à dimensão cognitiva de Ventre. Ou seja, diz respeito às pessoas que interagem com a infraestrutura da informação, os usuários participantes do ciberespaço" (MANDARINO JR., 2010 e VENTRE, 2012a apud CASTRO, 2020, p. 76).

forma, há uma fraqueza notória no ciberespaço e ameaças que exploram tais pontos, tais como cibercrimes, roubo de dados, terrorismo e outros ataques através do ciberespaço (CAVELTY, 2012 apud CASTRO, 2020).

A título de exemplificação, um dos episódios mais famosos de cibercrime, ficou conhecido como *Stuxnet* e ocorreu em 2010 no Irã. O ataque cibernético consistiu em uma implantação física de um malware (software maligno) nos computadores do programa nuclear iraniano. O malware danificou todo o processo de enriquecimento de urânio da fábrica, fazendo com que os motores de centrifugação funcionassem de maneira anormal, danificando as centrífugas de forma drástica. Este foi o primeiro caso de um ataque cibernético que teve consequências físicas e impactantes, no caso, prejudicando o enriquecimento de urânio do Irã (VALO, 2014 apud RÊ, 2019).

Partiremos agora para um maior entendimento dos possíveis perigos que o ciberespaço comporta, tais como *malwares*, ciberterrorismo, espionagem cibernética, sequestro e roubo de dados, além de guerras cibernéticas.

### 2.2 - Crimes e ataques - os desafios do Ciberespaço

Desde o início do século XXI, o ciberespaço tem um crescimento exponencial positivamente, ou seja, não há uma estagnação ou retração no número de usuários - pessoas que utilizam a rede - ao longo dos anos. Segundo dados do Internet World Stats (2022), no ano de 2000 o número de usuários era em torno de 360 milhões, um percentual de 5,88% da população mundial. Para efeito de comparação, o site informa que esse número subiu para 5,47 bilhões de usuários até julho de 2022, o que representa 69% da população mundial, ou seja, um crescimento de mais de 1400% em número de usuários, em cerca de duas décadas. Segundo a obra de Juliana Ferreira (2017),

> Esse crescimento reflete o desenvolvimento de todo um ecossistema que a internet proporcionou, impactando na geração de novos empregos, redução de custos, facilidade de acessos a produtos, serviços e mão de obra, tornando possível que países em todo o globo pudessem investir em conhecimentos na área das TICs, criando um ambiente de competição e cooperação entre os países (OLIVEIRA, 2014 apud FERREIRA, 2017, p. 19).

Apesar disso, com uma maior inserção de pessoas, organizações, grupos, empresas e Estados, naturalmente surgem novas ameaças cibernéticas, atuando nas vulnerabilidades do sistema e instabilidades do espaço virtual. Cavelty concebe uma divisão que denomina de conflitos cibernéticos, em seis classificações: hacktivismo, crime cibernético, espionagem

cibernética, sabotagem cibernética, terrorismo cibernético e guerra cibernética (CAVELTY, 2012b apud FERREIRA, 2017). Ainda, tal classificação segue a lógica do ataque com menor possibilidade de impacto (hacktivismo) para o que possui maior possibilidade (guerra cibernética), assim como a probabilidade maior de ocorrer (hacktivismo) para aquele que carrega menor probabilidade (guerra cibernética) (CAVELTY, 2012b apud FERREIRA, 2017). A fim de tornar mais didática a definição de cada ataque, o Quadro 1 irá explicar cada tipo com mais clareza.

**Quadro 1 -** Tipos de conflitos cibernéticos, definições, atribuição securitária e alvos

| **Tipos de conflitos cibernético** | **Descrição (segundo Cavelty, 2012b)** | **Atribuição securitária** | **Alvos principais** |
|---|---|---|---|
| Hacktivismo | "A combinação de hacking e ativismo, incluindo operações que usam técnicas de hacking contra um site de internet, que é alvo, com a intenção de interromper operações normais" (p. 116). | CIBERSEGURANÇA | Alvo principal é a área Privada/Sociedade Civil |
| Crime cibernético | "Uma atividade criminal realizada com a utilização de computadores e da internet" (p. 116). | | |
| Espionagem cibernética | "A sondagem não autorizada para testar uma configuração de um computador de destino ou avaliar seus sistemas de defesa, ou a visualização de cópias não autorizadas de arquivos de dados" (p. 116). | CIBERSEGURANÇA / CIBERDEFESA | Alvo principal é tanto a área Privada/Sociedade Civil como o setor Público |
| Sabotagem cibernética | "A perturbação deliberada de um processo econômico ou militar para alcançar um objetivo específico (geralmente político) com meios cibernéticos" (p. 116). | | |
| Terror cibernético | "Ataques ilegais contra computadores, redes e as informações neles armazenadas, para intimidar ou coagir um governo ou seu povo em prol de objetivos políticos ou sociais. Este tipo de ataque deve resultar em violência contra pessoas ou propriedade ou, pelo menos, causar danos suficientes para gerar o nível de | CIBERDEFESA | Alvo principal é o setor público e suas infraestruturas críticas |

| | | | |
|---|---|---|---|
| | medo necessário para ser considerado "ciberterrorismo". O termo também é usado livremente para caracterizar incidentes cibernéticos de natureza política" (p. 116). | | |
| Guerra cibernética | "O uso de computadores para interromper as atividades de um país inimigo, especialmente ataques deliberados aos sistemas de comunicação. O termo também é usado livremente para caracterizar incidentes cibernéticos de natureza política" (p. 116). | | |

Fonte: Quadro elaborado pelo autor a partir de definições apresentadas por Cavelty (2012b) (tradução nossa) e também nas obras de Ferreira (2017) e Re (2021).

Entendendo melhor sobre as classificações dos ataques, é necessário saber que, assim como ocorre a inexistência de fronteiras dentro do ciberespaço, tais ataques também não respeitam esses limites territoriais nacionais, são muito mais rápidos que conflitos convencionais e podem ter múltiplos alvos, sempre atingindo um computador e suas informações/dados (GALOYAN, 2019).

Dentro do crime cibernético e hacktivismo, pode-se identificar um dos tipos mais comuns de ataques, o *Malware.* Este pode ser caracterizado, segundo Galoyan (2019), como um programa ou arquivo que seja prejudicial a um usuário de computador, o que pode incluir vírus, minhocas, cavalos de Tróia e *spyware*. Tal software malicioso pode ser usado para coletar dados pessoais de qualquer usuários, criptografá-los, manipular ações e até mesmo sequestrá-los de seu usuário proprietário (GALOYAN, 2019). Baseado nisso, existem muitos tipos de *malware* que são criados com funções específicas, com objetivos diferentes, que Galoyan (2019) categoriza em três, sendo eles: *ataques de disponibilidade*, programas que tentam impedir acessos em uma rede do ciberespaço, seja negando, sobrecarregando ou encerrando acessos e processos físicos ou virtuais; *ataques de confidencialidade*, programas que são direcionados para a inserção em computadores para monitorar as atividades e extrair informações sobre os sistemas e os dados dos usuários; *ataques de integridade*, programas que envolvem penetração no sistema para mudá-lo, ao contrário de extrair informações, manipulando dados no mundo virtual, o que prejudica diretamente os usuários, sistemas e pessoas que dependem desses dados. É importante ressaltar que, em alguns casos, há a dificuldade ou, até mesmo, a existência de dois tipos de ataques simultaneamente, como em

um ataque de confidencialidade e um ataque de integridade, ambos exploram vulnerabilidades para obter acesso a um sistema (GALOYAN, 2019).

Ainda, há três mais importantes fatores que fazem com que existam vários tipos de *malware* e os tornam tão efetivos durante ataques, que são eles: a) a inexistência de limites geográficos no ciberespaço - exemplo, alguém no Brasil pode acessar computadores e sistemas presentes fisicamentes na África do Sul, lançando ataques cibernéticos na Rússia; b) o usuário não possui clareza se seu computador foi invadido ou não; c) mesmo com uma análise muito qualificada, no melhor dos casos, é possível identificar somente o computador que está sendo usado para iniciar o ataque (SINGER; FRIEDMAN, 2014, p. 72 apud GALOYAN, 2019). Como no ambiente virtual o anonimato prevalece, podendo ser disparado um ataque de qualquer servidor no mundo, torna-se quase impossível a atribuição da responsabilidade a alguém, grupo ou Estado. Isso significa que um Estado pode mobilizar o ciberespaço como uma ferramenta ou um meio para alcançar com maior facilidade seus objetivos de projeção de poder, atuando às margens das convenções e tratados internacionais (CARVALHO, 2021).

A título de exemplificação e direcionamento para o decorrer do trabalho, descreve-se a seguir três dos seis tipos de ataques cibernéticos citados no Quadro 1, que são eles: hacktivismo, crimes cibernéticos e espionagem cibernética.

O hacktivismo é uma operação que usa “técnicas de hacking contra um site de internet, com intenção de interromper operações normais” (CAVELTY, 2012, p. 116 apud FAVERO, 2020, p. 26). Apesar de seu alvo principal seja a área privada e sociedade civil, como apresentado no Quadro 1 por Cavelty (2012), seus propósitos também podem ser políticos, apoiando causas ou busca por mais transparência, agindo a fim de expor informações sigilosas e punir aqueles que agem contra o interesse comum, agindo, nesse caso, com foco de ataque em governos, autoridades e grandes empresas (CARVALHO, 2021). Como exemplo, temos um caso não muito distante, de 2019, da invasão dos celulares do então Ministro da Justiça e Segurança Pública, Sérgio Moro, e do procurador da República na época, Deltan Dallagnol, dentre outras autoridades políticas, com o objetivo de vasculhar os dispositivos em buscas de provas da suposta parcialidade no julgamento do presidente Luiz Inácio Lula da Silva, acusado na época de crime de corrupção (EXAME, 2019). Desse modo, percebe-se que o hacktivismo não possui alvos pré-definidos, mas possui uma motivação voltada para grandes repercussões públicas e despertar a opinião pública para determinado assunto, além de poder

ser praticada pelos mesmos agentes que o combatem, tornando-se também uma arma política (CARVALHO, 2021).

Os crimes cibernéticos, apesar de também poderem ser praticados contra órgãos e agentes públicos, vem se apresentando, ao longo dos últimos anos, como uma potente arma contra a sociedade civil e agentes privados. Segundo a revista IstoÉ Dinheiro (2020), a prática tem consistido em uma série de métodos utilizados para interceptar, falsificar e roubar dados, principalmente bancários, públicos e corporativos, totalizando um prejuízo de 1 trilhão de dólares para a economia mundial em 2020. A atribuição para a quantidade de ocorrências se deve a uma série de fatores, tais como o anonimato dos agentes criminosos, dificultando a identificação dos mesmos; o descuido da sociedade civil, agentes públicos e privados ao navegar pelas redes expondo e tornando seus dados vulneráveis; além da falta de soluções mais robustas em prol da instauração de uma maior segurança cibernética dentro dessas instituições (CARVALHO, 2021).

Por fim, a espionagem cibernética pode ter vários alvos diferentes, mas principalmente o espaço público, em especial entre países do sistema internacional. Segundo Carvalho,

> [...] devido à grande permeabilidade do meio digital nas atividades dos indivíduos, empresas e Estados, [a espionagem cibernética] tornou-se não somente uma prática em si, mas também uma atividade que viabiliza as outras ameaças à segurança do ciberespaço, na medida em que monitora e captura informações (CARVALHO, 2021, p. 8).

Ainda sim, tem-se dois lados importantes a serem ressaltados, aquele que alcança um sucesso em sua espionagem, realizando a "captação de informações valiosas que podem vir a servir aos propósitos de inteligência do Estado" (ASSIS, 2020, p. 21 apud CARVALHO, 2021, p. 8); mas também o lado que incorre em prejuízo, sendo que "dados roubados podem revelar os planos estratégicos de um país ou minar a competitividade de toda uma indústria" (GALOYAN, 2012, p. 12 apud CARVALHO, 2021, p. 8). Desse modo, a ação da espionagem tem como objetivo captar informações adversárias para que se assuma uma posição favorável sobre seu adversário, seja ele uma sociedade, governo, grupo de oposição, agente privado, dentre outros.

É importante ressaltar que, apesar de existirem distinções entre os diferentes tipos de ataques, muitas vezes os mesmos se assemelham ou mesmo se misturam, não sendo possível caracterizar um ataque somente, mas uma série deles. Um dos melhores exemplos de ataque

cibernético que envolveu alguns tipos de ações, sendo classificado ao final como Guerra Cibernética, foi do grupo hacker *Sandworm*, em junho de 2017, lançado na Ucrânia, com a acusação de ter como mandatário a nação russa (GALOYAN, 2019). Segundo Mesquita (2019), o malware, chamado de *NotPetya*, tinha o objetivo de contaminar vários computadores de forma rápida e, diferentes de *ransomwares*[3], seu objetivo era destrutivo. O vírus se propagava e destruía toda a utilidade restante da máquina, sendo inútil qualquer tipo de pagamento para o grupo, a fim de descontaminar as máquinas. Mesmo lançado inicialmente no país ucraniano, o autor explica que o vírus se espalhou por diversos países e computadores, contaminando redes e grandes empresas, deixando um rastro de prejuízos na casa de centenas de milhões de dólares. Algumas das multinacionais afetadas foram a dinamarquesa A. P. Moller-Maersk, a francesa Saint-Gobain e a filial europeia da norte-americana FedEx, a TNT Express (MESQUITA, 2019).

Nesse ínterim, compreendidas as possíveis ameaças ao ciberespaço, redes de dados, sociedade civil, órgãos públicos e empresas privadas, partiremos para o entendimento do que pode ser feito em termos de segurança cibernética para esses agentes, assim como medidas preventivas e corretivas acerca de crimes no ciberespaço.

### 2.3 - A Segurança Cibernética

Ao se estudar a segurança enquanto um conceito acadêmico, nos deparamos com uma série de diferentes definições e autores. Segundo Buzan, Wæver e Wilde (1998), por exemplo, a segurança é um campo que se torna necessário ser estudado simplesmente pela sua própria existência, justamente pela sua importância acadêmica (SOUZA, 2013). Apesar disso, para que seja entendido o conceito de segurança cibernética, é necessário entender os conceitos de "defesa" e "segurança" enquanto termos relacionados.

Desse modo, apesar de os termos apresentarem semelhanças e até serem considerados sinônimos, ambos possuem suas especificidades. O conceito de "defesa" está associado aos conceitos de garantia estatal, da soberania, território e nação, algo mais próximo da ideia de militarização e segurança internacional (SOUZA, 2013). Já a segurança, como apresentado de forma breve anteriormente, segundo Castro (2020), "está firmemente enraizada nas tradições

[3] "*Ransomware* é um tipo de malware que impede o alvo de acessar a rede e exige um pagamento para retornar o serviço ao normal" (SINGER; FRIEDMAN, 2014, p. 298 apud MESQUITA, 2019, p. 15, tradução nossa). "Um exemplo de ataque assim é considerado ataque sobre as contas bancárias individuais, ou até direcionados às informações bancárias das grandes companhias" (SINGER; FRIEDMAN, 2014, p. 35 apud GALOYAN, 2019, p. 11).

da política de poder, se ocupando da ameaça a existência de um dado objeto, da sua sobrevivência – seja Estado, governo, território, sociedade, entre outros" (BUZAN; WAEVER; WILDE, 1998 apud CASTRO, 2020, p. 28).

Partindo para a combinação de tais conceitos com o ciberespaço, o Instituto Igarapé (2021, p. 6) define segurança cibernética (ou cibersegurança) enquanto "de acordo com padrões como ISO/IEC 27032:2012, o termo se refere à preservação da confidencialidade, integridade e disponibilidade de informações no ciberespaço, ou seja, aos princípios que norteiam as atividades de segurança"; enquanto Carvalho (2011a, p. 8 apud CASTRO, 2020, p. 30), define a defesa cibernética enquanto "um conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético[...]". Desse modo, o segundo termo diz respeito mais ao âmbito militar, de defesa estatal e das Forças Armadas (FA), aplicando um caráter estratégico, com o intuito de prevenir ou lançar ataques, configurando, em casos mais extremos, uma guerra cibernética (SOUZA, 2013).

Apesar disso, de acordo com o Instituto Igarapé (2021), não há um consenso geral sobre a definição do termo segurança cibernética. O mesmo ainda ressalta que, para a União Europeia, o termo abrange as atividades necessárias para proteger redes e sistemas de informações, assim como os usuários desses sistemas e outras pessoas afetadas por ameaças cibernéticas, tendo como objetivo final a segurança do ciberespaço (IGARAPÉ, 2021). Enquanto isso, segurança cibernética no Brasil, segundo o Glossário de Segurança da Informação, se refere às

> Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (GSI/PR, 2022 apud IGARAPÉ, 2021, p. 6).

Desse modo, há uma linha muito tênue entre segurança e defesa cibernética e, mesmo a presente monografia partindo de uma análise acerca do primeiro termo, em muitos casos, ambos se difundirão e não será necessário, ou até mesmo possível, distingui-los. Portanto, será adotado o termo de "segurança cibernética" como o mais frequente a ser usado, seguindo indicações das atribuições securitárias segundo exposto anteriormente no Quadro 1.

A segurança cibernética começou a ser debatida nos anos 1970, nos Estados Unidos, ganhando força ao final da década de 1980, expandindo-se em definitivo para outros países

somente na década de 1990 e consecutiva virada do século (CAVELTY, 2012b). Um fato relevante levantado por Cavelty (2012b) é que o debate nunca foi estático, se mostrando sempre diversificado; conforme a evolução tecnológica, o próprio debate tinha que se mostrar propício também às mudanças, fazendo com que aspectos técnicos da infraestrutura da informação mudassem seu rumo. Porém, foi após o incidente do *Stuxnet*[4], em 2010, que o debate adquiriu novas esferas do conhecimento e aplicação. Logo, um debate que antes era tratado somente no âmbito de segurança cibernética tornou-se também uma problemática de questão estratégica militar, com foco em medidas de defesa cibernética (CAVELTY, 2012b). Além deste caso, segundo a autora, o crescimento da espionagem chinesa, sofisticação crescente de criminosos cibernéticos e o aumento de atividades *hackers* motivaram outros países do sistema internacional a se organizarem e considerarem a segurança cibernética um tópico importante para a agenda de segurança, bem como futuros ataques que poderiam causar impactos catastróficos internamente (CAVELTY, 2012b).

Mesmo com tal evolução no debate, Castro (2020) afirma existir

> [...] um desafio que circunda a proteção das infraestruturas críticas, relacionado com a privatização e a desregulação de grande parte do setor público, nos anos 1980, e dos processos de globalização nos anos 1990, os quais colocaram grande parte dessas infraestruturas na mão de grandes corporações privadas (CASTRO, 2020, p. 31).

Desse modo, ambos os setores passaram a ter que atuar juntos a fim de unirem forças e promover níveis de segurança maiores no âmbito interno, gerando desgastes acerca da titularidade estratégica ou mesmo a centralização de medidas de segurança cibernética, algo que será abordado no próximo capítulo.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE), em 2012, lançou o relatório chamado de *Cibersecurity Policy Making at a Turning Point*, o qual destaca as estratégias nacionais em comum de dez de seus membros acerca da cibersegurança e sua importância na política contemporânea: "(a) a internet e as tecnologias da informação são

[4] Já apresentado anteriormente, o Stuxnet foi um vírus de tipo *worm* (minhoca - programas que replicam cópias de si mesmos, contaminando computadores de forma rápida), "responsável por um dos maiores ataques cibernéticos da história, ocorrido em uma instalação nuclear de Natanz-Irã, em 2010, que danificou as centrífugas de usinas nucleares de enriquecimento de urânio do país, causando danos irreversíveis às estruturas nucleares do país, um exemplo claro de como um ataque utilizando software pode causar danos ao hardware de alguma infraestrutura crítica estatal" (FEITOSA 2017, p. 15 apud CASTRO, 2020, p. 33).

essenciais para o desenvolvimento econômico e social e compõem uma infraestrutura vital; (b) as ameaças cibernéticas estão evoluindo e aumentando em um ritmo rápido" (OCDE, 2012 apud MESQUITA, 2019, p. 4). O relatório chama atenção para a importância dos Estados em adotar medidas de segurança cibernética e de forma rápida, já que as ameaças evoluem de forma exponencial.

Ainda, para além dos debates, existem três tipos de discursos sobre o tema de segurança cibernética, apontados por Cavelty (2012a apud CASTRO, 2020, p. 33), que são: "o discurso técnico direcionado para *malwares* e as intrusões de sistemas; o discurso direcionado ao fenômeno do crime e espionagem cibernética; e o discurso direcionado à guerra cibernética" (CAVELTY, 2012a apud CASTRO, 2020, p. 33). Para o desenvolvimento dos próximos capítulos, serão usados, majoritariamente, os dois primeiros discursos.

Por fim, quando comparam-se países desenvolvidos a países emergentes, identificam-se fraquezas nas estruturas e infraestruturas da cibersegurança, envolvendo uma quebra de comunicação entre setores privados e centros de pesquisa públicos, dependência tecnológica estrangeira por conta da limitação de esforços de pesquisas internos proveniente de evasão de capital humano (MARTINS; GONZALO; SZAPIRO, 2018 apud CASTRO, 2020). Tal fato possui também relação com o setor militar dos países, quando se não se tem uma maior organização deste, há uma maior fragilidade em aderir o campo cibernético às políticas de segurança e defesa nacionais do país.

Alguns setores da infraestrutura de base e crítica nacional de alguns países têm sido alvo de ataques cibernéticos, tais como instituições financeiras, instalações de energia nuclear, indústrias petrolíferas, rede de energia elétrica e estruturas de comunicação (WILLETT, 2019 apud MESQUITA, 2019). Porém, como visto, quanto maior a dependência de infraestruturas ao espaço cibernético (incluindo investimentos e organização do setor público/privado e sociedade civil) - sendo atribuídos aqui a países não desenvolvidos, maior a sua vulnerabilidade. Mesmo usuários de diversos países participando ativamente todos os dias do ciberespaço, nem todos podem alcançar níveis de segurança, poderio e tecnologia como os de EUA e China, os quais travam uma "corrida" de desenvolvimento de suas capacidades nacionais estatais, defensivas e ofensivas, dentro do campo cibernético (VENTRE, 2012b apud CASTRO, 2020). Desse modo, é necessário entender em que nível o Brasil se encontra em termos de segurança cibernética, incluindo infraestrutura e dependência tecnológica, assim como seu potencial para abrigar novas tecnologias que têm surgido com promessas benéficas

revolucionárias - como é o caso da tecnologia 5G[5] -, porém, com amplo potencial também para ameaçar a segurança dos Estados e da sociedade.

[5] Tipo de tecnologia de internet móvel que será tratado mais a fundo adiante.

## 3. O SETOR CIBERNÉTICO BRASILEIRO AO LONGO DO SÉCULO XXI

Antes de ser entendido como a construção do setor cibernético brasileiro ocorreu no século XXI, é necessário dar um passo atrás e compreender um panorama geral das últimas décadas que antecederam. Apesar de ser ressaltado aqui toda a construção do ciberespaço, internet, dispositivos de tecnologia e acesso de redes móveis, hardwares e softwares antes mesmo do século atual, no caso do Brasil será dado um enfoque maior nos últimos 22 anos, já que foram esses os períodos de maior impacto de propostas envolvendo o ciberespaço, assim como medidas para o fortalecimento da cibersegurança.

Até os anos 1950, o Brasil passava por uma construção de sua infraestrutura de telecomunicações, precursora do que pode ser entendido como o ciberespaço atual. Após 15 anos de governo militar, foi construída a Empresa Brasileira de Telecomunicações (EMBRATEL), que tinha como objetivo obter o controle de concessionárias privadas e assumir a rede de serviços nacionais de telecomunicações (CARVALHO, 2006). Ao longo dos anos, foram criados alguns órgãos para a instauração de políticas públicas em razão da informática, muitas vezes controlados pelo Ministério da Defesa (MD) e, em alguns momentos, pelo Ministério da Ciência e Tecnologia (MCT), porém, mesmo com as mudanças no mundo e a evolução tecnológica,

> [...] as preocupações acerca da segurança nacional e dos fluxos de poder por detrás do fluxo das informações, entretanto, foram paulatinamente sendo esquecidas, no Brasil e no mundo, com o advento da globalização e a expansão da Internet (CARVALHO, 2006, p. 62).

O curioso é que, ao mesmo tempo em que a tecnologia se expandia e se democratizava gradualmente, a preocupação acerca dele permanecia a mesma, pelo menos em âmbito estatal, enquanto que acadêmicos desempenhavam um papel fundamental no mesmo período, como pontua Castro (2020). Ainda, a autora exemplifica sua ideia com uma iniciativa da década de 1970, chamada Rede Sul de Teleprocessamento (RST), a qual visava a interligação de computadores de diferentes universidades do Estado do Rio Grande do Sul.

Um importante passo a ser citado que geraria desdobramentos fundamentais para toda a estrutura cibernética brasileira atual é o fim do monopólio estatal da EMBRATEL na metade da década de 1990, ainda no governo Fernando Henrique Cardoso (KNIGHT, 2014). Desse modo, há a ampliação da competição por provedores de internet no Brasil, assim como serviços de Internet, dispositivos, hardwares, softwares, empresas de telefonia, entre outras,

os quais, gradualmente, foram se estabelecendo no país proveniente e, principalmente, de tecnologia estrangeira (CARVALHO, 2006).

Diferentemente de China e Estados Unidos - países estes que são importantes para o entendimento da disseminação da tecnologia 5G no Brasil e no mundo -, o Brasil passou a investir no setor cibernético, militarmente, somente neste século. Em se tratando de números, no ano de 2021, destinava-se 1,642 bilhão de reais para a área de Defesa no país, sendo cerca de 1,13% de todo o orçamento aprovado para o ano em questão (CÂMARA, 2021). Já em 2022, o orçamento para o ministério sofreu maiores investimentos, recebendo 4,9 bilhões de reais (AGÊNCIA SENADO, 2021). Porém, para o ano de 2023, a previsão orçamentária para a Defesa é de cerca de R$ 22,4 bilhões, representando 33% dos recursos para investimentos do ano em questão (CÂMARA, 2022a).

Ainda, nos documentos tratados aqui, não fica totalmente claro qual a porcentagem ou valores destinados ao setor cibernético em específico, a órgãos específicos ou mesmo para aquele tratado como o principal atualmente, o chamado Comando de Defesa Cibernética (ComDCiber)[6] - órgão militar responsável pelo setor no país. Uma das poucas informações claras encontradas, são direcionamentos contidos no Projeto de Lei Orçamentária Anual de 2023 (PLOA 2023), dentro da pasta do Ministério da Defesa, o qual direciona investimento na chamada "Implantação de Sistema de Defesa Cibernética para a Defesa Nacional" no valor de aproximadamente R$ 75 milhões sob administração direta do ministério e também, sob o Comando do Exército - sendo entendido aqui como o órgão deste setor das Forças Armadas responsável pela cibernética brasileira, o ComDCiber -, um investimento em cerca de R$ 15,8 milhões (GOV, 2022). Ainda neste raciocínio sobre a falta de clareza sobre a destinação de orçamentos para o setor cibernético, o senador Esperidião Amin, ao fim de 2019, chegou a relatar sua insatisfação e apontar "um quadro dramático, que expõe o país a enormes riscos", ao se referir ao olhar dado à segurança cibernética brasileira, ressaltando, ainda, que a proposta orçamentária para 2020 destinava somente R$ 22 milhões para o setor, sendo R$ 6,3 milhões para o ComDCiber, apesar do próprio órgão calcular que precisaria de pelo menos R$ 60 milhões para implantar um modelo capaz de atender as necessidades do país (AGENCIA

[6] Órgão responsável por executar o Programa da Defesa Cibernética na Defesa Nacional do Ministério da defesa que tem como dois principais objetivos: (i) aglutinar as iniciativas do Setor Cibernético na área da Defesa Nacional; e (ii) contribuir para dotar a Defesa Nacional com a infraestrutura necessária para desenvolver todo o espectro de ações cibernéticas, visando a proteger e defender os ativos de informação do Ministério da Defesa e das Forças Armadas (BRASIL, 2018)

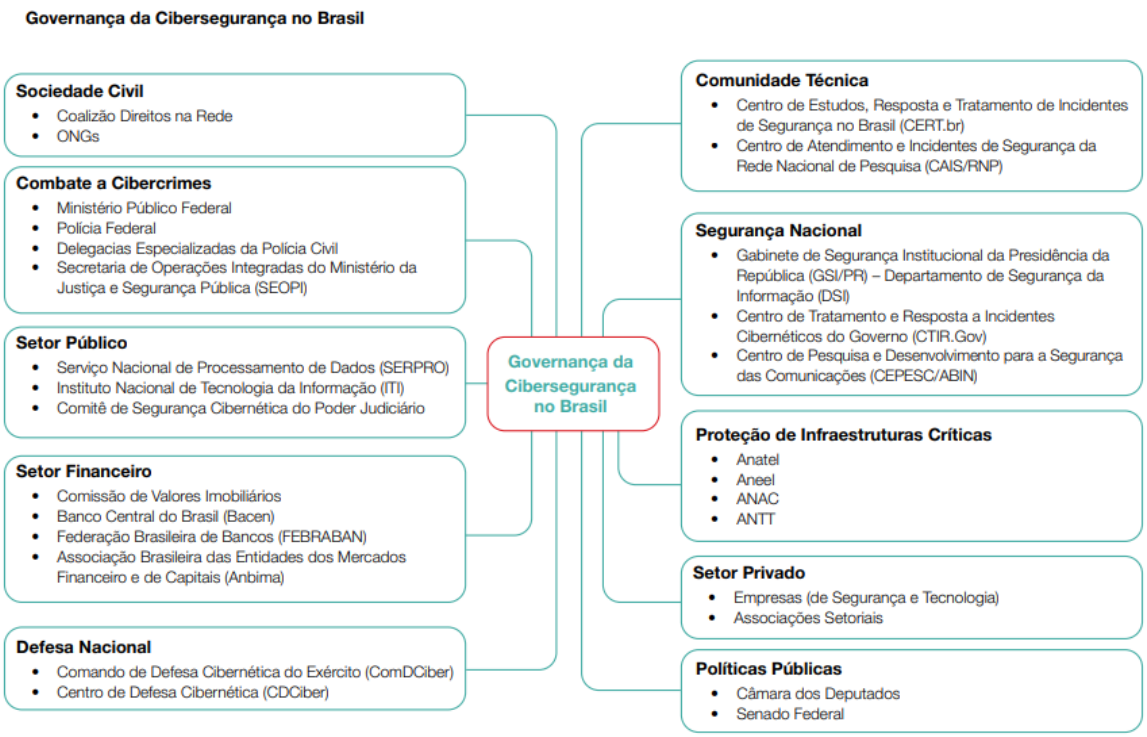
SENADO, 2019). Por fim, o senador desferiu duras críticas ao setor cibernético, afirmando que

> Estamos ficando para trás e podemos pagar um preço caro, imprevisível, por isso. Muito em breve o mundo estará numa nova era, com computadores quânticos, tecnologia 5G, e nós continuamos apegados a uma espécie de Linha Maginot: as fortificações, muralhas e túneis construídos pela França para prevenir um ataque da Alemanha na 2ª Guerra Mundial, mas que não adiantaram nada. Baseavam-se em técnicas ultrapassadas de guerra e não impediram um ataque alemão devastador, que ocupou o país (AMIM, 2019 apud AGENCIA SENADO, 2019, s/p).

Em partes, pode-se considerar que o senador, há cerca de 4 anos, estava correto em suas palavras ao considerar o atraso tecnológico brasileiro em relação à tecnologia 5G, o qual será tratado com mais detalhes no próximo capítulo. Ainda, a máxima desconcentração de recursos e, principalmente, de projetos, investimentos e órgãos para o tratamento da cibersegurança no Brasil, pode ser identificada como um dos principais desafios para o país, uma vez que diferentes "braços" governamentais e não-governamentais são responsáveis pelo ciberespaço brasileiro. Para a exemplificação, o Quadro 2, retirado do estudo de análise acerca da estratégia nacional de segurança cibernética do Instituto Igarapé (2021) - o primeiro e mais confiável portal sobre cibersegurança no Brasil - mostra a pluralidade de agências que fazem a gestão do tema no país.

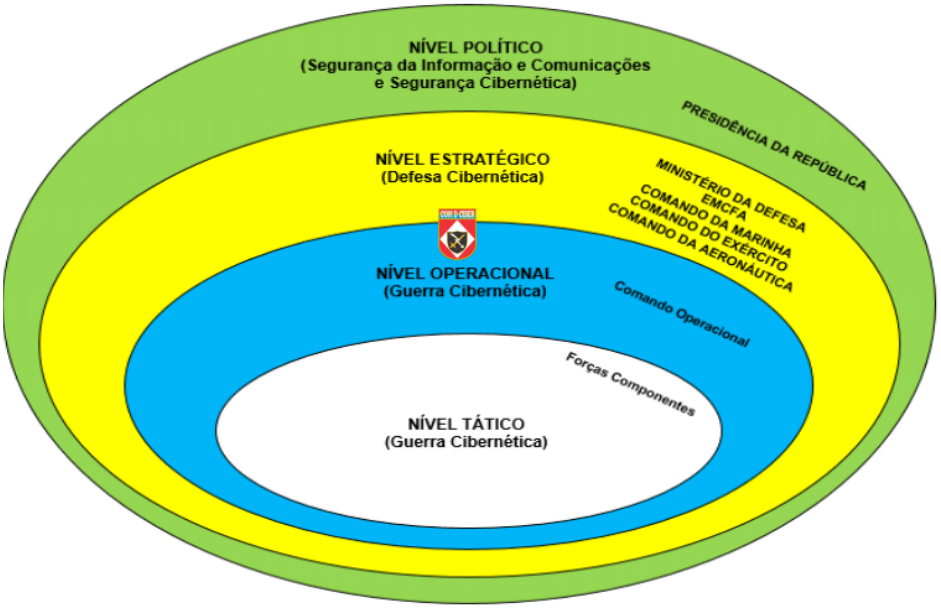
Nesta linha, segundo o Programa de Defesa Cibernética na Defesa Nacional (PDCDN) (2018), o ComDCiber é o órgão superior das FA na questão, estando o Estado-Maior Conjunto, Departamento de Gestão e Ensino e o CDCiber, em termos de hierarquia, abaixo dele (BRASIL, 2018a). Há de ressaltar a existência da Escola Nacional de Defesa Cibernética (EnaDCiber) a qual está localizada no Forte Marechal Rondon, juntamente com o ComDCiber e CDCiber e tem como objetivo contribuir com as áreas de pesquisa, desenvolvimento, operação e gestão de Defesa Cibernética, tornando-se um "centro polarizador de ensino e pesquisa da área" (BRASIL, 2018a). Ainda, percebe-se que o ComDCiber seria somente parte de um sistema complexo de governança, composto pelas forças de diferentes setores, dentre eles a própria sociedade civil e o setor privado, os quais contribuem, respectivamente, para o estudo sobre a operacionalização de TICs do ciberespaço e investimentos em segurança, dispositivos e educação, por exemplo.

**Quadro 2 -** Governança da Cibersegurança no Brasil




Fonte: Instituto Igarapé, 2021

**Figura 2 -** Níveis de atuação




Fonte: BRASIL, 2018a

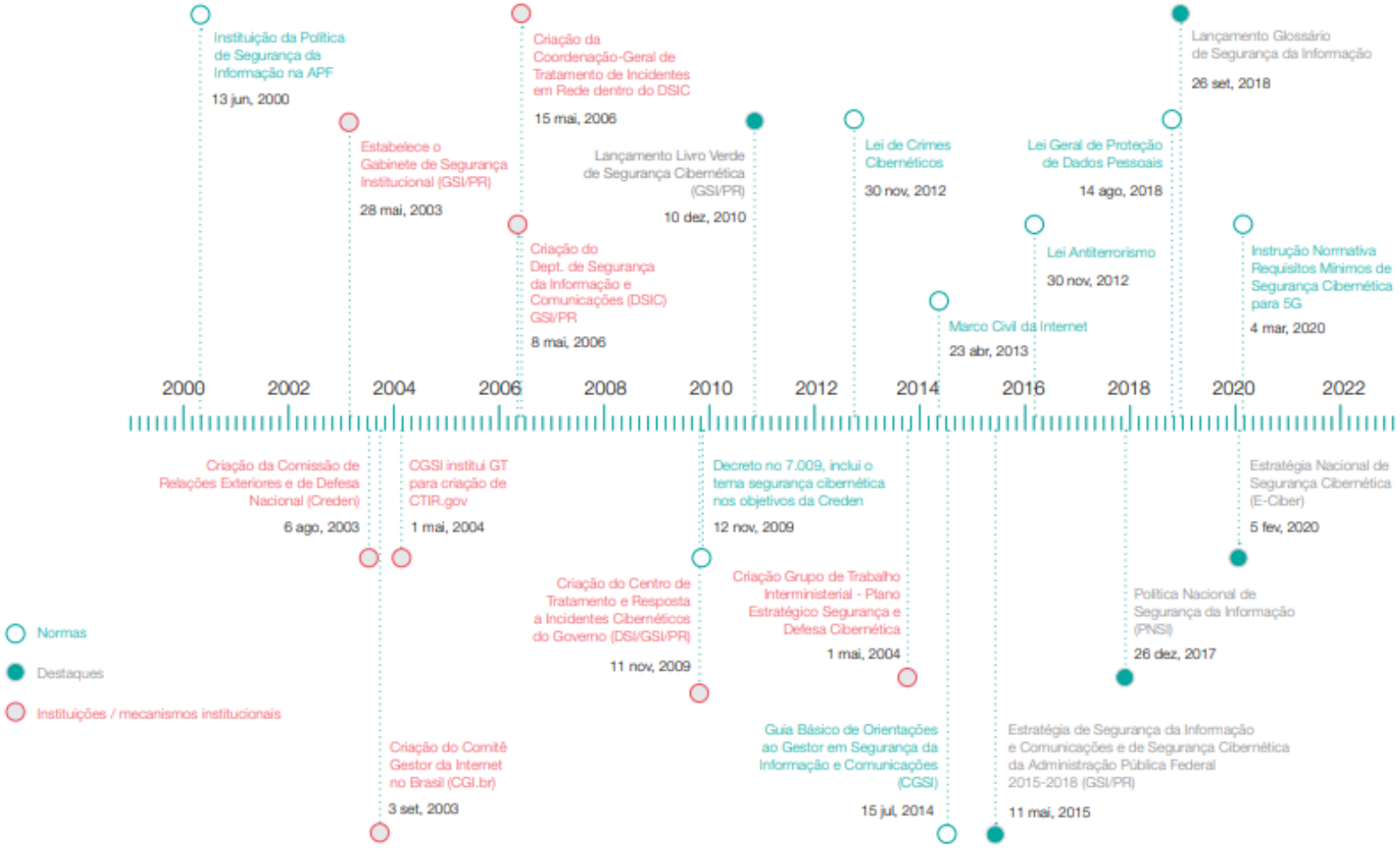
Nesse contexto, percebe-se que, por se tratar das Forças Armadas, o tema do ciberespaço segue muito na linha de defesa cibernética, não somente de segurança como um todo, como foi retratado no capítulo 1. Desse modo, toda a hierarquia do sistema cibernético

militar brasileiro segue esta ideia, representada na Figura 2 logo a seguir. Nela, é possível identificar quatro níveis distintos, cada qual com suas competências: (i) primeiro nível é o nível político, referente à segurança cibernética, sob competência da Presidência da República e do Gabinete de Segurança Institucional (GSI); (ii) o segundo nível é o estratégico, referente à defesa cibernética, sob competência do Ministério da Defesa e Forças Armadas; (iii) o terceiro nível é o operacional, referente à guerra cibernética, sob competência do comando operacional; e, (iv) o quarto nível é o tático, também referente à guerra cibernética, mas sob competência das forças componentes (BRASIL, 2018a).

Para que seja melhor visualizada toda a ordem cronológica de propostas, projetos de leis, programas governamentais, entre outros, será apresentada uma linha do tempo demonstrada na Figura 3 na página a seguir. Nela, é possível identificar vários marcos importantes para a consolidação cibernética brasileira. Seguindo tal lógica, os próximos subcapítulos serão divididos por períodos e terão como objetivo ressaltar aqueles documentos mais importantes para o tema central desta monografia, que é analisar em que medida o Brasil tem se preparado, tecnológica e institucionalmente, para garantir sua cibersegurança e enfrentar os desafios que a tecnologia 5G apresenta.

Para isso,  Pedro Henrique Favero (2022) reúne uma série de documentos sobre a área cibernética no Brasil entre 2008 e 2020, identificando seu autor, ano, caráter do órgão responsável e se o mesmo seria legislativo ou estratégico. Ademais, reitera-se que nem todos os documentos apresentados no Quadro 3 (p. 33) serão tratados com maior profundidade nos subcapítulos, mas somente aqueles que permeiam o objetivo central do trabalho aqui proposto.

**Figura 3 -** Linha do tempo: Segurança Cibernética Brasileira (Administração Pública Federal)




Fonte: Instituto Igarapé, 2021

**Quadro 3 -** Documentos brasileiros sobre cibersegurança de 2008 a 2020

| Título | Ano | Autor/Órgão responsável | Caráter do órgão responsável | Legislativo ou estratégico? |
|---|---|---|---|---|
| Estratégia Nacional de Defesa (END) | 2008 | MD | Público | Político Estratégico |
| Livro Verde de segurança cibernética | 2010 | GSI | Público | Político Estratégico |
| Política Cibernética de Defesa (PCD) | 2012 | MD | Público | Político Estratégico |
| Livro Branco | 2012 | MD | Público | Político Estratégico |
| Estratégia Nacional de Defesa e Política Nacional de Defesa | 2012 | MD | Público | Político Estratégico |
| Marco civil da internet | 2014 | Legislativo | Público | Legislativo |
| Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal | 2015 | GSI | Público | Político Estratégico |
| Guia Básico de orientações ao gestor em segurança da informação e comunicações | 2015 | Comitê Gestor da Segurança da Informação | Público | Político Estratégico |
| Política Nacional de Inteligência (PNI) | 2016 | GSI | Público | Político Estratégico |
| Diretriz para a implantação do comando de defesa cibernética | 2016 | MD | Público | Estratégico |
| Estratégia Nacional de Inteligência | 2017 | GSI | Público | Político Estratégico |
| Norma Brasileira de Gestão de Segurança da Informação (NBSI) | 2017 | Associação Brasileira de profissionais e empresas da segurança da informação e defesa cibernética | Privado | - |
| E-Digital - Estratégia Brasileira para a Transformação Digital | 2018 | Presidência da República | Público | Político Estratégico |
| Política Nacional de Segurança da Informação | 2018 | GSI | Público | Político Estratégico |
| Estratégia Nacional de Ciência, Tecnologia e Inovação (2016-2022) | 2018 | Ministério da Ciência, Tecnologia, Inovações e | Público | Político Estratégico |

| | | | | |
|---|---|---|---|---|
| | | Comunicações MCTIC) | | |
| Transformação do Projeto Estratégico do Exército de Defesa Cibernética (PEE Def CIBER) em Programa Estratégico do Exército de Defesa Cibernética | 2019 | MD | Público | Político Estratégico |
| Glossário de Segurança da Informação | 2019 | GSI | Público | Estratégico |
| Lei geral de proteção de dados (LGPD) | 2020 | Presidência da República | Público | Legislativo |
| Diretrizes para a Consecução das Ações Setoriais de Defesa voltadas para a Guerra Eletrônica | 2020 | MD | Público | Estratégico |
| Livro Branco | 2020 | MD | Público | Político Estratégico |
| Estratégia Nacional de segurança cibernética (E-Ciber) | 2020 | GSI | Público | Político Estratégico |
| Revisão da capacidade de cibersegurança do brasil | 2020 | OEA (Organização de Estados Americanos) | OI | - |
| Estratégia Nacional de Segurança de Infraestruturas Críticas | 2020 | GSI | Público | Político Estratégico |
| Política Nacional de Defesa & Estratégia Nacional de Defesa | 2020 | MD | Público | Político Estratégico |
| Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações | 2020 | ANATEL (Agência Nacional de Telecomunicações) | Público | - |
| Sistema Militar de Defesa Cibernética | 2020 | MD | Público | Estratégico |

Fonte: Favero, 2022 (adaptado)

Resumidamente, Favero (2022, p. 40) destaca que todas essas produções, como mostrado, podem ser tanto legislativa quanto estratégica, porém, a primeira possui caráter normativo, portanto não tanto suscetível a mudanças; já a segunda possui um caráter mais informativo e, portanto, são mais suscetíveis a atualizações ao longo dos anos, já que grupos podem tanto mudar a estratégia como um todo, retirar ou acrescentar pontos a ela (como no caso dos Livros Brancos).

Apesar disso, o autor ressalta que a diferença entre estes documentos pode ser mínima e a principal distinção de fato é o seu público alvo. Quando se analisam documentos estratégicos, os mesmos podem contêm formatação e caráter de lei, como, por exemplo, programas nacionais, se direcionando principalmente para informar a sociedade civil, diferente dos jurídicos, que se destinam às forças armadas, geralmente, e ao legislativo. Enquanto os documentos legislativos possuem como função criar normas jurídicas, os estratégicos buscam fomentar os estudos e criar uma estrutura que alicerça estratégias sobre determinados assuntos (FAVERO, 2022). O autor cita como exemplos bem nítidos a distinção entre o marco civil da internet (BRASIL, 2014b apud FAVERO, 2022), o qual cria normas jurídicas, e a política nacional de segurança da informação (BRASIL, 2018b apud FAVERO, 2022), o qual traça as diretrizes e objetivos de uma estratégia em nível nacional.

A partir disso, surgem questionamentos acerca do tema central, como, por exemplo, quais documentos fomentaram a cibersegurança brasileira que conhecemos hoje? Quais as reais capacidades brasileiras? Quais os principais problemas enfrentados pelo Brasil no setor cibernético? Desse modo, serão destrinchados, a seguir, aqueles documentos mais importantes para a construção da segurança cibernética brasileira como a conhecemos hoje. É importante ressaltar que, apesar de todos serem importantes, nem todos os documentos serão detalhados, somente aqueles que são julgados fundamentais para a presente pesquisa.

## 3.1 - Segurança cibernética brasileira antes de 2018

Dentre diversos documentos, normas, planos e estratégias anteriores ao ano de 2018, os principais que serão aqui descritos são a Estratégia Nacional de Defesa (END) (2008); o Livro Verde de segurança cibernética (2010); o Marco civil da internet (2014); e a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (2015-2018). Além disso, serão compilados, quando houver necessidade, exemplos de situações que aconteceram no período, as quais podem (ou não) ter motivado a criação e implementação de tais ações.

### 3.1.1 - Estratégia Nacional de Defesa (END) - 2008

Como já visto, apesar de a temática acerca de comunicação já fazer parte de produções acadêmicas e da agenda do governo brasileiro antes mesmo de 2008, a END foi a primeira estratégia que introduziu a segurança cibernética como pauta de governo. Este é um período em que o tema começa a ter um interesse estratégico maior, porém, ainda com ressalvas e uma

quase necessidade de haver ações, episódios e ataques marcantes para o surgimento de novas iniciativas acerca do tema.

> Ao contrário de cem anos atrás, tempo do Barão do Rio Branco, quando o Brasil comprava do exterior praticamente todos seus principais equipamentos de defesa sem a capacidade de nacionalizar sua produção, hoje o desenvolvimento de capacidades autônomas na indústria de defesa é um objetivo fundamental de nossa política. A Estratégia Nacional de Defesa [...] define três áreas prioritárias desse esforço: a nuclear, a cibernética e a espacial (AMORIM, 2013, p. 308-309 apud PIRES NETO, 2020, p. 34).

Dessa forma, desde 2008 já se tinha a ideia de desenvolver as bases tecnológicas do Brasil, como Amorim (2013) apresenta, mas também apontava o texto original de 2008, o qual estabelecia que "os setores espacial e cibernético permitirão, em conjunto, que a capacidade de visualizar o próprio país não dependa de tecnologia estrangeira e que as três Forças, em conjunto, possam atuar em rede, instruídas por monitoramento que se faça também a partir do espaço" (BRASIL, 2008). Ao longo das análises, percebemos que tal feito não foi de fato cumprido, notando-se evoluções substanciais, mas não a ponto de tornar o país independente tecnologicamente, principalmente, quando inserimos o debate acerca do 5G..

Além disso, a estratégia definia a compra de ferramentas, maquinário e o desenvolvimento de infraestruturas de defesa, seguindo a tríade mencionada anteriormente. Três pontos são citados que irão se repetir em outros documentos posteriores, que seriam a necessidade de introdução da sociedade civil ao debate acerca de assuntos de defesa, maior e contínua alocação de orçamento para o setor, além de maior integração entre instituições científicas e privadas,

> A identificação e a análise dos principais aspectos positivos e das vulnerabilidades permitem vislumbrar as seguintes oportunidades a serem exploradas: (1) maior engajamento da sociedade brasileira nos assuntos de defesa, assim como maior integração entre os diferentes setores dos três poderes do Estado brasileiro e desses setores com os institutos nacionais de estudos estratégicos, públicos ou privados; (2) otimização dos esforços em Ciência, Tecnologia e Inovação para a Defesa, por intermédio, dentre outras, das seguintes medidas: (a) maior integração entre as instituições científicas e tecnológicas, tanto militares como civis, e a indústria nacional de defesa; (b) definição de pesquisas de uso dual; e (c) fomento à pesquisa e ao desenvolvimento de produtos de interesse da defesa; (3) maior integração entre as indústrias estatal e privada de material de defesa, com a definição de um modelo de participação na produção nacional de meios de defesa [...] (BRASIL, 2008, s/p)

Com isso, a primeira END tem sua importância ressaltada por ser o primeiro documento a salientar a importância da cibersegurança, com base nos pontos de vulnerabilidade apresentada nas capacidades brasileiras à época, sugerindo novas medidas e

aplicando prazos para tarefas a serem realizadas, assim como os responsáveis, de modo organizado e conciso.

### 3.1.2 - Livro Verde de segurança cibernética - 2010

O Livro Verde de segurança cibernética, ainda em 2010, cerca de 12 anos atrás, já apontava, segundo Favero (2022), para uma necessidade maior do país em encarar a área cibernética como prioridade, tanto interna quanto externamente, em âmbito de defesa. Além disso, o autor salienta que tal prioridade à área, é uma condição essencial para o seu desenvolvimento de forma consolidada no país, algo que ainda não foi feito de forma substancial (FAVERO, 2022).

Apesar disso, o Livro Verde foi produzido pelo Gabinete de Segurança Institucional (GSI), órgão essencial da Presidência da República, e visava coordenar atividades acerca de segurança da informação, ampliando o debate social, econômico, político e técnico-científico acerca do tema no Brasil (BRASIL, 2010). Desse modo, o documento traz, com apoio de um grupo técnico instituído, assim como especialistas de diferentes órgãos da Administração Pública, uma breve visão da área no país, destacando alguns marcos, oportunidades e desafios, nos vetores político-estratégico, econômico, social e ambiental, educacional, legal, de cooperação internacional e de segurança das infraestruturas críticas (BRASIL, 2010). E,

> [..] sinaliza potenciais diretrizes estratégicas para cada vetor em análise, como subsídios ao amplo debate no âmbito do governo e da sociedade em geral, visando à construção da Política Nacional de Segurança Cibernética, a qual se constituirá no Livro Branco do País para enfrentamento de tal temática, reconhecidamente o grande desafio do século XXI (BRASIL, 2010, p. 15).

Com isso, o documento teve como finalidade uma maior instrução da sociedade acerca do tema, como o próprio pontua a necessidade e agilidade com que o país precisa desenvolver sua segurança cibernética, para que a sociedade possa se apropriar dos benefícios da internet, “rede global em mudança contínua” (BRASIL, 2010, p. 15). Além disso, algumas diretrizes foram estabelecidas para que se estendesse a capacidade da defesa do país para a sua proteção no espaço cibernético, como, por exemplo, duplicar o orçamento vigente para segurança cibernética a cada dois anos, valendo a partir de 2011 - o que não foi cumprido à risca, já que cada governo estabelece por lei o orçamento do MD, qual valor é destinado para o setor (BRASIL, 2010).

Desse modo, o Livro Verde teria como objetivo que os impactos negativos decorrentes de ações e usos maliciosos da rede fossem minimizados, já que o documento à época

apontava que 80% dos serviços de rede eram de propriedade e operados pelo setor privado e por empresas internacionais, logo se tornando um grande desafio, dentre outros mais citados, à sua implementação (BRASIL, 2010).

### 3.1.3 - Marco civil da internet - 2014

Segundo Pires Neto, apesar de uma série de documentos e estratégias relevantes até o ano em questão, "o conjunto de ações tomadas pelo governo brasileiro para promover um ambiente ciberneticamente seguro não é dos mais eficazes" (PIRES NETO, 2020, p. 43). Em 2012, tramitava a lei do Marco Civil no Congresso Nacional, porém, ele só foi aprovado alguns meses após o vazamento de Edward Snowden, o que fez com que o tema de segurança cibernética ganhasse de fato uma centralidade na agenda política apenas em 2013 (CARVALHO, 2021). O caso em questão se caracteriza pelos vazamentos de documentos da NSA e da Central Intelligence Agency (CIA) por Edward Snowden, revelando o esquema de espionagem norte-americano no qual, dentre os alvos, encontrava-se a então presidente da República, Dilma Rousseff, e a empresa Petrobras.

O caso ressaltou a total ineficiência dos mecanismos e órgãos brasileiros de segurança cibernética - mesmo que ainda recentes - para detectar as ofensivas de espionagem estadunidenses. Desse modo, o Marco Civil surgiu para estabelecer princípios e deveres fundamentais para a utilização da internet pelos usuários. Logo, estabele marcos regulatórios importantes para o setor e a sociedade civil, quando associada à lei nº 14.155/2021 (antiga Lei Carolina Dieckmann) e à Lei Geral de Proteção de Dados (LGPD), de 2020, formando importantes frentes para o combate a ataques cibernéticos no país (CASTRO, 2020). Ainda assim, mesmo com o Marco Civil de 2014 - ainda que fora essencial para a fundamentação de estratégias subsequentes -, segundo o documento de Estratégia Nacional de Segurança Cibernética de 2020, "o nível de articulação e de normatização das instituições brasileiras nos temas relacionados à segurança cibernética ainda é tímido, e exigem esforço adicional" (BRASIL, 2020a, p. 24).

Desse modo, após quase 10 anos, pode-se concluir que a lei cumpriu com o seu objetivo de estabelecer direitos e deveres quanto ao uso da internet, de forma inicial, propiciando mudanças como a neutralidade da rede; o armazenamento de dados; a liberdade de expressão e responsabilidade; e as obrigações do Poder Público, fazendo com que a internet se torne um ambiente mais seguro e que infratores sejam identificados e punidos com maior facilidade.

### 3.1.4 - Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015-2018

O ano de 2015 foi um daqueles com maiores destaques para o setor historicamente, em que se descobrem que hackers vinham roubando mais de US$ 1 bilhão (R$ 2,8 bilhões na cotação da época e cerca de R$ 5,36 bilhões na cotação atual, sem considerar correções), todos realizados através de ataques a bancos desde 2013 em mais de 30 países (BBC, 2015). Aliado a isso, a notícia que ataques cibernéticos no Brasil cresceram 7 vezes mais que a média mundial no mesmo ano (PWC, 2016) fez com que o país voltasse a atenção para o setor mais uma vez.

A Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal foi lançada em 2015, com o intuito de atuação até o ano de 2018, e tinha como objetivo fomentar um maior suporte ao planejamento estratégico governamental durante o período, assim como respaldar o importante papel da segurança cibernética para o país (OLIVEIRA, 2017). Desse modo, descrevia todo o mapa estratégico e metodológico para que se atingisse os objetivos e metas para a cibersegurança no Brasil.

> [..] a elaboração desta Estratégia é motivada pela missão do GSI/PR de coordenar as atividades de segurança da informação do governo e considera tanto a necessidade ímpar de assegurar ações efetivas nestas áreas, quanto a possibilidade real e crescente de uso das Tecnologias de Informação e Comunicação (TIC) para ações ofensivas e exploratórias, entre outras, acesso indevido às redes de computadores de setores e de infraestruturas críticas.
>
> Destaco ainda a ameaça relativa à elevada interconectividade mundial entre os maiores desafios da atualidade, confirmadas pelo World Economic Forum em suas análises sobre os riscos globais, tanto em 2014 quanto em 2015, em que são evidenciados, entre os grandes riscos tecnológicos, os ataques a redes e infraestruturas críticas da informação; o aumento dos ataques cibernéticos; e os incidentes de fraudes e roubos de dados (BRASIL, 2015, s/p).

É notado que a preocupação acerca das TICs e a "elevada interconectividade mundial" já se fazia muito presente, se intensificando mais ao longo dos anos, dando destaque ao crescente número de ciberataques. Como veremos no próximo capítulo, o fomento da tecnologia 5G está muito atrelada a esses desafios destacados, uma vez que muitos desses ainda se perpetuam nos dias atuais, porém com maiores impactos para nossa sociedade.

## 3.2 - Segurança cibernética brasileira entre 2018-2020

Durante o início do governo Bolsonaro até meados da pandemia do Covid-19, houve uma intensificação da produção de documentos acerca de segurança cibernética no país, muito por conta do próprio caráter do governo de valorização da defesa do país, mas também por

conta da transformação digital na sociedade iniciada pelo período pandêmico (FGV, 2022). Desse modo, serão citados aqui alguns dos documentos mais importantes para o fomento das capacidades de segurança cibernética brasileiras atuais, dentre eles a Política Nacional de Segurança da Informação (2018); a Lei Geral de Proteção de Dados (LGPD) (2018)/2020; a PND e a END de 2020; e o E-Ciber (2020).

### 3.2.1 - Política Nacional de Segurança da Informação - 2018

A Política Nacional de Segurança da Informação (PNSI), além de apresentar o tema de segurança da informação englobando tanto segurança quanto defesa cibernética, teve como principal objetivo "assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em nível nacional" (BRASIL, 2018b, s/p).

O documento possui um destaque para a superficialidade que possui, definindo objetivos muito gerais, apesar de apresentar partes importantes de infraestruturas críticas e segurança cibernética; um dos problemas citados no início do capítulo volta a tona nessa estratégia, uma vez que a própria não apresenta o capital investido no programa de defesa cibernética especificamente, mas sim como um todo (FAVERO, 2022).

Um fato importante sobre a PNSI foi a estipulação da criação da Estratégia Nacional de Segurança da Informação (ENSI), o qual previa uma maior participação da sociedade civil, sendo dividida em três módulos: i) segurança cibernética; ii) defesa cibernética; iii) segurança das infraestruturas críticas (BRASIL, 2018b). Os dois primeiros foram efetuados, porém, o último acabou por mesclar-se com outras estratégias nacionais de defesa (FAVERO, 2022). Apesar disso, Favero (2022) considera o documento um importante passo para estabelecer pontos mais específicos que o PNSI não contemplava, além de destacar eixos em que o Brasil precisa se desenvolver, como o de conscientização e capacitação (BRASIL, 2020a apud FAVERO, 2022).

### 3.2.2 - Lei Geral de Proteção de Dados (LGPD) - 2018/2020

A Lei Geral de Proteção de Dados (LGPD), como o próprio nome já informa, não se trata de documentos estratégicos ou políticas destinadas à segurança cibernética, mas sim uma lei que visa "proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo" (BRASIL, 2018c, s/p). Além disso, a lei "fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações

que podem ocorrer em meios manuais ou digitais" (BRASIL, 2018c, s/p). Desse modo, a lei em questão surge para regular o tratamento dos dados, principalmente digitais, mas também físicos, da sociedade em geral, além de estipular penalidades para aqueles que não a cumprirem.

Apesar de ter sua vigência efetuada entre 2019 e 2020, sua execução vem sendo ainda adaptada, de modo que qualquer dado pessoal utilizado para quaisquer fins deve contar com a concordância do proprietário de tais dados (BRASIL, 2018c). Dentre as possíveis operações de tratamento de dados, estão: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018c). Todos os tipos de operações realizadas com os dados de usuários devem ser comunicadas e aprovadas pelos mesmos antes de ser efetuada (BRASIL, 2018c).

Segundo a LGPD Brasil (2022), com o advento da tecnologia 5G sendo implementada no cotidiano da sociedade civil, há uma preocupação acerca do provável aumento de atividades de ataques cibernéticos, tanto nos ambientes pessoais quanto corporativos (LGPD BRASIL, 2022). Logo, a intensificação da conexão e velocidade de troca de dados entre dispositivos, fomenta a importância da segurança cibernética e também da inclusão das práticas da LGPD à sociedade (LGPD BRASIL, 2022). O site ainda ressalta a necessidade das organizações de aumentar suas capacidades cibernéticas, a fim de evitar ataques cibernéticos, além de investir em equipamentos que possuem a tecnologia 5G para garantir uma melhora nos processos tecnológicos, assim como se pautar na LGPD para o aumento na proteção de dados (LGPD BRASIL, 2022).

### 3.2.3 - PND e END - 2020

Há de se considerar, em primeiro lugar, que o PND e a END não são documentos específicos de cibernética, mas sim de defesa e segurança brasileira, o qual cita o tema como um tópico, sem muita profundidade (FAVERO, 2022). Desse modo, ambos os documentos precisaram ser atualizados com o passar do tempo, sendo que a END teve sua primeira versão lançada em 2008, seguidas de versões em 2012, 2016 e 2020; e a PND sua primeira versão em 2012, seguidas de 2016 e 2020 (FAVERO, 2022). Novas atualizações da END, PND e do Livro Branco de Defesa Nacional foram aprovadas no Senado em julho do ano de 2022, porém, o Projeto de Decreto Legislativo (PDL) nº 1.127/2021, destinado à atualização, segue

retido na Câmara dos Deputados até a data de redação desta monografia (AGÊNCIA SENADO, 2022).

Apesar disso, a PND é importante para a defesa brasileira, uma vez que,

> A PND é o documento condicionante de mais alto nível para o planejamento de ações destinadas à defesa do País. Voltada prioritariamente para ameaças externas, estabelece objetivos para o preparo e o emprego de todas as expressões do Poder Nacional, em prol da Defesa Nacional (BRASIL, 2020b, p. 7).

O texto diz respeito à segurança de modo abrangente e também reconhece a insuficiência de tecnologia, ou até mesmo a obsolescência dos equipamentos das Forças Armadas e ressalta a necessidade de aumentar a autonomia produtiva e tecnológica da área de defesa (BRASIL, 2020b). Ou seja, aponta para pontos já citados em outros documentos e desde a elaboração da primeira END de 2008, a qual destacava a importância de se diminuir a dependência da importação de tecnologia estrangeira.

Com isso, como a END e a PND foram lançadas na forma de um só livro, esperava-se que a primeira fosse continuação natural da PND, sendo que o primeiro documento colocaria em prática estratégias levantadas pelo segundo (FAVERO, 2022). Porém, para Favero (2022), não é isso que acontece, já que a Estratégia Nacional de Defesa não aprofunda nas estratégias a serem seguidas no espaço cibernético, além de possuir "um tom de semelhança com a PND e o Livro Branco (2020): estratégias cibernéticas mencionadas de forma genérica, mas não específicas" (FAVERO, 2022, p. 46).

### 3.2.4 - E-Ciber - 2020 - 2023

O E-Ciber - Estratégia Nacional de Segurança Cibernética - pode ser considerado o mais relevante documento vigente no país em matéria de segurança cibernética (FAVERO, 2022). Apesar de formulado pelo GSI, faz parte do primeiro módulo de implementação da Política Nacional de Segurança da Informação (Decreto 9.367/BRASIL, 2018b) e teve a inclusão da participação de instituições em sua formulação, assim como participação da comunidade acadêmica brasileira (FAVERO, 2022). O documento tem sua efetividade estendida até o ano de 2023, logo, até o momento de escrita desta monografia, é a estratégia base para a segurança cibernética brasileira.

Como apontado por Favero (2022), a superficialidade dos documentos de segurança no Brasil predomina e acaba prejudicando não só o entendimento do setor como um todo, mas principalmente a cibernética, já que há divergências de definições de termos, falta de clareza

de orçamentos, falta de clareza de estratégias e efetividade de implementação. Nessa linha, a E-Ciber destaca que, em relação aos problemas da segurança cibernética no país,

> Em primeiro lugar, verifica-se que há boas iniciativas gerenciais nessa área, entretanto, mostram-se fragmentadas e pontuais, o que dificulta a convergência de esforços no setor. Em segundo, nota-se a falta de um alinhamento normativo, estratégico e operacional, o que frequentemente gera retrabalho ou resulta na constituição de forças-tarefa para ações pontuais, que prejudicam a absorção de lições aprendidas e colocam em risco a eficácia prolongada dessas ações (BRASIL, 2020a, p. 2).

Desse modo, ressalta a superficialidade e descentralização do cuidado com a segurança cibernética brasileira citadas na presente monografia, assim como em Favero (2022), Castro (2020) e Carvalho (2020).

Além disso, segundo o documento, há três objetivos estratégicos que permeiam o objetivo central de transformar as capacidades de segurança do Brasil, que são eles: i) tornar o Brasil mais próspero e confiável no ambiente digital; ii) aumentar a resiliência brasileira às ameaças cibernéticas; e iii) fortalecer a atuação brasileira em segurança cibernética no cenário internacional (BRASIL, 2020a, p. 4-5).

Segundo a E-Ciber, alguns dados contribuíram para uma maior coordenação na temática de segurança cibernética brasileira, uma vez que o diagnóstico traçado no período de lançamento da estratégia apontava o Brasil como o segundo país com maiores perdas por ataques cibernético, assim como apenas 11% dos órgãos federais tendo capacidade suficiente em governança cibernética (BRASIL, 2020a). Além disso, dados da ITU (International Telecommunication Union) apontava o Brasil como o 70º colocado no índice de segurança global (ITU, 2018 apud FAVERO, 2022, p. 59) e 66º no ranking das Nações Unidas de tecnologia da informação e comunicação (ITU, 2017 apud FAVERO, 2022, p. 59).

Um dos pontos já salientados ao longo do presente texto se torna nítido e necessário, que seria a chamada tríplice hélice, uma união das esferas públicas, privadas e acadêmicas, a qual é citada na E-Ciber e foi estabelecida para que sua criação fosse concluída (PAGLIARI; AYRES PINTO; VIGGIANO, 2020 apud FAVERO, 2022). Por isso, nenhum ator sozinho consegue cuidar efetivamente das mudanças que ocorrem no ciberespaço e na rede informacional, sendo necessários, segundo o documento, uma maior capacitação de profissionais em cibernética, assim como uma “maior conscientização dos usuários” no uso de TICs e do ciberespaço (BRASIL, 2020a). A carência de leis efetivas para o combate a crimes cibernéticos no país - assim como apontado na “Revisão da Capacidade de

Cibersegurança do Brasil (2020)[7]" - (FAVERO, 2022, p. 61), somado à "carência de alfabetização digital no país" aumenta a probabilidade de ataques cibernéticos, já que os usuários tendem a fazer um uso não seguro da internet (BRASIL, 2020a).

### 3.3 - Segurança cibernética pós-pandemia e dias atuais

Atualmente, toda a segurança cibernética brasileira é direcionada pelo documento citado anteriormente, o E-Ciber, sendo o Ministério da Defesa um dos principais órgãos de implementação dos programas e iniciativas que iriam aumentar a segurança na área. Além disso, o ComDCiber e o CDCiber (Centro de Defesa Cibernética), sob comando do MD, atuam em medidas em prol da defesa cibernética brasileira (INSTITUTO IGARAPÉ, 2021).

Outros dois órgãos importantes para o cenário brasileiro atual são a Agência Brasileira de Inteligência (ABIN) e a Agência Nacional de Telecomunicações (ANATEL). A primeira é responsável por fornecer inteligência civil ao Brasil, sendo o órgão central do Sistema Brasileiro de Inteligência, além de atuar para aprimorar a capacidade em inteligência cibernética, segurança da informação e comunicações (BRASIL, 2020c). A segunda é responsável pela regulação de todo o setor de telecomunicações do país, desde 1997, além de ser uma entidade integrante da Administração Pública Federal, vinculada ao Ministério das Comunicações, porém administrativamente independente e financeiramente autônoma (BRASIL, 2020d).

Desse modo, quando somado à quantidade de órgãos, estratégias e programas, entende-se que a cibernética brasileira é tratada de forma genérica, sem muitas especificidades, ressaltando a falta de estratégia clara do governo brasileiro no tema, segundo Favero (2020). A simples falta de mensuração com exatidão da quantidade de capital necessária para atuar nos problemas do setor e de cada área da cibersegurança, mostra sérias debilidades (FAVERO, 2020). Como o relatório do Igarapé (2021) aponta, um dos pontos fracos atualmente seria a "ausência de um plano orçamentário (ou expectativa de um) para desenvolvimento de planos para a implementação de ações estratégicas" (INSTITUTO IGARAPÉ, 2021, p. 32).

---

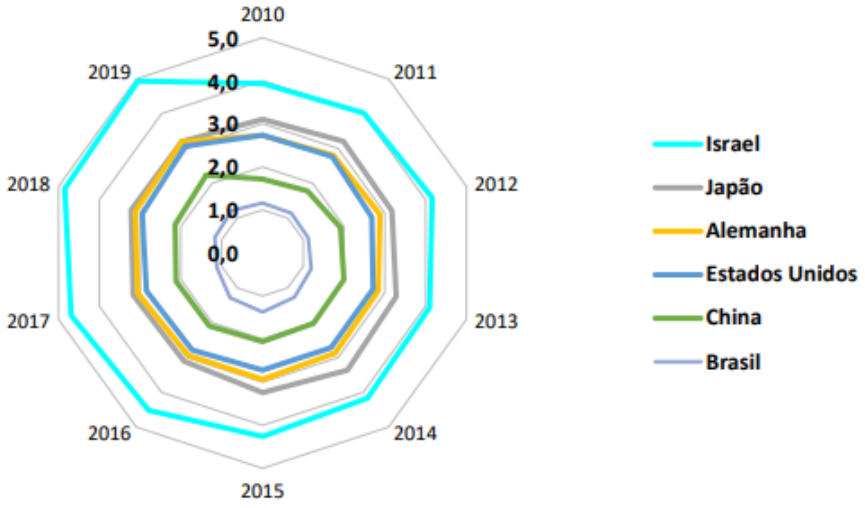
[7] A Revisão da Capacidade de Cibersegurança do Brasil é um documento elaborado pela Organização dos Estados Americanos (OEA), em 2020, o qual analisava cinco principais esferas sobre o setor no país, com destaques negativos para a cultura cibernética brasileira, educação e treinamento em segurança cibernética, assim como a falta de leis efetivas que punem autores de crimes cibernético (FAVERO, 2022). As esferas citadas são: a) Política e estratégia de segurança cibernética, b) cultura cibernética e sociedade, c) educação, treinamento e competências em segurança cibernética, d) normas, organizações e tecnologias e e) Estruturas jurídicas e regulamentações (OEA, 2020 apud FAVERO, 2022).

Ainda, como destaca Castro (2020) em seu texto, o Brasil possui recursos orçamentários para investimento no setor, porém peca ao não alocar de maneira regular e adquirindo produtos para a área de defesa cibernética, além de continuar dependendo tecnologicamente de países estrangeiros, algo que desde do primeiro END de 2008, era previsto que fosse dada a devida atenção e alocação de recursos (CASTRO, 2020).

> No caso brasileiro, desde a Estratégia Nacional de Defesa de 2008 - que tinha como objetivo máximo a modernização da estrutura de defesa nacional, incluindo quando na reestruturação da indústria brasileira de material de defesa - (SOUZA, 2013), a defesa cibernética era vista como uma possibilitadora, dado que ela indiretamente traria capacidade tecnológica ao país, que, a seu turno, fomentaria o seu desenvolvimento nacional (CASTRO, 2020, p. 86).

Em termos de pesquisa e desenvolvimento tecnológico (P&D), como já dito, o Brasil possui evidentes dependências tecnológicas (FAVERO, 2020). Na Figura 4 é possível perceber a diferença de investimento no setor, comparado a outros países no mundo:

**Figura 4 -** Brasil e os países que mais investem em P&D (% PIB) - 2010-2019




Fonte: Fonseca, 2018

Desse modo, é possível perceber o quanto é desproporcional e pequeno o investimento brasileiro na infraestrutura tecnológica quando comparado aos países que mais investem no mundo, demonstrando uma nítida fragilidade, talvez não tanto pelo comparativo em si, mas pelo fato de que o investimento em ciência e tecnologia vem caindo ao longo dos últimos anos (FONSECA, 2018). Somente entre 2013 e 2020, houve uma queda de 37%, atingindo, principalmente, o Ministério da Educação e o Ministério da Ciência e Tecnologia que, por sua vez, de 2014 a 2020, teve uma redução de seu orçamento de 8,5 bilhões para 3,4 bilhões (NEGRI, 2021; MCTI, 2020 apud FONSECA, 2018).

Tal assunto é tão relevante que, neste trecho de Favero (2020), o autor aponta o quanto a dependência tecnológica pode vir a ser um problema que "afeta(rá)" tanto a governança quando a soberania cibernética:

> O assunto da dependência tecnológica é tratado pelo documento Diretrizes para a Consecução das Ações Setoriais de Defesa voltadas para a Guerra Eletrônica (BRASIL, 2020e). O documento cita claramente a necessidade do país de reduzir sua dependência tecnológica, o que seria vital para garantir o poder militar nacional (BRASIL, 2020e). Uma medida mitigadora seria justamente o aumento de investimento em pesquisa e desenvolvimento, além da aquisição de recursos e softwares (BRASIL, 2020e). Ainda sobre a questão da dependência tecnológica e as vulnerabilidades por elas causadas, Fernandes (2015a) afirma que estes são obstáculos tão sérios que impedem que o Brasil se torne soberano ciberneticamente (FAVERO, 2020, p. 69).

Segundo o relatório acerca da estratégia nacional do Instituto Igarapé (2021), a E-Ciber ainda pode ser considerada um importante passo para o país, ainda que haja um longo caminho para que a implementação das estratégias seja de fato concretizada. Sendo a segurança cibernética setor que não deve ser ignorado, também "não deve ser vista somente como uma propriedade de sistemas, redes, máquinas e infraestruturas [mas também como] um componente fundamental para o enfrentamento de ameaças híbridas no século XX", como vazamentos e sequestros de dados em massa que acontecem em todo o mundo (INSTITUTO IGARAPÉ, 2020, p. 33). Ainda, o próprio documento faz seis recomendações para o fortalecimento do tema no Brasil, dentre elas: maior transparência dos objetivos alcançados pela E-Ciber através de relatórios anuais; estabelecimento de canais de comunicação com a sociedade civil; aprimoramento da segurança no compartilhamento de dados entre o setor público e privado; priorização de um planejamento multissetorial para implementação da E-Ciber; e também avaliação da necessidade da criação de uma lei de segurança cibernética que destaque crimes cibernéticos (INSTITUTO IGARAPÉ, 2020).

Quando analisados os dois principais países em termos de segurança cibernética e tecnologia 5G, China e Estados Unidos ganham destaque em relação ao Brasil. O país sulamericano e o asiático, acabaram por seguir o modelo de implementação estadunidense, desenvolvendo suas redes em épocas similares e com objetivos semelhantes, voltados à pesquisa científica (CASTRO, 2020). Porém, os chineses acabaram por politizar e securitizar a temática ainda no século XX, enquanto que, no Brasil, não havia qualquer tipo de discussão do assunto até o fim dos anos 90 (SOUZA; ALMEIDA, 2016 apud CASTRO, 2020). Apesar da desigualdade de recursos, determinante para o nível da cibersegurança brasileira, a China, desde a implantação das primeiras redes no país, já direcionava a produção acadêmica para a

necessidade de se desenvolver de forma efetiva, aumentando suas capacidades cibernéticas e tecnológicas, além de "atentar-se ao fato de que as tecnologias passavam a desempenhar papéis críticos" (LYU, 2019 apud CASTRO, 2020). Desse modo, Castro (2020) pontua bem quando ressalta o fortalecimento exponencial chinês no sistema nacional de inovação e aceleração de sua indústria,

> São exemplos de resultados concretos o seu próprio sistema operacional, intitulado de Kylin, e o desenvolvimento de microprocessador para servidores e roteadores da Huawei (MOREIRA; CORDEIRO, 2014). Ademais, em termos específicos de empresas atuantes em tecnologia da informação e comunicação, destacam-se a Huawei, a Lenovo (YUEN, 2015), o Alibaba Cloud, o Baidu, o TikTok e o Wechat (SCMP RESEARCH, 2020 apud CASTRO, 2020, p. 88-89).

Somado a isso, os Estados Unidos também possuem forte atuação junto a suas empresas, tais como a utilização global de ferramentas como o Google, do sistema Microsoft, da cadeia da Amazon, das tecnologias criadas pela Cisco e pela Apple, contribuindo para uma influência poderosa do país em várias redes cibernéticas ao redor do globo (CASTRO, 2020).

Apesar disso, há uma notória diferença entre os dois países e o Brasil. Enquanto este atua para criar uma base sólida de segurança cibernética, produção acadêmica, aumento de pesquisas e desenvolvimento tecnológico, pelo estabelecimento de uma defesa sólida contra ataques cibernéticos, entre outros, Estados Unidos e China estão mais voltados para a atenção a ameaças como o crime cibernético e o hacktivismo, ou "para conflitos que, de fato, ameaçariam às infraestruturas críticas estatais, a exemplo da espionagem cibernética, da sabotagem cibernética, do terrorismo cibernético e da guerra cibernética" (CASTRO, 2020, p. 92).

Em termos de documentação mais voltada para a internet, em março de 2020, foi criada a Instrução Normativa sobre Requisitos Mínimos de Segurança Cibernética para 5G, através do GSI/PR, a qual estabelecia "requisitos mínimos de segurança cibernética que deverão ser adotados no estabelecimento das redes de 5ª geração (5G) de telefonia móvel, de cumprimento obrigatório pelos órgãos e entidades da administração pública federal encarregados da implementação das redes 5G" (DOU, 2020, p. 1). Desse modo, a Instrução Normativa estabelece até mesmo requisitos mínimos de segurança acerca de provedores, tipos de conexões, redes e, até mesmo, termos mais técnicos como, "a fim de evitar que redes

*roaming*[8] acessem os sistemas de núcleo, as empresas prestadoras de serviço deverão implementar o SEPP (*Security Edge Protection Proxy*)[9] no 5G." (DOU, 2020, p. 2).

Um ponto importante sobre a norma é que estabelecia como regra a auditoria dos serviços na rede 5G, o qual englobaria empresas, consumidores, parceiros, governo e instituições de pesquisa, incentivando a cooperação entre estes atores para que fosse garantida uma maior segurança cibernética, assim como a tomada de decisão acerca do uso de equipamentos e dispositivos TICs (DOU, 2020). Por fim, três incisos do Artigo 5º, chamam atenção para o tratamento com a tecnologia no país,

> XVIII - cabe à empresa prestadora de serviços manter os aspectos de segurança da informação, quais sejam: disponibilidade, integridade, e confidencialidade na atividade de tráfego na rede 5G, em cumprimento às recomendações deste ato normativo, sem prejuízo, em caso de comprometimento da segurança, da esfera penal, cível e administrativa; XXI - mensalmente, as prestadoras de serviço deverão registrar o estado de configuração dos equipamentos de sua rede (resultado do gerenciamento de configuração), contendo informações como topologia de rede, versões de hardware e de software dos equipamentos, a fim de auxiliar a atividade de auditoria; e XXII - os incidentes de segurança cibernética ocorridos deverão ser informados, imediatamente, ao Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (DOU, 2020, p. 3).

Tais pontos apresentam uma maior fomentação da segurança cibernética no Brasil, direcionando estratégias práticas e direcionadas para o tema. Apesar disso, a Instrução Normativa foi anulada com base em um Projeto de Decreto Legislativo (nº 447/20), aprovado em maio de 2022, o qual alegava que o GSI não possuía competência para tratar sobre o tema, mas sim a ANATEL, alegando até mesmo que a o órgão teria invadido a competência da agência de telecomunicações brasileira (CÂMARA, 2022b). Apesar do ocorrido, não se deve descartar o documento por inteiro, mas sim utilizá-lo como uma base para o futuro desenvolvimento de estratégias ainda mais robustas e precisas sobre a segurança cibernética e a rede 5G no país.

[8] Roaming: capacidade de enviar e receber dados na telefonia móvel por intermédio de redes móveis fora do local em que a própria companhia fornece os serviços, numa zona onde o serviço é provido por outra operadora (DOU, 2020, p. 1).

[9] Tipo de criptografia que garantem a confiabilidade e integridade da rede 5G, fazendo com que seja possível a conexão segura entre redes 5G (BROADFOWARD, 2022)

# 4. A TECNOLOGIA 5G E OS POSSÍVEIS DESAFIOS DO BRASIL COM SUA IMPLANTAÇÃO

A partir dessa discussão, ao analisarmos a evolução da tecnologia na área de telecomunicações, identifica-se o termo "G" como as gerações dos tipos de conexões móveis. Em 1991, surgiu a tecnologia 1G de forma popularizada e para os civis, mas foi durante a Segunda Guerra Mundial que os comunicadores via rádio se tornaram um poderoso e decisivo artifício de guerra (TEKIR, 2020). Ao longo dos anos, do tipo de conexão de rádio e analógica, passamos por banda larga, introdução de SMSs, TV pelo celular e internet móvel (já nos anos 2000), e principalmente o aumento da velocidade de conexão como, por exemplo o download de um vídeo em Full HD, dentro de poucos minutos, em um celular com chip 4G (TECMUNDO, 2021).

É neste contexto que surge a tecnologia 5G, o qual promete integrar ecossistemas dos lares (casas), carros inteligentes, implemento da telemedicina, revolução do entretenimento, uma forma de conectar não só pessoas, mas pessoas e coisas (Internet das Coisas[10]) (REPLY, 2021). Logo, surge uma gama de possibilidades positivas para a sociedade, mas também para práticas ilegais e danosas para a mesma, uma vez que estamos intensificando cada vez mais a integração entre as pessoas em todo o mundo, em um sistema internacional já conectado e vulnerável.

O 5G surge para mudar todo o modo como a sociedade trabalha, se comunica e vive, transformando de um ambiente em que o uso da tecnologia celular era de quase somente troca de mensagens para interações mais aprofundadas hoje em dia, tais como redes sociais, jogos e softwares estruturados, chegando a atingir uma interação de bilhões de artefatos conversando entre si, formando uma malha digital para um mundo plenamente conectado (CEBRI, 2020). De acordo com o relatório apresentado pelo Centro Brasileiro de Relações Internacionais (CEBRI) acerca da segurança cibernética brasileira e a tecnologia 5G no cenário nacional, a transformação tecnológica provocada pelo 5G ocorrerá em três aspectos:

> a) aumento do potencial de banda para aplicações, chegando de uma a duas ordens de magnitude maior que a tecnologia 4G do Brasil, onde câmeras de segurança pública de alta definição poderão ser usadas para capturar detalhes do rosto de pessoas ou vídeos de realidade virtual e aumentada, bem como poderão ser

[10] "A chamada Internet das Coisas consiste na implementação de sensores e circuitos integrados (chips) nos objetos. Os sensores transformam os sinais analógicos em digitais, e os chips armazenam, processam e modulam/desmodulam sinais de radiofrequência que são comunicados por antenas e conectados pela infraestrutura de telecomunicações, permitindo sua utilização em rede e processamento/armazenagem na nuvem" (MAJEROWICZ, 2019, p. 17-18 apud CASTRO, 2020, p. 51).

> sobrepostas em tempo real para auxiliar em operações nas fábricas, por exemplo;
> b) queda da latência em uma ordem de grandeza, permitindo tempo de resposta instantâneo, exemplificando: pode-se solicitar a um carro autônomo que pare em nanosegundos; e
> c) incremento em duas ordens de magnitude do número de dispositivos conectados simultaneamente, possibilitando, entre outros casos, que milhares de sistemas de controle industrial possam trabalhar em completa coordenação por meio sem fio (CEBRI, 2020, p. 9).

Desse modo, diferentemente das gerações anteriores (2G, 3G e 4G) que focavam somente em expansão e melhoramento das taxas de transmissão de comunicação, o 5G tem foco também na especificação de serviços variados, prometendo diversificar e massificar a Internet das Coisas (IoT) (ANATEL, 2021). A exemplo do 4G, o qual foi conhecido como a "era dos aplicativos", introduzindo novos modelos de negócios e tendências mundiais de consumo, empresariais e comportamentais, os avanços que o 5G trará no decorrer do tempo prometem transformar todo o mundo digital e encontrar soluções para atender diversas demandas pessoais e de negócios (ANATEL, 2021).

Com cerca de cinco avanços esperados em relação à tecnologia anterior, o 5G promete, segundo a agência de telecomunicações brasileira (ANATEL): (1) um aumento das taxas de transmissão - maior velocidade; (2) baixa latência: redução do tempo entre o estímulo e a resposta da rede de telecomunicações; (3) maior densidade de conexões: aumento da quantidade de dispositivos conectados em uma determinada área; (4) maior eficiência espectral: incremento da quantidade de dados transmitidos por unidade de espectro eletromagnético; e (5) maior eficiência energética dos equipamentos: redução do consumo de energia, com consequente aumento da sustentabilidade (ANATEL, 2021). Aliado a estes cinco avanços, há três modos de usos esperados pela agência até o momento:

> (a) Banda Larga Móvel Avançada: focada em altas velocidades de download e upload, para as novas necessidades do usuário convencional; (b) Controle de Missão Crítica: focada em prover conexão com baixíssima latência e altíssima confiabilidade, voltada para aplicações sensíveis a atrasos e erros como carros autônomos, cirurgias remotas, controle remoto de maquinário industrial; e (c) Internet das Coisas Massiva: focada em atender grande quantidade de dispositivos IoT, com alta cobertura e baixo consumo de bateria, levando a Internet das Coisas a um novo patamar de atendimento (ANATEL, 2021, s/p).

Com isso, entende-se que, como o próprio órgão responsável atualmente pela implantação da tecnologia no Brasil coloca, o 5G trará grandes mudanças para o país, que atua contra o tempo para criar uma infraestrutura que possa comportar a tecnologia. Como no

relatório emitido pelo CEBRI em 2020, o país ainda se mostrava precário durante os chamados grandes eventos - Copa do Mundo e Olimpíadas -, com pouco compartilhamento de dados e tecnologia entre a esfera pública, privada e civil, a chamada tríade (CEBRI, 2020).

Quando comparamos o Brasil com outros países no mundo que começaram sua infraestrutura tecnológica antes mesmo da implantação do 5G, percebemos um verdadeiro abismo de inovação em comparação a países como EUA e China. Nesse contexto, há de se discutir a capacidade tecnológica do 5G, seu poder, a capacidade brasileira de implantação da tecnologia, assim como a sua relação com o Sistema Internacional.

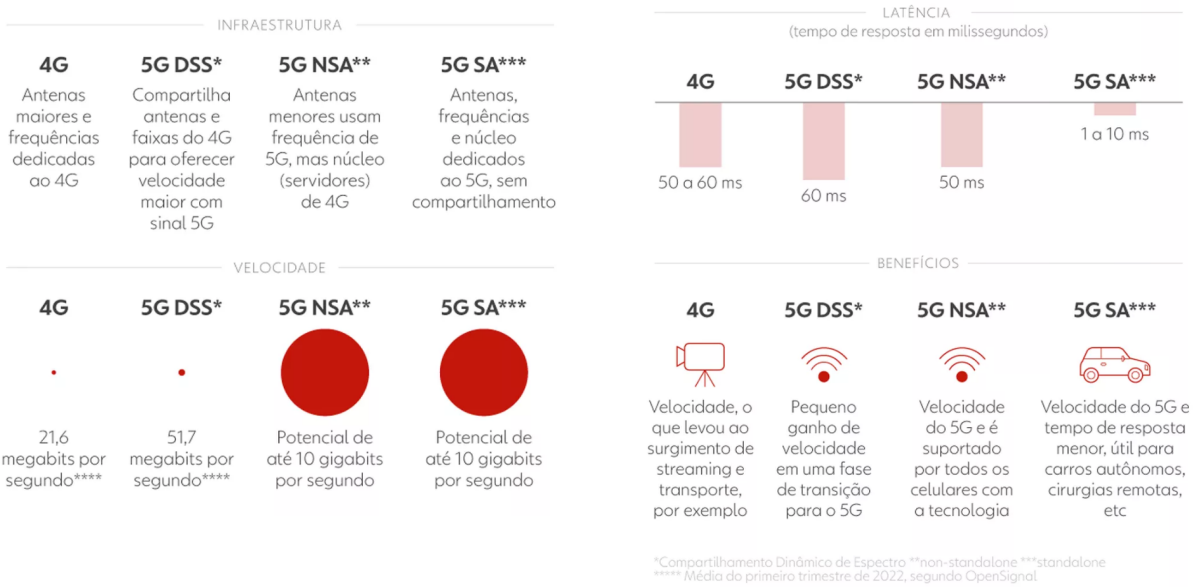
### 4.1 - Capacidade tecnológica e sua relação com o Sistema Internacional

Ainda não se sabe a real capacidade da tecnologia 5G e seu poder de aplicação na sociedade, seja para o bem ou para o mal. Porém, há algumas projeções de sua extensão tecnológica, a qual atualmente não faz parte de nossa realidade. Como já dito, sua diferença e seus avanços em relação às gerações antecessoras traduzem uma grande evolução, podendo ser considerado um novo marco para a tecnologia.

Dentre suas possibilidades, a Anatel (2022) cita sua flexibilidade de acordo com a aplicação utilizada, chamada de *network slicing* ou “fatiamento da rede”. Este processo é caracterizado pela adaptação que a rede executa automaticamente, de acordo com a necessidade. Como exemplo, vídeos de alta resolução podem demandar uma grande largura de banda (demanda mais da rede), enquanto que outras aplicações, como cirurgias assistidas ou até mesmo carros autônomos, demandarão latências bem menores - demanda menos da rede (ANATEL, 2021). Em outras palavras, a rede 5G será capaz de se adaptar e entregar o melhor desempenho para a determinada tarefa, não importando o quanto isso demande da rede (uma alta latência e largura de banda), otimizando a rede através do “fatiamento”, isolando virtualmente os segmentos de rede necessários para a aplicação demandada (ANATEL, 2021).

A Figura 5, trazida pelo veículo web G1, exemplifica a infraestrutura, latência e benefícios da tecnologia 5G em três modos distintos: (1) DSS: uma evolução simples em relação ao 4G; (2) NSA: evolução maior, porém utilizando servidores 4G; (3) SA: autossuficiência da rede, em que há o emprego total da tecnologia 5G (G1, 2022).

**Figura 5 -** Informações técnicas acerca do 5G




Fonte: G1, 2022

Resgatando alguns dos termos já utilizados na presente monografia, o ciberespaço tende a se expandir tecnologicamente e, como visto, sua estrutura está cada vez mais se transportando para armazenamento em nuvem[11] e um maior fluxo de dados. A quinta geração está sendo desenvolvida para que todo este fluxo de dados, através das TICs, dentro do ciberespaço, seja mais eficiente, facilitando e otimizando atividades, seja em âmbito público/militar, privado ou civil. Desse modo,

> [..] a tecnologia tende a se intensificar no uso de dispositivos baseados em *softwares* e sensores conectados à rede –de assistentes virtuais, eletrodomésticos a maquinário fabril– e de projetos de inteligência artificial, automatização de transportes e lares, dentre outros necessários à implementação das chamadas cidades inteligentes (CARVALHO, 2021, p. 12).

Já em relação à IoT (Internet das coisas), existem diversas iniciativas, majoritariamente privadas para sua expansão, principalmente no âmbito doméstico, mas também nas chamadas cidades inteligentes. Estas, em suma, têm como objetivo melhorar a vida de seus cidadãos através de "uma profunda automação tecnológica e integração do espaço urbano à rede digital" (CARVALHO, 2021, p. 12). Ou seja, sensores de IoT fariam o controle de câmeras de vídeo, coleta e análise de diversos dados que possibilitarão antecipar ações nocivas à sociedade, ou até mesmo o controle do tráfego de forma automatizada e mais

[11] "O armazenamento em nuvem é um modelo de computação em nuvem que permite armazenar dados e arquivos na Internet por meio de um provedor de computação em nuvem que você acessa usando a Internet pública ou uma conexão de rede privada dedicada" (AWS, 2022, p. 1).

rápida. Já em âmbito doméstico, podemos citar, por exemplo, a implementação de IoT em geladeiras que analisam os alimentos com maior consumo e informam quando atingirem determinada quantidade e, até mesmo, já realizam a compra em um supermercado online (CARVALHO, 2021); aumentos de velocidade do tempo de resposta na frenagem de carros em 10x, ou a mudança do tempo de downloads de minutos para milissegundos (G1, 2022).

Antecipando parte do tema que será tratado no ponto 4.2 deste trabalho, a aplicação da tecnologia de quinta geração pode beneficiar diretamente o agronegócio brasileiro, que hoje utiliza de comunicação via satélite, possuindo um grande potencial de utilização, a fim de automatizar processos e atingir níveis maiores de eficiência e precisão para a agricultura e agropecuária (CEBRI, 2020). Além disso, outro setor brasileiro que poderá ser diretamente afetado é a mineração, a qual poderá eliminar riscos humanos, segundo o relatório da CEBRI (2020), substituindo suas frotas de grandes veículos por autônomos, assim como robôs ao invés de pessoas dentro das minas.

Em âmbito industrial, poderá ser feita a automatização fabril de máquinas, sensores, controladores e atuadores, os quais terão uma troca de dados em alta velocidade, aumentando a produção e diminuindo o tempo gasto através da tecnologia, permitindo a orquestração completa do ciclo de fabricação de produtos (CEBRI, 2020). Além disso, neste caso, será possível que empresas (e órgãos capazes) criem redes privadas 5G, as quais poderão controlar o fluxo de dados, isolando o tráfego dos registros dos sensores do ambiente externo, ou seja, aumentando a segurança cibernética destas organizações (CEBRI, 2020).

Apesar de existirem muitas oportunidades e projeções positivas acerca do 5G, há também um grande receio acerca deste fluxo de dados, a vulnerabilidade da rede e o aumento de crimes como espionagem, sabotagem ou até guerra cibernética. É por isso que o relatório do CEBRI ressalta a “necessidade do aumento da segurança cibernética, com uma exposição cada vez maior de sistemas ciberfísicos, em um contexto de desconfiança em relação a fornecedores” (CEBRI, 2020, p. 14). Desse modo, a padronização das redes e ações de certificação que garantam uma ampla validação da segurança será fundamental, assim como o projeto *EU Toolbox on 5G Cibersecurity* instaurado na União Europeia, que cria regras rígidas entre os países-membros, a fim de minimizar riscos e aumentar os critérios de segurança cibernética frente às redes 5G (CEBRI, 2020).

Logo, com o crescente aumento do fluxo de dados entre redes e dispositivos, além do avanço impressionante que o 5G trará, aumentam também as possibilidades para a realização de ataques cibernéticos, ou seja, os riscos e ameaças (CARVALHO, 2021). Com isso, um fato se destaca, partindo de uma análise sistêmica internacional: tal tecnologia não é neutra, ela representa interesses e poder, na perspectiva estatal, atuar como uma projeção de poder (MAJEROWICZ, 2020). Logo, não é de se estranhar que os Estados estejam cautelosos quanto à aquisição de tecnologias estrangeiras para seus sistemas de informação e comunicação:

> O fato de as operadoras de rede móvel precisarem contar com fornecedores de componentes terceirizados exigirá um foco maior no gerenciamento de riscos da cadeia de suprimentos. As ameaças - em particular apoiadas pelo Estado - podem tentar explorar os pontos fracos da cadeia de suprimentos para realizar ataques às redes de telecomunicações [...]. Como as redes 5G serão predominantemente baseadas em software, os invasores podem tentar inserir backdoors difíceis de encontrar nos produtos que os provedores de serviços usam para fornecer funções 5G (CIO, 2020, s/p).

Atualmente, a quinta geração da internet (5G) se apresenta como o novo ponto de inflexão para a ordem internacional, como apontam os recentes desentendimentos entre EUA e China em relação à tecnologia (G1, 2021a). A hegemonia estadunidense no setor cibernético, a qual detém boa parte das empresas responsáveis por implementar as novas estruturas de redes 5G, permite que o país possua vantagens estratégicas e de manipulação frente a seus aliados, transformando-as em recurso de poder da geopolítica contemporânea (ASSIS, 2020 apud CARVALHO, 2021). Em contrapartida, empresas estatais e privadas chinesas, tais como Huawei e ZTE, avançam na produção interna de suprimento tecnológico para criar infraestruturas 5G e de dispositivos capazes de navegar pela rede de forma satisfatória (CASTRO, 2020), criando um cenário de embate tecnológico entre as duas potências frente à chamada “Corrida do 5G” (G1, 2021a).

Naturalmente, surgem desconfianças de ambos os lados, como até mesmo o relatório do CEBRI (2020) apontava em relação aos fornecedores; os americanos acusam as empresas chinesas de não terem uma segurança de seus equipamentos e dispositivos, fazendo com que os países do grupo “Five Eyes Alliance” (Cinco Olhos)[12] também barrasse os chineses em seus países (G1, 2021a). Já os chineses argumentam que os americanos têm como objetivo “minar o crescimento tecnológico chinês”, além de alegarem que seus equipamentos não são vulneráveis e que não compartilham informações com o governo chinês (G1, 2021a).

[12] Aliança entre Estados Unidos, Reino Unido, Nova Zelândia, Canadá e Austrália, a partir do Tratado de UKUSA, que visa a cooperação entre as inteligências dessas nações (THE GUARDIAN, 2010).

De todo modo, o Brasil se encontra no meio deste conflito, em um estágio de "atraso no desenvolvimento da tecnologia 5G" (CEBRI, 2020, p. 17), com pouca produção acadêmica e governamental acerca do tema, enquanto outros países no mundo avançam com a implementação da tecnologia e o "Leilão do 5G" cria mais incertezas sobre a infraestrutura da quinta geração de internet em território nacional.

### 4.2 - A implementação do 5G no Brasil

Para que fosse dado o primeiro passo na implementação da tecnologia 5G no país, foi preciso realizar o chamado Leilão do 5G, em 2021, ou seja, licitações dos lotes das faixas de frequência de rede - no caso do 5G foram disponibilizadas de 700 MHz; 2,3 GHz; 3,5 GHz e 26 GHz (G1, 2021b). Foi realizado literalmente um leilão por tais frequências de rede, que tinha como objetivo determinar as empresas que teriam o aval da Anatel para operacionalização este tipo de tecnologia de comunicação dentro do Brasil, sendo que o leilão movimentou um total de R$ 47,2 bilhões, cerca de 2,5 bilhões a menos do que o esperado (G1, 2021b). Parte dos valores levantados, vai diretamente para o governo, mas parte vai para compromissos de investimentos feitos pelas empresas vencedoras do leilão - que se resumem em 11 ao todo, 5 delas já possuem autorização para prestação de serviço móvel no país (G1, 2021b).

Em 2022, um ano após o leilão realizado pela Anatel e o Ministério das Comunicações (MCom), a tecnologia caminha para um estabelecimento completo no país. Até novembro do mesmo ano, foram instaladas mais de 6 mil antenas de 5G nas faixas de frequência 2,3 GHz; 3,5 GHz e 26 GHz, sendo Brasília a primeira cidade a receber o sinal ainda em julho (MCOM, 2022). Segundo o MCom, a capital do país é considerada a segunda rede de conexão 5G com maior velocidade do mundo, com base no relatório elaborado pela *Opensignal* (MCOM, 2022).

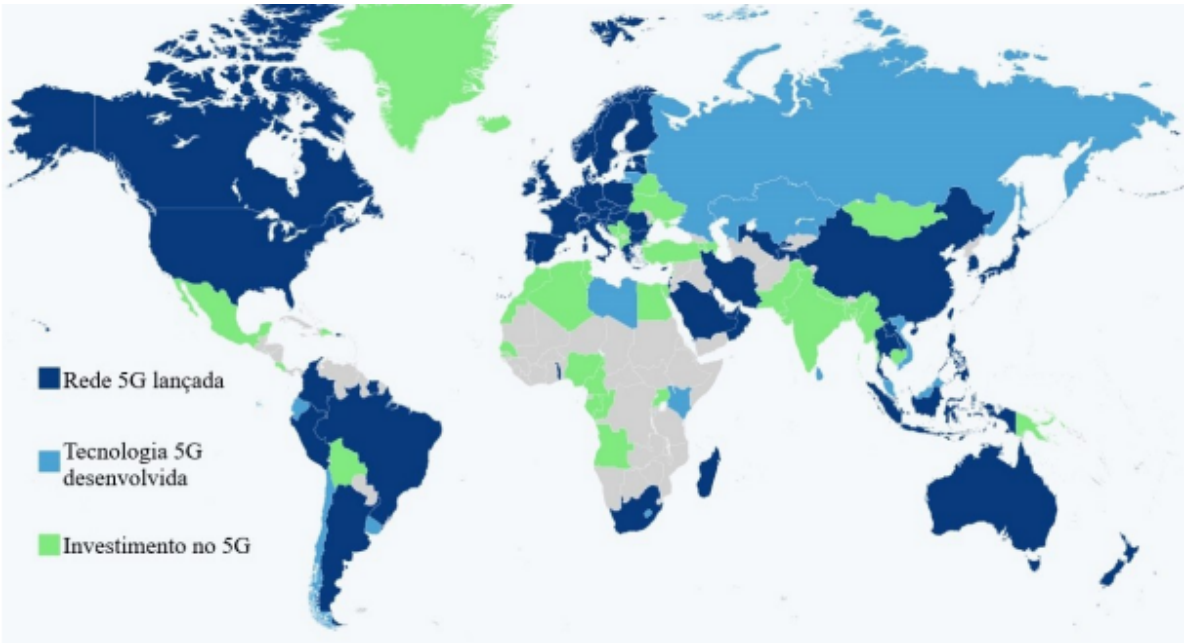
Há um cronograma de implementação e compromissos de abrangência do 5G por parte dos responsáveis, disponibilizado pela Anatel, que prevê a conclusão de instalação da conexão em 100% somente em 2029 (ANATEL, 2022a). A implementação nas principais cidades do país tem sua previsão de conclusão em 2025, quatro anos após o leilão ter sido realizado. O calendário salienta problemas já ressaltados por documentos brasileiros acerca da segurança nacional, em que ressalta a dependência tecnológica externa, insuficiência de infraestrutura interna, assim como falta de diretrizes mais claras para a criação de estruturas sólidas no país. Em contrapartida, o cronograma vem se provando eficiente até o momento de

escrita da presente monografia, tendo o 5G sido ativado em todas as capitais nacionais em outubro de 2022, segundo o MCom (2022).

Já em âmbito internacional, algumas projeções são feitas de forma bem otimista, tais como: que em 2024 o número de usuários do 5G alcance 1 bilhão de pessoas no mundo; até 2025, metade das conexões móveis dos estadunidenses serão via 5G; até 2025, na China e Europa, a conexão móvel via 5G será de ao menos 30% (CARNEIRO, 2022). Como pode-se conferir na Figura 6, o Brasil alcançou um posto satisfatório e sob as expectativas quanto a implementação da tecnologia no país, quando comparado a outros países com maior investimento e capacidade tecnológica.

Ainda, além do Ministério das Comunicações trabalhar junto à Anatel para o fomento do 5G em território nacional, a Associação Brasileira de Telecomunicações (Telebrás), associação privada com 65 instituições associadas, idealizou o projeto chamado "5G Brasil", que conta com 20 instituições associadas - entre elas indústrias, universidades, centros de pesquisas e operadoras de telecomunicações -, tendo como objetivo viabilizar e estabelecer a comunicação entre diversos setores e esferas do governo (CARNEIRO, 2022). Buscando, desse modo, o apoio financeiro para disseminação e uso da tecnologia e até mesmo propiciando a elaboração de acordos de cooperação nacional e internacional para o desenvolvimento do 5G no Brasil.

**Figura 6 -** Panorama mundial da implementação da tecnologia 5G




Fonte: BUCHHOLZ, 2021 apud CARNEIRO, 2022, p. 29

Em termos de impacto econômico, estima-se que o 5G movimentará cerca de “3,3 trilhões de dólares e resultará em um aumento de produtividade em 8,7 bilhões de dólares em 2035” na América Latina (CARNEIRO, 2022, p. 48). Para o Brasil, é estimado um impacto econômico de a 1,2 trilhão de dólares, com um aumento da produtividade acima de 3 trilhões de dólares, até 2035 (SWAIN, et al., 2020 apud CARNEIRO, 2022). Além disso, há a expectativa de que o 5G movimente R$ 590 bilhões por ano, de acordo com levantamento feito pelo Ministério da Economia, em parceria com o Programa das Nações Unidas para o Desenvolvimento (PNUD) (MCOM, 2022).

Desse modo, a quinta geração da internet traz grandes impactos, perspectivas, oportunidades, mas também algumas ameaças para a sociedade brasileira. Com isso, é necessário um planejamento estratégico que construa uma infraestrutura de comunicações efetiva no país e, para isso, ao fim de novembro de 2022, a Anatel - a responsável pelo setor de telecomunicações no país e uma das principais responsáveis pelo 5G -, apresentou o Plano Estratégico 2023-2027, baseado em quatro principais valores: inovação, segurança regulatória, foco em resultados para a sociedade e efetividade e construção participativa (ANATEL, 2022b).

O planejamento é destrinchado em grandes objetivos estratégicos de resultado (voltados para os quatro eixos citados anteriormente) e de processos (eixos mais técnicos, de qualidade e infraestrutura da organização), além de metas, cenários prospectivos e usos futuros da conectividade (ANATEL, 2022b). O documento relata a atenção necessária para o aumento da capacidade de conexão e infraestrutura cibernética que a Indústria 4.0[13] vai requerer, sendo fundamental um grande volume de investimentos, de modo constante e permanente (ANATEL, 2022b). Além disso, especifica e ressalta a importância da tecnologia para a economia e setores do país:

> O 5G será catalisador de uma revolução digital em termos de suas aplicações, tendo um grande impacto sobre a oferta e fruição de serviços. Indústria, energia, segurança pública, medicina e entretenimento são exemplos de setores em que o 5G terá grande impacto (ANATEL, 2022, p. 28).

Quando comparado à China e aos Estados Unidos - países precursores e líderes da disputa do 5G, além de serem os principais em desenvolvimento tecnológico no mundo -, o

[13] Pode ser considerada a “quarta revolução industrial” e teve seu início nos anos 2000, a chamada “Indústria 4.0” é caracterizada pelo “crescimento exponencial da capacidade de computação e combinação de tecnologias físicas, digitais e biológicas” (MAGALHÃES; VENDRAMINI, 2018, p. 42 apud CASTRO, p. 17).

Brasil ocupa uma colocação aquém do esperado. Ainda durante o Governo de W. Bush, o governo estadunidense encarava o desenvolvimento tecnológico e a segurança cibernética como oportunidades, não como vulnerabilidades (CAVELTY, 2008 apud CASTRO, 2020). Atualmente, sob governo Biden, há uma hegemonia norte-americana no setor cibernético, baseado em uma coordenação elaborada entre o governo, empresas privadas e civis, sendo que o governante se reúne regularmente com as gigantes nacionais da tecnologia para discutir os rumos da segurança cibernética, como, por exemplo, no ano de 2021 que foi anunciado mais de 30 bilhões de dólares do Google e Microsoft em investimentos no setor para os próximos anos, além de treinamentos gratuitos e novas faculdades com foco no tema (CISO, 2021). Já no país asiático, desde a implementação de redes em território nacional se entendia a necessidade de fomentar suas bases de defesa cibernética, baseado em premissas acadêmicas e relatórios sobre o tema, se atentando ao fato de que as tecnologias passavam a desempenhar papéis críticos (LYU, 2019 apud CASTRO, 2020).

Logo, no que diz respeito à estrutura de segurança cibernética e a tecnologia 5G, segundo o CEBRI,

> Infelizmente, o Brasil se encontra em situação de atraso no desenvolvimento da tecnologia 5G e também na representatividade de sua padronização. No âmbito da academia, temos poucas pesquisas relevantes e patentes nas áreas de ondas milimétricas ou rádios com maciça quantidade de antenas (MIMOs) para esse tipo de aplicação, destacando-se, neste quesito, apenas poucos institutos de pesquisa (CEBRI, 2020, p. 17).

Do ponto de vista da implantação da tecnologia 5G no país, foi visto que segue de acordo com o cronograma apresentado e aprovado pelo MCom e a Anatel. Porém, quando analisado da ótica de evolução tecnológica de dispositivos e TICs, é onde se encontram as principais discussões. O principal foco da indústria nacional de equipamentos de redes é em redes óticas e redes cabeadas, destacando-se as empresas Padtec e Datacom, respectivamente (CEBRI, 2020). Algumas iniciativas isoladas existem, mas a maioria dos produtos de redes móveis, utilizados nas operadoras e outras empresas brasileiras, são provenientes de tecnologia estrangeira, fazendo com que a perspectiva tecnológica do Brasil fique restrita a parcerias com empresas estrangeiras, ou à importação da tecnologia (CEBRI, 2020). Ainda neste âmbito, o relatório do órgão de Relações Internacionais destaca que,

> [...] no espectro de segurança cibernética na tecnologia 5G, a preocupação da alta gestão nacional está em nível elevado. Como já foi mencionado, trata-se da tecnologia para viabilizar a sociedade digital do futuro, então é preciso se precaver apropriadamente. Além disso, há a discussão geopolítica de alinhamento entre países. Enfim, nesse sentido, vários decretos e normatizações têm sido apresentados,

> ao longo do último ano, com o objetivo de conferir segurança a essa transição para a tecnologia 5G. Do ponto de vista da normatização de segurança, o governo federal emitiu o Decreto N. 10.222, em 5 de fevereiro de 2020, da Estratégia Nacional de Segurança Cibernética (E-Ciber), que traz diretrizes para todo o sistema de gestão administrativo federal sobre como lidar com segurança cibernética, e qual é a nossa estratégia para ficarmos mais fortes nessa área, como país (CEBRI, 2020, p. 18).

O trecho, então, salienta, mais uma vez, a importância da tecnologia e de se ter uma segurança cibernética consolidada, além de que o E-Ciber é o plano administrativo federal principal para lidar com o tema. Apesar disso, é sabido que o mesmo apresenta falhas, além de não discorrer especificamente a respeito de requisitos mínimos de segurança cibernética em relação às redes 5G, ressaltando a falta de uma coordenação sólida em âmbito federal, que ainda de forma muito incipiente.

Com isso, é perceptível o avanço tecnológico que o 5G proporcionará nos próximos anos, em vários setores da nossa sociedade, impactando desde o nível macro, até o doméstico com a automatização de casas, ou seja, como a sociedade trabalha, se comunica e vive. Segundo números da Infra News Telecom (2023), o Brasil precisa formar 70 mil profissionais de tecnologia até 2024, número que poderá representar um déficit de 260 mil pessoas qualificadas no período. Ainda segundo o veículo, hoje o setor de TIC é responsável por 845 mil empregos e forma 46 mil alunos anualmente em cursos de tecnologia. Desse modo, é fundamental que o Brasil fomente sua capacidade de segurança, capacitando sua população como um todo, para que o país esteja preparado tanto para usufruir dos benefícios que a tecnologia 5G irá propiciar às pessoas, empresas e instituições, quanto para se defender contra crimes, delitos e ataques cibernéticos.

## 5. CONSIDERAÇÕES FINAIS

Como apresentado desde a introdução, a tecnologia tem sido um marco de poder e transformação da sociedade e do Sistema Internacional. A relação entre a tecnologia e o Estado tem se mostrado fundamental na história da humanidade, algumas vezes vista como inovações ou criações. Atualmente, esse aspecto pode ser usado para a manutenção de poder, transformação da sociedade, mudança de hegemonia internacional ou até mesmo para ditar regras e tendências socioeconômicas.

Ao longo dos anos, o conceito tem se transformado por si só e tem transformado a sociedade, trazendo inovação e desenvolvimento constante, ou até mesmo uma vantagem estratégica e posições de destaque no sistema internacional. Como exemplo, temos os casos do domínio do metal e da pólvora, o qual possibilitou a consolidação e expansão do colonialismo europeu; da bomba nuclear, após o fim à Segunda Guerra, ao equilíbrio de poder e que sustentou a ordem bipolar por décadas; do domínio sobre as TICs (Tecnologia da Informação e Comunicações), que garantiu aos EUA a posição de grande potência mundial no pós-Guerra Fria (TEKIR, 2020).

Já no âmbito da internet, esta inovação é extremamente recente, datada ainda do final do século XX, tendo o Brasil se inserido formalmente na internet global a partir de 1992, e começado a comercializá-la em 1995 (CASTRO, 2020). Desde o início, o país se posicionou de forma atrasada em relação à implementação das redes, estruturando tardiamente o seu espaço cibernético, com infraestruturas simples e suficientes para atender parte da população. O começo do século XXI não foi diferente, tendo um atraso também no começo de produções e debates intelectuais acerca da capacidade do ciberespaço, seus riscos e vulnerabilidades nacionais.

Nesse contexto, a presente monografia teve como objetivo analisar em que medida o Brasil tem se preparado, tecnológica e institucionalmente, para garantir sua cibersegurança e enfrentar os desafios que a tecnologia 5G apresenta, uma vez que o papel do espaço cibernético na política global contemporânea tem se tornado cada vez mais importante. Para isso, o trabalho foi desenvolvido em três principais eixos, que são: o ciberespaço, a segurança cibernética brasileira e a tecnologia 5G no país.

O primeiro capítulo teve como foco analisar o ciberespaço como um todo, investigando suas características, assim como as relações entre países, pessoas e coisas; a

emergência dos desafios do mundo virtual; quais são os principais crimes e ataques cibernéticos que ocorrem desde o princípio da tecnologia; a estruturação da segurança cibernética; além dos possíveis impactos desses conceitos na sociedade contemporânea. Assim, compreendeu-se que a temática é de extrema importância, não só para o Brasil, mas para todo o mundo, já que se trata de um ambiente sem fronteiras, com capacidades e potenciais de impacto imprevisíveis. Com isso, o debate internacional deve ser incentivado, não só pela sociedade civil, acadêmicos ou empresas privadas, mas por órgãos internacionais competentes, tais como a ONU e outros encontros recentes que acontecem para o estabelecimento de cooperação cibernética.

Já o segundo capítulo teve como objetivo analisar como o Brasil tem se preparado ao longo dos anos, em termos de segurança cibernética e integração ao ciberespaço, além das capacidades de produção tecnológica própria e a evolução de estratégias e políticas em nível nacional acerca do tema. Para isso, a seção foi dividida entre três recortes temporais, sendo eles: antes de 2018, quando houve teve a estruturação primária da segurança cibernética brasileira, inserção da tecnologia e internet no país; 2018 a 2020, período com alta consistência de produções intelectuais, principalmente por parte do governo, sendo identificados os principais documentos que impactaram o setor de cibersegurança do país; e, por fim, o período pós 2020 e dias atuais, o qual marca medidas em vigor propostas pelo governo brasileiro, assim como a implementação de estratégias e estruturas para a tecnologia 5G.

Foi identificado que o Brasil teve avanços materiais significativos na temática, desde sua primeira formulação na Estratégia Nacional de Defesa (END), de 2008, com a elaboração de documentos que apontam erros e sugerem soluções a curto, médio e longo prazo, porém, a própria efetividade das ações não é respeitada, não sendo implementadas à risca ou dando a importância que se deveria. Isso, aliado ao fato da descentralização da abordagem da questão cibernética, principalmente a respeito de órgãos responsáveis - em determinado momento são as Forças Armadas, em outro momento o Ministério da Defesa, CDCiber, ComDCiber, Gabinete de Segurança Institucional (GSI) ou Anatel - gera-se confusão e dificulta-se ações efetivas na área.

Além disso, o principal problema encontrado é a deficiência na progressão de capacidade tecnológica nacional capaz de suportar a evolução mundial, sem gerar dependência brasileira em relação a outros países. Este aspecto é apontado como alerta desde

o END de 2008 e a impressão que se tem é que assim seguiu, até o último documento, o E-Ciber, de 2022. Este, por sua vez, foi um dos poucos a citar a tríade necessária para a estruturação de uma estratégia cibernética eficiente nacionalmente, envolvendo o âmbito público (governo, órgãos públicos e legislativo), privado (empresas e instituições) e civil (acadêmicos e sociedade).

O terceiro e último capítulo, teve como objetivo caracterizar a tecnologia 5G e seus desafios, além de analisar como o Brasil tem se preparado para a implantação da tecnologia no território. Compreendeu-se que a quinta geração da internet vai muito além do que um mero aumento de velocidade de tráfego na rede, maior capacidade de download ou menor latência em relação à rede 4G; seu objetivo é expandir a digitalização das sociedades e a capacidade de processamento do crescente fluxo de dados do ciberespaço. Isso representa um novo passo nas capacidades dos dispositivos, comunicação, armazenamento em nuvem, número de servidores no mundo, processos entre pessoas e dispositivos (a chamada Internet das Coisas) de forma mais dinâmica e eficiente, o que, consequentemente, aumenta os riscos, uma vez que os dados se apresentam dispersos no ciberespaço.

Ainda, entende-se que, do mesmo modo que o 5G proporcionará evoluções importantes para a sociedade, aumentará o risco e a vulnerabilidade de dados e processos nas redes. Para isso, é necessária a atuação nas três frentes principais do país: âmbito privado, público e civil. Segundo a Instrução Normativa Nº 4, que dispunha acerca dos requisitos mínimos de Segurança Cibernética que deveriam ser adotados no território nacional para o estabelecimento do 5G, já se apontava a necessidade de uma estrutura robusta brasileira, além da responsabilidade das empresas produtoras de TICs e dispositivos quanto a se atentar para possíveis vulnerabilidades de seus hardwares e softwares. Desse modo, quando o país terceiriza esse tipo de tecnologia e opta por importar quase que sua totalidade, há uma dificuldade na vigilância, auditoria, controle e própria segurança dos dados, dispositivos e redes, já apontada pela instrução que foi barrada pelo Congresso, com a prerrogativa de que a Anatel seria a responsável principal pela estratégia no país.

Retomando a pergunta base trabalhada no presente trabalho, “Em que medida o Brasil tem se preparado, tecnológica e institucionalmente, para garantir sua cibersegurança, implantar e enfrentar os desafios que a tecnologia 5G apresenta?”, conclui-se que o país ainda tem um árduo caminho a percorrer, se tratando de capacidades nacionais tecnológicas, de infraestrutura, legislação e normas voltadas para o tema. O próprio histórico negativo em

relação à importância para a pesquisa e desenvolvimento, assim como a falta de clareza e constância de investimentos destinados à segurança cibernética, fomenta o desinteresse - no caso da sociedade civil e privada - e o descaso - no caso do governo e órgãos públicos -, quanto ao tema. Uma vez que, no Brasil, 74,9% dos domicílios (116 milhões de pessoas) têm acesso à internet e 98% das empresas e 100% dos órgãos federais e estaduais utilizam a internet (BRASIL, 2020a), a união dessas três forças é importante para novos planejamentos estratégicos e ações efetivas.

Nesse ínterim, como citado no documento estratégico do governo, o E-Ciber, o país deve se alinhar academia e área produtiva, incentivando a pesquisa e o desenvolvimento de soluções em segurança cibernética, de modo que tragam a necessária inovação aos produtos nacionais nessa área crítica, atual e imprescindível. O papel do Estado brasileiro deve ser financiar pesquisas e progresso científico, elaborando estratégias claras que contribuam para boas práticas no ciberespaço, criando mecanismos para solucionar problemas, além de coordenar políticas públicas que incluam a sociedade civil e as empresas privadas. Desse modo, o Brasil poderá caminhar para atingir uma capacidade tecnológica, pensada ainda no END de 2008, capaz de coordenar os diversos setores do país, em que o cibernético adquira a capacidade suficiente para que não dependa de tecnologia estrangeira.

## 6. REFERÊNCIAS BIBLIOGRÁFICAS


AGÊNCIA BRASIL. **Ensino a distância conquista adeptos e aumenta após fim de restrições.** Brasília, 27 de nov. de 2021. Disponível em: <https://agenciabrasil.ebc.com.br/educacao/noticia/2021-11/ensino-distancia-conquista-adeptos-e-aumenta-apos-fim-de-restricoes>. Acesso em: 02 nov. 2022.

AGÊNCIA SENADO. **Ministério da Defesa fica com maior parte dos novos investimentos do Orçamento de 2022**. 21 de set. 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/09/21/ministerio-da-defesa-fica-com-maior-parte-dos-novos-investimentos-do-orcamento-de-2022>. Acesso em: 12 de nov. de 2022.

AGÊNCIA SENADO. **Governo negligencia defesa cibernética do país, aponta relatório da CRE**. 12 de dez. 2019. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/12/12/governo-negligencia-defesa-cibernetica-do-pais-aponta-relatorio-da-cre>. Acesso em: 13 de nov. 2022.

AGÊNCIA SENADO. **Política Nacional de Defesa é aprovada no Senado e segue para Câmara**. 02 de jul. 2022. Disponível em: <https://www12.senado.leg.br/noticias/materias/2022/06/02/politica-nacional-de-defesa-e-aprovada-no-senado-e-segue-para-camara>. Acesso em: 22 de nov. 2022.

ANATEL. **Tecnologia 5G**. Ministério das Comunicações. 22 jan. 2021. Agência Nacional de Telecomunicações. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/5G/tecnologia-5g>. Acesso em: 01 dez. 2022.

ANATEL. 2022a. **Compromissos de Abrangência do Leilão do 5G**. Agência Nacional de Telecomunicações. 19 jan. 2022. Disponível em: <https://www.gov.br/anatel/pt-br/regulado/universalizacao/compromissos-do-leilao-do-5g>. Acesso em: 27 dez. 2022.

ANATEL. 2022b. **Anatel aprova Plano Estratégico 2023-2027**. Agência Nacional de Telecomunicações. 21 nov. 2022. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-aprova-plano-estrategico-2023-2027>. Acesso em: 27 dez. 2022.

AWS. **O que é o armazenamento em nuvem?**. 2022. Disponível em: <https://aws.amazon.com/pt/what-is/cloud-storage/>. Acesso em: 22 de dez. 2022.

BBC. **Hackers 'roubam mais de US$ 1 bilhão em ataques a bancos'**. 16 de fevereiro de 2015. Disponível em: <https://www.bbc.com/portuguese/noticias/2015/02/150216_gch_quadrilha_hackers_lk>. Acesso em: 22 de nov. 2022.

BRASIL. Decreto nº 6.703. **Estratégia Nacional de Defesa**. Brasília, DF, 2008.

BRASIL. **Livro verde segurança cibernética no Brasil**. Brasília, DF, 2010. Disponível em: <https://redectidc.com.br/assets/files/2010%20-%20Livro%20Verde%20-%20Seguran%C3%A7a%20Cibern%C3%A9tica%20no%20Brasil.pdf>. Acesso em 20 nov. de 2022.

BRASIL, MINISTÉRIO DA DEFESA. **Manual de campanha**: guerra cibernética. EB70-MC-10.232. Brasília: COTER, 2017

BRASIL. **Programa de Defesa Cibernética na Defesa Nacional** (PDCND). 2018. 2018a. XV Congresso acadêmico sobre Defesa Nacional. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/palestra_cadn_xi/xv_cadn/programaa_daa_defesaa_ciberneticaa_naa_defesaa_nacional.pdf>. Acesso em: 10 de nov. 2022.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. **Institui a Política Nacional de Segurança da Informação**. 2018b. Decreto no 9.637. Brasília, DF. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/56970098/do1-2018-12-27-decreto-n-9-637-de-26-de-dezembro-de-2018-56969938#:~:text=1%C2%BA%20Fica%20institu%C3%ADda%20a%20Pol%C3%ADtica,da%20informa%C3%A7%C3%A3o%20a%20n%C3%ADvel%20nacional>. Acesso em 22 de nov. de 2022.

BRASIL. Lei n 13.709, de 14 de agosto de 2018. **Lei geral de proteção de dados (LGPD)**. 2018c. Lei no 13.709. Brasília, DF:Diário Oficial da União, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 22 nov. de 2022.

BRASIL. Portaria No 93, de 26 de setembro de 2019. **Aprova o Glossário de Segurança da Informação**. 2019. Portaria no 93. Brasília, DF. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em: 23 nov de 2022.

BRASIL. Decreto n° 10.222 de 5 de fevereiro de 2020. **Aprova a Estratégia Nacional de Segurança Cibernética**. 2020a. Decreto N 10.222. Brasília, DF: Diário Oficial da União de 6 de fevereiro de 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm>. Acesso em: 22 de nov. de 2022.

BRASIL. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF, 2020b.

BRASIL. **Missão, Visão e Valores** - Agência Brasileira de Inteligência. 22 de setembro de 2020. 2020c. Disponível em: <thttps://www.gov.br/abin/pt-br/acesso-a-informacao/institucional/missao-visao-e-valores>. Acesso em: 24 de nov. 2022.

BRASIL. **Institucional** - Agência Nacional de Telecomunicações. 17 de novembro de 2020. 2020d. Disponível em: <https://www.gov.br/anatel/pt-br/acesso-a-informacao/institucional>. Acesso em: 24 de nov. 2022.

BRASIL, MINISTÉRIO DA DEFESA. **Relatório de Gestão Integrado**. 2021. Transparência e Prestação de Contas da União. Disponível em: <https://www.gov.br/defesa/pt-br/acesso-a-informacao/transparencia-e-prestacao-de-contas/2022/rgmd21_300522.pdf> Acesso em: 10 de nov. 2022.

BRASIL. **Orçamento Anual 2023**. 2022. Orçamentos Anuais PLDO | LDO | PLOA | LOA - Atos Normativos. Disponível em: <https://www.gov.br/economia/pt-br/assuntos/planejamento-e-orcamento/orcamento/orcamentos-anuais/2023>. Acesso em: 13 de nov. 2022.

BROADFOWARD. **Security Edge Protection Proxy (SEPP)**. 2022. Disponível em: <https://www.broadforward.com/security-edge-protection-proxy/>. Acesso em: 23 de nov. 2022.

CÂMARA. **Defesa concentra 1/3 dos recursos para investimentos em 2023**. Política e Administração Pública. Reportagem - Sílvia Mugnatto. 29 de set. 2022a. Disponível em: <https://www.camara.leg.br/noticias/910851-defesa-concentra-1-3-dos-recursos-para-investimentos-em-2023/>. Acesso em: 13 de nov. 2022.

CÂMARA. **Comissão aprova projeto que anula norma do governo sobre segurança cibernética na rede 5G**. Política e Administração Pública. 13 de maio. 2022b. Disponível em: <https://www.camara.leg.br/noticias/875433-comissao-aprova-projeto-que-anula-norma-do-governo-sobre-seguranca-cibernetica-na-rede-5g/>. Acesso em: 23 de nov. 2022.

CÂMARA. **Orçamento 2021 é sancionado**; Educação, Economia e Defesa têm maiores cortes. Política e Administração Pública. Reportagem – Francisco Brandão. 23 de abr. 2021. Disponível em: <https://www.camara.leg.br/noticias/749955-orcamento-2021-e-sancionado-educacao-economia-e-defesa-tem-maiores-cortes/. Acesso em: 13 de nov. 2022.

CARNEIRO, Tiago Moreira. **Impacto econômico decorrente da implementação da quinta geração de telefonia móvel**. 2022. 55 f. Trabalho de Conclusão de Curso (Graduação em Engenharia Eletrônica e de Telecomunicações) - Universidade Federal de Uberlândia, Patos de Minas, 2022.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da Internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de segurança. 2006. Dissertação (Mestrado) - Curso de Engenharia de Sistemas e Computação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

CARVALHO, Davison Lucas Landim. **Segurança Cibernética:** o Brasil à luz da implementação do 5G. 2021. Trabalho de conclusão de curso de graduação, Universidade Federal de São Paulo, São Paulo, 2021. Disponível em: <https://repositorio.unifesp.br/handle/11600/63057>. Acesso em: 05 set. 2022.

CASTRO, Maria Carolina de. **As competências brasileiras na produção de recursos para o setor de defesa cibernética e suas implicações**. Trabalho Conclusão do Curso de Graduação em Relações Internacionais do Centro Socioeconômico da Universidade Federal de Santa Catarina. Florianópolis, 2020. Disponível em <https://repositorio.ufsc.br/bitstream/handle/123456789/218387/TCC_MariaCarolinadeCastro.pdf?sequence=1&isAllowed=y> Acesso em: 02 nov. 2022.

CAVELTY, Myriam Dunn. Cyber-security. In: COLLINS, Alan. **Contemporary Security Studies**. 3. ed. Oxford: Oxford University Press, 2012a, p. 362-378.

CAVELTY, Myriam Dunn. The Militarization of Cyber Security as a Source of Global Tension. In: Wenger, Andreas; Möckli, Daniel; Mahadevan, Prem. **Strategic Trends 2012: Key Developments in Global Affairs**. Zurique: Center for Security Studies (CSS), 2012b. p. 103-124.

CEBRI. **A Segurança Cibernética e a tecnologia 5G no cenário brasileiro**. 31 dez. 2020. Policy Paper. Autor: Paulo Sergio Melo de Carvalho. Disponível em:

<https://www.cebri.org/br/doc/28/a-seguranca-cibernetica-e-a-tecnologia-5g-no-cenario-brasileiro>. Acesso em: 14 dez. 2022.

CIO. **Precisamos falar sobre segurança cibernética em tempos de 5G**. 2020. Disponível: <cio.com.br/tendencias/precisamos-falar-sobre-seguranca-cibernetica-em-tempos-de-5g/>. Acesso em: 26 dez. 2022.

CISO. **Líderes de tech prometem a Biden muita verba para cyber**. 26 ago. 2021. Disponível em: <https://www.cisoadvisor.com.br/lideres-de-tech-prometem-a-biden-muita-verba-para-cyber/>. Acesso em: 26 dez. 2022.

CISCO. **What Is a Data Center?**. 2022. Disponível em: <https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html>. Acesso em: 01 nov. 2022.

CLARKE, R; KNAKE, R. **Guerra cibernética**: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2015.

CNN. **Do ENIAC ao notebook: confira a evolução dos computadores nas últimas décadas**. 23 de fev. de 2021. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/do-eniac-ao-notebook-confira-a-evolucao-dos-computadores-nas-ultimas-decadas>. Acesso em: 28 de out. de 2022.

DIGITAL REALTY. Colocation Data Center **350 East Cermak** Road Chicago Data Center. 2022. Disponível em: <https://www.digitalrealty.com/data-centers/chicago/350-e-cermak-rd-chicago-il>. Acesso em: 01 nov. 2022.

DOU. Diário Oficial da União. **Instrução Normativa Nº 4**. 27 de março de 2020. Edição 60, seção 1, página 2. Disponível em: <https://www.stj.jus.br/internet_docs/biblioteca/clippinglegislacao/IN_4_2020_AGU.pdf>. Acesso em: 22 de nov. 2022.

EL PAÍS. **Há governos que querem desconectar seus cidadãos da Internet, e alguns já têm seu botão vermelho**. 2020. Disponível em: <brasil.elpais.com/ideas/2020-03-10/ha-governos-que-querem-desconectar-seus-cidadaos-da-internet-e-alguns-ja-tem-seu-botao-vermelho.html> Acesso em: 06 nov. 2022.

EXAME. **Hacker confessa ter invadido celular de Moro e de centenas de autoridades**. 2019. Disponível em: <https://exame.com/brasil/hacker-confessa-ter-invadido-celular-de-moro-e-centenas-de-autoridades>. Acesso em: 07 nov. 2022.

FERREIRA, Juliana A.B. **A Questão Cibernética nas Relações entre os Estados**: Uma Nova Forma de Projeção de Poder na Atualidade. 2017. 121f. Dissertação de Mestrado em Estudos Estratégicos da Defesa e da Segurança, Universidade Federal Fluminense, Niterói, 2017.

FGV. **Pandemia acelerou processo de transformação digital das empresas no Brasil, revela pesquisa**. 26 de maio de 2022. Disponível em: <https://portal.fgv.br/noticias/pandemia-acelerou-processo-transformacao-digital-empresas-brasil-revela-pesquisa>. Acesso em: 22 de nov. 2022.

FAVERO, Pedro Henrique Paulette. **O amanhecer do poder cibernético brasileiro?** Uma análise documental sobre defesa e segurança cibernética no Brasil de 2018 a 2020. 2022. Trabalho de conclusão de curso de Relações Internacionais, Universidade Federal de Santa Catarina, Florianópolis, 2022.

FONSECA, Leila Oliveira da. **Cibersegurança:** o Brasil e o México em uma perspectiva comparada. Trabalho de Conclusão de Curso - Pontifícia Universidade Católica de Goiás. Relações Internacionais. 2018. Disponível em: <https://www.academia.edu/44141949/Ciberseguran%C3%A7a_O_Brasil_e_o_M%C3%A9xico_em_uma_perspectiva_comparada_Monografia_>. Acesso em: 24 de nov. 2022.

GALOYAN, Albert. **Segurança cibernética no âmbito das relações internacionais**. Trabalho de conclusão de curso de Relações Internacionais da Universidade de Brasília. Brasília, 2019. Disponível em <https://bdm.unb.br/bitstream/10483/22386/1/2019_AlbertGaloyan_tcc.pdf> Acesso em: 06 nov. 2022.

G1. **5G:** entenda a briga entre Estados Unidos e China. 05 nov. 2021. 2021a. Disponível em: <https://g1.globo.com/tecnologia/noticia/2021/11/05/5g-entenda-a-briga-entre-estados-unidos-e-china.ghtml>. Acesso em: 06 nov. 2022.

G1. **Leilão do 5G movimenta R$ 47,2 bilhões, abaixo do esperado por governo e Anatel**. 05 nov. 2021. 2021b. Disponível em: <https://g1.globo.com/economia/noticia/2021/11/05/leilao-do-5g-movimenta-r-4679-bilhoes-informa-anatel.ghtml>. Acesso em: 27 dez. 2022.

G1. **5G no Brasil**: guia explica o que vai mudar com a nova tecnologia. 06 jul. 2022. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/07/06/5g-chega-ao-brasil-nesta-quarta-guia-explica-o-que-vai-mudar-com-a-nova-tecnologia.ghtml>. Acesso em: 26 dez. 2022.

G1. **Veja a íntegra do discurso do presidente Lula no Congresso.** 01 jan. 2023. Disponível em: <https://g1.globo.com/politica/noticia/2023/01/01/veja-a-integra-do-discurso-do-presidente-lula-no-congresso.ghtml>. Acesso em: 02 jan. 2023.

INTERNET WORLD STATS. **World Internet Usage and Population Statistics**. 2022. Disponível em:< https://www.internetworldstats.com/stats.htm#links> Acesso em: 07 nov. 2022.

IGARAPÉ, Instituto. **Cibersegurança no Brasil:** uma análise da estratégia nacional. Abril de 2021. Artigo estratégico 54. Disponível em: <https://igarape.org.br/ciberseguranca-no-brasil-uma-analise-da-estrategia-nacional/>. Acesso em: 11 de nov. 2022

INFRA NEWS TELECOM. **Brasil precisa formar 70 mil profissionais de tecnologia ao ano até 2024**. 2023. Disponível em: <https://www.infranewstelecom.com.br/brasil-precisa-formar-70-mil-profissionais-de-tecnologia-ao-ano-ate-2024/>. Acesso em: 21 jan. 2023.

ISTO É DINHEIRO. **Cibercrimes terão impacto de mais de US$ 1 trilhão na economia global em 2020**. 2020. Disponível em:

<istoedinheiro.com.br/cibercrimes-terao-impacto-de-mais-de-us-1-trilhao-na-economia-global-em-2020/>. Acesso em: 07 nov. 2022.

KNIGHT, Peter T.. **The Internet in Brazil**: origins, strategy, development, and governance. Bloomington: Authorhouse, 2014. 176 p. Disponível em: <https://books.google.com.br/books?id=SWE6AwAAQBAJ&pg=PA1&hl=ptBR&source=gbs_toc_r&cad=4#v=onepage&q&f=false>. Acesso em: 16 nov. 2022.

KUEHL, D. T. From Cyberspace to Cyberpower: defining the problem. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. (Ed.). **Cyberpower and National Security**. National Defense University Press; Potomac Books, 2009.

LGPD BRASIL. **5G e proteção de dados pessoais: o que foi alterado?**. 17 de março de 2022. Disponível em:<https://www.lgpdbrasil.com.br/5g-e-protecao-de-dados-pessoais-o-que-foi-alterado/>. Acesso em: 23 de nov. 2022

LE DRIAN, Jean-Yves. **Cybersécurité : le rôle et la responsabilité des acteurs privés dans le renforcement de la stabilité et de la sécurité internationale du cyberespace**. Intervention de M. Jean-Yves Le Drian, ministre de l'Europe et des affaires étrangères de la République française. 72ème Assemblée générale des Nations unies. New York, 18 set. 2017. Disponível em: <https://basedoc.diplomatie.gouv.fr/vues/Kiosque/FranceDiplomatie/kiosque.php?fic>.

MAJEROWICZ, Esther. A China e a economia política internacional das tecnologias da informação e comunicação. **Geosul**, Florianópolis, v. 35, n. 77, dez. 2020, p. 73-102.

MCOM. **Um ano após leilão, Brasil avança com expansão do sinal 5G**. Ministério das Comunicações. 04 nov. 2022. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2022/novembro/um-ano-apos-leilao-brasil-avanca-com-expansao-do-sinal-5g>. Acesso em: 26 dez. 2022.

MESQUITA, Felipe Sousa. **Segurança Cibernética e a Política Internacional Contemporânea**: novos desafios e oportunidades. Artigo apresentado como requisito parcial para obtenção do título de Especialista em Relações Internacionais. Brasília-DF, 2019.

MOTOYAMA, Shozo. **Para Shozo Motoyama**, sociedade deve discutir o desenvolvimento de armas [Junho de 2002]. Entrevistador: Marta Kanashiro. Com Ciência, 2002. Entrevista concedida para a reportagem: As guerras e o desenvolvimento científico. Disponível em: <https://www.comciencia.br/dossies-1-72/entrevistas/guerra/motoyama.htm>. Acesso em: 01 nov. 2022.

OLIVEIRA, Marcos Aurélio Guedes de. **Guia De Defesa Cibernética Na América Do Sul** / Marcos Aurélio Guedes De Oliveira; Graciela De Conti Pagliari; Adriana Aparecida Marques; Lucas Soares Portela; Walfredo Bento Ferreira Neto. Recife, PE : UFPE, 2017. Disponível em: <https://pandia.defesa.gov.br/pt/acervodigital/35-programa-%C3%A1lvaro-alberto-de-indu%C3%A7%C3%A3o-%C3%A0-pesquisa-em-defesa-nacional-e-seguran%C3%A7a-internacional/826-guia-de-defesacibern%C3%A9tica-na-am%C3%A9rica-do-sul,-por-marcos-aurelio-guedes-et-al>. Acesso em: 20 dez. 2022.

PIRES NETO, Antônio Valter. **Segurança da informação no Brasil**: estratégia de defesa e desenvolvimento econômico. Trabalho de Conclusão de Curso de Graduação em Relações Internacionais da Universidade do Sul de Santa Catarina. Tubarão, 2020. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/16791/1/TCC-%20Ant%c3%b4nio%20V..pdf> Acesso em 18 nov. 2022.

PWC. **Pesquisa Global de Segurança da Informação 2016**. 2016. Disponível em: <https://www.pwc.com.br/pt/estudos/giss-pesquisa-global-seguranca-informacao-2016.html>. Acesso em 23 nov. 2022.

RÊ, Eduardo de. **Ciberespaço e Segurança Cibernética:** as estratégias cibernéticas de EUA, China e Israel e as suas relações com a estratégia cibernética do Brasil. Artigo apresentado como requisito parcial para obtenção do título de Especialista em Relações Internacionais. Florianópolis, 2021.

REPLY. **5g e cidades inteligentes**: soluções para um futuro hiperconectado. 2021. Disponível em: <www.reply.com/br/industries/telco-and-media/5g-smart-cities>. Acesso em: 12 dez. 2022.

RODRIGUES, Ricardo Batista. **Novas Tecnologias da Informação e da Comunicação**. Recife: IFPE, 2016. Disponível em <https://www.ufsm.br/app/uploads/sites/413/2018/12/arte_tecnologias_informacao_comunicacao.pdf> Acesso em: 02 nov. 2022.

SOUZA, G. L. Mâcedo. **Reflexos da digitalização da Guerra na Política Internacional do Século XXI**: Uma análise exploratória da securitização do Ciberespaço nos Estados Unidos, Brasil e Canadá. 2013. 129f. Dissertação (Mestrado em Ciência Política) - Centro de Filosofia e Ciências Humanas, Universidade Federal de Pernambuco, Recife, 2013

TELEGEOGRAPHY. **Submarine Cable Map: Brazil**. 2022. Disponível em: <https://www.submarinecablemap.com/#/country/brazil>. Acesso em: 02 Out. 2022.

TEKIR, Gökhan. Huawei, 5G Networks and digital geopolitics. **International Journal of Politics and Security (IJPS)**, Vol. 2, No. 4, Julho/2020, p. 113-135.

THE GUARDIAN. **Not so secret**: deal at the heart of UK-US intelligence. 25 jun. 2010. Disponível em: <https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released>. Acesso em: 26 dez. 2022.