UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS V
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS
CURSO DE RELAÇÕES INTERNACIONAIS

MARIA GISELE MACEDO SILVA

UMA ANÁLISE COMPARATIVA DO AVANÇO DO IMPERIALISMO NO CIBERESPAÇO: OS CASOS DO BRASIL E ÍNDIA

JOÃO PESSOA
2024

MARIA GISELE MACEDO SILVA

UMA ANÁLISE COMPARATIVA DO AVANÇO DO IMPERIALISMO NO CIBERESPAÇO: OS CASOS DO BRASIL E ÍNDIA

Trabalho de Conclusão de Curso (Artigo) apresentado à Coordenação do Curso de Relações Internacionais da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Relações Internacionais.

Orientador: Fábio Rodrigo Ferreira Nobre

JOÃO PESSOA
2024

S586u Silva, Maria Gisele Macedo.
Uma análise comparativa do avanço do imperialismo no ciberespaço [manuscrito] : os casos do Brasil e Índia / Maria Gisele Macedo Silva. - 2024.
47 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2024.
"Orientação : Prof. Dr. Fábio Rodrigo Ferreira Nobre, Coordenação do Curso de Relações Internacionais - CCBSA. "

1. Cibersegurança. 2. Imperialismo no Ciberespaço. 3. Brasil. 4. Índia. I. Título

21. ed. CDD 327.17

Elaborada por Livaneide da Silva - CRB - CRB15/638 BSC5/UEPB

MARIA GISELE MACEDO SILVA

UMA ANÁLISE COMPARATIVA DO AVANÇO DO IMPERIALISMO NO CIBERESPAÇO: OS CASOS DO BRASIL E ÍNDIA

Trabalho de Conclusão de Curso (Artigo) apresentado à Coordenação do Curso de Relações Internacionais da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Relações Internacionais.

Aprovada em: 21/06/2024

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br
FABIO RODRIGO FERREIRA NOBRE
Data: 21/06/2024 09:43:52-0300
Verifique em https://validar.iti.gov.br

Fábio Rodrigo Ferreira Nobre (Orientador)
Universidade Estadual da Paraíba (UEPB)

Documento assinado digitalmente
gov.br
ALEXANDRE CESAR CUNHA LEITE
Data: 22/06/2024 15:53:11-0300
Verifique em https://validar.iti.gov.br

Alexandre César Cunha Leite
Universidade Estadual da Paraíba (UEPB)

Documento assinado digitalmente
ICP-Edu
Danielle Jacon Ayres Pinto
Data: 23/06/2024 15:05:03-0300
CPF: ***.367.488-**
Verifique as assinaturas em https://v.ufsc.br

Danielle Jacon Ayres Pinto
Universidade Federal de Santa Catarina (UFSC)

À minha mãe, Jaucilene, e às minhas avós, Antonieta e Luzia Maria; as raízes da minha vida que me permitiram florescer até aqui.

“O amor, o perdão e a tecnologia irão nos levar para outro planeta.” - FBC.

LISTA DE TABELAS

SUMÁRIO

UMA ANÁLISE COMPARATIVA DO AVANÇO DO IMPERIALISMO NO CIBERESPAÇO: OS CASOS DO BRASIL E ÍNDIA

A COMPARATIVE ANALYSIS OF THE RISE OF IMPERIALISM IN CYBERSPACE: THE CASES OF BRAZIL AND INDIA

Maria Gisele Macedo Silva[1]

RESUMO

Como o Brasil e a Índia são afetados pelo imperialismo no ciberespaço? Esta pesquisa investiga os impactos do avanço do imperialismo no domínio do ciberespaço, especificamente no Brasil e na Índia, países do Sul Global com um histórico de experiências subalternas de dominação e colonização. Testa-se a hipótese de que o Brasil e a Índia são afetados pelo ciberimperialismo independentemente do seu desempenho no ciberespaço, diante da submissão existente frente ao domínio do Norte Global. O desenho de pesquisa realiza o método da comparação histórica através de fontes primárias documentais dos países explorados; como leis, políticas públicas e recomendações na área da cibersegurança. Explora, também, as variáveis de legislação, técnica, capacidade organizacional, capacidade de desenvolvimento e cooperação coletadas por meio do Global Cybersecurity Index 2020. Mesmo o Brasil e a Índia apresentando um bom desempenho no desenvolvimento de iniciativas para a segurança cibernética, existem dificuldades técnicas e operacionais para sua execução, com um progresso lento na criação de um ciberespaço seguro. Além disso, exibe a assimetria de poder cibernético entre países do Norte e Sul Global. Essa pesquisa proporciona uma visão crítica em torno da identificação da correlação entre experiências subalternas e o desenvolvimento de tecnologias no ciberespaço, adicionando à literatura de cibersegurança um tema negligenciado, estudando casos de países do Sul Global.

Palavras-chave: Cibersegurança. Imperialismo no Ciberespaço. Brasil. Índia.

ABSTRACT

How are Brazil and India affected by imperialism in cyberspace? This research investigates the impacts of the advance of imperialism in the domain of cyberspace, specifically in Brazil and India, countries of the Global South with a history of subaltern experiences of domination and colonization. It tests the hypothesis that Brazil and India are affected by cyberimperialism regardless of their performance in cyberspace, given their existing submission to the domination of the Global North. The research design uses the method of historical comparison through primary documentary sources from the countries explored, such as laws, public policies and recommendations in the area of cybersecurity. It also explores the variables of legal measures, technique measures, organizational measures, capacity

[1] Graduanda em Relações Internacionais pela Universidade Estadual da Paraíba.
maria.gisele@aluno.uepb.br

development and cooperation collected through the Global Cybersecurity Index 2020. Even though Brazil and India are performing well in the development of cybersecurity initiatives, there are technical and operational difficulties in their implementation, with slow progress in creating a secure cyberspace. It also shows the asymmetry of cyber power between countries in the Global North and South. This work provides a critical view of identifying the correlation between subaltern experiences and the development of technologies in cyberspace, adding a neglected topic to the cybersecurity literature by studying cases from countries in the Global South.

Keywords: Cybersecurity. Imperialism in Cyberspace. Brazil. India.

CONSIDERAÇÕES INICIAIS

Alguns temas da política internacional enfrentam obstáculos para a sua inserção dentro da literatura acadêmica e da promoção de políticas públicas que dialoguem com eles. Isto ocorre devido ao caráter invisível desses temas, não sendo possíveis de serem visualizados materialmente no dia-a-dia do cidadão comum e refletindo na falta de incentivo de governos para seu fomento. O Ciberespaço, principalmente no fim década de 1990, expressava essa característica limitante como consequência de um alcance restrito a elites econômicas que iniciavam a ocupação do mesmo, através de redes sociais e tecnologias em geral que começavam seu processo de disseminação.

No momento da história em que nos encontramos, o Ciberespaço não se restringe apenas ao mundo virtual, alcançando esferas da sociedade que revelam sua capacidade de materialização. Assim, o que um dia foi um tema isolado, atualmente expressa uma relevância social que o transforma em uma pauta de preocupações governamentais e também da população civil.

O processo de popularização do Ciberespaço acompanhou o desenvolvimento social, político e econômico de cada localidade do mundo em que ele se construiu. Em outras palavras, o nível de interação popular e adesão de políticas a essa área é posta em paralelo com o desenvolvimento socioeconômico do país, que só a partir disso, viabiliza a evolução do próprio Ciberespaço. Em decorrência disso, a adesão de países do Sul Global a pautas cibernéticas sofre um atraso em comparação ao Norte Global, isto pois, ao passo que o Sul direcionava esforços para recuperação de um passado colonial (Santos, 2007), o Norte já iniciava o processo de transformação para uma sociedade modernizada em termos tecnológicos.

O Ciberespaço incorpora à literatura das Relações Internacionais enquanto subcampo dos Estudos Estratégicos e de Segurança Internacional no século XX, se inserindo em

agendas de Segurança Pública, Defesa Nacional e Governança Global. Adentrando, dessa forma, para a área de Segurança Estratégica enquanto o campo de Segurança Cibernética ou Cibersegurança (Lopes, 2016). Uma discussão emergente para a área da Cibersegurança é a identificação de vulnerabilidades que possam estar se apresentando enquanto um limite para a evolução de cultura de segurança cibernética global, consequentemente, para a evolução da sociedade.

A relação de desigualdade enfrentada pelo Sul Global no processo desenvolvimento de um ciberespaço seguro enquadra-se como um dos desafios identificados para consolidação de uma agenda cibernética que quebre os princípios de exploração e dependência entre o Norte e o Sul. Desvantagem essa que se materializa em uma assimetria de poder que reforça o fenômeno do imperialismo no ciberespaço, denominado no presente artigo como ciberimperialismo.

O Ciberimperialismo é um fenômeno caracterizado enquanto uma extensão do imperialismo colonial que se moderniza às dinâmicas da sociedade do século XXI e se renova para a sua perpetuação no Ciberespaço e na relação com que suas ex-colônias desenvolvem com o mesmo (Rusciano, 2001; Kwet, 2019). Esse processo de desequilíbrio no fluxo e acesso à informação é o que gera a manutenção de potências hegemônicas enquanto líderes da Cibersegurança e países do Sul Global expostos a vulnerabilidades, insegurança e incidentes cibernéticos.

O Brasil e a Índia, colonizados por Portugal e Reino Unido respectivamente, enfrentam o obstáculo exposto e se inserem na corrida para a promoção de um ciberespaço seguro com pontos em desvantagens. O Brasil é reconhecido pelo seu avanço na proteção de dados com a Lei Geral de Proteção de Dados Pessoais (LGPD), caminhando para a construção ativa de meios para assegurar o ciberespaço. A Índia, que atravessa pelo mesmo caminho que o Brasil, tem como viabilizador de seu crescimento econômico e de sua posição como um *global player* o seu desenvolvimento tecnológico, com a promoção de serviços e soluções tecnológicas a nível mundial. Entretanto, ambos são alvo do mesmo processo: o ciberimperialismo, que os insere em uma dinâmica de assimetria de poder em nível internacional diante da submissão existente frente ao domínio do Norte Global.

Isto posto, este trabalho investiga os impactos do avanço do imperialismo no domínio do ciberespaço, especificamente no Brasil e na Índia, países do Sul Global com um histórico de experiências subalternas de dominação e colonização. Parte-se da hipótese de que o Brasil e a Índia são afetados pelo ciberimperialismo independentemente do seu desempenho no ciberespaço, diante da submissão existente frente ao domínio do Norte Global.

Para responder a pergunta de “como o Brasil e a Índia são afetados pelo imperialismo no ciberespaço?”, esta pesquisa propôs um desenho que utiliza o Método da Comparação Histórica, buscando uma pesquisa para além do observacional, aprofundando-se na comparação com o objetivo de chegar a resultados mais precisos.

O artigo parte do Método da Semelhança – também conhecido como *Most Similar Systems Design* (MSSD) – em que compara casos em que partilham de um fenômeno em comum neste caso, o ciberimperialismo, apesar de terem características distintas (Bolognesi, 2022). Mesmo sendo países que pertencem ao Sul Global, metáfora aplicada por Boaventura (Santos, 2007), o Brasil e a Índia estão em pólos opostos em questões culturais, políticas e econômicas. A trajetória da Cibersegurança em cada um deles expõem caminhos distintos, além de momentos diferentes em que iniciam seu processo de desenvolvimento de políticas e iniciativas para a construção de um ciberespaço seguro.

O Método da Comparação Histórica é explorada nesta pesquisa de forma a identificar padrões e explicar de forma causal os seus processos. A comparação histórica abrange um guarda-chuva de três conceitos: *Path dependence*, Conjuntura Crítica e localização/estrutura temporal. O primeiro, os que estão no início da linha do tempo desempenham um impacto causal sobre os eventos seguintes, em que a primeira tomada de decisão gera uma cadeia de eventos iniciado por ele, em outras palavras, condicionada pelas primeiras escolhas (Perissinotto, 2022). Já a conjuntura crítica, aponta eventos marcantes que gera uma sequência de escolhas que geram aceleração ou retardo das mudanças, sendo ligado também ao *path dependence* diante do contexto histórico em que ele está inserido. Por último, a localização temporal ou estrutura temporal é a relevância da duração dos fenômenos para o resultado do processo político estudado (Perissinotto, 2022).

Sendo um artigo dividido em três seções, na primeira, realizou-se uma revisão bibliográfica de livros e artigos científicos que exploram o subcampo da Cibersegurança, bem como seu histórico e definições, o conceito de Ciberpoder e a discussão sobre Ciberimperialismo.

Em seguida, na segunda seção, partindo do Método da Comparação Histórica, realizou-se uma análise comparativa histórica entre os casos do Brasil e da Índia. Esse trabalho foi guiado pelo conceito de Conjuntura Crítica, observando através de uma pesquisa documental e bibliográfica os eventos marcantes para o desenvolvimento da cibersegurança no Brasil e na Índia, em que identificou o histórico, as iniciativas e o estado da cibersegurança de ambos até o ano de 2020, para o Brasil, e 2019, para a Índia devido a limitação do acesso a fontes primárias que abordassem a temática.

Por fim, na terceira seção, é explorado as variáveis de legislação, técnica, capacidade organizacional, capacidade de desenvolvimento e cooperação coletadas por meio do Global Cybersecurity Index 2020 (ITU, 2021). Buscou trazer nesse tópico uma visualização, através de quadros comparativos, da performance do Brasil e da Índia em termos de Cibersegurança, acrescentando também os casos de países considerados líderes da Cibersegurança Internacional.

1 CIBERESPAÇO: o quinto domínio e suas particularidades

Se existe uma política internacional que atravessa fronteiras no século XXI, evidenciando sua porosidade e modificando a conexão mundial entre nações, deve-se atentar sobre o Ciberespaço; um sistema social que atravessa toda a humanidade com o evoluir da história e é incorporado enquanto espaço de projeção de poder e fluxo contínuo de informação também para as Relações Internacionais (Kovacs, 2021). A abrangência da Segurança Internacional dentro desse novo domínio se configura como a Segurança Cibernética ou, como mais popularizado dentro da literatura, a Cibersegurança (Lopes, 2016; Kassab, 2013). Todavia, existe um processo e um histórico que determina esse subcampo da grande área das Relações Internacionais e o define para sua incorporação dentro das dinâmicas de poder, que será explorado ao decorrer deste tópico.

1.1 Segurança no Ciberespaço: histórico e definições

Apesar de emergir enquanto subcampo dos Estudos Estratégicos e de Segurança Internacional de maneira direta no século XXI, o conceito de Ciberespaço e suas ramificações atingiram um alto grau de relevância na segurança no presente século devido o seu uso estratégico-militar, e não pelo crescimento da noção de ciberespaço vinculada a internet. Isto é, embora tenha tido luzes postas sobre o tema de estudo, previamente, no século XX, já existia um crescente de conhecimento sobre o mesmo (Lopes, 2016).

Em termos do mundo virtual, o domínio da internet teve seu início em 1983, e, em seguida o Google – que engloba diversas empresas de tecnologia na atualidade – foi inserido no sistema *World Wide Web* em 1989. Quando partimos para a noção estratégico-militar, no fim da década de 1990 alguns atores estatais e não-estatais deram início a incorporação de uma nova tecnologia vinculada a um complexo global. Como primeira iniciativa dentro desse âmbito, encontra-se o ICANN, sigla para *Internet Corporation for Assigned Names and*

Numbers, criada em 1998 pelo governo dos Estados Unidos para o desenvolvimento de planos nacionais sobre a cibersegurança. (Nye Jr, 2011)

Mesmo que pareçam ser sinônimos quando abordados, a Internet e o Ciberespaço não dão significado à mesma conceituação. Pode-se afirmar, no entanto, que a Internet é englobada pelo ciberespaço, além de demonstrar ser uma força de projeção tanto social – no sentido de sua disseminação nos anos 2000 –, como também em sua evolução de projeção de poder por parte dos Estados. Os avanços tecnológicos da Internet traçaram um caminho em que uma ampla classe de atores (estatais ou não estatais) são capazes de agir enquanto construtores de redes, software e hardware. Ao mesmo tempo, é perceptível que nem todas os entrelaces da internet se configuram como uma agência do ciberespaço, apresentando uma dificuldade na intenção da ação tomada e o que está por trás da mesma (Choucri; Goldsmith, 2012; Lopes, 2017).

Tendo isso em vista, é preciso entender de que forma o Ciberespaço é incorporado enquanto domínio com capacidade de gerar uma mudança no status da Segurança Internacional. O caso do Stuxnet é analisado, atualmente, enquanto "a primeira arma cibernética projetada para as guerras do século XXI" (Lopes, 2017, p. 9). O Stuxnet é um software malicioso (*malware*) que teria sido desenvolvido como uma ameaça para as instalações de enriquecimento de urânio que haviam sido desenvolvidas como um Programa Nuclear Iraniano.

O Stuxnet apresenta, nesse sentido, uma ameaça às Infraestruturas Crítica, que, segundo Mandarino Júnior (2010, p. 38), "são instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional e à segurança do Estado e da sociedade". Mesmo com sua descoberta em 2010, a origem do Stuxnet continua em disputa devido a limitação da identificação da raiz da questão no ciberespaço, exibindo Estados Unidos e Israel como acusados de serem os precursores de um ato de guerra, não se atendo apenas como um ato de guerra do ciberespaço (Nye Jr, 2011; Choucri; Goldsmith, 2012; Knoepfel, 2013; Lopes, 2017).

A partir do caso do Stuxnet, é passível de pontuação outro demais casos que se localizam enquanto marcos para as questões precursoras de ameaças e ataques no ciberespaço. Por exemplo, o caso da Estônia em 2007 em que ataques cibernéticos sobrecarregaram WebSites e os paralisaram, abrangendo agências do setor público, bancos e entre outros, tendo como suspeito do ataque a Rússia.

Outro exemplo é o episódio da Google em 2010, a empresa anunciou que ela e outras empresas de tecnologia, segurança e defesa tecnológica haviam sofrido uma tentativa de

roubo de dados e informações importantes por parte do Governo Chinês. O caso, mesmo tendo sido apenas uma tentativa de obtenção de informações e acesso, teve como consequência uma indisponibilidade do site da Google no território da China (Nye Jr, 2011 Choucri; Goldsmith, 2012; Radu, 2013; Read, 2013).

A conceituação dos termos Ciberespaço e Cibersegurança é realizada de maneira dependente às próprias teorias de Segurança das Relações Internacionais, não sendo uma força ou domínio que se extingue dos demais, e sim um novo espaço adicionado na política internacional desenvolvido pelo ser humano para satisfazer necessidades e demandas do mesmo.

O espaço cibernético ou ciberespaço em si não é uma definição nova, o "cyber" remonta a "navegador web" e " browser de Internet", vem sendo utilizado em outros contextos – como o matemático – em meados do século XX. Assim, temos definições como uma realidade digital, multidimensional ou virtual, composto por diversos softwares e hardwares ligados a rede de conectividade ou não, pelo qual cruzam informações digitais dos mais diversos níveis e tipos, incluindo funcionalidades como gerenciamento, armazenamento e comunicação.

O Ciberespaço, ainda mais, depende da interação direta das atividades humanas e deriva do imenso tráfego de informações, mas não se configura apenas como um locus social, como aponta Lopes (2017), como também para a atuação estratégica de Estados. Para além do termo, o domínio discutido exemplifica a premissa da ausência de vácuo de poder nas relações internacionais, ora sendo utilizado como meio de transição, ora como fim (Kremer; Benedikt, 2013; Lopes, 2016; Lopes, 2017; Segundo, 2019) .

O ciberespaço apresenta, da mesma forma que demais espaços, objetos que o delimitam e atribuem seu significado, sendo eles a infraestrutura, redes, softwares e habilidades humanas. Cada objeto que o compõem apresenta seu nível de análise, em que o nível físico (*hardware*) consiste em radiação eletromagnética, cabos, satélites, conexão de rádio, roteadores e *switches;* no nível sintático (software), redes e subredes, protocolos, software, criptografia, banda larga, hosts e outros; por fim, no nível semântico interliga, de maneira direta, a própria informação (Lopes, 2017; Kukkola, 2017)

Como mencionado anteriormente, a máxima dos princípios de estudos de estratégia para as Relações Internacionais se estende para a área da Cibersegurança. Assim, a noção de Segurança Pública, quando se trata de prover segurança externa, e Defesa Nacional, no âmbito externo, também se aplica para o subcampo abordado que advém das noções de território e soberania. É a partir disso que pode-se afirmar que, por não ser o primeiro

momento na história humana que a tecnologia da informação promove mudanças pontuais na política e na sociedade, a evolução apontada previamente do uso estratégico-militar a partir do ciberespaço coloca tais conceitos à prova. Em outras palavras, é possível afirmar que o ciberespaço tem apresentado uma crescente preocupação de Segurança Estratégica (Lopes, 2017).

O conceito de cibersegurança, embora consolidado, não é interpretado como algo estático e fechado, podendo precisar de atualizações do mesmo a partir de mudanças na política internacional (Radu, 2014). Assim, "a junção entre essa segurança estratégica e o ciberespaço é o que se pode chamar de Segurança Cibernética" (Lopes, 2016, p. 6). Saindo da noção de uma cibersegurança que se limita como uma questão de política externa imutável e sim um problema transnacional, Abassi (2021) descreve cibersegurança como:

> "...a ausência de conflitos entre os intervenientes, de modo a promover a segurança e a estabilidade no ciberespaço, permitindo ao mesmo tempo o intercâmbio de informações e de bens económicos. Olhar para a cibersegurança deste ponto de vista reflete melhor o facto de se tratar de um problema de segurança global, e, consequentemente, todos os utilizadores do ciberespaço são vulneráveis a ciberataques." (Abassi, 2021, p. 4)

A União Internacional das Telecomunicações (UIT), a agência especializada das Nações Unidas para assuntos de tecnologia digital, traz como definição de cibersegurança como um conjunto de tecnologias, políticas, estratégias e análises de gerenciamento, bem como também proteção de redes que têm como objetivo a seguridade do ciberespaço e dos processos e indivíduos que o estão relacionados (ITU, 2008). Demais definições continuam seguindo a mesma junção de tecnologias e políticas sobre o que é a cibersegurança, como

> Um conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gerenciamento de risco, ações, treinamento, práticas recomendadas, garantia e tecnologias que podem ser usadas para proteger o ambiente cibernético e os ativos da organização e do usuário. (Radu, 2014, p.6, tradução nossa)

Embora existam diversas definições que postulam sobre a cibersegurança, para abrangência de um mundo conectado em rede é necessário ampliar tais lentes para uma compreensão de fraquezas e dificuldades que cada Estado apresenta frente a esse domínio.

1.1.2 Governança Cibernética

A governança do ciberespaço – tanto no nível interno como externo – consiste em procedimentos adotados para a institucionalização do fomento de um ciberespaço "estável e sólido", com o intuito de minimizar os danos gerados pelo mesmo e torná-lo benéfico para o bem-estar humano (Choucri; Goldsmith, 2012). Ao abordar o termo de segurança dentro do contexto político do século XXI, a noção de governança é atribuída como uma variável dependente para que a cibersegurança seja concretizada.

É fato que a ligação entre a garantia de proteção e segurança é atribuída enquanto uma responsabilidade dos governos e do seu projeto de governança. Essa atribuição é articulada e relacionada, dentro das demais áreas, a partir da imposição de barreiras territoriais definidas que é designado para defesa de um território. Para o domínio do ciberespaço, no entanto, barreiras e muros desenvolvidos tendem a ter valor nulo em redes influentes e movimentos transfronteiriços que desmistificam a ideia de uma hegemonia unilateral (Radu, 2014; Abassi, 2021).

O conceito de governança cibernética torna-se indispensável para a literatura da cibersegurança, muitas vezes associadas a ideologias de que ameaças e combates ao cibercrime só poderão ser alcançado a partir da governança em busca de um ciberespaço estável, não sendo possível que atores estatais o resolvam de maneira individual. Entretanto, essa lacuna dessa governança se agrava mais ainda quando voltamos para a disparidade entre países do Norte e Sul Global (Abassi, 2021). Essa assimetria, que será abordada em breve no trabalho, evidencia-se em processos de negociação, ao passo que países do Norte Global apresentam capacidades tecnológicas superiores aos demais, acabando por assumir posições de liderança no âmbito da governança cibernética (Radu, 2014)

1.2 Ciberpoder

Quando refere-se a uma revisão de literatura voltada à noção de poder, serão encontradas diversas formulações que apontam um caminho de projeção e maximização por parte da estratégia estatal, devido à relevância do conceito de poder para a definição da área de Relações Internacionais. Entretanto, um ponto claro em meio às discussões das teorias e suas vertentes é não só a falta de consenso sobre o conceito de poder, mas mais importante, as diversas expressões e formas que o poder remonta terminam por dificultar uma conceitualização única e imutável do conceito (Drezner, 2020).

A concepção de uma política internacional com o núcleo no poder teve como precursor Hans Morgenthau (2003), um dos pioneiros da corrente realista, em "A Política entre as Nações". Morgenthau (1960) define a política internacional como uma batalha entre unidades independentes que buscam domínio sobre outras. Essa lógica de dominação predomina, de certo modo, na corrente neoliberal institucionalista quando Dahl (1957) explica a lógica de poder que uma *unidade A* pode levar a *unidade B* a realizar certa tomada de decisão que B não o faria em outro cenário. Por fim, o construtivismo define poder como a capacidade de "reproduzir, disciplinar e policiar", demonstrando um processo de concretização desse poder que uma vez materializado na política internacional, dificilmente terá uma mudança nessa dinâmica (Hopf, 1998). Dentro dessa discussão, ainda é válido abordar a visão de Foucault (1977), sendo válida para o debate proposto no presente artigo mesmo destoando da centralidade das teorias das relações internacionais, em que analisa uma relação entre poder e conhecimento de maneira intrínseca, onde a construção de um campo de conhecimento fornece espaço para o desenvolvimento de uma relação de poder.

O ciberespaço dá significado para um novo domínio que influencia o poder na política internacional, sendo discutido e analisado por diversos autores. Mas essa nova definição incorpora a possibilidade de uma mudança nos locais de poder tradicional e, a partir desse desenvolvimento, desafia o *"modus operandi"* e sua teoria sobre o poder para as Relações Internacionais (Radu, 2014). A questão da informação não é uma novidade dentro das teorias de poder, ou seja, o *"Smart Power"*. Ciberpoder ou *cyberpower*, no entanto, se insere em uma teorização mais profunda e específica do que a proposição neoliberal, sendo um ponto chave dentro para a apuração da análise internacionalista sobre poder nas RI.

O ciberpoder habilita atores a conquistar seus melhores resultados a partir da utilização dos recursos ligados ao ciberdomínio, sendo uma das formas de absorção do poder e da instrumentalização do mesmo dentro do sistema internacional em um âmbito comportamental. A sua definição não se restringe a um ponto só o ciberpoder abrange um "...conjunto de recursos relacionados com a criação, o controle e a comunicação de eletrônica e informática"(Nye Jr, 2011, p. 82, tradução do autor), significando uma organização de variáveis como a própria infraestrutura, redes, softwares e habilidades humanas. Os Estados, especificamente as grandes potências cibernéticas, se comportam de maneira a utilizar e substituir ferramentas políticas para o desenvolvimento da estrutura do ciber poder a depender da demanda apresentada (Radu, 2014; Kassab, 2013; Kukkola, 2017).

Retomando a discussão, o ciberespaço é caracterizado por sua mutabilidade e acaba por evidenciar a dificuldade da definição de uma barreira entre um território e outro, em

outras palavras, a porosidade das fronteiras. Esse processo é dado através de uma simples movimentação, se diferenciando dos outros demais domínios (territorial, marítimo e aéreo), definindo uma tomada de decisão a partir de um clique e contribuindo para a projeção de poder (Nye Jr, 2011; Kassab, 2013). O que une a inserção desse tema para as Relações Internacionais é a projeção e a obtenção de poder na política internacional, sendo o centro para a sobrevivência dos Estados, avançando debates que revelam a questão da assimetria de poder entre o Sul e o Norte Global.

Tendo sido definido idiossincrasias do ciberespaço e, principalmente, como o poder atravessa essa discussão, a assimetria cibernética ou ciber assimetria é entendida como a "criação e exploração de vantagens estruturais através da modelação do ciberespaço" (Kukkola, 2017, p. 133, tradução do autor). A assimetria aqui discutida não faz referência a um mero recurso ou capacidade estratégica de um Estado, mas sim sobre a criação estrutural do ciberespaço e a implicação disto na modulação de atributos e, consequentemente, nos seus trâmites (Kukkola, 2017).

A assimetria a partir do contexto conceitual do ciberespaço é direcionada a compreensão sobre o uso da força, e assim, o ciberpoder apresenta capacidade de exercer a força de maneira violenta. Esse apontamento pode ser observado em momentos da história em que o ciberpoder foi materializado em disputas, mas também a partir das capacidades tanto físicas como de nível estratégico de um Estado. A análise da assimetria militar geralmente é atrelada – entre outras variáveis do nível estratégico-militar – com o espaço, sua estrutura e os atributos presentes nesse contexto. O espaço aqui discutido não apresenta um território físico, mas sim digital, configurando assim uma assimetria cibernética estrutural que apresenta rotas e fronteiras digitais invisíveis (Klimburg, 2020; Kukkola, 2017).

O ciberespaço, ora chamado de território digital, não representa pontos fixos imutáveis, estando constantemente passando por atualizações, seja no seu próprio conceito como também em sua estrutura. É a partir disso que a mesma conceituação não apresenta o mesmo significado intrínseco para todos os atores, apresentando em cada um de seus atributos e sua estrutura uma particularidade, tendo essa característica explicitada principalmente quando relacionamos tal conceito à assimetria estrutural. A assimetria cibernética estrutural, por fim, é intermediada e modificada pelas a estrutura e os atributos do ciberespaço, que como já mencionado anteriormente, tem sua postulação moldada pela capacidade tecnológica, normas e governos (Klimburg, 2020; Kukkola, 2017). A variável discutida é uma ferramenta chave para a compreensão do fenômeno abordado nesta pesquisa, representando uma ponte direta entre o ciberimperialismo e o ciberpoder.

1.3 Ciberimperialismo

O imperialismo colonial e europeu que se é abordado em geral, no contexto da política internacional, é destinado a análises sobre assentamentos de terras e subjugação de populações através da exploração do trabalho, implicando em uma conquista colonial em que se obtém um controle das infraestruturas pelas potências. A relação desenvolvida nesse mecanismo, necessariamente, resulta em um benefício direto para o país que se instaura como metrópole e na dominação econômica e cultural da "colônia". O presente trabalho não se distancia dessas definições, mas estende o debate para uma nova forma de imperialismo: o digital, que mantém os princípios de exploração e dependência da "metrópole", configurando-se como Ciberimperialismo (Kwet, 2019).

O debate do ciberimperialismo foi explorado por diversos autores em 2001 no livro *"Cyberimperialism: Global Reactions in the New Electronic Frontier"*, editado por Bosah Ebo. O avanço da tecnologia na última década permitiu com que novos recursos e tecnologias adentrassem na sociedade, fazendo com que a cultura do ciberimperialismo que fora discutida em 2001 no livro não abarcasse o desenrolar da atualidade (Gittinger, 2017).

É diante de um debate de uma estrutura que passa por um processo de inovação constante que autores questionam a própria aplicação do termo ciberimperialismo, o interpretando como uma definição equivocada devido à própria estrutura descentralizada da internet (Gittinger, 2017). O que é proposto em contrapartida ao termo é o imperialismo profundo, que sustenta a noção de um imperialismo onipresente que é visto de forma normativa no mundo digital. Esse termo, no entanto, abarca as noções do ciberespaço focado apenas na internet e seu aspecto cultural, limitando sua análise aos demais fatores.

O Ciberimperialismo – muitas vezes explicado como colonialismo digital na literatura, que aqui será utilizado como sinônimo – é analisado como uma extensão e manutenção do imperialismo que se moderniza às novas formas de acesso a uma população no século XXI. Gittinger (2017) sustenta que principalmente a partir da globalização e de sua intensificação das relações sociais em escala mundial, a velocidade desse processo promoveu um cruzamento de fronteiras e compartilhamento de informações, tornando o ciberimperialismo um tema mais denso do que fora abordado no início do século.

Também definido como um desequilíbrio ou uma desigualdade no fluxo e acesso à informação (Gittinger, 2017), esse processo vem sendo desenvolvido especialmente a partir das multinacionais dos Estados Unidos, por um grupo que é descrito como GAFAM:

Google/Alphabet, Amazon, Facebook, Apple e Microsoft[2]. Essas empresas dominam os mecanismos de pesquisa, sistemas operacionais, infraestrutura, serviços de nuvem, plataformas de software e redes sociais, streaming de vídeo e entre outros (Kwet, 2019).

Mas de que maneira isso afeta a população e sua política internacional? Ora, é fato que as empresas mencionadas fazem parte do dia-a-dia de todos os cidadãos e os influenciam de forma indireta. Apesar dessa noção de controle da população ser válida, existe uma camada para além disso. Tendo em vista que essas multinacionais mencionadas pertencem em sua maioria a pessoas jurídicas ou, em alguns casos, desenvolvidos em função de seu país, que são do Norte Global (mais especificamente, lideradas pelo Estados Unidos da América), essa inserção de produtos de *High Tech* em Estados do Sul Global resulta em uma submissão não só econômica e tecnológica, como também cultural e discursiva (Gittinger, 2017; Kwet, 2019).

Essa movimentação que de primeira análise pode ser vista como um investimento do Norte para com o Sul, em que a tecnologia digital implementada e seus produtos são assimilados na sociedade do Sul Global, garante o domínio do Norte Global. A partir disso, o lucro gerado proveniente tanto do aluguel da propriedade intelectual e infraestrutura, como também dos dados reforça a potencialidade dessas multinacionais, além de fornecer autoridade sobre o fluxo de informação e subserviência das infraestruturas tecnológicas daquele Estado. O poder exercido do Norte para o Sul Global no nível digital cessa a autonomia tecnológica desses países e habilita que novas formas de governança se insiram no contexto socioeconômico e político (Kwet, 2019).

O ciberimperialismo necessita de uma discussão em torno da terminologia do imperialismo, uma discussão que permita entender de que maneira essa nova forma de dominação acontece e em quais estruturas ela se associa para manter sua legitimidade. Entretanto, vale ressaltar que para que se possa definir relações cibernéticas como ciberimperialistas, as atividades envolvidas só podem ser interpretadas dessa maneira se houver uma forma de dominação política e econômica como resultado, seja de maneira intencional ou não.

Para compreender de que forma o ciberimperialismo se manifesta na atualidade a partir de suas relações resultantes, é necessário explorar as três formas ou teorias que distinguem o imperialismo: sistêmico, metrocêntrico e pericêntrico[3]. O primeiro é o

[2]Essas três multinacionais englobam outras diversas empresas que estão presente no dia-a-dia e na estrutura digital, como Google, Google Chrome, Google Android, Apple iOS, Microsoft Office, Google G Suíte, Amazon, Microsoft Office, IBM, Uber, Lyft, Microsoft LinkedIn, Google YouTube, Netflix, Hulu e o Facebook.
[3] Do inglês *systemic, metrocentric* e *pericentric imeperialism* (Rusciano, 2001). Tradução livre da autora.

imperialismo sistêmico, que se remota pela interação entre Estados centrais e periféricos, em que o central domina o periférico diante do ímpeto de expandir sua influência para proteger o seu própria declínio, enquanto o periférico aceita as condições diante de sua desvantagem de poder. Em seguida, o imperialismo metrocêntrico incentiva uma relação em termo de poder entre Estados centrais e periféricos para a obtenção de ganhos econômicos, com o foco na exploração. Por fim, o imperialismo pericêntrico é determinado pela condição do Estado periférico, em que classes internas identificam vantagens econômicas na relação com as potências (Doyle, 1986).

Quando analisamos o imperialismo sistêmico manifestado dentro do contexto ciberimperialismo, Rusciano (2001) sugere que este é realizado através da imposição imperialismo cultural de nações centrais sob as periféricas. A disseminação de uma cultura pode ser realizada através das ferramentas que cada Estado tem a sua disposição, entretanto, Estados centrais optam pelas vias do acesso a internet, frente a sua disponibilidade tecnológica. Os Estados periféricos, frente a essa desvantagem posta, encontram dificuldades em lutar contra a influência cultural e em projetar sua cultura na esfera internacional (Gittinger, 2017; Rusciano, 2001).

Já na forma do *imperialismo metrocêntrico*, o controle sobre as tecnologias se manifesta em forma de um discurso hegemônico imperialista em que Estados centrais conscientemente ou inconscientemente disseminam sua linguagem e construções narrativas, fazendo com que os eventos de mundo político sejam interpretados através e por suas lentes. Em outras palavras, o imperialismo metrocêntrico – manifestado dentro do ciberespaço – determina o controle sobre o discurso político e econômico, principalmente quando analisamos a disseminação em veículos de notícia e as suas narrativas construídas (Rusciano, 2001).

O *imperialismo pericêntrico*, por fim, é manifestado para o ciberimperialismo em forma de imperialismo econômico sendo praticado pelas potências para com os países periféricos. Como mencionado anteriormente, o imperialismo pericêntrico realiza sua movimentação inicial através da conciliação entre as potências com as elites do país periférico. Os países centrais buscam alianças e promovem o acesso ao mercado e infraestruturas específicas, entretanto, esses materiais disponibilizados assumem uma nova forma quando passados para os países periféricos. Os materiais vendidos (sejam hardware ou software) são manufaturados, processados e em valores monetários mais altos, repassando esse *raw data*[4] de maneira a confirmar as desvantagens e limitações na relação de

[4] Dados não tratados (tradução livre).

comercialização entre os países do Norte e Sul Global (Rusciano, 2001). A presente pesquisa, portanto, dialoga com as três formas de ciberimperialismo, mas se dedica de maneira mais específica a este, que aborda um viés de dominação econômica.

Dentro desse contexto em que o poder se alastra através das esferas digitais, o software, hardware e as redes de conectividade são os três pilares para a sua consolidação. Começando pelo último, quando tratamos de redes de conectividade estamos discutindo sobre um conjunto de protocolos e normas que máquinas e equipamentos utilizam para o estabelecimento de ligação e comunicação, se configurando como a terceira fonte de dominação digital. As leis e regulamentos da Internet indicam um tráfego neutro de forma que os ISPs (*Internet Service Providers)* tratem os dados que atravessam seus cabos, torres de celular e satélites de maneira igual. O tráfego neutro protege os direitos e liberdade civis do usuário final, regulando a utilização da Internet sem a intervenção de terceiros, por exemplo, no caso do uso de navegadores anônimos para comunicação via Internet, embora seja anônimo, ainda é possível detectar pelo ISPs o uso do navegador, ou até mesmo na disponibilização de Internet via satélite em Estados que estão em conflito (Kwet, 2019).

A segunda fonte de dominação digital é o hardware, que representa a parte física para as experiências de informática. O hardware abrange três formas de controle: o software executado em servidores terceiros, a propriedade centralizada do hardware e aqueles hardwares que são utilizados para privar o utilizador de alterar o software. O primeiro caso faz referência aos softwares que executadas em computadores terceiros e são controlados através do Software as a Service (SaaS), na tradução livre, serviços de nuvem, impedindo com que o usuário final modifique o software e gerando um poder sobre a sociedade em que o serviço de nuvem é instalado. No segundo cenário, a propriedade do hardware permanece sob domínio da empresa ou Estado que o possui e o consumidor final não teria acesso ao controle dos softwares e dados, estando sob responsabilidade dos operadores das nuvens. No último caso, o desenvolvimento do hardware insere travas que restringe os usuários de alterar o software do dispositivo, determinando quais softwares podem ou não serem executados nele (Kwet, 2019).

Todos os casos mencionados dialogam diretamente com o software, devido a centralidade do mesmo para a utilização digital do hardware. O software é o conjunto de componentes lógicos que definem a funcionalidade de uma máquina, funcionando através de lógica codificada que determina a experiência do usuário final. A partir do desenvolvimento do software será possível fixar as suas funcionalidades e suas limitações, incluindo as regras e licenças para sua utilização. O proprietário do software, especificamente no caso de

multinacionais e operações estatais, bloqueia o acesso ao código-fonte e diante disso, acaba por restringir o acesso ao software sem a licença paga e não permite que ele seja modificado ou compartilhado. A dominação através do software é exercida, principalmente, através de licenças de software e da propriedade de hardware. Como exemplo, temos o software Microsoft Windows, em que ele só pode ser utilizado diante do pagamento de sua licença (Kwet, 2019).

2 BRASIL E ÍNDIA: a corrida da cibersegurança

Quais posições da corrida tecnológica da cibersegurança países do Sul Global conseguem ocupar? A conjuntura internacional, pressupondo um sistema anárquico, precede a existência de uma assimetria entre países. Entretanto, é através da dinâmica da assimetria de poder que países que foram colonizadores e países colonizados expressam a disparidade entre eles, principalmente:

> Na medida em que as modernas tecnologias tendem a favorecer a moldura temporal e a duração da ação estatal, tanto na administração pública como na política (o ciclo eleitoral,por exemplo), as experiências subalternas do Sul global têm sido forçadas a responder tanto à curta duração das necessidades imediatas de sobrevivência como à longa duração do capitalismo e do colonialismo. (Santos, 2007, p. 89)

Isto é, países com experiências subalternas estão simultaneamente na tentativa de reduzir suas limitações no processo de desenvolvimento capitalista e se recuperar dos resultados a longo prazo do processo colonialista e exploratório vivenciado.

O Brasil e a Índia são países multiculturais, com uma política única e um histórico acompanhado por um processo de colonização e apropriação de suas terras (Kshetri, 2026; Ebert, 2020). Pensar na posição que ambos ocupam no cenário internacional implica em desvendar as consequências que os países carregam do seu passado. Em outras palavras, é necessário compreender como os estudos de caso do Brasil e Índia são atravessados pelo seu histórico imperialista e de que maneira isso é revelado em seu desenvolvimento na atualidade.

Santos (2007) insere no debate a existência do Sul Global: uma metáfora que remete a um sofrimento sistêmico como resultante do capitalismo global e pelo colonialismo. Essa metáfora, que evidencia relações assimétricas entre o Norte e o Sul, não necessariamente dialoga com o Sul Geográfico mas propõe um novo arranjo para aqueles países com demandas sobrepostas no pós-Guerra Fria, tendo como plano de fundo o colonialismo e a dependência econômica. O Brasil, como um país da América Latina, e a Índia, na Ásia,

expressam a heterogeneidade do Sul Global e demonstram os resquícios do colonialismo em seus desenvolvimentos econômicos e suas capacidades estatais.

No ano de 2023, o Fundo Monetário Internacional em um relatório do *World Economic Outlook* que apontava a escala de que, entre os países de economias em desenvolvimento, a Índia estava em em quinto lugar e o Brasil em nono (FMI, 2023). Mesmo que em comparação global, ambos os países estejam em posições de desenvolvimento econômico, as suas taxas de ataque por cibercrime se destacam, principalmente em comparação a suas regiões.

O cibercrime, embora interpretado muitas vezes como um fenômeno invisível, é tido como um dos maiores desafios enfrentados globalmente com uma estimativa de cem milhões de custos (Bruce et al, 2024). O termo utilizado não apresenta um consenso em sua literatura que o defina, porém, uma dos definições utilizadas frequentemente é a de Thomas e Loader (2000, p.3), em que define o cibercrime como "atividades mediadas por computador que são ilegais ou ilícitas e que podem ser conduzidas através de redes eletrônicas globais". No World Cybercrime Index (Bruce et al, 2024)[5], o Brasil estava em nono lugar e a Índia em décimo em taxa de cibercrime. O Brasil é o único país da América Latina que está entre 15 países da lista, enquanto entre os países asiáticos a Índia está abaixo da China (em terceiro lugar) e Coreia do Norte (em sétimo lugar).

Embora se possa constatar que quanto mais dependente digitalmente um país seja, mais vulnerável ele é, quando analisamos casos de países de experiência subalterna, outras variáveis implicam no resultado tido na área da cibersegurança. Diante disso, será realizada uma análise comparativa histórica entre os casos do Brasil e da Índia – países que se apresentam como palco do fenômeno do ciberimperialismo, mesmo sendo países com trajetórias diferentes no desenvolvimento da segurança cibernética – com intuito de identificar o seu histórico, suas iniciativas na área e o estado da mesma na atualidade.

2.1 Brasil

O Brasil agrega suas características de utilização dos meios digitais a suas questões culturais, fazendo com que a arena do ciberespaço tenha sua particularidade e seus desafios próprios. O caso do Brasil permite que a questão da cibersegurança seja observada a partir de um lugar que é, ao mesmo tempo, o país da América Latina que nos últimos anos mais sofreu ataques cibernéticos e também uma grande fonte para o cibercrime (Grassi; Pinto, 2022;

[5]Disponível em "Mapping the global geography of cybercrime with the World Cybercrime Index." Artigo produzido por Miranda Bruce, Jonathan Lusthaus, Ridhi Kashyap, Nigel Phair,Federico Varese, no ano de 2024.

Kshetri, 2016). Os marcos sociais, econômicos e políticos que atravessam o Brasil resultam em um ciberespaço ameaçado não só pelos fatores externos, como também domésticos, em que as ciberameaças também são consequências de motivação política. Analisar o Brasil requer a noção que o quinto domínio também dialoga com todo o contexto histórico que antecede o momento atual.

A utilização da internet no caso brasileiro reflete a individualidade do país, no qual a população apresenta um fascínio por redes sociais, sendo este um ponto que converge com o início das preocupações em torno da segurança do ciberespaço. Em 15 de maio de 1995, o Ministério das Comunicações (MC) em conjunto com o Ministério da Ciência, Tecnologia e Inovação (MCTI) iniciam os diálogos para a constituição de um Comitê Gestor da Internet no Brasil (CGI) e em 31 de maio do mesmo ano a Portaria Interministerial nº147 cria o CGI. É importante ressaltar que logo no início dos anos 2000, após o marco supracitado, as redes sociais começaram a ser utilizadas de maneira surpreendente no país, como por exemplo o Orkut e o Fotolog que tiveram grande repercussão no país (Oppermann, 2021). A adesão de brasileiros às redes sociais abre brecha para o início do mapeamento para a implementação de publicidades e recolhimento de dados dos usuários de plataformas digitais.

Nos anos 2000, órgãos importantes para a cibersegurança começam a ser desenvolvidos, mesmo que de maneira direta não signifique uma iniciativa consciente para a segurança do ciberespaço. Em 1999, o que antes era a Casa Militar da Presidência da República passou a ser o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), adquirindo novas atribuições como a vinculação à Agência Brasileira de Inteligência (Abin). No ano seguinte, em 13 de junho de 2000, é criado o Comitê Gestor da Segurança de Informação (CGSI) tendo como algumas de suas funções a "criação, desenvolvimento e manutenção de mentalidade de segurança da informação" e a "capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado". O CGSI, atualmente, assume novas atribuições após o Decreto nº 9.637 de 2018, sendo agora o responsável por assessorar o GSI/PR (Brasil, 2023).

Entre os anos de 2000 à 2004 não foram identificados documentos, emendas ou leis que abordassem as questões do ciberespaço, bem como também nenhuma iniciativa que demonstrasse mudanças práticas no que havia sido instituído nos anos 2000. É apenas em 2005 que é implementada a Política Nacional de Defesa (PND), que, embora tenha como foco principal a defesa do Brasil, é o primeiro documento que apresenta pela primeira vez a o debate sobre a cibersegurança como um dos setores estratégicos (Brasil, 2005). A PND tem como um de seus objetivos o aperfeiçoamento dos dispositivos de segurança para a redução

da vulnerabilidade da Defesa Nacional contra ataques cibernéticos e a minimização de possíveis danos. No ano 2006, é criado o Departamento de Segurança da Informação e Comunicações (DSIC) dentro do GSI/PR, tendo a competência da coordenação, execução e implementação da segurança da informação (Brasil, 2006; Sena, 2016). No entanto, o DSIC passou por diversas mudanças ao decorrer dos governos seguintes e, na atualidade, o departamento foi extinguido e substituído pelo Departamento de Segurança Cibernética e da Informação (DSIC) em 30 de agosto de 2023 (Brasil, 2023).

Entre os anos de 2007 e 2008 é desenvolvida e aprovada a Estratégia de Defesa Nacional (END), em que é argumentada a aprimoração da defesa através do desenvolvimento, e, por isso, tem como objetivo também o aprimoramento dos aspectos tecnológicos e o fortalecimento do setor cibernética com a disposição da parceria das três Forças. É colocada como uma das razões para a centralidade do desenvolvimento cibernético a conquista de uma independência tecnológica do Brasil por meio da capacitação cibernética nos campos industrial e militar, ressaltando a autonomia cibernética do país frente a potências estrangeiras. Analisemos nesse ponto um Brasil que identifica uma dependência tecnológica e que enxerga a necessidade de uma mudança em um contexto em que sua capacidade de defesa cibernética também afeta a segurança nacional.

No ano de 2010, é lançado o Livro Verde de Segurança Cibernética (LVSC), reunindo as propostas de diretrizes básicas e com o objetivo de fomentar o debate sobre o social, político e técnico-científico sobre a segurança cibernética no Brasil (Brasil, 2010) . O documento tem uma grande importância para a área, trazendo a visão do país sobre a cibersegurança e afirma de maneira direta a sua preocupação com a política de segurança estratégica. O LVSC abarca os pontos político-estratégicos, econômico, social e ambiental, CT&I, educação, cooperação internacional, e segurança das Infraestruturas Críticas, e, a partir disso, sinaliza as possíveis diretrizes estratégicas para os pontos trabalhados.

A partir desse momento da trajetória da cibersegurança no Brasil, é possível ver o desenvolvimento de iniciativas com foco direto na área. Seguindo a lógica Livro Verde, em 2012 é lançado com Livro Branco da Defesa Nacional (LBDN) que reitera a área da cibernética enquanto um pilar para a segurança nacional, e determina a adição do Centro de Defesa Cibernético. Determina, nesse sentido, o setor cibernético enquanto um setor estratégico para a Defesa Nacional sob a coordenação do Exército, bem como também o setor aeroespacial e nuclear. (Grassi; Pinto, 2022) Em continuidade, ainda em 2012, é aprovada e implementada a Política Cibernética de Defesa (PCD), para orientação de atividades da Defesa e Guerra Cibernética. Essas políticas aplicadas no ano de 2012 permanecem em

constante atualização em acordo com as demandas governamentais no âmbito da defesa nacional, como por exemplo, foi publicada uma portaria em novembro de 2023 para a atualização do LBDN através da formação de um Grupo de Trabalho Interministerial (Brasil, 2023).

Direcionando-se agora ao apanhado documental do ano de 2014, existe uma preocupação direta com as questões do uso da internet no Brasil expressas através da Lei nº 12.965/2014, também conhecido como Marco Civil da Internet (Brasil, 2014). A Lei, decretada pela então Presidenta Dilma Rousseff, estabelece as diretrizes que apontam os direitos e deveres do usuário na internet, frisando o direito ao acesso à internet como pilar para o exercício da cidadania; e assegura os direitos dos mesmos no que concerne à inviolabilidade e sigilo dos dados do usuário e sua utilização – envolvendo questões de coleta, uso, tratamento e armazenamento de dados (Oppermann, 2021; Kshetri, 2016). Da mesma forma, os deveres estabelecem as responsabilidades e neutralidade do provedor de conexão à internet e os possíveis danos gerados dentro do domínio. Assim, apenas no ano de 2014, o Brasil estabelece uma regulamentação e assegura os usuários da internet, fornecendo uma visão técnica aplicada às formas de inserir uma política de segurança a esse campo diante das necessidades do país.

Entretanto, o Brasil não se desprendeu das iniciativas voltadas para a defesa nacional. Ainda no mesmo ano, em novembro de 2014, o Ministro de Estado da Defesa, Celso Amorim, aprova a Doutrina Militar de Defesa Cibernética (DMDC). O objetivo do documento é reafirmar a unificação do pensamento das Forças Armadas para a defesa do Brasil no espaço cibernético, para o que o Estado desenvolva a capacidade de se posicionar frente a ameaças externas diante da posição fundamental da defesa cibernética nas operações militares (Brasil, 2014). O DMDC atribui as competências, diretrizes, fundamentos e determina a visão estatal frente a defesa cibernética, sendo um documento essencial para a evolução da da segurança no ciberespaço no Brasil. É importante, no entanto, enxergar que embora a Doutrina tenha sido desenvolvida, documentos como esse geralmente apresentam características vagas no ponto de vista de aplicabilidade prática de medidas dos elementos abordados (Grassi; Pinto, 2022). Uma comprovação disso é a ausência de um documento próprio no ano de 2014 que elabore a Estratégia Nacional de Defesa Cibernética.

Chegando nos últimos anos abarcados pelo recorte da presente pesquisa, em 2018, é aprovada a Política Nacional de Segurança da Informação (PNSI) com a finalidade de assegurar a integridade da informação, garantindo a segurança dos dados que estão sobre responsabilidade de entidades públicas, assegurar a informação das infraestruturas críticas e

está a frente de questões paralelas a estas (Brasil, 2018). É importante ressaltar, mais uma vez, que o presente documento também expressa questões estritamente de defesa nacional (Grassi; Pinto, 2022).

Mas o ano de 2018 marca a ampliação das preocupações governamentais em torno do ciberespaço. Em 14 de agosto de 2018 é sancionada a Lei Geral de Proteção de Dados Pessoais (LGPD) que guia as normas para o tratamento de dados pessoais – incluindo nos meios digitais –, iniciando a resolução de uma das maiores questões gerais brasileiras, que envolve em sua grande maioria o acesso de empresas aos dados pessoais dos usuários, com uma ausência de uma proteção jurídica de dados. Em concordância com a última lei apresentada, ainda em 2018 é estabelecida a Autoridade Nacional de Proteção de Dados (ANPD), através da medida provisória nº 869 – convertida em lei de número 13.856 em 2019 (Brasil, 2018). A ANPD é um órgão com autonomia técnico-decisório com a responsabilidade da orientação, regulamentação e fiscalização do cumprimento da legislação no que diz respeito à proteção de dados pessoais (Oppermann, 2021).

No ano de 2020, o Brasil, através da figura do então Presidente da República, Jair Messias Bolsonaro, aprova e decreta a Estratégia Nacional de Segurança Cibernética (E-Ciber), sendo este um documento técnico mas também simbólico para a cibersegurança brasileira em que formaliza objetivo da conquista de uma estágio avançado da atuação do país no âmbito nacional e internacional em segurança cibernética (Brasil, 2020).

Apesar de uma trajetória lenta e, em comparação a demais potências emergentes, atrasada em nível estratégico-técnico em questões de segurança do ciberespaço, o Brasil estabelece uma legislação em torno da temática. O que foi desenvolvido pelo Estado brasileiro apresenta um caráter quase estritamente voltado à ciberdefesa, conversando de maneira superficial com os aspectos de segurança de dados. A partir disso, o que se é preciso realizar é uma análise geral do reflexo do que foi desenvolvido na área de ciberdefesa e *dat*a *security* na segurança nacional cibernética do Brasil. Para compreensão apurada deste caso, é preciso visitar outro semelhante, como o da Índia, que revela nuances específicas, assim como o Brasil, enquanto país do Sul Global.

2.2 Índia

A Índia apresenta uma lacuna em sua capacidade estatal de evoluir seus sistemas de cibersegurança em paralelo à velocidade do desenvolvimento digital do país. A sua multiplicidade étnica, política e religiosa, aliado com um processo eleitoral digital, permite que operações de influência cibernética expressem os resultados do estado da segurança no

ciberespaço indiano. Muito embora a Índia esteja na posição de uma superpotência tecnológica, alguns testes realizados em urnas mostram a fragilidade estrutural do sistema. Os poucos relatórios disponíveis sobre ciberataques – seja estatal, terrorista ou criminal, a nível individual e institucional – expressam que estes cresceram desproporcionalmente em comparação aos recursos humanos e tecnológicos da Índia (Ebert, 2020; Parmar, 2018). Além disso, a Índia está em terceiro lugar entre os países do G20 e o primeiro lugar entre os BRICS (Brasil, Rússia, Índia, China e África do Sul) na escala de taxa de infecção de malware no ano de 2019 (Ebert, 2020). O cenário do país indica uma limitação da efetividade da legislação e de suas instituições desenvolvidas ao colocar em perspectiva suas vulnerabilidades crescentes em termos de ciberataque.

O início da trajetória tecnológica da Índia foi impulsionada no fim da década de 1970, como resultado das medidas de liberalização setorial. O fim do século XX representa um momento da história da cibersegurança na Índia marcada por uma substituição do modelo de planejamento socialista para uma economia liberal, que no início da década de 1990 repercutiu em uma preocupação política por parte do governo indiano em voltar suas atenções para a temática. Esse momento determina o início da transformação na posição indiana, tornando-se uma superpotência emergente do setor tecnológico no início dos anos 2000 (Ebert, 2020; Kovacs, 2021).

Nos anos 2000, dois marcos importantes definem a abertura para o quinto domínio: a aprovação da *Information Technology Act* (*IT Act*) e a criação do *Counter-terrorism Working Group*. Em fevereiro de 2000, após a revolta popular no Vale da Caxemira contra o domínio indiano, em que a disseminação de tecnologia começou a afetar a segurança nacional mediante ataques terroristas particulares, foi estabelecido o *Counterterrorism Working Group,* uma iniciativa na área da segurança em conjunto com os Estados Unidos (US State Department, 2000).[6] A parceria estratégica entre Índia e Estados Unidos define um ponto de dependência indiano em torno da segurança nacional, mas também estabelece uma agenda militar contra o terrorismo. O terrorismo permanece sendo uma pauta primordial para a Índia até os dias atuais, mas, principalmente no início dos anos 2000, o país tomou para si uma agenda militarizada da cibersegurança como herança da parceria com os EUA (Kovacs, 2021.)

[6] A estratégia de parceria com países do Sul Global, como a Índia, foi um pilar na estratégia dos Estados Unidos no pós Guerra Fria. As relações Índia-EUA para a formação do Counterterrorism Working Group é um exemplo, acontecendo no momento do início do crescimento indiano. (Mahapatra, 2014)

As iniciativas seguintes mantiveram um teor militar, como a aprovação, em 17 de outubro de 2000, da *IT Act*, uma lei que aborda o cibercrime e o *E-commerce*, sendo a Índia o décimo segundo país a aprovar uma lei dentro dessa categoria e representando um símbolo de seu desenvolvimento enquanto uma potência emergente (Kshetri, 2017). A IT Act é considerada também como uma medida militar em razão de sua abordagem centralizada na regulamentação do cibercrime, apesar de abrir brechas para iniciativas futuras que abrangem outras áreas da segurança do ciberespaço. A *IT Act* abarca diversas iniciativas que foram tomadas ao decorrer dos anos 2000, sendo um guarda-chuva para a proteção tecnológica da Índia (IT Act, 2000).

As parcerias Índia-EUA continuaram evoluindo e aprimorando o diálogo cibernético entre os países. Em 2001, foi desenvolvido o Cyber Security Forum como resultado das trocas entre ambos países sobre as questões contra-terroristas, dedicado para a proteção de infraestruturas críticas. As relações entre Índia e Estados Unidos apresentam um caráter evolutivo, em que uma iniciativa leva a outra. Tendo isso em vista, em 2005 foi elaborado o ICT Working Group, com os preceitos acumulados dos seus demais projetos de parceria (Ebert, 2020).

Retomando para o IT Act, uma das iniciativas da lei que foi concretizada na mesma década se encontra na seção 48 da lei, sendo estabelecido pela Central de Governança, a *Cyber Appellate Tribunal* (CAT) começou a funcionar em 2006. O panorama da tecnologia indiana é atravessado pelas parcerias público-privadas, agindo enquanto um impulsionador da evolução das medidas de proteção e segurança cibernética do país (Kshetri, 2017). A NASSCOM (*National Association of Software and Service Companies*) é uma associação não governamental fundada em 1988 e age como uma figura chave no setor tecnológico indiano. Em agosto de 2008, a NASSCOM desenvolveu o *Data Security Council of India* (DSCI) com o intuito de garantir um ciberespaço seguro e assegurar a privacidade (Kshetri, 2017). Essa iniciativa, vigente até os dias atuais, evidencia a evolução da preocupação de uma cibersegurança na Índia, além de demonstrar a dimensão das parcerias público-privada (Kovacs, 2021). Nesse ponto da história da cibersegurança indiana, podemos afirmar que a legislação ainda não havia alcançado a discussão de ajustes nas políticas estratégicas de cibersegurança, mas já havia bases para o desenvolvimento das mesmas.

O desenvolvimento de uma política que enxergasse a emergência de uma cibersegurança na Índia caminha entre as questões público-privadas, fazendo com que essas iniciativas se complementem e impulsionem umas às outras. Como continuidade desse momento, entre 2008 e 2009, a *Information Technology* passou pelo parlamento indiano, mas

não mais em formato de lei e sim de emenda, sendo aprovada no órgão no fim de 2008 e recebendo o consentimento da presidente Pratibha Patil em fevereiro de 2009 (IT Act, 2008). Em 2011, o *Reserve Bank of India* (RBI) disponibilizou uma série de recomendações e diretrizes para auxiliar a promoção da inserção do país na economia global assegurando sua segurança, sugerindo formação de grupos especializados em cibersegurança e manutenção de recursos, reafirmando uma política econômica liberalizante (Parmar, 2018; Kshetri, 2017)

A mudança que começava a dar seus primeiros sinais nos últimos anos teve seu ponto de virada de chave no ano de 2012, iniciando uma transição de uma cibersegurança puramente militar, com uma abordagem centrada no terrorismo, para uma visão ampla. Dois relatórios participam dessa mudança, sendo um realizado pelo *Joint Working Group* (JWG) e o outra carta de recomendação a *Task Force Naresh Chandra*. O JWG foi estabelecido sob a presidência do Vice-Conselheiro de Segurança Nacional, com o intuito de fornecer a concretização de uma cibersegurança com a colaboração do governo e do setor privado.

Com representantes de ambos setores para sua construção, foi disponibilizado o relatório *"Engagement with Private Sector on Cyber Security"* em outubro de 2012 com a atenção destinada à cooperação necessária para que a área estabeleça capacidades para além do militar (Joint Working Group, 2012). Em complemento, a carta de recomendação da *Task Force Naresh Chandra* sugere a criação da *Defence Cyber Agency (*DCyA) enquanto uma demanda para a aprimoração da cibersegurança indiana a partir de uma agência tri-serviço – isto é, com a marinha, aeronáutica e exército (Ebert, 2020; Kovacs, 2021; Kshetri, 2017). Essa demanda expressa uma noção de nacionalização da segurança cibernética, que mesmo envolvendo as três forças, quebra uma abordagem militarizada devido as características de inclusão de regulamentações para além do terrorismo.

Em 2013, os esforços para a concretização dos objetivos indianos continuaram através de uma iniciativa regulamentar do Governo da Índia (GOI) que divulgou a Política Nacional de Cibersegurança (NCSP) com 14 objetivos para o reforço das infraestruturas críticas e o desenvolvimento de 500 mil profissionais qualificados em cibersegurança nos próximos cinco anos (India, 2013). A NCSP também direciona esforços para a demanda de um plano de gestão de crises cibernéticas, com o intuito de proteger os processos nacionais críticos e a segurança pública. Muito embora essa resolução tivesse sido liberada em julho de 2013, ela só veio a ser publicada em uma notificação do Diário da República no início de 2014, adicionando também o *National Critical Information Infrastructure Protection Centre* (NCIIPC), uma organização criada sob a seção 70A da *IT Act* e sendo apontada como a Agência Nodal Nacional sobre matéria de proteção de infraestrutura crítica (Kovacs, 2021).

Entre os anos de 2014 e 2015 não foram encontrados dados que tracem o desenvolvimento de uma política ou iniciativa de reforço da cibersegurança indiana. No ano seguinte, em 2016, foi lançada uma rede integrada chamada *Defence Communication Network* (DCN) com o objetivo de facilitar o fluxo de dados e informações através da criação de redes e automatização de serviços, com uma visão direcionada para o enfrentamento de ciberguerras (Kovacs, 2021).

Finalmente, no ano de 2017, o Ministério da Defesa seguiu a recomendação feita em 2012 para a criação da Doutrina Conjunto das Forças Armadas, apontado por Kovacs (2021) com um documento raro que pretendia operar os três serviços militares em sinergia, adicionando nas instituições indianas uma visão de união (Índia, 2017). Nele as questões de defesa do ciberespaço são posicionadas como objetivos de segurança nacional, direcionando o papel da cibersegurança diretamente para uma posição fundamental nas operações militares e tomando uma visão do quinto domínio para além de questões da agenda terrorista. Além disso, ainda no mesmo ano, o *Insurance Regulatory and Development Authority* (IRDAI) – uma entidade regulamentadora da Índia – emitiu uma diretriz que exige que todas as companhias de segurança nomeiem um CISO (c*hief information security officer*), fazendo com que essas empresas tenham um executivo à frente da segurança do ciberespaço e estabelecendo sua responsabilidade com esse domínio (Ebert, 2020; Kovacs, 2021; Kshetri, 2017).

Em 2018, o primeiro ministro Narendra Modi aprovou a criação do *Defence Cyber Agency,* mencionado anteriormente no relatório da *Task Force Naresh Chandra* (2012), funcionando sob a alçada do Estado-Maior Integrado da Defesa e como uma agência tri-serviço simplificada, indicando seu teor de coordenação e integração das forças armadas. Os relatórios do DCyA mostram que sua atividade permanecerá limitada ao papel defensivo, muito embora existam capacidades para contribuições defensivas, também apontando uma responsabilidade em torno da detecção de ameaças no fluxo de dados, a identificação dos tipos e fontes dessas ameaçadas e uma resposta para limitação de impactos, bem como também uma plano de crise (Kovacs, 2021; Kshetri, 2017).

Ainda em 2018, um projeto de lei sobre a proteção de dados pessoais (*Personal Data Protection Bill*) foi desenvolvido, caracterizado por um quadro regular de utilização de dados pessoais por atores privados e públicos (India, 2017). Essa lei tem como público alvo direto atores importantes de setores privados que se mobilizaram para que os seus dados fossem protegidos e bem tratados, tendo o foco de proteger os direitos dos usuários em segundo plano (Kovacs, 2021). No ano de 2019, a Índia ainda continuava a discutir o desenvolvimento de

uma lei de proteção de dados pessoais, e agências de informação já discutiam novas demandas para o projeto de lei.

Mesmo com uma trajetória com um progresso de medidas e políticas para a garantia de uma cibersegurança indiana, seus esforços ainda não são suficientes e continuam limitados. Isso acontece devido a pouca atenção que os formuladores de políticas do governo destinam à segurança cibernética, principalmente diante do crescimento tecnológico da Índia (Ebert, 2020). A disparidade nas tentativas de uma regulamentação e em sua efetivação é um questionamento com diversos pontos subjetivos de análise, mas dialoga de maneira central com o tema proposto: o ciberimperialismo e seus possíveis resultados.

3 IMPERIALISMO NO CIBERESPAÇO: a posição do Brasil e da Índia

O campo da cibersegurança requer um olhar multidisciplinar para a conclusão de qualquer diagnóstico diante da magnitude do alcance que o ciberespaço apresenta na atualidade. A constatação da existência de um imperialismo que se renova e assume novas formas de manutenção, alcançando também o ciberespaço, é um desafio para o desenvolvimento de um cibersegurança global que demonstre resultados efetivos (Kwet, 2019). Isto se dá porque o ciberespaço e suas nuances desafiam limites fronteiriços, fazendo com que a vulnerabilidade cibernética de um país afete os demais, em efeito cascata (Radu, 2014; Abassi, 2021)

No entanto, quem se beneficia pelo atraso cibernético de países em desenvolvimento são os mesmos países que estiveram à frente de processos de colonização e exploração, estando sempre ocupando a posição de líderes. O imperialismo pericêntrico é a categoria específica em que esse artigo se debruça, expondo a relação entre países do Sul Global com processos de desenvolvimento de segurança cibernética (Rusciano, 2001). Para fins conclusivos, será utilizada a base de dados do Global Cybersecurity Index 2020 (ITU, 2021), uma iniciativa da União Internacional das Telecomunicações.

A União Internacional das Telecomunicações, no ano de 2015, deu início a um projeto de construção da confiança e segurança na transparência dos dados da segurança cibernética. O Global Cybersecurity Index (GCI) teve sua primeira publicação em 2015, com a adesão de 105 estados membros participando da pesquisa relacionada aos dados coletados de 2013 e 2014. Depois dessa edição, houveram outras duas, no ano de 2017 e 2019, respectivamente com a participação de 136 e 155 países. O intuito da UIT é promover um meio em que governos pudessem desenvolver estratégias e compartilhar informações, para que assim fosse

possível estabelecer uma cultura global de cibersegurança por meio da integração (ITU, 2021).

O Global Cybersecurity Index é formulado a partir da disponibilização de dados dos Estados membros da UIT, tendo também a adição de contribuintes como: o Instituto Australiano de Política Estratégica, FIRST (Fórum de Respostas a Incidentes e Time de Segurança), Universidade de Grenoble (França), Universidade de Indiana, INTERPOL (Organização Internacional de Polícia Criminal), ITU-Arab, Coreia Internet e Agência de Segurança, Autoridade Reguladora Nacional de Telecomunicações (NTRA-Egito), Read Team Cyber, Instituto Potomac de Estudos Políticos, UNICRI (Instituto Inter-regional de Pesquisas das Nações Unidas para o crime e a Justiça), Universidade de Tecnologia da Jamaica, UNODC (Escritório das Nações Unidas sobre Drogas e Crime) e o Banco Mundial (ITU, 2021).

Os dados e diagnósticos disponibilizados pelo GCI são reforçados pela robustez e preparo técnico que envolve o processo de formulação do Índice, sendo uma das fontes mais confiáveis sobre segurança cibernética. O seu objetivo, através dos seus pilares de descrição, é medir as questões de comprometimento com a cibersegurança de cada Estado membro nos níveis de comparação relativa a outros países, em uma perspectiva global, regional e internamente (ITU, 2021). Com isso, o Global Cybersecurity Index maneja formas de ajudar países a identificar campos específicos da área que necessitam de esforços mais efetivos e encorajá-los a direcionar estratégias para isso. Em resumo, através desses dados o União Internacional de Comunicação, através da produção GCI, almeja alcançar uma ascensão no nível de comprometimento internacional com a cibersegurança e gerar uma cultura global sobre o tema (ITU, 2021).

No ano de 2021, a União Internacional das Telecomunicações lançou a quarta edição do *Global Cybersecurity Index (*GCI*)*, sendo a atualização de versões anteriormente publicadas. O dado mais atualizado do GCI contém as respostas de 168 Estados membros e o Estado da Palestina[7] sobre o panorama da cibersegurança do ano de 2020. Esse Índice será utilizado como fonte de dados neste artigo para fins comparativos, permitindo que análises sejam feitas em torno do estado da cibersegurança nos casos propostos do Brasil e Índia.

Antes de explorar os dados contidos no Índice, é importante inserir na visualização do mesmo sua metodologia e as variáveis utilizadas para a sua construção. O resultado de cada

[7] A participação do Estado da Palestina é realizada sobre a Resolução 99 do ano de 2018. Disponível em: https://www.itu.int/online/mm/scripts/gensel9

país é medido por meio de um questionário[8], com 20 indicadores construídos a partir de 82 perguntas, tendo estes sido selecionados com base nos pilares do GCI, seu objetivo principal, disponibilidade de dados e possibilidade de verificação dos mesmos. A partir disso, um questionário é enviado para os países membros da UIT e para o Estado da Palestina. Ao retornar, as informações contidas no questionário passam por uma dupla verificação, em que procura faltas de documentos ou links e a veracidade dos dados. Para o caso de países que não são membros, a própria agência desenvolve um rascunho sobre o estado da cibersegurança do mesmo por meio de dados e pesquisas onlines e solicita uma revisão de um grupo focal, realiza a verificação dos dados e insere o país a suas análises (ITU, 2021).

O Global Cybersecurity Index é sustentado por cinco pilares: medidas legais, técnica, capacidade organizacional, capacidade de desenvolvimento e cooperação. A cada variável dessa, é calculado um valor que varia de 0 a 20 de acordo com as respostas contidas no formulário. Sobre medidas legais (I), o GCI define como "medidas baseadas na existência de quadros legais que lidam com cibersegurança e cibercrime" (ITU, p. 132, tradução da autora). O objetivo deste pilar é conter legislação suficiente para harmonizar as práticas de cibersegurança a nível regional e internacional, incluindo não só a lei, como também regulamentos e legislação de contenção de spam.

Para definir medidas técnicas (II), "medidas baseadas na existência de instituições técnicas e quadro para lidar com a cibersegurança" (ITU,, 2021, p. 132, tradução da autora), que envolve questões como o desenvolvimento de critérios para a implementação de tecnologias dentro do país, bem como também o desenvolvimento de uma autoridade nacional para respostas e monitoramento de incidentes. As questões de capacidade organizacional (III) abordam a identificação de estratégia e objetivos nacionais sobre cibersegurança aliadas da definição das responsabilidades de instituições para a aplicação e manutenção das mesmas, sendo ditas pelo GCI como "medidas baseadas na existência de instituições de coordenação, políticas e estratégias para o desenvolvimento da cibersegurança ao nível nacional" (ITU, 2021, p. 132, tradução da autora).

O pilar de capacidade de desenvolvimento (IV) é interligado com os três anteriores e dialoga também com questões socioeconômicas e implicações políticas do país. O GCI define como "medidas baseadas na existência de pesquisa e desenvolvimento, educação e programas de treinamento, profissionais certificados e agências do setor público que promovam reforço das capacidades" (ITU, 2021, p. 133, tradução da autora). A subjetividade que esse tópico

[8] O questionário está disponível no documento do Global Cybersecurity Index 2020 (ITU, 2021).

aborda revela também as implicações da própria cibersegurança na sociedade e como a estrutura da mesma define os caminhos traçados para a área.

Por fim, como já reforçado no primeiro capítulo, questões de cibersegurança necessitam de esforços de interconexão entre Estados diante de sua caracterização de um tópico que supera a existência de fronteiras e as ultrapassa, fazendo com que a mesma seja uma responsabilidade e um desafio transnacional. Por isso, a cooperação, último pilar do GCI direciona sua investigação, é definido como "medidas baseadas na existência de parcerias, quadros de cooperação e redes de compartilhamento de informações" (ITU, 2021, p. 133, tradução da autora).

Dentre outros resultados, no índice abordado, é possível ter acesso a pontuação de todos países em torno das temáticas de cibersegurança supracitadas. Disso, foi feito um ranking que classifica o Brasil na 18º posição global e 3º lugar na região das Américas, atrás dos Estados Unidos e Canadá, com uma pontuação de 96.6. No caso da Índia, o país se encontra na 10º posição global e 4º lugar na região Ásia-Pacífico (ITU, 2021).

Considerado pelo índice como um país em desenvolvimento, o Brasil tem como área de força relativa, dentro das cinco abordadas, as medidas legais, e, como potencial de crescimento, as técnicas e medidas organizacionais. A Índia, também enquanto país em desenvolvimento, tem como áreas de força relativa a legislação, cooperação e capacidade de desenvolvimento, com capacidade organizacional com potencial de crescimento (ITU, 2021). Na tabela 1, é possível enxergar os números alcançados por cada país nas cinco categorias.

Tabela 1- Perfil do Brasil e da Índia.

	Brasil	**Índia**
Medidas Legais	20.00	20.00
Técnicas	18.73	19.08
Medidas Organizacionais	18.98	18.41
Capacidade de Desenvolvimento	19.48	20.00
Cooperação	19.41	20.00
Pontuação Geral	96.00	97.49

Fonte: ITU, 2021.

Tendo como pano de fundo o histórico de ambos os países, assim como também seus documentos, legislação e políticas que envolvem a área da cibersegurança, é possível traçar resultados em torno de cada caso.

Como visto, ambos países demonstram boa capacidade legislativa. Entretanto, é na questão técnica e de medidas organizacionais que ambos os países diferem e demonstram situações particulares. O Brasil, muito embora apresente um desempenho de 20.00 pontos em legislação, cada processo que envolve essa área necessita de renovação constante em que leis são revogadas e outras são implementadas em seu lugar. Até mesmo se analisarmos em agências de segurança cibernética, podemos ver um padrão de realocação de grupos, podendo interpretar a cibersegurança para o Brasil como um assunto secundário. Para o caso brasileiro, a questão técnica e organizacional acaba sendo uma variante contribuinte para o enfraquecimento da cibersegurança, pois, mesmo com a lei que inicia o processo da construção de um ambiente digital seguro, a capacidade técnica e organizacional ainda são um obstáculo.

A legislação indiana acaba não sendo uma grande questão quando colocadas ao lado de suas questões internas. A Índia apresenta um bom nível de medidas técnicas, mas que, como abordado previamente, não são o suficiente para o tamanho da demanda do país (Ebert, 2020). É necessário, a partir disso, um direcionamento que analise as lacunas do país e trace estratégias, como a capacitação de mão de obra especializada em comparação a grande demanda. Em suas questões de cibersegurança e ciberdefesa, o estado da cibersegurança demonstra um valor inferior ao do Brasil em medidas organizacionais. Ao voltarmos no histórico da Índia, vemos a incorporação de agendas estadunidenses relacionadas ao terrorismo. A partir das medidas organizacionais podemos ver a urgência de objetivos e estratégias nacionais bem definidos que dialoguem com os princípios e contexto socioeconômico da Índia.

O tópico concernente à cooperação técnica acabou não sendo foco da presente pesquisa, uma vez que sua especificidade demandaria uma abordagem mais ampla do que o espaço atual nos permite. Dessa forma, a inserção e avaliação de documentos que explorem a área serão objeto de pesquisas futuras.

Mesmo tendo o panorama geral em torno da Índia e do Brasil, uma grande questão ainda apresenta uma lacuna. Se o Brasil e a Índia apresentam esses resultados, qual a situação dos líderes da cibersegurança? Em um dado mais atualizado, o MIT (Instituto de Tecnologia de Massachusetts) divulgou um ranking dos líderes da segurança cibernética, sendo os quintos primeiros, em ordem: Austrália, Países Baixos, Coreia do Sul, Estados Unidos e Canadá. Nesse mesmo ranking, a Índia ocupa a 17º posição e o Brasil a 18º, sendo classificados entre os cinco países com progresso lento em torno da criação de um ciberespaço seguro (MIT, 2022).

Utilizando ainda o Global Cybersecurity Index, os dados com relação a esses cinco líderes da segurança cibernética são os seguintes:

Tabela 2 - Perfil dos Líderes da Cibersegurança

	Austrália	**Países Baixos**	**Coreia do Sul**	**Estados Unidos**	**Canadá**
Medidas Legais	20.00	20.00	20.00	20.00	20.00
Técnicas	19.08	19.84	19.54	20.00	18.27
Medidas Organizacionais	18.98	18.98	18.98	20.00	20.00
Capacidade de Desenvolvimento	20.00	18.82	20.00	20.00	20.00
Cooperação	19.41	19.41	20.00	20.00	20.00
Pontuação Geral	97.47	97.05	98.52	100.00	96.67

Fonte: ITU, 2021.

Todos os países listados como líderes, com exceção da Coreia do Sul, são países do Norte Global. A partir disso, quando esses casos são comparados com a situação do Brasil e da Índia, podemos chegar a certas conclusões. Tendo como base os números para o Brasil de 96.00 e para Índia de 97.49, podemos ver a diferença entre a pontuação geral da Austrália, Países Baixos, Coreia do Sul, Estados Unidos e Canadá com os dois casos analisados.

Tabela 3 - Comparação entre a Pontuação Geral de Líderes com o Brasil e Índia

	Pontuação Geral	**Diferença (Brasil)**	**Diferença (Índia)**
Austrália	97.47	4.47	-0.02
Países Baixos	97.05	1.05	-0.44
Coreia do Sul	98.52	2.52	1.03
Estados Unidos	100.00	4.00	2.51
Canadá	96.67	0.67	-0.82

Fonte: ITU, 2021

Muito embora o Brasil e a Índia tenham desenvolvido uma maturidade na área da cibersegurança e estejam entre os líderes em suas respectivas regiões, existem limites para sua evolução na área. Retomando a conclusão de Santos (2007), países explorados e colonizados estão passando pelo processo mútuo da superação do seu passado e da sua tentativa de alcançar o desenvolvimento tecnológico. Em números absolutos, é possível visualizar uma

diferença significativa entre o Brasil e a Índia com os casos comparados. Mas, ao analisarmos de maneira mais específica, podemos notar que em alguns casos – como a Austrália, em comparação com a Índia – a diferença chega a ser negativa, e mesmo assim, a Índia enfrenta desafios de medidas técnicas e capacidade organizacional, exprimindo de maneira pontual as particularidades que países do Sul Global enfrentam.

O imperialismo e a assimetria de poder, cultivada em benefício próprio pelas potências do sistema em que estamos inseridos, posiciona suas ferramentas de maneira estratégica no ciberespaço. Os casos dos dois países do Sul Global, considerados potências regionais, expressam a desvantagem e os desafios que limitam o desenvolvimento de um ciberespaço seguro. Principalmente quando tocamos nos pilares de técnica, medidas organizacionais e capacidade de desenvolvimento, é exposto o processo de assimetria de poder impulsionada pelo imperialismo pericêntrico. O Brasil e a Índia enfrentam uma corrida na cibersegurança que é trapaceada constantemente devido suas experiências subalternas que ditam sua projeção em assimetria com o Norte Global.

CONSIDERAÇÕES FINAIS

A pesquisa teve como objetivo investigar os impactos do imperialismo no Ciberespaço, com foco no Brasil e na Índia. Estes países, marcados por histórias de dominação e colonização, servem como exemplos cruciais para entender as dinâmicas subalternas no Ciberespaço, e, especificamente, na cibersegurança. Partiu-se da ideia de que o Brasil e a Índia, apesar de seus desempenho no ciberespaço, sucumbem ao ciberimperialismo, diante da dominação do Norte Global no quinto domínio

Buscou-se explorar a literatura da área da Cibersegurança, bem como também as discussões sobre Ciberpoder e, aborda por fim, o fenômeno em que esta pesquisa debruça, o Ciberimperialismo. Definir a cibersegurança em uma noção estática, ignorando atualizações que venham a incluir novos desdobramentos de suas implicações, termina por ser limitante, e por isso, o significado tem caráter fluido e aberto para possíveis inovações. Dentro do domínio do Ciberespaço, o ciberpoder se insere nas dinâmicas enquanto uma ferramenta de poder tradicional que habilita que atores do Norte Global alcancem os melhores resultados. É no sentido de uma assimetria de poder, que o imperialismo no ciberespaço (ciberimperialismo) se instaura e desenvolve técnicas de controle, em que impõe limites em termos de desenvolvimento tecnológico, reforçando a perpetuação de um sistema de domínio.

Ao analisar o caso do Brasil e da Índia, é possível enxergar particularidades para cada caso, sendo distintos em termos evolutivos e processuais. Começando pelo segundo, é identificado uma boa dedicação para a relevância do subcampo de dados, mas a cibersegurança indiana ainda apresenta lacunas para a proteção dos mesmos. Isto muito em razão do progresso lento da segurança cibernética da Índia em comparação ao ritmo de sua evolução tecnológica. No caso do Brasil, observa-se esforços para a construção de políticas e leis que garantam a segurança do ciberespaço, mas focam em sua maioria em termos de ciberdefesa. Além disso, o país expressa um perfil de iniciativas em que apresentam dificuldades de serem postas em prática de maneira efetiva.

Utilizando-se de dados coletados por meio do Global Cybersecurity Index 2020 (ITU, 2021), foi possível comparar a situação do Brasil e da Índia nas categorias de: medidas legais, técnica, capacidade organizacional, capacidade de desenvolvimento e cooperação. Além disso, pela seleção e comparação das pontuações gerais dos cinco países considerados líderes da cibersegurança pelo MIT (MIT, 2022), conseguiu-se enxergar uma desigualdade pontual que mostra as particularidades que países como o Brasil e a Índia enfrentam no ciberespaço, em razão do seu atraso relativo a países do Norte Global. Isto torna-se ainda mais evidente ao tocarmos nos pilares de técnica, medidas organizacionais e capacidade de desenvolvimento.

Compreender as dinâmicas internas de países do Sul Global permite a visualização plena da realidade do ciberespaço e seu *modus operandi* em âmbito internacional. Isto pois, negligenciar países como o Brasil e a Índia de análises técnicas e políticas, tem como resultado trabalhos imprecisos que não abarcam a totalidade da soma de poder do jogo político internacional.

A hipótese proposta é comprovada, sendo possível notar uma correlação entre os limites do Brasil e da Índia em termos de cibersegurança com a existência do ciberimperialismo e sua consequente ligação com a dominação do Norte Global sobre o desenvolvimento cibernético do Sul. A pesquisa, diante da limitação enfrentada por seu locus de desenvolvimento, buscou entender a maneira com que o Brasil e a Índia se manifestam na área de cibersegurança e qual seu desempenho em comparação com líderes globais. Indica para pesquisas futuras, nesse sentido, a investigação da maneira com que é realizada a manutenção e perpetuação do ciberimperialismo, adentrando na seara de estratégias e movimentações realizadas para a fixação desse fenômeno.

REFERÊNCIAS

ABBASI, Mohammad. Security in Cyberspace in the Field of International Relations. **Journal of Archives in Military Medicine**, v. 8, n. 4, 2020. Disponível em: https://brieflands.com/articles/jamm-114485.pdf . Acesso em: 04 de abril de 2024.

Bolognesi, B. O que é e para que serve? Prós e contras do método comparado em Ciência Política. In: Perissinotto, R. et al. **Política Comparada:** Teoria e Método. Rio de Janeiro: Editora UERJ, 2022, p. 19-42.

BRASIL, CGI.BR - Comitê Gestor da Internet no Brasil. Portaria Interministerial nº147/1995. Criação do Comitê Gestor Internet do Brasil. CGI, 1995. Disponível em: https://www.cgi.br/portarias/numero/Portaria_147.pdf. Acesso em: 11 de junho de 2024.

_____. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 11 de junho de 2024.

_____. Gabinete de Segurança Institucional. Livro Verde: Segurança Cibernética no Brasil. Brasília, DF. 2010. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf . Acesso em: 11 de junho de 2024.

_____. Governo do Brasil. Estratégia Nacional de Defesa. Brasília, DF. 200. Disponível em: https://bibliotecadigital.economia.gov.br/bitstream/123456789/459/1/end.pdf . Acesso em: 11 de junho de 2024.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 11 de junho de 2024.

_____. Ministério da Defesa. Doutrina Militar de Defesa Cibernética. Brasília, DF, 2014. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf . Acesso em: 11 de junho de 2024.

_____. Ministério da Defesa. Portaria N° 5.586, 16 de novembro de 2023. o Grupo de Trabalho Interministerial - GTI instituído para atualizar o Livro Branco de Defesa Nacional. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gm-md-n-5.586-de-16-de-novembro-de-2023-523989123. Acesso em: 11 de junho de 2024.

_____. Medida Provisória nº869, de 27 de dezembro de 2018. Criação da Autoridade Nacional de Proteção de Dados e outras providências. Brasília, DF. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 11 de junho de 2024.

_____. Decreto Nº 11.676, de 30 de agosto de 2023. prova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das Gratificações do Gabinete de Segurança Institucional da Presidência da República, e remaneja e transforma cargos em comissão, funções de confiança e gratificações. Brasília, DF. 2010. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5772.html . Acesso em: 11 de junho de 2024.

_____. Decreto Nº 5,772, de 8 de maio de 2006.Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República, e dá outras providências.. Brasília, DF. 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5772.html. Acesso em: 11 de junho de 2024.

_____. Decreto Nº 5.484, de 30 de junho de 2005. Aprova a Política de Defesa Nacional, e dá outras providências. Brasília, DF 2005. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5484.htm . Acesso em: 11 de junho de 2024.

_____. Decreto Nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. Brasília, DF. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 11 de junho de 2024.

_____. Histórico do Gabinete de Segurança Institucional. 2023. Disponível em: https://www.gov.br/gsi/pt-br/acesso-a-informacao/institucional/historico#:~:text=Em%202023%20o%20GSI%2FPR,sobre%20assuntos%20militares%20e%20de. Acesso em: 31 maio. 2024. Acesso em: 11 de junho de 2024.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 de junho de 2024.

_____. Lei Nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Diário Oficial da União, 1990. Acesso em: 11 de junho de 2024.

BRUCE, Miranda et al. Mapping the global geography of cybercrime with the World Cybercrime Index. **Plos one**, v. 19, n. 4, p. e0297312, 2024. Disponível em: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312&utm_referrer=https%3A%2F%2Fdzen.ru%2Fmedia%2Fid%2F595abe97e86a9e3f7efbbda3%2F6618d2c4a470023246f00b1b. Acesso: 10 de maio de 2024.

CHOUCRI, Nazli; GOLDSMITH, Daniel. Lost in cyberspace: Harnessing the Internet, international relations, and global security. **Bulletin of the Atomic Scientists**, v. 68, n. 2, p. 70-77, 2012. Disponível em: https://journals.sagepub.com/doi/full/10.1177/0096340212438696. Acesso em: 04 de abril de 2024.

DAHL, Robert A. The concept of power. **Behavioral science**, v. 2, n. 3, p. 201-215, 1957. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/bs.3830020303 . Acesso em: 04 de abril de 2024.

DOYLE, Michael W. **Empires**. Cornell University Press, 1986.

DREZNER, Daniel. Power and international relations: a temporal view. **European Journal of International Relations**, v. 27, n. 1, p. 29-52, 2021. Disponível em: https://journals.sagepub.com/doi/full/10.1177/1354066120969800. Acesso em: 04 de abril de 2024.

EBERT, Hannes. Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. **India Review**, v. 19, n. 4, p. 376-413, 2020. Disponível em: https://www.tandfonline.com/doi/full/10.1080/14736489.2020.1797317. Acesso em: 10 de maio de 2024.

FMI [Fundo Monetário Internacional]. World Economic Outlook: Navigating Global Divergences. Washington, DC: October, 2023. Disponível em: https://www.imf.org/en/Publications/WEO/Issues/2023/10/10/world-economic-outlook-october-2023. Acesso em: 11 de junho de 2024.

FOUCAULT, Michel; DELEUZE, Gilles. Intellectuals and power. **Language, counter-memory, practice:** Selected essays and interviews, v. 205, p. 209, 1977.

GITTINGER, Juli L. Is there such a thing as ‘cyberimperialism?’. **Continuum**, v. 28, n. 4, p. 509-519, 2014. Disponível em: https://www.tandfonline.com/doi/full/10.1080/10304312.2014.907873. Acesso em: 04 de maio de 2024.

GRASSI, Jéssica; PINTO, Danielle Jacon Ayres. O Sistema de Defesa Cibernética do Brasil: dinâmica civil-militar e maturidade democrática. **Nação e Defesa**, n. 163, 2022. Disponível em: https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD163/4.pdf . Acesso em: 11 de maio de 2024.

HOPF, Ted. The promise of constructivism in international relations theory. International security, v. 23, n. 1, p. 171-200, 1998.Disponível em: https://direct.mit.edu/isec/article-abstract/23/1/171/11597/The-Promise-of-Constructivism-in-International. Acesso em: 04 de abril de 2024.

INDIA, Governo da Índia. National Cyber Security Policy, 2013. Disponível em: https://usp.br/sddarquivos/arquivos/abnt6023.pdf. Acesso em: 11 de junho de 2024.

INDIA, Governo da Índia. Shanker, R. (ED.). **The Gazette of India: Extraordinary**. [s.l: s.n.]. 27 out. 2009. Disponível em: https://xn--m1bdba5a7gresc7dsa.xn--11b7cb3a6a.xn--h2brj9c/writereaddata/files/The%20Cyber%20Appellate%20Tribunal%28Chairperson_Members%29%20Rules%2C%202009.pdf. Acesso em: 11 de junho de 2024.

INDIA, Governo da India. The Gazette of India: Extraordinary. [s.l: s.n.]. 16 jan. 2014. Disponível em: https://www.meity.gov.in/writereaddata/files/GSR_19%28E%29_0.pdf. Acesso em: 11 de junho de 2024.

INDIA, Governo da Índia. **The Information Technology ACT**. Nova Delhi. 2008. Disponível em: https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf. Acesso em: 11 de junho de 2024.

INDIA, **Joint Doctrine Indian Armed Forces,** 2017. Disponível em: https://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf . Acesso em: 11 de junho de 2024.

INDIA, The Information Technology Act, IT ACT. , 17 de outubro de 2000. Disponível em: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf. Acesso em: 11 de junho de 2024.

INDIA, **The Personal Data Protection Bill**, 2018. Disponível em: https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf. Acesso em: 11 de junho de 2024

INDIA-US, **Cyber Security Forum** ([s.d.]). Ministry of External Affairs, Government of India. 2006. Disponível em: https://www.mea.gov.in/bilateral-documents.htm?dtl/6014/IndiaUS+Cyber+Security+Forum++Fact+Sheet/ . Acesso em: 11 de junho de 2024.

ITU-T, International Telecommunication Union. **Recomendation ITU-T X.1205**, 2008. Disponível em: <https://handle.itu.int/11.1002/1000/9136>. Acesso em: 11 junho 2024.

ITU, INTERNATIONAL TELECOMMUNICATION UNION. **Global Cybersecurity Index 2020**. International telecommunication union development sector. 2021. Disponível em: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf>. Acesso em: 11 de junho de 2024.

JOINT WORKING GROUP. **Engagement with Private Sector on Cyber Security.** [s.l: s.n.]. 2012. Disponível em: https://cii.in/WebCMS/Upload/JWG%20report.pdf. Acesso em: 11 de junho de 2024.

KASSAB, Hanna Samir. In search of cyber stability: international relations, mutually assured destruction and the age of cyber warfare. In: **Cyberspace and International Relations:** Theory, Prospects and Challenges. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 59-76, 2013. Disponível em: https://link.springer.com/book/10.1007/978-3-642-37481-4. Acesso em: 04 de abril de 2024.

KLIMBURG, Alexander; FAESEN, Louk. A balance of power in cyberspace. Broeders, D. & van der Berg, B.(1st. Ed) **Governing Cyberspace**: Behavior, Power and Diplomacy, p. 145-172, 2020.

KNOEPFEL, Sascha. Clarifying the international debate on Stuxnet: Arguments for Stuxnet as an act of war. In: **Cyberspace and International Relations:** Theory, Prospects and Challenges. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 117-124, 2013. Disponível em: https://link.springer.com/book/10.1007/978-3-642-37481-4. Acesso em: 04 de abril de 2024.

KOVACS, Anja. Cybersecurity and Data Protection Regulation in India: An Uneven Patchwork. **CyberBRICS: Cybersecurity Regulations in the BRICS Countries**, p. 133-181, 2021.

KREMER, Jan-Frederik; MÜLLER, Benedikt. SAM: a framework to understand emerging challenges to states in an interconnected world. In: **Cyberspace and International Relations:** Theory, Prospects and Challenges. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 41-58. 2013.

KSHETRI, Nir; KSHETRI, Nir. Cybersecurity in India: Regulations, governance, institutional capacity and market mechanisms. **Asian Research Policy**, v. 8, n. 1, p. 64-76, 2017. Disponível em: https://core.ac.uk/download/pdf/345085119.pdf. Acesso em: 04 de abril de 2024.

KUKKOLA, Juha. Cyber asymmetry–Towards new strategic thinking?. **GAME CHANGER Structural transformation of cyberspace**, p. 131. 2017. Disponível em: https://ilmavoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+10.pdf/5d341704-816e-47be-b36d-cb1a0ccae398/PVTUTKL+julkaisuja+10.pdf#page=146. Acesso em: 04 de abril de 2024.

KWET, Michael. Digital colonialism: US empire and the new imperialism in the Global South. **Race & Class**, v. 60, n. 4, p. 3-26, 2019. Disponível em:https://journals.sagepub.com/doi/full/10.1177/0306396818823172?casa_token=yI2VzxJQ00cAAAAA%3A7L1_i4-WGXFsv_tHkGfDKnqyype_W1Rh4xnRuByGi2NpdxxRwH5OyROAAgKUEDGxqYctWMkIu9hUQ. Acesso em: 11 de maio de 2024.

LOPES, Gills Vilar**. Relações internacionais cibernéticas (CiberRI):** uma defesa acadêmica a partir dos estudos de segurança internacional. 2016. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/54333114/gills-vilar-lopes-alacip-2017-relacoes-internacionais-ciberneticas-ciberri-libre.pdf?1504532031=&response-content-disposition=inline%3B+filename%3DRELACOES_INTERNACIONAIS_CIBERNETICAS_Cib.pdf&Expires=1718123303&Signature=Ua011dEI-GbBomi-bSF4QpSUjTNXwu2yfc9WwGZvc8CsKZSfHRVGiCoxP1hraPiyb9~FCxT7UXvzAHnzJv3wfAn86ONp4e35-Jnh1f1vCWtyGmx4Eh1I3qNBLDWtcpm7Cls6Afr1gCLRA7SXj3sTn055kBo-wx1MU9766dNIoIeK73ju3ltJTXH3S2xOn9~DxUQyn-HRO-VW6hhSFxZdBHv4QxilIliKPuBkrAcEsmqXU4nEj66njlQjwDDOCYSahoiMxc5lh-xP-K7IdGVqp0Lc6WfhhbHOEzz6GNqVbxYDKnOh1wO8548p7R-NuF7p92AoNUk3SBqWD4spwGzNDw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 04 de abril de 2024.

LOPES, Gills Vilar. Relações Internacionais cibernéticas (CiberRI): o impacto dos estudos estratégicos sobre o ciberespaço nas Relações Internacionais. In: **Congresso Latinoamericano de Ciência Política.** 2017. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/54333114/gills-vilar-lopes-alacip-2017-relacoes-internacionais-ciberneticas-ciberri-libre.pdf?1504532031=&response-content-disposition=inline%3B+filename%3DRELACOES_INTERNACIONAIS_CIBERNETICAS_Cib.pdf&Expires=1718123328&Signature=WbgzhHT2JfNVRUG~zpOybPM1fkHTZeyqGeRpVv3IKS99RpxkAGa0PKhGbbQuHEXI5UKqGecBA3Px3~ytv6B579Cs3-7FEGCecc14D8kKELkUB0VH9X4HM1VpHkXEYm7JM53IPisDKE9RgheRlNYJgRNBDHeR8tj2fr~ihPqEwiNN1lBLffR290jwIzMZA2N6JJ01WzxC2jFIpRjsvEIu4jdKOXKPWHRerRJZlzgoVtufq~CVKR8wMFZQ8WpbqMIh886QXkluQ3tD7XZpHW~U8TuxgRnMlMUrGgOCAQYAZD2IGVcmjTlmAXFOOS~-fho07ZWLhO~9IVMvZVVinjxDcg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 04 de abril de 2024.

MAHAPATRA, Padmalaya. INDO-US COUNTER-TERRORISM COOPERATION. **The Indian Journal of Political Science**, p. 119-128, 2014. Disponível em: https://www.jstor.org/stable/24701088. Acesso em: 11 de maio de 2024

MANDARINO JR, Raphael. Segurança e defesa do espaço cibernético brasileiro. **Cubzac**, 2010.

MIT, MIT Technology Review Insights. **The Cyber Defense Index,** 2022. Disponível em: <https://mittrinsights.s3.amazonaws.com/CDIreport.pdf>. Acesso em: 15 de maio de 2024.

MORGENTHAU, Hans Joachim. A política entre as nações: a luta pelo poder e pela paz. **Editora Universidade de Brasília,** 2003.

NYE JR, Joseph S. The future of power. **PublicAffairs**, 2011.

OPPERMANN, Daniel. Dimensions of Cybersecurity in Brazil. **CyberBRICS: Cybersecurity Regulations in the BRICS Countries**, p. 35-65, 2021. Disponível em: https://link.springer.com/chapter/10.1007/978-3-030-56405-6_2. Acesso em: 11 de maio de 2024;=.

PARMAR, Sushma Devi. Cybersecurity in India: An evolving concern for national security. **The Journal of Intelligence and Cyber Security**, v. 1, n. 1, 2018. Disponível em: https://www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf. Acesso em 11 de maio de 2024.

Perissinotto, R. Comparação histórica e Process Tracing. In: Perissinotto, R. et al. **Política Comparada:** Teoria e Método. Rio de Janeiro: Editora UERJ, 2022, p. 141-172.

RADU, Roxana. Power technology and powerful technologies: global governmentality and security in the cyberspace. In: **Cyberspace and International Relations:** Theory, Prospects and Challenges. Berlin, Heidelberg: Springer Berlin Heidelberg,p. 3-20. 2013.

READ, Oliver. How the 2010 attack on Google changed the US government's threat perception of economic cyber espionage. In**: Cyberspace and International Relations:** Theory, Prospects and Challenges. Berlin, Heidelberg: Springer Berlin Heidelberg,. p. 203-230. 2013.

RUSCIANO, Frank Louis. The three faces of cyberimperialism.In: **Cyberimperialism? Global relations in the new electronic frontier**, p. 9-26, 2001.

SANTOS, Boaventura de Sousa. **Para além do pensamento abissal:** das linhas globais a uma ecologia de saberes. Novos estudos CEBRAP [online]. 2007, n. 79, pp. 71-94.

SEGUNDO, Célio Borges Taquary**. A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos.** 2019. Disponível em: https://repositorio.esg.br/handle/123456789/1205. Acesso em: 04 de abril de 2024.

SENA, Danielly Alcina Freitas de. **Ciberdefesa**: estrutura de defesa cibernética brasileira. 2016. Disponível em: http://repositorio.asces.edu.br/handle/123456789/490. Acesso em: 10 de maio de 2024.

US STATE DEPARTMENT. Joint U.S.- **India Statement on Counter-terrorism Working Group**. 2000. Disponível em: https://www.indianembassyusa.gov.in/ArchivesDetails?id=363 . Acesso em: 5 de maio 2024.

THOMAS, Douglas; LOADER, Brian D. Introduction. In: **Cybercrime:** Law enforcement, security and surveillance in the information age.THOMAS, Douglas; LOADER, Brian D. Routledge.2000. p. 1-14.

AGRADECIMENTOS

Ao Grande Arquiteto do Universo, que me permitiu traçar os caminhos que ele planejou para mim com sua grande bondade, permitindo que os bons frutos fossem colhidos nesse momento.

À todas as minhas mães; Jaucilene, Francilene, Antonieta e Luzia Maria, que antes que eu soubesse caminhar com meus próprios pés, caminharam por mim. Em especial, à minha mãe, a minha melhor amiga que desde do ventre luta para que meus sonhos sejam realizados, a sua luta é a inspiração que me guia. Os nossos sonhos são infinitos e olhar para você faz com que eu sinta que tudo é possível, se eu estiver ao seu lado.

Ao meu pai, Francisco das Chagas, que em meio a pedras me presenteia com o seu amor e carinho incodicional. Os conhecimentos que adquiri em todo esse caminho se multiplicam e renovam seu significado quando volto para a nossa casa.

Ao meu irmão, Samuel Ravi, que mesmo tão pequeno me ensina novas formas de viver. Ravi, o meu sol, ressignifica a minha existência, me dando um propósito e um amor que nunca imaginei sentir.

Às Filhas de Jó Internacional, minha segunda família que compartilha comigo as provações e meus propósitos. Em especial, às minhas irmãs Raissa Ohana, Danieli Medeiros e Anna Beatriz, que são a prova da recompensa merecida em minha vida.

A Rafael Araújo, sei que éramos irmãos em outras vidas. Sem a sua amizade essa vida seria impossível.

À Rayanne Macedo, minha alma gêmea e melhor amiga, agradeço por ter me mostrado novas possibilidades e me provado por A+B que eu sou capaz de tudo.

À Raissa Ohana Fernandes, eu sou porque nós somos, em todos os momentos difíceis e felizes, sempre será eu e você.

A Giordano Arnóbio, a minha pessoa, é com você que quero viver esse espaço-tempo. Percebo que a vida é bem mais do que eu imaginei, agora que sonho com você. “Seremos os donos do nosso amanhã”.

Ao meu orientador, Fábio Nobre, que me acompanhou do início ao fim da minha graduação, comprando minhas ideias e me fornecendo todo o suporte possível.

À todos os professores e professoras que estiveram em minha trajetória acadêmica, em especial, aos professores da Universidade Estadual da Paraíba que abriram as portas para um universo de conhecimento que me acolhe e me renova. Agradeço, com um carinho especial, à Anna Beatriz Henriques, André Pini, Neto Galdino e Vanessa Lira, esse momento não seria possível sem o apoio e esperança que vocês depositaram em mim.

Aos meus amigos de graduação, com quem tanto contei e me inspirei para seguir essa caminhada turbulenta. Edson Edrey, Milena Mello, Paloma Reina, Noemi Santos, eu nunca serei possível de retribuir tudo que vocês fizeram por mim

“Mas enquanto houver amor;
Eu mudarei o curso da vida;
Farei um altar para comunhão;
Nele eu serei um com o mundo;
Até ver o ubuntu da emancipação;
Porque eu descobri o segredo que me faz humano.” - Pastor Henrique Vieira