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

MARIA VITÓRIA PAIVA DOS SANTOS

DESAFIOS PARA A CONSTRUÇÃO DE CAPACIDADE CIBERNÉTICA NO BRASIL

Porto Alegre
2024

MARIA VITÓRIA PAIVA DOS SANTOS

DESAFIOS PARA A CONSTRUÇÃO DE CAPACIDADE CIBERNÉTICA NO BRASIL

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

Orientador: Prof. Dr. José Miguel Quedi Martins

Porto Alegre

2024

CIP - Catalogação na Publicação

dos Santos, Maria Vitória Paiva
Desafios para a construção de capacidade cibernética no Brasil / Maria Vitória Paiva dos Santos. -- 2024.
96 f.
Orientador: José Miguel Quedi Martins.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Curso de Relações Internacionais, Porto Alegre, BR-RS, 2024.

1. Capacidade cibernética. 2. Segurança cibernética. 3. Relações Internacionais. 4. Brasil. I. Martins, José Miguel Quedi, orient. II. Título.

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

MARIA VITÓRIA PAIVA DOS SANTOS

DESAFIOS PARA A CONSTRUÇÃO DE CAPACIDADE CIBERNÉTICA NO BRASIL

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

Aprovada em: Porto Alegre, _____de _____de 2024.

BANCA EXAMINADORA:

Prof. Dr. José Miguel Quedi Martins – Orientador

UFRGS

Profa. Dra. Analucia Danilevicz Pereira

UFRGS

Prof. Me. João Gabriel Burmann da Costa

UNIRITTER

AGRADECIMENTOS

Àqueles que moldaram minha jornada acadêmica e tornaram possível a realização deste sonho, expresso profunda gratidão a cada um que contribuiu de maneira significativa para o meu percurso.

Primeiramente, quero dedicar palavras de agradecimento aos meus paisSem a oportunidade que me concederam, eu não estaria hoje celebrando esta conquista.

À Oficina de Estudos Estratégicos, por proporcionar um espaço de troca de conhecimento que desempenhou um papel para minha formação e para o desenvolvimento desse trabalho.

Ao meu orientador, o professor José Miguel Quedi, pela paciência, boa vontade para orientar e, é claro, as paçoquinhas. Agradeço por cada conselho, correção e por acreditar no meu potencial.

Aos amigos que foram faróis nesta jornada, meu agradecimento especial. A Juliana, pelo apoio constante durante a escrita do TCC; ao João Pedro, cujo suporte no projeto foi fundamental, e à Maria Antônia, pela serenidade e apoio tranquilo que sempre ofereceu. Suas presenças fizeram toda a diferença.

RESUMO

Este trabalho tem como tema os desafios para a construção de capacidade cibernética no Brasil. Percebe-se a importância do ciberespaço para o exercício de poder e influência internacional, o que exige capacidades cibernéticas estatais que garantam essa possibilidade para o Estado. O Brasil ainda enfrenta desafios para fortalecer suas capacidades cibernéticas, sendo crucial identificá-los. Assim, a pergunta que orienta a pesquisa é a seguinte: quais são os principais desafios para a construção de capacidade cibernética brasileira? Como hipótese de trabalho, tem-se que os principais obstáculos dizem respeito à dificuldade de mobilizar recursos para concretizar o processo por meio de um arcabouço estratégico capaz de conciliar os principais atores do processo. O objetivo geral da pesquisa, assim, é identificar o estado atual das capacidades cibernéticas do Brasil, identificando lacunas existentes e possíveis meios de geração de capacidade. Em termos específicos, busca-se compreender como as lentes de Relações Internacionais, especificamente do Realismo Neoclássico, podem auxiliar a compreensão do objeto de estudo. Em seguida, pretende-se apresentar o conceito de capacidade cibernética, situando a segurança cibernética no contexto das relações internacionais como pré-requisito para desenvolvimento estatal, segurança e projeção de influência. Por fim, objetiva-se analisar a capacidade cibernética brasileira atual e identificar avanços e obstáculos enfrentados pelo país a partir de dados, documentos oficiais e índices internacionais de maturidade de capacidade cibernética. Para atingir seus resultados, a pesquisa adota o Realismo Neoclássico, analisando a capacidade estatal por meio de índices internacionais, literatura temática e pesquisa em fontes primárias. Como resultado da pesquisa, tem-se que, além da dificuldade em mobilizar recursos, a dependência externa causada pela baixa capacidade de produção da base material da capacidade cibernética.

Palavras-chave: Segurança cibernética; Capacidade cibernética; Brasil.

ABSTRACT

This study addresses the obstacles associated with developing cyber capabilities in Brazil. The significance of cyberspace for the exercise of international power and influence is evident, requiring the presence of state cyber capabilities to secure this potential for the nation. Brazil continues to encounter difficulties in enhancing its cyber capacities, underscoring the necessity to recognize and address these challenges. Thus, the research question guiding this study is as follows: What are the main challenges for cyber capacity building in Brazil? The working hypothesis is that the primary obstacles relate to the difficulty of mobilizing resources to materialize the process through a strategic framework capable of reconciling the key actors involved. The general objective of the research is to identify the current state of Brazil's cyber capabilities, pinpointing existing gaps and possible means of capacity generation. The first specific objective is to understand how International Relations theory, specifically Neoclassical Realism, can assist in comprehending the object of research. Subsequently, the second specific objective is to present the concept of cyber capacity, situating cyber security in the context of international relations as a prerequisite for state development, security, and projection of influence. Finally, the third specific objective is to analyze Brazil's current cyber capacity and identify advances and obstacles faced by the country based on data, official documents, and international reports of cyber security capacity maturity. As a result of the research, it is found that, in addition to the difficulty in mobilizing resources, external dependence is caused by the low capacity to produce the material base of cyber capacity.

Keywords: Cybersecurity; Cyber Capacity; Brazil.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABINEE	Associação Brasileira da Indústria Elétrica e Eletrônica
ABISEMI	Associação Brasileira da Indústria de Semicondutores
CDCiber	Centro de Defesa Cibernética
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI	Comitê Gestor da Internet
CISA	Agência de Cibersegurança e Segurança de Infraestruturas dos Estados Unidos
CMM	Cyber Security Capability Maturity Model
COMDCiber	Comando de Defesa Cibernética
CSIRT	Grupos de Segurança e Resposta a Incidentes
CSIS	Centro de Estudos Estratégicos e Internacionais
EGA	E-Governance Academy
END	Estratégia Nacional de Defesa
ENISA	Agência da União Europeia para a Cibersegurança
ENSIC	Estratégia Nacional de Segurança de Infraestruturas Críticas
GCSCC	Global Cyber Security Capacity Centre
GSI	Gabinete de Segurança Institucional da Presidência da República
IPEA	Instituto de Pesquisa Econômica Aplicada
LME	Laboratório de Microeletrônica
NCPI	National Cyber Power Index
NCSI	National Cyber Security Index
NIC.br	Núcleo de Coordenação do ponto BR
OEA	Organização dos Estados Americanos
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte

PADIS	Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores
PJERJ	Poder Judiciário do Estado do Rio de Janeiro
PNCiber	Política Nacional de Cibersegurança
PND	Política Nacional de Defes
PNSI	Política Nacional de Segurança da Informação
PNSIC	Plano Nacional de Segurança de Infraestruturas Críticas
PNUD	Programa das Nações Unidas para o Desenvolvimento
SIAFI	Sistema Integrado de Administração Financeira do Governo Federal
TCU	Tribunal de Contas da União
UIT	União Internacional de Telecomunicações
USP	Universidade de São Paulo
WEF	World Economic Forum

SUMÁRIO

1 INTRODUÇÃO

Este trabalho trata da construção de capacidade cibernética no Brasil, utilizando como abordagem teórica o Realismo Neoclássico. Com a difusão mundial das redes de computadores e o avanço da tecnologia computacional a partir do século XX, o ciberespaço tornou-se um campo fundamental para a projeção de poder no âmbito internacional. Instrumentos e infraestruturas essenciais para a sociedade e para o exercício das funções estatais têm sido transportados para o espaço cibernético e estão cada vez mais interconectados na rede, o que cria vulnerabilidades que podem ser exploradas por adversários para obter superioridade em eventuais conflitos interestatais. Assim, torna-se cada vez mais relevante a possibilidade de os Estados conduzirem operações cibernéticas, além de exercer poder e influência nos meios digitais, tanto em termos de *hard power* quanto de *soft power* e, consequentemente, de *smart power*, conceitos que serão expostos mais adiante.

Essas novas formas de exercício do poder, aliadas à crescente dependência de sistemas computacionais e à interconectividade global das redes, criam a necessidade de desenvolver capacidades cibernéticas estatais para conferir suporte ao desenvolvimento, defender as estruturas críticas conectadas à rede e, eventualmente, explorar vulnerabilidades de outros Estados. Tais dinâmicas fazem com que os Estados procurem cercar-se de toda sorte de recursos cibernéticos para implementar telecomunicações, serviços bancários e outras infraestruturas críticas de relevância social.

Contudo, essas infraestruturas, quando instaladas no ciberespaço, criam vulnerabilidades que exigem dos Estados o desenvolvimento de dispositivos ofensivos e defensivos, a fim de proteger esses recursos e, eventualmente, explorar os de adversários (Muller, 2015). A construção de recursos cibernéticos é, nesse sentido, crucial para a manutenção da segurança nacional, tanto na esfera virtual do espaço cibernético quanto em sua esfera física, visto que as duas são interligadas (Calderaro; Craig, 2020). Essa urgência se confirma por meio de dados: segundo o Fórum Econômico Mundial, ataques cibernéticos estão entre os 10 riscos de maior severidade percebidos para os próximos dez anos (WEF, 2023). A partir disso, compreende-se que

existe a necessidade de os Estados mobilizarem recursos internos para reforçar seu leque de possibilidades de atuação frente a ameaças externas advindas desse novo domínio.

A crescente importância da segurança cibernética no cenário global tem levado muitos países, incluindo o Brasil, a repensar suas abordagens e estratégias para lidar com as ameaças cibernéticas em constante evolução, o que envolve os mais variados domínios e mecanismos. O Brasil, apesar de inserido no debate internacional de segurança cibernética, ainda enfrenta desafios para a concretização de suas capacidades cibernéticas. O país reconhece a importância dos instrumentos digitais para o desenvolvimento econômico e projeção de poder e influência internacionais e é alvo constante de ameaças cibernéticas: ao longo das duas últimas décadas vem enfrentando uma série de desafios relacionados à segurança cibernética, com destaque para o cibercrime com motivações econômicas, tanto a nível doméstico quanto a nível externo (Lobato, 2017).

Esse cenário é suficiente para desencadear discussões e políticas, por parte do Estado, de reforço do aparato de segurança cibernética brasileiro, tendo o progresso se dado de forma auspiciosa. Entretanto, a resposta prática a esses desafios ainda encontra obstáculos. A resposta do governo tem sido implementada gradualmente, dando-se, principalmente, na forma de documentos estratégicos pertinentes ao tema e do reconhecimento da importância de investir no setor nos mecanismos político-estratégicos de defesa; entretanto, as ações de segurança cibernética ainda são pouco difundidas (Hurel, 2021).

Criaram-se, nos últimos anos, múltiplos mecanismos normativos e estratégicos para enfrentar as questões emergentes de segurança digital. Dentre essas questões, situa-se a segurança cibernética, mas também a defesa de infraestruturas críticas, a proteção de dados pessoais, entre outros elementos fundamentais para a administração e defesa eficiente do espaço virtual e das transformações digitais observadas no século XXI.

Apesar disso, os instrumentos legais brasileiros têm sido questionados por serem de difícil operacionalização: na prática, o Estado não teria uma estratégia material, apenas meramente formal. Apesar de haver certos órgãos responsáveis por

determinados instrumentos estratégicos relativos ao ciberespaço, a ausência de uma agência específica responsável pela implementação da estratégia e política de segurança cibernética levanta questões sobre a eficácia da resposta do Brasil às ameaças crescentes. Dessa maneira, cabe examinar o panorama de segurança cibernética atual para, posteriormente, pensar em como suprir essas lacunas para incrementar as capacidades cibernéticas brasileiras.

Em caráter preliminar, cumpre percorrer os conceitos de *hard power, soft power e smart power. O hard power*, conforme Nye (2012), envolve uma abordagem de influência e coerção que se baseia em recursos tangíveis e medidas diretas, muitas vezes envolvendo o uso da força militar, econômica ou outras formas de pressão explícitas. Diferentemente do *soft power*, que se concentra na persuasão e atração cultural, o *hard power* busca impor a vontade de um país por meio de meios mais concretos e, em alguns casos, confrontacionais. Os elementos típicos do *hard power* incluem, a título de exemplo, força militar e capacidade econômica e outras formas de poder que o emprego ou ameaça de medidas coercitivas (Nye, 1990). É no âmbito do *hard power* que se encontram mais dúvidas a respeito dos limites do ciberespaço. Nye (2010) argumenta que o *hard power* no ciberespaço pode ser exercido por meio de ataques de negação de serviço e da inserção de código malicioso para prejudicar sistemas, por exemplo, mas também são instâncias de *hard power* no ciberespaço a destruição da infraestrutura cibernética física e o controle governamental de recursos cibernéticos, empresas e indivíduos.

Outro elemento do *hard power* cibernético é a posse da base material da capacidade cibernética, principalmente os chips e a fibra óptica, o que corresponde a poder econômico, uma das fontes do poder duro, dada sua centralidade para o desenvolvimento holístico de capacidades cibernéticas (Peters, 2022). Tais recursos dizem respeito às capacidades de o país centralizar a produção material de elementos essenciais ao desenvolvimento da cibernética, de modo que não pode haver segurança, capacidade ou poder cibernético sem eles. A segurança das redes e recursos cibernéticos do Estado depende da habilidade de controlá-los, sem depender de outros Estados para prover a própria conexão à rede do país.

O *soft power*, por outro lado, engloba a capacidade de um país moldar as preferências e ações de outros por meio de sua atração cultural, ideológica e política, de forma persuasiva. Em vez de exercer autoridade por meio da coação, o *soft power* opera por meio da persuasão, promovendo a adesão voluntária a princípios e padrões estabelecidos pelo Estado propagador. As fontes de poder *soft power* são variadas, incluindo a cultura e valores do Estado dominante, recursos econômicos e mesmo recursos militares, por meio da atração gerada pela força ou aparência de força de determinado Estado; o mesmo pode ser dito dos recursos econômicos (Nye, 2011). O autor também ressalta que os recursos de difusão desse tipo de poder também são diversos, incluindo diplomacia, programas de treinamento e assistência, programas de intercâmbio, entre outras medidas. O ciberespaço, nesse sentido, proporciona mais um meio de propagação de *soft power*, facilitando a distribuição do poder sobre informação. A difusão da informação obscurece as fronteiras estatais e novos agentes encontram-se aptos a atuar na política internacional.

O conceito de *smart power,* por fim, diz respeito à "integralidade de poder que abrange as vertentes de poder militar e econômico de um Estado, e vai procurar desenvolver outras áreas, com o intuito de complementar as duas primeiras vertentes" (Pinto, 2011, p. 5). A autora classifica o surgimento do *smart power* como uma forma de integrar neorrealismo e liberalismo institucional, este fazendo concessões àquele no que tange ao reconhecimento da anarquia internacional e do Estado como ator de destaque na política internacional. Conforme Nye (2012), o poder inteligente está relacionado à combinação de recursos em estratégias bem-sucedidas para atingir os objetivos pretendidos. Para isso, deve-se levar em consideração, além dos meios disponíveis, as preferências dos alvos que se quer influenciar, a probabilidade de sucesso e quais comportamentos empregar para tal, aliando poder duro e brando.

No contexto da ascensão do ciberespaço, em que a abordagem de segurança deve perpassar as mais diversas esferas do Estado – setores financeiro e bancário, militar, energético, de telecomunicações, entre outros elementos dependentes da mediação das redes – a integração de recursos se torna primordial para desenvolver capacidades cibernéticas resilientes que apoiem o desenvolvimento estatal. O

ciberespaço configura-se, dessa forma, como um campo fundamental para a projeção de poder e influência no âmbito internacional.

Nesse sentido, evidencia-se o conceito de Transformação Digital, compreendido como a revolução produtiva, econômica e social que emerge a partir do aprofundamento dos processos de digitização e digitalização, possibilitado pelo avanço das Tecnologias de Informação de Comunicação. Esse fenômeno culmina na Terceira e na Quarta Revolução Industrial – essa prenunciada pelo advento do chip quântico e pela crescente importância da comunicação sem fio e, por conseguinte, dos satélites (Cravo, 2023; Martins, 2023). A Quarta Revolução Industrial é um termo cunhado por Klaus Schwab, que a caracteriza como uma integração mais estreita e interconectada entre o mundo físico e a tecnologia (Schwab, 2016). A segurança cibernética, dessa forma, emerge como pré-requisito para a operação no espaço cibernético, um domínio que transcende fronteiras, desafiando as noções tradicionais de segurança dentro dos Estados e nas relações internacionais. Ao lidar com ameaças virtuais, os limites geográficos tornam-se menos definidos, ampliando a complexidade das questões de segurança. Entretanto,

Considerando o caráter dessa transformação, a construção de capacidade cibernética exige uma abordagem colaborativa, ágil e inovadora entre as esferas do Estado para possibilitar um aparato estatal que se traduza em capacidade. Quanto a isso, cumpre abordar dois conceitos. O primeiro é o de Centro de Decisão Econômica, definido por Celso Furtado como a capacidade de um país concentrar as decisões em sua vida econômica no próprio território, possuindo, inclusive, tecnologias essenciais dos diferentes ciclos econômicos que possibilitem o controle interno da produção e do mercado (Furtado, 1962).

Ainda tratando da construção de capacidade cibernética integrada, o segundo conceito que interessa abordar é o de esfera pública não-estatal, definida por Bresser-Pereira e Nuria Grau como um espaço intermediário entre a propriedade estatal e privada, sendo caracterizado pela presença de organizações de controle que atuam conforme o interesse público, de forma multidimensional. Essa esfera exige atuação conjunta da sociedade e do Estado, cada um com parte da responsabilidade (Bresser-Pereira; Grau, 1999). Essa noção se adequa à construção de capacidades cibernéticas

pela necessidade de mobilização integrada de recursos públicos e privados para a construção de capacidade estatal. A esfera pública não-estatal pode se concretizar na forma do Instituto do Consórcio (Salles, 2019). Esse, exposto adiante, constitui-se como a associação entre dois ou mais entes para atingir objetivo comum.

Aqui cumpre destacar três níveis que importam para analisar o comportamento estatal considerando elementos externos e internos: a tomada de decisão dos estadistas, a capacidade estatal e a competição internacional. Aqui se trata, então, do segundo nível por meio do Realismo Neoclássico para abordar a problemática do trabalho.

Apesar da consideração de elementos do neoinstitucionalismo e do Realismo Estrutural fornecer instrumentos valiosos para a compreensão das dinâmicas do ciberespaço, o Realismo Neoclássico se mostra mais adequado por duas razões. A escolha da teoria se justifica, principalmente, pela consideração da influência do âmbito interno na projeção do poder estatal, fator que se busca trabalhar no presente trabalho e que inexiste em outras vertentes do realismo. Essa característica amplia a capacidade explicativa do neorrealismo, por exemplo, ao enfatizar a análise de política externa dos Estados, desconsiderando a ideia de homogeneidade dos Estados no sistema internacional em favor da análise de elementos domésticos como normas, cultura estratégica e objetivos nacionais; o ambiente interno é visto, dessa forma, como um dos fatores que molda o comportamento do Estado (Snyder, 1977; Schweller, 1993; Zakaria, 1999). Argumenta-se que os elementos internos são cruciais, pois influenciam as políticas adotadas pelos Estados, muitas vezes divergindo dos incentivos estruturais previstos pelo neorrealismo. Ademais, essa corrente aborda a incerteza relacionada às intenções e capacidades dos estados, baseando-se no comportamento observado na política externa.

Como as outras vertentes do realismo, parte-se do pressuposto de que a incerteza é gerada pelo caráter anárquico do sistema internacional, permitindo a identificação das condições essenciais que influenciam as políticas externas e as preferências estratégicas dos estados na região, sobretudo as que impactam o desenvolvimento de capacidades – ou seja, a teoria deixa mais claro o modo como são produzidas as capacidades. O Realismo Neoclássico, dessa forma, é relevante para

compreender como tem se dado a construção de capacidades de segurança cibernética no sistema internacional sem ignorar a diversidade de mecanismos domésticos, desde instrumentos técnicos e materiais até os normativo-institucionais e estratégicos, necessários para o desenvolvimento desses recursos de forma que os Estados consigam manifestar poder por meio do espaço cibernético.

O segundo motivo pelo qual se optou pelo Realismo Neoclássico é que ele se destaca ao abordar desvios na política externa de estados que não seguem os incentivos estruturais previstos pelo neorrealismo. O Realismo Neoclássico propõe quatro motivos pelos quais os Estados falham em tomar responder adequada e racionalmente em determinadas situações: primeiro, os líderes estatais nem sempre compreendem a situação internacional corretamente; em segundo lugar, o sistema internacional nem sempre se faz claro a respeito das ameaças existentes; terceiro, os líderes nem sempre respondem de forma racional aos eventos do sistema; por fim, os Estados nem sempre têm a possibilidade de mobilizar seus recursos efetiva e eficientemente (Lobell; Ripsman; Taliaferro, 2016). No contexto do espaço cibernético, Considerando essas premissas, busca-se enquadrar os desafios brasileiros em construir capacidades cibernética em um deles – a inabilidade de o Estado mobilizar recursos para tal. Portanto, pretende-se empreender estudo exploratório relacionado ao tema para cumprir com o escopo do trabalho.

O Realismo Neoclássico, assim como outras correntes realistas, também considera que a estrutura ajuda a moldar o comportamento dos Estados, mas não é o único fator de importância para determinar sua atuação no sistema internacional. Também compartilha a visão de poder relativo, da existência da anarquia e da predominância do Estado como ator principal nas relações internacionais, embora não considere esses elementos suficientes para explicar as relações interestatais (Foulon, 2015).

A teoria utiliza elementos de nível estatal num esforço de análise de política externa, não tendo como premissa a existência de unidades não diferenciadas presente em outras correntes realistas. Com isso, também buscam explicar desvios no comportamento dos Estados em relação ao previsto na teoria neorrealista (Taliaferro, 2006). Nesse sentido, os elementos domésticos levariam os Estados à adoção de

políticas inadequadas a incentivos sistêmicos, aumentando as incertezas em âmbito regional; Domingo (2018) defende a capacidade da teoria para explicar o conflito e o desenvolvimento de capacidades cibernéticas justamente por enfatizar a segurança nacional como questão central para o comportamento estatal e formulação de políticas públicas, unindo argumentos estruturais e domésticos. Considerando que, mesmo para conter ameaças externas, é necessário desenvolver recursos que perpassam e integram todas as esferas que compõem o Estado, conciliando contradições criadas entre eles pela natureza do ciberespaço, faz-se necessário analisar todo o cenário da infraestrutura cibernética do país para investigar sua resiliência a ciberataques como um todo. Isso se dá porque, independentemente do local de origem do ataque, criminosos ou agentes externos podem utilizar brechas em qualquer tipo de sistema para infectar vários outros, atingindo a sociedade inteira e, portanto, ameaçando a segurança nacional.

No contexto da segurança cibernética, pode-se argumentar que há, de fato, um incentivo sistêmico ao desenvolvimento de capacidades cibernéticas, uma vez que essas ocupam espaço cada vez maior na produção, na guerra e na vida social como um todo. Nesse contexto, a construção de capacidade estatal como um todo nas próximas décadas dependerá, em grande medida, da capacidade cibernética do Estado. Essa capacidade, se desenvolvida, permitirá que o Estado participe ativamente das próximas Revoluções Industriais, e não em posição de dependência. Além disso, o uso da cibernética permite o desenvolvimento de novos tipos de arma e o aprimoramento das existentes, além de modificar a própria forma de fazer guerra. Nesse sentido, grande parte do debate sobre essas capacidades diz respeito a como elas podem auxiliar os Estados a alcançarem seus objetivos.

Esse debate importa em razão de o espaço cibernético ser um domínio novo em que os fenômenos sociais e internacionais e produtivos não assumem a mesma forma que possuem fora dele. Exemplo disso são as operações militares: as operações cibernéticas, mais que ferramentas destrutivas, seriam meios de sinalizar preferências dos Estados sem danificar as relações diplomáticas de forma irreparável – uma vez que são dotadas de negabilidade, dada a dificuldade de rastrear a origem e os agentes de

um ataque cibernético, por exemplo. Assim, são ferramentas que amplificam o poder de atores com capacidades sólidas o suficiente (Libicki, 2009; Lindsay; Gartzke, 2018).

Em face disso, Kello (2017) defende que o desenvolvimento de capacidades cibernéticas militares são poderosos instrumentos estratégicos, pois têm capacidade de impactar as infraestruturas inimigas de forma mais ampla e menos detectável, instigando a ampliação de ameaças à segurança nacional além dos meios convencionais. Entretanto, a construção dessas capacidades vai além de seu uso bélico; desenvolver esses recursos permite que os Estados utilizem o domínio cibernético para atingir objetivos de desenvolvimento que forneçam suporte à segurança nacional – isso envolve, além de capacidades ofensivas e defensivas, a segurança de redes nacionais públicas e privadas, a proteção de infraestruturas críticas e a própria base material do ciberespaço.

Para o Brasil, o Instituto Igarapé[1] (2021) identifica cinco principais desafios a superar, sendo eles a falta de capacitação de profissionais da área, a desinformação, crimes cibernéticos, acesso indevido a sistemas e ameaças à infraestrutura crítica do país. Apesar dos esforços de desenvolvimento de recursos cibernéticos, a infraestrutura cibernética do Brasil ainda não é coesa de forma a minimizar ataques à sociedade como um todo. Isso pode ser visto, por exemplo, por meio do número de ataques cibernéticos – consumados ou tentados – em 2023, que foi de 23 bilhões no país (Fortinet, 2023).

Nesse contexto, não se pode deixar de observar a publicação do Decreto 11.856/2023, que instituiu a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança, em dezembro de 2023, quando o presente trabalho já se encontrava em vias de encaminhar-se à banca – impossibilitando análise profunda do instrumento. Ressalta-se, entretanto, o caráter integrador da política e seu foco na construção de capacidades cibernéticas, simultaneamente buscando a cooperação entre os setores público e privado para promover a segurança cibernética e resguardar os direitos fundamentais, o que confirma a necessidade de desenvolvimento conjunto desses recursos.

[1] O Instituto Igarapé é um think tank que atua com temas emergentes de segurança, com ênfase nas 10áreas de segurança pública, digital e climática. Sua atuação abrange parcerias e projetos em mais de 20 países, refletindo seu compromisso em fornecer soluções em escala para os desafios globais

Considerando a problemática exposta, a pergunta que orientou a pesquisa foi a seguinte: quais são os principais desafios para a construção de capacidade cibernética brasileira? Como hipótese, formula-se que os principais obstáculos dizem respeito à dificuldade de mobilizar recursos para concretizar o processo. Isso ocorreria devido à dificuldade de conciliar os principais atores (setores público e privado, além da sociedade civil) e suas respectivas responsabilidades e recursos em um arcabouço normativo passível de ser posto em prática. Essas dificuldades prejudicam que o país responda às pressões sistêmicas. Nesse sentido, ainda não foi elaborada uma política nacional de segurança cibernética coesa para orientar esse processo e seus atores de forma concreta e compatível com o estado insuficiente da segurança cibernética no Brasil. Dessa forma, os princípios estabelecidos nos instrumentos normativos já existentes, bem como os objetivos neles dispostos, seriam meramente formais, necessitando de alterações que os tornem mais específicos e pragmáticos, orientando-os em direção a metas do país no espaço cibernético.

A partir disso, o objetivo geral da pesquisa é identificar o estado atual das capacidades cibernéticas do Brasil, identificando lacunas existentes e possíveis meios de geração de capacidade, orientando-se pelo Realismo Neoclássico. Os objetivos específicos são três: inicialmente, compreender como as lentes de Relações Internacionais, especificamente do Realismo Neoclássico, podem auxiliar a compreensão do objeto de estudo; em seguida, apresentar o conceito de capacidade cibernética, situando a segurança cibernética no contexto das relações internacionais como pré-requisito para desenvolvimento estatal, segurança e projeção de influência; por fim, analisar a capacidade cibernética brasileira atual e identificar avanços e obstáculos enfrentados pelo país a partir de dados, documentos oficiais e índices internacionais de maturidade de capacidade cibernética, sem negligenciar o contexto brasileiro que os índices, como ferramentas gerais e exportadas, deixam de abordar.

A presente pesquisa se justifica academicamente pela necessidade de compreender como o Brasil pode incrementar suas capacidades no ciberespaço de forma a intensificar sua influência nesse domínio em expansão. O próprio conceito de capacidade cibernética não é consenso, o que torna cruciais mais pesquisas a respeito de como se dá a influência internacional considerando as dinâmicas únicas do espaço

cibernético. Nesse sentido, empreende-se um estudo exploratório a fim de identificar novos desenvolvimentos sobre o tema em questão, além de acrescentar à discussão. Além disso, justifica-se o trabalho socialmente pela importância crescente do ciberespaço na sociedade contemporânea, o que intensifica a necessidade da segurança cibernética. A construção de capacidade cibernética, portanto, é fundamental para que a sociedade se veja segura no espaço cibernético, que ocupa um papel cada vez maior na vida dos indivíduos. Diante desses tópicos, essa pesquisa pode facilitar a compreensão do ciberespaço como ferramenta de projeção para o Brasil, bem como das dinâmicas específicas desse domínio.

Adotando a tipologia de literatura proposta por Van Evera, o presente trabalho comportou avaliação de política pública (Van Evera, 2002, p. 106). A metodologia utilizada consistiu em pesquisa bibliográfica em fontes primárias e secundárias para atingir os objetivos propostos. Buscou-se cumprir o primeiro objetivo específico ainda no primeiro capítulo, de natureza teórica, por meio de revisão de literatura teórica focada no Realismo Neoclássico. O segundo objetivo específico foi atingido no segundo capítulo, por meio de revisão bibliográfica temática a respeito do tema do trabalho. A literatura temática selecionada foi aquela produzida por pesquisadores com ampla participação em pesquisas na área, de preferência no âmbito de programas de pesquisa e universidades, e será composta por artigos científicos, teses de doutorado e dissertações de mestrado, entre outros trabalhos científicos. O terceiro objetivo específico, por fim, foi satisfeito no capítulo final, por meio de análise de dados presentes em índices internacionais de capacidade cibernética e de documentos oficiais do Governo Federal, além de revisão de literatura sobre mensuração de capacidade cibernética, em especial a brasileira. Os índices escolhidos foram selecionados por serem provenientes de esforço metodológico cuidadoso, além de serem usados por organizações internacionais e Estados como forma de avaliar lacunas existentes na capacidade de segurança cibernética desses atores. Os modelos utilizados foram três: o Modelo de Maturidade de Capacidade de Cibersegurança de Oxford; O *National Cyber Power Index*, de Harvard; e o *National Cyber Security Index*, da e-Governance Academy. Os documentos oficiais abordados foram, principalmente, políticas e estratégias relativas à segurança cibernética e temas correlatos. Dois exemplos

fundamentais são a Estratégia Nacional de Segurança Cibernética (E-Ciber), a Política Nacional de Segurança da Informação. Os documentos foram utilizados como forma de reconhecer os esforços já existentes para construção de capacidade cibernética. A literatura temática pertinente foi escolhida de acordo com os mesmos critérios apresentados para o objetivo anterior.

Com base nesses objetivos, a pesquisa foi estruturada em três capítulos: o primeiro aborda a teoria escolhida, buscando operacionalizá-la de forma que se compreenda como pode ser adequada ao estudo da capacidade cibernética brasileira; o segundo, por sua vez, tem como objetivo esclarecer os principais conceitos pertinentes à análise do problema de pesquisa enunciado. O terceiro, por fim, busca explorar o estado atual da capacidade cibernética no Brasil e os desafios enfrentados para concretizar a construção dessa capacidade no país, utilizando-se de índices internacionais de maturidade de capacidade cibernética e levando em conta os conceitos pertinentes do Realismo Neoclássico para indicar lacunas internas que possam afetar a projeção de poder do país por meio do espaço cibernético.

2 MARCO TEÓRICO: O REALISMO NEOCLÁSSICO

Este capítulo tem como tema o marco teórico que orienta essa pesquisa. Trata-se do Realismo Neoclássico, a teoria que norteia a investigação acerca da relevância das capacidades de segurança cibernética na projeção internacional dos Estados. A adoção dessa vertente de Realismo se dá pela maior ênfase que esta teoria atribui aos Estados e à capacidade estatal como meio de angariar poder.

Simplificadamente, pode-se dizer que o Realismo Estrutural explica a distribuição de poder no sistema internacional em função das capacidades. Por sua vez, o Realismo Neoclássico preocupa-se em saber como essas capacidades são produzidas. Neste sentido, pode-se concluir que o Realismo Neoclássico prioriza as respostas dos estados aos desafios sistêmicos.

Adicionalmente, entende-se que essa vertente teórica valoriza o papel do sujeito, ou seja, os Estados (unidades do Sistema Internacional) na construção de sua inserção internacional. Por esse motivo, afigurou-se como a escolha mais apropriada para um trabalho que pretende examinar as capacidades e vulnerabilidades do Brasil no tocante a segurança cibernética.

Para tanto, partiu-se pressuposto que a inserção nacional do Brasil depende de, pelo menos, cinco elementos sobre os quais incidem decisões tomadas no âmbito doméstico. São eles: (1) marco legal; (2) instrumentos administrativos; (3) instituições; (4) base material; e (5) educação.

No que diz respeito ao Marco Legal, trata-se do elemento que autoriza aos diferentes agentes e níveis da Administração Pública efetuar seu planejamento baseado nos diagnósticos e percepções acerca das prioridades ou vulnerabilidades relacionadas à segurança cibernética. A despeito de algumas lacunas, pode-se dizer que o Brasil se encontra em uma posição consolidada no tocante a esse quesito. Como indicador da posição brasileira, pode-se mencionar a publicação da Política Nacional de Cibersegurança (Decreto 11.856/2023), em dezembro de 2023 (Brasil, 2023a).

O segundo elemento que incide sobre a tomada de decisão no nível doméstico são os instrumentos administrativos. Ou seja, aqueles que efetuam o cumprimento da lei (Di Pietro, 2014). Os instrumentos administrativos podem ser distribuídos em, pelo

menos, três tipos: (a) outorgar novas atribuições para órgãos já existentes – e.g caso da Polícia Federal; (b) promover a criação de novos órgãos – caso do CDCiber; e (c) arranjos ad hoc que, a depender da experiência – trata-se de operações interagência que podem constituir futuramente órgãos ou até mesmo instituições especializadas.

A primeira vista pode parecer estranho cogitar-se uma instituição especializada para a segurança cibernética. Cabe, pois, uma breve reflexão acerca da natureza do Estado. A função principal do Estado é a de regular e qualificar as práticas sociais – portanto, a de controle (Genro Filho, 1984). Contudo, o principal elemento por intermédio do qual o Estado exerce essa atividade regulatória é a Memória. Exemplo dessa função de Memória, cumprida pelo Estado, é o Sistema Integrado de Administração Financeira do Governo Federal (SIAFI). Criado em 1987, trata-se de uma rede interna para processamento, controle, execução financeira, patrimonial e contábil de todo o Governo Federal. A partir do SIAFI, diversos órgãos da Administração Pública têm seus documentos e instrumentos administrativos centralizados, em um sistema distribuído, permitindo rapidez, agilidade e confiança na execução dos serviços. Atualmente, o SIAFI é referência na administração pública internacional, sendo a implantação de sistemas similares recomendada pelo Fundo Monetário Internacional (FMI) (Brasil, 2023b).

Para exercer suas atribuições, o Estado estabelece aos diferentes órgãos finalidades altamente especializadas e compartimentaliza as tarefas pelas quais estes são responsáveis. Ou seja, a organização do Estado é feita a partir da alienação estabelecida entre os órgãos. Isto é, da subtração da competência de uns, daquilo que é característico das atribuições de outros. Dessa forma, todos conseguem cumprir com a sua respectiva parcela de encargos. Tal segmentação entre órgãos e instâncias da administração é especialmente observada no que tange à construção, execução e fiscalização do orçamento – por isso Fernando Prestes Motta (1981) já resumiu “burocracia” em poder, controle e alienação.

A despeito das inconveniências desta forma de administração, não existe em lugar algum no mundo outra forma de organizar o serviço público (burocracia) que não essa. O problema é que a segurança cibernética se dá de modo transversal, perpassando níveis e competências distintos da administração pública de tal sorte que

se torna imprescindível o uso da “imaginação institucional” (Godoy, 2009, p. 18; Unger et al., 2021, p. 02).

O terceiro elemento que importa ser discutido são as Instituições. Trata-se de arranjos que possam congregar órgãos públicos nos diferentes níveis da administração – federal, estadual, municipal – bem como o setor privado, sobretudo relacionado às infraestruturas críticas, e a sociedade. Este é o caso dos consórcios públicos (Salles, 2019) facultados pela Emenda Constitucional 19/1998 e inseridos na Constituição Federal por intermédio do Art. 241 – que prevê a gestão associada – e regulamentados pela Lei 11.107/2005. Este último caso, eventualmente, pode se constituir como uma resposta holística de atuação conjunta de diferentes órgãos e esferas da administração pública, privada e societal. Dada esta natureza, eventualmente um consórcio público de segurança cibernética poderia, também, fazer frente ao desafio da endogeneidade.

Entretanto, na ausência de outros dois elementos, toda a organização acima descrita, ficaria carente de fundamentos. O primeiro deles diz respeito à Base Material. De acordo com Celso Furtado (1984, p. 106-7), uma sociedade só consegue se autodeterminar se for capaz de produzir os elementos dos quais dependem sua vida material. Embora à primeira vista possa afigurar-se como algo estranho à segurança cibernética, a produção de chips (pastilhas com transistores) vitais para todo o processo de conversão e transmissão de dados telecomunicações, informática e robótica (Miller, 2023, p. 15-16), torna-se uma questão crucial. A operação da sociedade inteira depende deste tipo de insumo industrial.

Por fim, é necessário a Educação, o principal aspecto de natureza societal, fundamental para a conscientização da população sobre a natureza vital da segurança cibernética, bem como a adesão às boas práticas relacionadas à prevenção e à denúncia de ataques ou crimes cibernéticos. Este elemento se demonstra vital por razão da complexificação das relações sociais alicerçadas em rede que se erigiu a partir da Terceira Revolução Industrial (Martins, 2023, p. 19).

Como todos esses elementos dizem respeito à ação do sujeito, às condições internas do país, parece ser adequado valer-se da abordagem proposta pelo Realismo Neoclássico – que será descrito adiante.

2.1 REALISMO NEOCLÁSSICO E OS DESAFIOS DO OBJETO

Em seguida, interessa discutir o Realismo Neoclássico, teoria que norteará o desenvolvimento do tema. A partir disso, será possível investigar a relevância da segurança cibernética doméstica para a projeção internacional dos Estados. A decisão pelo realismo se deu pela ênfase dada pela teoria aos Estados e à capacidade estatal como meio de angariar poder.

Inicialmente, cumpre justificar a escolha do Realismo Neoclássico. Para tal, parte-se de breve exposição sobre a contribuição do neorrealismo. Essa está calcada na proposição de existência de uma estrutura, composta por múltiplas unidades não diferenciadas, que, considerando o contexto anárquico que envolve o sistema internacional, encoraja certos comportamentos e reprime outros, constrangendo a ação dos atores. Assim, a soberania dos Estados não os permite agir da forma como querem sem medo de represálias (Waltz, 1979). Considerando as ameaças inerentes a um sistema anárquico, o conceito de poder é fundamental quando se fala da sobrevivência dos Estados. Waltz defende que o poder é mensurado por meio da comparação entre capacidades das unidades - ou seja, observando a distribuição de capacidades. Para atingir seus objetivos e construir capacidades, os Estados tomam medidas internas e externas, visando à aquisição, por fim, de poder (Waltz, 1979).

Entretanto, o neorrealismo não se ocupa das questões internas, o que torna o Realismo Neoclássico uma escolha mais adequada ao estudo das capacidades cibernéticas estatais. O Realismo Neoclássico reconhece a predominância da estrutura, mas se ocupa das capacidades de poder material relativo, ou seja, recursos materiais comparados entre os Estados (Rose, 1998). Logo, considera a construção de capacidade com mais detalhamento. Em relação ao ciberespaço, nota-se que essa distribuição de capacidades é de difícil observação, uma vez que não há consenso sobre como medir esses recursos, além de os Estados (especialmente as grandes potências) terem muito mais facilidade para esconder seus reais potenciais no setor cibernético (Domingo, 2018).

De fato, pode-se considerar o incentivo à construção de capacidades cibernéticas como sistêmico. Aqui não se questiona essa premissa. Entende-se esse fenômeno como advindo da transformação digital que impacta a produção, os recursos

militares e a vida social como um todo, tornando recursos cibernéticos cruciais para inserir-se como ator relevante na economia internacional. Entretanto, o modo como essa resposta se dá depende de estruturas internas do Estado – por isso o Realismo Neoclássico.

O realismo considera os Estados como principais atores das relações internacionais, tendo estes a sobrevivência como objetivo principal. Em termos simples, isso se dá pela inexistência de uma autoridade internacional que garanta a segurança dos atores e, por consequência, suas existências, gerando desconfiança em todo o sistema (Mearsheimer, 2013). Contudo, cada corrente realista enfatiza diferentes aspectos do processo decisório dos Estados para agir no sistema internacional, apesar de todas compartilharem princípios básicos.

No caso deste trabalho, as diferenças entre o Realismo Neoclássico e o neorrealismo que justificam a escolha da primeira corrente dizem respeito ao nível de análise. O Realismo Estrutural busca explicar padrões de resultados internacionais com enfoque sistêmico, sem se preocupar com as políticas externas individuais dos Estados. Por sua vez, o neoclássico se interessa por investigar variações entre as políticas externas de diferentes Estados ao longo do tempo quando confrontados por situações parecidas, uma vez que nem sempre as decisões tomadas são ótimas ou mesmo semelhantes (Taliaferro, 2006). Em relação ao desenvolvimento de capacidades cibernéticas, uma possível identificação de padrão poderia vir de comparação com outros momentos em que surgiram tecnologias disruptivas (e potencialmente ameaçadoras). Contudo, os neoclássicos se utilizam de avanços feitos pelos neorrealistas, motivo pelo qual cabe considerar preceitos neorrealistas para discutir capacidade cibernética.

Em relação ao Realismo Neoclássico, faz-se necessário atentar ao fato de que ele se propõe a considerar, em conjunto, o domínio internacional e o interno. A teoria também considera os desafios inerentes à interpretação do sistema internacional, que raramente se faz claro o suficiente para os líderes estatais, e o fato de esses líderes nem sempre fazerem escolhas ideais. Dessa forma, o Realismo Neoclássico busca suprir essas lacunas, identificando elementos que influenciam o comportamento estatal

em mais de um nível de análise e demonstrando seus efeitos a nível sistêmico (Lobell et al., 2016).

Taliaferro (2006, p. 484) argumenta que “forças sistêmicas moldam processos domésticos nos Estados, que restringem as habilidades estatais de responder a imperativos sistêmicos”; Rose (1998, p. 152), por sua vez, entende que os Estados “respondem às incertezas do sistema internacional tentando controlar e moldar seus ambientes internos”. No que diz respeito ao ciberespaço, os Estados se adaptam por meio do desenvolvimento de recursos que os permitam enfrentar potenciais ameaças. Isso envolve tanto capacidades ofensivas e defensivas quanto a base material que possibilita o uso do ciberespaço de forma autônoma, visto que a proteção contra ciberataques possui múltiplas dimensões (Calderaro; Craig, 2020).

Lobell et al. (2016) vão ao encontro desse pensamento, considerando as decisões de curto prazo em momentos de crise e as respostas de política externa a eventos estruturais como respostas à estrutura do sistema internacional. Segundo os autores, os elementos domésticos teriam papel interveniente, sendo, portanto, elementos auxiliares na determinação do comportamento dos Estados.

Portanto, os Estados agem de acordo com incentivos da estrutura, mas a qualidade e a eficiência da resposta depende dos mecanismos internos. No caso da capacidade cibernética, o incentivo sistêmico se dá pela intensificação dos processos de digitalização e digitização. Nesse contexto, a inserção e a competitividade internacional do Estado dependem de sua capacidade de operar no ciberespaço. Contudo, a resposta a esse incentivo depende dos processos domésticos: a elaboração e implementação de estratégia específica, a adaptação da indústria doméstica, educação da sociedade, entre outros exemplos. A agilidade com que o país concretizará esse processo é proporcional à eficiência estatal na mobilização de recursos pertinentes.

O Realismo Neoclássico concorda com os preceitos neorrealistas de que os Estados agem pensando em ameaças e oportunidades externas, mas também considera seu predecessor limitado em outros termos. As lacunas do Realismo Estrutural que o Realismo Neoclássico busca suprir são quatro: em primeiro lugar, os líderes estatais nem sempre compreendem a situação internacional corretamente,

mesmo ela estando clara; em segundo lugar, o sistema internacional nem sempre se faz claro a respeito das ameaças existentes; terceiro, os líderes nem sempre respondem racionalmente aos eventos do sistema; por fim, os Estados nem sempre têm a possibilidade de mobilizar seus recursos efetiva e eficientemente. O presente trabalho trata, principalmente, dessa última situação.

Taliaferro (2006) identifica, ainda, dois tipos de Realismo Neoclássico: o tipo I, que procura explicar anomalias nos comportamentos dos atores e considera que, mesmo que o sistema internacional mande sinais claros para os Estados, os processos internos imperfeitos de decisão prejudicam a percepção dos líderes. O tipo II, por sua vez, busca se mostrar como ferramenta de explicação de política externa. Essa abordagem considera que, em períodos de crise e ameaça imediata, os Estados se comportam da maneira prevista pelos neorrealistas. Entretanto, tais situações são raras, tendo os atores, geralmente, amplas possibilidades de escolha em política externa.

Considerando esses conceitos de poder e capacidade, nota-se que a construção de capacidade cibernética pode figurar no âmbito interno como uma face da construção de capacidade, e depende de estruturas internas do Estado para ser construída efetivamente. O modelo realista neoclássico argumenta que a medida em que os Estados podem exercer poder, ou seja, extrair e mobilizar recursos de forma coercitiva, depende de instituições estatais e nacionalismo patrocinado pelo Estado (Taliaferro, 2006). Além disso, o ciberespaço tem uma configuração semelhante ao sistema internacional, visto que os dois são espaços anárquicos, cada um a seu modo. Com a crescente dependência dos recursos cibernéticos, o ciberespaço também vem se tornando palco para competição internacional (Craig; Valeriano, 2016).

Ainda em relação ao realismo aplicado ao ciberespaço, Craig e Valeriano (2018) se destacam ao interpretarem as relações de poder nesse domínio por meio das lentes realistas. Os autores analisam uma gama de conceitos comuns às vertentes do realismo e aplicam ao ciberespaço. Argumentam que uma das contribuições do realismo seria sua capacidade de explicar conflitos e corridas armamentistas no ciberespaço, anárquico por natureza, por meio do dilema de segurança – caracterizado pela ameaça causada pelo aumento de medidas de segurança em um Estado, levando

os outros a fazerem o mesmo. Dessa forma, se um Estado busca aumentar suas capacidades cibernéticas, os outros também o farão, criando um estímulo sistêmico ao desenvolvimento de instrumentos pertinentes ao poder cibernético.

Aqui se questiona o conceito usual de corrida armamentista transportada para o ciberespaço. Reconhece-se a possibilidade de um tipo diferente de competição, causada pela ampliação do uso do espaço cibernético na produção. Essa, facilitada pela Transformação Digital, cria um incentivo sistêmico para o desenvolvimento de tais capacidades. Isso pode levar à competição por superioridade tecnológica entre os Estados, que buscam estar mais bem equipados que seus concorrentes e, dessa forma, alcançar posições de influência no contexto das próximas Revoluções Industriais, que serão necessariamente baseadas em recursos cibernéticos.

Os autores também abordam a construção de capacidade cibernética como tática de dissuasão, em que a demonstração de poder cibernético desencorajaria os oponentes de realizarem um ciberataque. Nesse sentido, os autores defendem que a dificuldade de distinguir capacidades ofensivas no ciberespaço pode fazer com que mesmo medidas de construção de capacidade não voltadas à dimensão militar sejam interpretadas como ameaças, o que agravaria o dilema de segurança. Por outro lado, há também uma corrente que argumenta que os Estados evitariam se envolver em conflitos cibernéticos por temerem retaliações e os custos operacionais e normativos de agir dessa forma (Maness; Valeriano, 2015). Todavia, limitar a construção de capacidade cibernética à dissuasão de ataques restritos ao ciberespaço é restringir o impacto desse domínio em todos os setores fundamentais do Estado.

Cabe elencar, também, alguns desafios à interpretação realista do ciberespaço. Craig e Valeriano (2018) pontuam que o ciberespaço registra uma intensificação nunca vista da atuação de agentes não-estatais. Isso ocorreria devido às poucas barreiras de entrada e à maior facilidade de influência no espaço cibernético. Essa característica pode ir de encontro à percepção realista da primazia dos Estados. Ainda assim, a presença mais forte de atores não-estatais no ciberespaço não se traduz, necessariamente, em influência efetiva.

Os autores também questionam se a criação de capacidade cibernética poderia contribuir para o exercício de poder coercitivo. Para eles, tal questionamento vem do

fato de ataques cibernéticos não causarem dano expressivo para obter superioridade militar, não superando os meios convencionais de guerra mais eficazes para atingir esse objetivo. Retoma-se, entretanto, que o poder militar não é o único tipo de poder que importa. A capacidade cibernética parece ser, principalmente, uma forma de poder econômico. No entanto, conforme assume maior relevância no contexto da transformação digital que aproxima uma Quarta Revolução Industrial, a capacidade cibernética se torna mais fundamental para exercer poder coercitivo, posto que não raro as revoluções industriais causam mudanças na distribuição de poder no sistema internacional (Martins, 2023).

Outra dificuldade citada pelos autores é a dificuldade de demonstração de capacidade cibernética, dada a natureza do ciberespaço (em grande medida, virtual), o que dificultaria a dissuasão. Assim, as ferramentas realistas são úteis, em certa medida, para explicar os conflitos cibernéticos, mas não conseguem compreender algumas dinâmicas fundamentais próprias do ciberespaço. Ademais, põe-se em questão a habilidade das teorias realistas de prever se a construção de capacidade tem probabilidade significativa de resultar em conflito, cibernético ou convencional (Craig; Valeriano, 2018).

Por outro lado, Mazanec e Whyte (2019) apresentam o domínio cibernético como um domínio de guerra, mas considerando as limitações das armas cibernéticas para os conflitos e a dificuldade de desenvolver o ciberespaço e gerenciar a construção de capacidade cibernética. Os autores pontuam que o gerenciamento do ciberespaço depende de várias instituições, tanto aquelas criadas especificamente para tal quanto as que controlam o aparelho regulatório do Estado no geral. Dessa forma, as instituições normativas seriam essenciais para a governança do espaço cibernético e construção de capacidade.

Argumentam que, para o realismo, o principal desafio de analisar as questões cibernéticas é o foco geralmente dado às questões estruturais em detrimento dos elementos internos, visto que a guerra cibernética por si só é um fenômeno improvável. Portanto, não faria sentido ser observada por uma corrente que enfatiza em tamanha medida os conflitos internacionais. Não consideram que a competição pode assumir outras formas – ideia que o presente trabalho rejeita.

Apesar disso, consideram que o realismo serviria para observar o domínio cibernético como um dos componentes da segurança nacional, mas dependente de fatores internos. Nesse sentido, o Realismo Neoclássico se mostra uma boa opção para analisar a questão da segurança cibernética dos Estados, já que não se limita às questões estruturais enfatizadas pelo neorrealismo e considera elementos que limitam ou incentivam a construção de recursos cibernéticos em prol da segurança nacional. Não se nega, entretanto, a dimensão estrutural do objeto – os incentivos sistêmicos que suscitam respostas eficientes das unidades.

Considerando, ainda, o enfoque realista neoclássico, na posse de recursos de poder, há que se atentar para o conceito de capacidade cibernética e seus desdobramentos. Para a construção de capacidades cibernéticas, é fundamental que a segurança cibernética, além da defesa e da resiliência cibernética dos Estados, seja intensificada nos setores econômicos e sociais, não apenas no âmbito militar (Grassi; Pinto, 2022). Nesse sentido, a segurança cibernética seria apenas um dos elementos de capacidade cibernética. Para isso, é fundamental a criação de estratégias nacionais de segurança cibernética, especialmente na América Latina, região em que apenas cinco países, até 2020, possuíam estratégias bem delimitadas (Grassi; Pinto, 2022). O conceito de capacidade cibernética será explicado adiante, em seção específica.

Cabe, ainda, considerando as definições de poder cibernético e capacidade cibernética, explorar como a literatura trata os conflitos cibernéticos. Por um lado, o uso crescente das ferramentas cibernéticas sugere que essas serão cada vez mais utilizadas para obter superioridade em conflitos internacionais. Conforme aumenta a dependência das redes em escala internacional, torna-se mais vantajoso atacar essas redes para prejudicar os oponentes (Andress; Winterfeld, 2014). Dessa forma, é crucial o esforço de informar criadores de políticas públicas, empresários e profissionais de segurança sobre o tema, já que a segurança cibernética não deve se restringir à máquina pública; para maximizar a segurança cibernética, todos os pontos da rede devem estar protegidos.

Em contrapartida, Maness e Valeriano (2015) refletem sobre como o uso do ciberespaço evoluirá no contexto dos conflitos internacionais. Defendem que, embora o domínio cibernético esteja crescendo em importância para as relações internacionais, o

discurso produzido sobre os conflitos cibernéticos tem exagerado a gravidade do fenômeno, num processo de securitização que poderia causar a concretização dos medos existentes da guerra cibernética. Os autores definem conflito cibernético como “o uso de tecnologias computacionais no ciberespaço, com fins destrutivos, para impactar ou modificar as relações militares e diplomáticas entre entidades, sendo uma ferramenta de política externa usada por Estados ou indivíduos contra Estados” (Maness; Valeriano, 2015, p. 5). Os autores também reconhecem os desafios inerentes ao estudo de segurança cibernética, tais como a diversidade de nomenclaturas para instrumentos que, na prática, são iguais. Ademais, menciona-se a falta de consenso a respeito dos significados dessas nomenclaturas e a própria incerteza sobre o futuro dos conflitos internacionais no contexto da evolução tecnológica.

Portanto, percebe-se que, dado o ineditismo do estudo da cibernética em Relações Internacionais, os estudos são, em grande medida, incipientes. Há dificuldades em conceituar os principais elementos relacionados ao tema, e o debate acerca da interpretação das dinâmicas do ciberespaço segundo as teorias de Relações Internacionais continua em progresso – principalmente, por não conseguirem prever como as operações cibernéticas ocorrerão a longo prazo e se ocuparão espaço significativo nos conflitos internacionais. A interconexão das infraestruturas críticas precisaria ser ainda mais intensa para ser totalmente destruída por ataques virtuais, e os custos de um ataque cibernético de grande escala e o risco de uma contra-ofensiva fora do ciberespaço superam o eventual retorno.

Entretanto, essa evolução das infraestruturas críticas já vem acontecendo e já se observam usos militares do ciberespaço a ponto de ser razoável proteger-se de ameaças digitais. Defende-se, em geral, que o domínio cibernético será utilizado como uma das faces dos conflitos, apesar de não assumir papel principal. Está sujeito, dessa forma, a ser contemplado nos mecanismos de competição entre os Estados por superioridade – nesse caso, superioridade cibernética. Essa superioridade não se restringe a operações virtuais, mas também envolve a base material que é premissa necessária para pensar em operações cibernéticas.

Assim sendo, o Realismo Neoclássico se mostra como uma boa opção para analisar a questão em voga. Essa corrente mantém o núcleo realista, que enfatiza que

o comportamento dos Estados considera as ameaças que eles enfrentam no sistema internacional, mas também suas opções baseadas no âmbito interno – seus recursos ou a falta deles e a capacidade de mobilizá-los. Consequentemente, pode-se interpretar a capacidade cibernética como um dos recursos de capacidade estatal que devem ser mobilizados para que os Estados possuam uma gama maior de opções no sistema internacional.

A construção de capacidade cibernética deve, necessariamente, passar por uma política estatal de segurança cibernética para que seja construída de modo organizado e efetivo, o que será coberto mais detalhadamente nos capítulos seguintes. O debate, além disso, tem avançado de modo que já é possível elencar fatores de peso para a incrementação da segurança cibernética nos Estados, bem como para a governança do ciberespaço. Contudo, permanece o desafio de determinar a melhor maneira de mensurar e desenvolver recursos de capacidade cibernética. Isso posto, cabe discutir, a seguir, como mensurar a capacidade cibernética dos Estados, bem como analisar a capacidade cibernética do Brasil, foco da presente pesquisa.

2.2 CONCLUSÕES PARCIAIS

Considerando o exposto, o presente capítulo tratou do marco teórico utilizado, o Realismo Neoclássico, num esforço de associá-lo à construção de capacidade cibernética e operacionalizar a teoria no que tange à discussão sobre o curso do desenvolvimento de recursos de segurança cibernética no contexto brasileiro. Neste capítulo, cumpriu-se o primeiro objetivo específico, de operacionalizar a teoria de forma a entender como ela poderia auxiliar a compreensão do objeto de estudo.

Inicialmente, identificaram-se cinco elementos que influenciam a inserção nacional do Brasil no contexto da segurança cibernética: marco legal, instrumentos administrativos, instituições, base material e educação. No tocante à capacidade cibernética, buscou-se evidenciar que a inserção internacional do Brasil depende desses cinco itens de ordem doméstica, justificando a adoção do Realismo Neoclássico como vertente que orienta a pesquisa. Essa corrente é apropriada para analisar as respostas dos Estados aos desafios que o tema suscita, tendo em vista as

peculiaridades da segurança cibernética, que requer uma abordagem transversal para ser aprimorada.

Em seguida, buscou-se descrever a teoria e pontos de contato com outras vertentes realistas, apresentando fundamentos do Realismo Neoclássico e como esses contribuem para o estudo da construção de capacidade cibernética. Ademais, pretendeu-se identificar como o objeto vem sendo tratado em Relações Internacionais, em especial por perspectivas realistas. Depreende-se que a natureza do espaço cibernético suscita desafios teóricos e práticos para as relações internacionais, mas sua crescente importância torna o estudo desse domínio imprescindível. No capítulo que segue, procura-se definir os principais conceitos relativos ao objeto e explicitar a relevância do tema para a projeção de poder.

3 CAPACIDADE CIBERNÉTICA

O presente capítulo procura situar o conceito e a importância das capacidades cibernéticas em Relações Internacionais. Inicialmente, apresentam-se os principais conceitos para a compreensão do tema. Após, expõe-se um breve histórico do estudo da segurança cibernética no âmbito da disciplina. Por fim, aborda-se o Realismo Neoclássico, teoria escolhida para o embasamento do trabalho, expondo também como o realismo observa as questões relativas a segurança e defesa no contexto da Transformação Digital.

3.1 CIBERESPAÇO: PRINCIPAIS CONCEITOS

Inicialmente, cabe investigar as dinâmicas contemporâneas relacionadas à emergência do espaço cibernético. O campo de estudos de segurança cibernética em Relações Internacionais é relativamente recente e está ligado ao rápido processo de evolução de tecnologias disruptivas e consequente digitalização da vida social a partir de meados do século XX. Nesse contexto, faz-se necessário definir os conceitos de ciberespaço, segurança cibernética e capacidade cibernética. Ademais, cumpre expor os principais conceitos que sustentam o estudo das capacidades cibernéticas. Aqui os conceitos de ciberespaço e espaço cibernético se destacam.

Inicialmente, a ascensão das Tecnologias de Informação e Comunicação foi vista como uma oportunidade de democratizar a difusão de conhecimento e o acesso a serviços essenciais, especialmente após o surgimento da internet. Entretanto, a natureza descentralizada desses recursos permite o uso livre (e, por muito tempo, quase indiscriminado) dessas ferramentas sem forte interferência governamental (Calderaro; Craig, 2020). Essa característica se estende por todo o ciberespaço, cujo uso no âmbito das relações internacionais desafia o papel tradicional do Estado e a relação desse com seus entes subnacionais e os indivíduos, inclusive em termos de direitos individuais e coletivos.

Hodiernamente, o ciberespaço configura-se como um campo fundamental para a projeção de poder e influência no âmbito internacional. Seus efeitos nas relações interestatais são profundos, de forma que é fundamental conhecê-los para apreender a

extensão dessa transformação. O domínio em questão pode confundir os limites entre as esferas pública e privada; entre os direitos individuais de privacidade e os direitos coletivos à segurança; e entre as dimensões de tempo e espaço, além de desafiar as concepções clássicas de soberania e fronteira. Esses são elementos fundamentais para munir os Estados de capacidades que permitam a projeção de influência (Silva; Teixeira; Freitas, 2015).

Além disso, o ciberespaço representa parte cada vez mais essencial da produção, de modo que é impensável conduzir processos produtivos em escala sem que algum recurso cibernético seja utilizado. Nisso estão inclusas pesquisas em rede, a computação em nuvem e a automatização, por exemplo.

Considerando a crescente importância desse fenômeno, os Estados procuram cercar-se de toda sorte de recursos cibernéticos para implementar telecomunicações, serviços bancários e outras infraestruturas críticas de relevância social. Contudo, essas ferramentas, quando instaladas no ciberespaço, criam vulnerabilidades que exigem dos Estados o desenvolvimento de dispositivos ofensivos e defensivos, a fim de proteger esses recursos e, eventualmente, explorar os de adversários (Cravo, 2023). A partir disso, evidencia-se a crescente importância de prover uma experiência segura desses instrumentos em todas as esferas estatais.

Para compreender a necessidade e a dificuldade de investigar os impactos do ciberespaço nas relações internacionais, cabe destacar que não há consenso em relação a sua definição, existindo variados conceitos associados ao termo. Kuehl, por exemplo, propõe:

> [...] um domínio global dentro do ambiente da informação, cujo caráter distintivo e único é moldado pelo uso de eletrônicos e pelo espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas, utilizando tecnologias de informação e comunicação (Kuehl, 2009, p. 29, tradução nossa)[2].

Outro exemplo de definição entende o ciberespaço como o “domínio das redes de computadores em que as informações são armazenadas, compartilhadas e

[2] [cyberspace is] a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies” (KUEHL, 2009, p. 29, tradução livre).

comunicadas online" (Friedman; Singer, 2014, p. 13). Kuehl propõe um conceito mais abrangente que Friedman e Singer, visto que abarca qualquer ambiente de informação que faça uso do espectro eletromagnético. Entretanto, ignora o fato de o espectro eletromagnético ser um domínio por si (Ricciardi; Souque, 2021). Por sua vez, a definição de Singer e Friedman, por outro lado, tem um enfoque maior na internet. Lévy (1999) também conceitua o domínio em relação às redes de computadores, definindo-o como um espaço de redes digitais mundialmente interconectadas, o que traria à tona novos desafios à sociedade, tornando-se claro o protagonismo da internet nesse contexto, apesar de ela não ser a única componente do ciberespaço (Domingo, 2018).

Para efeitos deste trabalho, optou-se por utilizar a definição de Lévy – o ciberespaço como espaço de redes digitais mundialmente interconectadas – uma vez que essa ideia remete, também, à base material necessária para a operação dessas redes – a fibra óptica e os chips, especialmente.

O ponto de contato entre as definições é a natureza artificial do ambiente cibernético. Evidentemente, o ciberespaço não é um domínio natural, mas sim construído. Por consequência, a capacidade de afiançar sua segurança depende, necessariamente, da capacidade de erigi-lo. A segurança digital, a defesa contra ataques maliciosos e vírus é insuficiente se houver insegurança sobre o próprio controle do domínio. Assim, a segurança do ciberespaço advém, em primeiro lugar, do controle sobre sua manutenção em território nacional, sem depender do provimento de outrem. Nesse caso, fala-se da capacidade de construir e manter estruturas que compõem a base material do espaço cibernético, com destaque para a fibra óptica – que permite a instalação de cabos submarinos – e os chips, que permitem a ampliação do poder computacional. Esse último é fundamental para as transformações digitais que se aprofundam conforme a Terceira Revolução Industrial avança e se aproxima da Quarta Revolução Industrial.

No tocante à natureza do ciberespaço, há quem o considere fragmentado, de forma que cada indivíduo, empresa e governo teria um ciberespaço próprio conectado aos demais. Nesse sentido, Libicki (2012) se destaca por discutir o conceito de ciberespaço e questionar sua relevância como palco de conflitos internacionais, já que

ele é facilmente controlável por humanos. Aqui mais uma vez se retoma a necessidade de providenciar meios de manter o domínio cibernético de forma autônoma.

O autor considera que as operações cibernéticas têm apenas função de suporte em conflitos, sendo úteis para facilitar a obtenção de superioridade física em outros domínios e prejudicar os recursos do inimigo. Portanto, a abstração do ciberespaço seria um obstáculo para a concretização das conjecturas sobre o espaço cibernético como espaço de guerra – um ataque cibernético como fim não seria de grande utilidade para obter superioridade.

No entanto, essa consideração não aborda a relevância dos recursos cibernéticos para o funcionamento do Estado. De fato, é improvável que um ataque virtual prejudique sobremaneira as infraestruturas críticas[3] a ponto de causar danos semelhantes a um ataque físico. Contudo, a destruição da base material que sustenta o ciberespaço – cabos submarinos, torres de telecomunicações, entre outros exemplos – interromperia o funcionamento de diversos órgãos estatais e causaria profundos impactos na economia. Também cumpre ressaltar a facilidade de comprometer as redes de um Estado a partir do controle sobre elas, inclusive com menores dispêndios. Assim se justifica a necessidade de certificar a segurança cibernética não só em seu aspecto virtual, mas também no físico, garantindo autonomia sobre o espaço cibernético. Desse modo, observa-se o desafio de definir o termo.

O mesmo desafio conceitual está presente quando se fala de segurança cibernética. Há diversos termos utilizados para descrever o fenômeno: segurança cibernética, segurança da informação, segurança da internet, entre outros. Entretanto, esses vocábulos podem ou não ser usados como sinônimos, a depender de quem os utiliza e com qual finalidade (Cravo, 2023). A Agência de Cibersegurança e Segurança de Infraestruturas dos Estados Unidos (CISA), por exemplo, define segurança cibernética como “a atividade ou processo, habilidade, capacidade ou estado por meio do qual informações e sistemas de comunicação e a informação neles contida são protegidos e/ou defendidos contra danos, modificação não autorizada ou exploração”

[3] “Instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança” (Brasil, 2021)

(CISA, 2023, tradução livre). A agência estende a definição para, além de operações técnicas, estratégias e políticas que versem sobre a segurança de operações no ciberespaço, incluindo ações diplomáticas e militares, por exemplo.

Outra definição é aquela adotada pela Agência da União Europeia para a Cibersegurança (ENISA):

> Cibersegurança abrange todos os aspectos de prevenção, previsão, tolerância, detecção, mitigação, remoção, análise e investigação de incidentes cibernéticos. Considerando os diferentes tipos de componentes do ciberespaço, a cibersegurança deve abranger os seguintes atributos: Disponibilidade, Confiabilidade, Segurança, Confidencialidade, Integridade, Manutenibilidade, Robustez, Sobrevivência, Resiliência (para apoiar a dinâmica do ciberespaço), Responsabilidade, Autenticidade e Não-repúdio (para apoiar a segurança da informação) (ENISA, 2017, p. 6).

Por fim, cabe notar a definição empregada pelo Glossário de Segurança da Informação, elaborado pelo Gabinete de Segurança Institucional da Presidência da República (GSI), encarregado de fornecer suporte direto ao Presidente da República no exercício de suas responsabilidades, com foco especial em questões militares e de segurança:

> Segurança cibernética - ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (Brasil, 2021)

Nota-se que todas as definições enfatizam os aspectos técnicos de segurança cibernética, como detecção e mitigação de riscos, tarefas realizadas por profissionais da área. Em especial, as definições elaboradas pela ENISA e pelo GSI citam aspectos técnicos que dizem respeito aos sistemas virtuais, chamando atenção para incidentes cibernéticos e para a atributos como a manutenibilidade de software. Entretanto, pode-se argumentar que políticas e estratégias de segurança cibernética podem ser incluídas, visto que estabelecem diretrizes para prevenção de ataques e defesa contra ameaças do ciberespaço. Há, ainda, inúmeros outros exemplos, sendo impossível listá-los de forma exaustiva. Dessa forma, evidencia-se a natureza multifacetada do ciberespaço e dos conceitos que o rodeiam.

Considerando o exposto, percebe-se que o tema de segurança cibernética já se estabelece como de grande importância para as relações internacionais, levantando

desafios próprios, mas que também se relacionam a velhas questões de disparidade de poder e conflitos no sistema internacional. Um exemplo disso é apresentado por Calderaro e Craig (2020), que defendem que a natureza transnacional do ciberespaço e de suas tecnologias torna crucial que os Estados atuem em conjunto para estabelecer padrões de governança internacional da segurança cibernética. Isso aconteceria porque os desafios desse domínio podem se originar em um território e ocasionar desdobramentos em diversos outros. A desigualdade das capacidades cibernéticas entre os países pode agravar a situação, já que a alta ocorrência de incidentes cibernéticos em países cujos recursos cibernéticos são incipientes pode impactar outros Estados do sistema internacional (Calderaro; Craig, 2020). Essa visão permite notar a transcendência das ameaças cibernéticas por entre fronteiras.

Contudo, questiona-se o potencial da cooperação, uma vez que as iniciativas de cooperação mostram-se limitadas. Além de o ciberespaço também ser utilizado como ferramenta em conflitos internacionais, deve-se considerar que os Estados também competem por ele: a capacidade cibernética amplia a capacidade produtiva e possibilidade de inserção na Terceira Revolução Industrial e, futuramente, na Quarta, o que pode resultar em uma redistribuição de poder (Martins, 2023). Portanto, os Estados se preocupam com os ganhos relativos que podem resultar de uma cooperação nesse setor.

Outro conceito crucial para a compreensão das dinâmicas do ciberespaço é o de poder e capacidade cibernética, relacionado aos recursos estatais para obtenção de superioridade nesse domínio. Sheldon (2011, p. 95, tradução nossa) define poder cibernético como “a habilidade de usar o ciberespaço para criar vantagens e influenciar acontecimentos em todos os ambientes e instrumentos de poder, visando a alcançar os objetivos políticos nacionais”. Nye (2012, p. 162) propõe conceituação parecida, mas enfatiza a esfera virtual do ciberespaço: o poder cibernético seria o “conjunto de recursos que se relacionam à criação, ao controle e à comunicação de informações eletrônicas e baseadas em computador”. Conforme o autor, isso permitiria que o Estado atingisse resultados preferidos utilizando-se de recursos informacionais conectados ao ciberespaço. As capacidades cibernéticas, dessa forma, são um meio de permitir que o

Estado exerça poder cibernético, embora a real função dessas transcenda o domínio – trata-se de exercício de poder.

Vê-se, por fim, que a construção de processos e políticas nacionais de segurança cibernética permite que o Estado desenvolva uma postura ativa no investimento em segurança cibernética e na inclusão do domínio cibernético na construção de capacidades. Entretanto, é difícil mensurar a capacidade cibernética – ou seja, a dificuldade está em descobrir quais são os setores essenciais para o Estado obter uma maior resiliência (Creese et al., 2021). Nesse contexto, ressalta-se o desafio de mensurar a capacidade cibernética dos Estados, visto que os elementos envolvidos no processo de construção de tais capacidades são os mais variados e complexos.

3.2 3.2 O CIBERESPAÇO COMO ESPAÇO DE PROJEÇÃO DE PODER

Uma das principais características do ciberespaço é sua natureza transnacional e descentralizada, o que cria desafios aos Estados. Exemplos disso são a erosão de fronteiras geográficas e o crescimento do papel de atores não-estatais (Solar, 2020; Calderaro; Craig, 2020). O conceito tradicional de soberania, no contexto do ciberespaço, prescreveria que o fluxo de informação em um território soberano seria controlado pelo Estado, sem ingerência externa; no entanto, dadas as peculiaridades do espaço cibernético, isso não acontece: é difícil manter controle de informações ao mesmo tempo em que se adota mais liberdade no uso das redes e demais recursos digitais (Schmitt, 2013).

Ademais, considerando a proporção que o ciberespaço vem adquirindo nos processos produtivos, na guerra e na vida social, torna-se vantajoso desenvolver meios que possibilitem o uso do ciberespaço para ocupar uma posição mais proeminente no sistema internacional. Eventualmente, tais capacidades também podem ser utilizadas para explorar vulnerabilidades cibernéticas físicas e virtuais de adversários, quando necessário. Além disso, deve-se notar que os outros Estados podem fazer o mesmo, de forma que é fundamental criar recursos de segurança para proteger o ciberespaço e as infraestruturas que o sustentam. Dessa maneira, a atuação no espaço cibernético se torna um meio de exercer poder, atingir objetivos e obter vantagens. Tendo em vista

esse fenômeno, os Estados buscam meios de lidar com as incertezas advindas do domínio cibernético.

Um desses meios é a cooperação. No entanto, as múltiplas tentativas de cooperação e governança conjunta, apesar de antigas, não conseguiram lidar com as variadas questões criadas com o surgimento das tecnologias disruptivas. A cooperação, na prática, não se concretizou pela falta de coordenação entre os países e de interesses políticos dos Estados, que preferiram buscar desenvolver redes digitais regionais e domésticas em detrimento de sistemas internacionais de governança do espaço cibernético (Pohle; Thiel, 2020; Fifth Domain, 2019).

Cabe retomar a necessidade de autonomia para operar no ciberespaço sem limitações impostas por atores mais influentes. Depreende-se que os Estados percebem isso, uma vez que desconfiam da governança internacional do ciberespaço e preferem se voltar ao desenvolvimento de redes regionais e domésticas. Essa governança conjunta dependeria de interesses comuns entre os Estados – o que a distribuição de poder no sistema impede – ou um conjunto de objetivos a serem buscados por todos.

Contudo, questiona-se quem determinaria esses objetivos: o provável é que os mais poderosos o façam. Pode-se compreender a cooperação pela governança do ciberespaço (que enfatiza as ameaças virtuais conjuntas e ignora a base material que proporciona autonomia) como uma forma de poder brando, posto que este inclui a capacidade de um país modificar as preferências e ações de outros por meio de sua atração ideológica e política. No caso em questão, persuadindo outros Estados a enfatizar determinados atributos da segurança cibernética que, embora importantes, mantêm esses em posição dependente.

Nesse sentido, notam-se os limites da colaboração internacional, visto que em que os Estados só estão dispostos a trabalhar juntos enquanto seus interesses nacionais convergirem. Além do exposto, depreende-se, desse contexto, que a governança internacional do espaço cibernético poderia prejudicar elementos da soberania dos Estados, que, em última medida, buscam a superioridade de capacidades, dificultando a execução do projeto. Ademais, dada a relevância do domínio cibernético para as transformações produtivas decorrentes da automação e

das redes, é de se esperar que os Estados se preocupem com os ganhos relativos uns dos outros. Isso porque posse de recursos centrais dessas transformações – já observadas como prenúncio de uma Quarta Revolução Industrial – tende a conduzir a distribuição de poder no cenário emergente (Schwab, 2016). Segundo Taliaferro (2006), os Estados precisam levar em consideração a possibilidade de potenciais rivais utilizarem suas capacidades contra eles no futuro – por isso, destaca, é importante considerar as capacidades, não as intenções atuais dos outros Estados. Portanto, a construção de capacidade acaba seguindo um viés de autoajuda, visto que a cooperação possui riscos associados a ela.

Essa divergência de interesses nacionais e a discrepância entre as capacidades cibernéticas dos Estados são elementos que dificultam a cooperação. Tais características podem ser vistas nas desigualdades entre Norte e Sul Global. Calderaro e Craig (2020) pontuam que, em termos gerais, apesar de o aumento percentual da população conectada no Sul ser superior ao do Norte Global, é notável a superioridade da capacidade cibernética no Norte em relação ao Sul. Apesar de os autores categorizarem os países em termos de Norte e Sul, deve-se ressaltar a impossibilidade de generalização dos países nesse sentido. Na prática, o que se observa é, naturalmente, um aparato de segurança cibernética mais consolidado nos Estados que concentram mais recursos econômicos, técnicos e militares.

Outrossim, faz-se necessário discutir o aspecto militar do ciberespaço, observando-o como instrumento de poder duro. As Forças Armadas, como os outros componentes do Estado, foram impactadas com a evolução das tecnologias disruptivas. Discussões relativas à defesa de infraestruturas críticas e setores estratégicos do Estado contra ataques cibernéticos crescendo em importância, visto que esses recursos estão cada vez mais conectados à rede e dependentes dela (Ghernaouti, 2013; GCSC, 2019).

Isso posto, o ciberespaço já é considerado um domínio de guerra, considerando, entre outros fatores, a facilidade de produção de armas cibernéticas. Puyvelde e Brantly (2019) elencam diferentes usos para os recursos cibernéticos como forma de obter superioridade, como a ciberespionagem, utilizada com frequência para obter informações confidenciais que possam conferir vantagem ao Estado espião. A grande

vantagem das ofensivas cibernéticas é a negabilidade a eles atrelada, uma vez que é difícil atribuir responsabilidade a um ator específico e mesmo detectar a origem dos ataques. Isso permite que os atores explicitem preferências, influenciem outros Estados e atinjam objetivos de forma não agressiva e sem prejudicar relações diplomáticas (Maness; Valeriano, 2018).

No que diz respeito à visão que enfatiza o ciberespaço como um novo ambiente que molda a política externa dos Estados, Domingo (2018) aponta, como exemplo, o caso da resposta da Estônia aos ataques russos em 2007. A estratégia de política externa da Estônia passou a enfatizar o desenvolvimento de capacidades de segurança cibernética, por meio de iniciativas como o reforço dos acordos de segurança coletiva com a Organização do Tratado do Atlântico Norte (OTAN) para questões cibernéticas e no estabelecimento do Centro de Excelência em Defesa Cibernética, também em conjunto com a OTAN (Crandall; Collins, 2014; Crandall; Collins, 2015). O caso da Estônia é um exemplo das limitações impostas pela dependência para a segurança cibernética, mas mostra como o ciberespaço pode influenciar a política externa dos países. Ademais, é um caso muito diferente do que se pretende analisar neste trabalho, uma vez que o país se encontrava em posição desfavorável frente à Rússia e se aliou a outra potência para reduzir essa disparidade, numa estratégia de bandwagoning.

O processo de construção de capacidades cibernéticas, em diversos países, tem-se dado inicialmente sob uma abordagem centrada em desenvolver capacidades ofensivas e defensivas contra ameaças virtuais. Por exemplo, cita-se a proteção contra ataques de hackers, especialmente como forma de preparação para eventuais guerras. Solar (2020) argumenta que países como os da América Latina têm demonstrado preferência por delegar assuntos de capacidade cibernética às Forças Armadas, além de buscarem ações diplomáticas sobre segurança cibernética com Estados mais poderosos – em especial, os Estados Unidos. Além disso, os Estados teriam interesse em criar e fortalecer parcerias com o setor de defesa para aprimorar os recursos cibernéticos nacionais. Cumpre notar que essas alianças evidenciam-se como fator adicional de dependência, posto que a necessidade de se aliar aos poderosos para o incremento da segurança cibernética é causada pela incapacidade desses Estados de garantirem-na sozinhos.

Considerando o exposto, nota-se que as dinâmicas a respeito da utilidade do ciberespaço como recurso de poder vêm sendo amplamente discutidas e consideradas pelos Estados. Assim, faz-se necessário ter em mente as dinâmicas do contexto atual ao tomar decisões estratégicas de projeção de influência e defesa dos interesses nacionais no sistema internacional.

3.3 CAPACIDADE CIBERNÉTICA: CONCEITO, MENSURAÇÃO E DESENVOLVIMENTO

Infere-se, da evolução e disseminação de tecnologias disruptivas, que têm crescido as oportunidades de projeção de poder e influência por meio de ferramentas computacionais – tanto pelo desenvolvimento do ciberespaço doméstico quanto pela exploração dos recursos de outros Estados. Assim, os Estados vêm intensificando seus esforços de criação de recursos de defesa de estruturas críticas em face das novas ameaças decorrentes da digitalização. O debate sobre a importância desses mecanismos não ocorre somente no ambiente doméstico. Também há tentativas de encontrar formas de cooperação cibernética no âmbito de organizações internacionais, como se pode ver pela Convenção de Budapeste sobre o Crime Cibernético[4]. Nesse sentido, muito se fala do processo de construção de capacidade cibernética como forma de preparar o aparato estatal para possíveis ataques externos e explorar o ciberespaço como um meio de projeção de poder.

Pawlak (2016) aponta que o conceito de construção de capacidade foi definido pela ONU como um meio de criar e manter instituições sólidas e autossustentáveis, capazes de apoiar processos de desenvolvimento nacional. Isso envolveria buscar o desenvolvimento de recursos humanos, estruturas organizacionais e jurídicas (ONU, 2002). O autor explica que “a construção de capacidade é geralmente vista como um mecanismo para reduzir a lacuna entre os problemas de má governança e o que é considerado um nível aceitável de capacidade estatal para cumprir suas funções principais" (Pawlak, 2016, p. 84). No domínio cibernético, isso se torna ainda mais importante, visto que sua natureza descentralizada dificulta a concepção de uma

[4] Convenção que estabelece esforços conjuntos para tipificar crimes de natureza cibernética ou que ocorram no domínio cibernético, dispondo sobre medidas a serem adotadas nas jurisdições nacionais (direito penal e processual), jurisdição e cooperação internacional.

boa governança. As funções vitais do Estado estão cada vez mais centradas no ciberespaço e pautadas na automatização, inclusive setores bancários, de energia, industriais e outros fundamentais para o funcionamento do Estado. Assim, a construção de capacidade seria mais que mero apoio ao desenvolvimento econômico e social: seria uma ferramenta crucial para assegurar a defesa do interesse nacional (Pawlak, 2016).

Creese et al. (2021), por sua vez, definem capacidade cibernética pelos recursos capazes de mitigar ameaças cibernéticas aos recursos digitais do Estado. A construção dessa capacidade depende de premissas fundamentais, como a criação de processos, tecnologias e políticas nacionais de segurança cibernética. Entretanto, não há um consenso sobre como mensurá-la, visto que acadêmicos da área discordam sobre indicadores relevantes e sobre o próprio conceito de segurança cibernética. Conclui-se que a maioria desses Estados se encontram nos estágios iniciais de desenvolvimento de capacidades cibernéticas, o que indica a necessidade generalizada de desenvolver o setor em questão (Creese et al., 2021).

Nesse sentido, Bada et al. (2019, p. 280) apontam que a construção de capacidades de segurança cibernética é um amplo projeto político e estratégico. Logo, envolve “o desenvolvimento de iniciativas gerenciais, técnicas, sociais, legais, políticas e regulatórias por um grupo crescente de atores para melhorar a resiliência dos países a brechas de segurança cibernética, ao cibercrime e ao terrorismo”. Dessa forma, o aparato de capacidade cibernética compreende elementos como política e estratégia, processos técnicos e de resposta a incidentes, cultura de suporte à segurança cibernética, normas e padrões adequados, capacidade ofensiva e defensiva e, primordialmente, capacidades materiais que possam sustentar todos os outros pilares da segurança cibernética.

Ainda, Salles (2019) aponta que capacidades são definidas como atributo da soberania. O autor argumenta que desenvolver capacidades significa criar condições de desenvolvimento e riqueza que possibilitem que a política interna responda aos desafios sistêmicos e que o Estado adote medidas coercitivas. Em se tratando destas últimas, o autor retoma o papel das operações cibernéticas na transformação militar, que envolve, além do Comando do Espaço, o computador e a rede. Dessa forma, a

segurança cibernética também diz respeito à proteção de recursos militares que, sem as devidas medidas protetivas, ficarão vulneráveis a ataques de grupos externos e internos.

Essas capacidades, especialmente no contexto da cibernética, não podem ser desenvolvidas apenas no âmbito do Estado; devem abranger a integração desse com a sociedade. Um caminho para isso é sugerido por Salles: a operacionalização do conceito de esfera pública não-estatal de Bresser-Pereira (Bresser-Pereira, 1997). Essa esfera é entendida como um dispositivo econômico e político necessário para o desenvolvimento de capacidades cibernéticas por estas não se circunscreverem à esfera estatal (Cravo, 2023). A esfera pública não-estatal depende, assim, da atuação conjunta de Estado e sociedade (Bresser-Pereira; Grau, 1999, p. 44). Seria utilizada para atividades não exclusivas do Estado, mas de interesse público. A consolidação desse conceito, no contexto do ciberespaço, requer adaptação das normas vigentes para lidar com questões sociais, econômicas e políticas no domínio cibernético. Para isso, Salles propõe o Instituto do Consórcio como forma de realizar as intervenções estatais necessárias para a consolidação das capacidades – nesse caso, as cibernéticas – e fortalecendo ligações entre setor público e privado.

Ademais, a consolidação da capacidade cibernética depende da posse da base material, que é uma forma de poder econômico – esse, por sua vez, é espécie de *hard power*. Incluem-se aqui as infraestruturas que possibilitam o desenvolvimento do espaço cibernético – cabos submarinos, *data centers*, roteadores, semicondutores. Ainda que o ciberespaço seja um domínio relativamente novo, observam-se nele as mesmas dinâmicas de poder extrínsecas a ele. Recursos materiais continuam a ser fundamentais para o desenvolvimento de capacidades que podem ser utilizadas como meio de atingir objetivos do Estado.

Entretanto, construir capacidade não é simples. O ciberespaço é um domínio muito diferente dos outros, visto que nenhum país está completamente protegido de ameaças cibernéticas. Além disso, não se pode ignorar sua artificialidade, que confere notáveis vantagens aos que possuem as capacidades de moldá-lo. Muller (2015) pontua que novas maneiras de explorar recursos adversários surgem a todo momento, dada a rápida e constante evolução das tecnologias, e isso traz a necessidade de

vigilância permanente em busca de novas ameaças. Também adiciona que a evolução dessas ameaças é muito mais rápida do que a implementação de mecanismos para evitar incidentes cibernéticos. Complementa que o fortalecimento das capacidades estatais de segurança cibernética depende do fortalecimento de todos os elementos que contribuem para a segurança das redes internas. Isso inclui infraestruturas críticas e a implementação de políticas e estratégias de segurança cibernética, por exemplo: engloba tanto os aspectos materiais quanto estratégicos.

Além disso, é necessário que as estruturas de defesa cibernética estejam aptas a evitar não apenas ataques externos, mas também os domésticos, já que esses podem favorecer o enfraquecimento do ecossistema de segurança cibernética e, consequentemente, criar vulnerabilidades que serão aproveitadas por outros Estados. Assim, é crucial que se considerem os ambientes interno e externo ao projetar as prioridades estatais em termos de segurança cibernética.

Fica evidente, ao considerar os impactos da insegurança cibernética, que é fundamental buscar meios de garantir, o quanto possível, a segurança cibernética de forma holística e autônoma no ambiente doméstico, além de aprimorar capacidades de defesa cibernética contra ameaças externas. A existência de instituições internas consolidadas de segurança cibernética é requisito para que os Estados consigam ampliar o acesso a recursos de rede e outras tecnologias computacionais – consequentemente, inserindo-se de forma mais competitiva na economia internacional – sem criar novos desafios à segurança nacional.

Para implementar essas instituições, é essencial desenvolver mecanismos normativos e estratégicos que estabeleçam prioridades e diretrizes no processo de construção de capacidade, garantindo, assim, a continuação eficiente do processo. Entretanto, reconhecem-se desafios como o de conciliar liberdades individuais com o estabelecimento de instituições de segurança cibernética ao mesmo tempo em que se busca aumentar o acesso a esses recursos. Nesse sentido, Muller pontua que

> Um arcabouço legal funcional possibilita regular a governança, punir crimes e controlar a implementação no ciberespaço. No entanto, incluir o ciberespaço em um arcabouço legislativo é um desafio, inclusive no que diz respeito à amplitude do arcabouço e o número de regulamentações a se fazer. (Muller, 2015, p.12)

A estratégia nacional também deve considerar os comportamentos de outros Estados, observando ameaças e oportunidades (Devanny; Goldoni; Medeiros, 2022). Nota-se, dessa forma, que, apesar de o contexto cibernético ser relativamente novo, nele reproduzem-se as tradicionais questões sobre o papel do Estado desde a concepção das teorias políticas tradicionais.

Entretanto, para desenvolver políticas nacionais de segurança cibernética, faz-se necessário saber quais áreas devem ser enfatizadas e quais parâmetros serão utilizados para traçar objetivos pertinentes. Tendo em vista a crescente interconectividade das redes ao redor do globo, a segurança de recursos cruciais conectados a essas estruturas se torna mais difícil de garantir. Além disso, a segurança cibernética não compreende apenas fatores técnicos, como já visto, tornando urgente a necessidade de envolver mais políticas públicas e leis que, postas em prática, ajudem a manter a integridade dos recursos cibernéticos, tanto de forma proativa como reativa.

Considerando essas necessidades, diversas organizações internacionais e centros acadêmicos vêm desenvolvendo variados métodos e abordagens para mensurar e melhorar as capacidades cibernéticas dos Estados, utilizando-se de modelos e índices prescritivos e descritivos de mensuração e análise de maturidade de segurança cibernética (Pawlak, 2016). Ainda, leva-se em conta que mensurar capacidade cibernética é um desafio complexo e que necessita de abordagens multidisciplinares para ser superado. O desenvolvimento de índices internacionais busca, também, suprir essa lacuna.

As iniciativas de criar métodos de mensuração de capacidade cibernética se propõem como uma maneira de aumentar a eficiência na alocação de recursos, já escassos, para uma tarefa cada vez maior, uma vez que nem mesmo há consenso a respeito do conceito de capacidade cibernética e sobre quais são seus atributos. Além disso, “a amplitude do campo, dados não confiáveis e o rápido desenvolvimento do ciberespaço pode resultar na criação de abordagens e métodos insuficientes”, criando a necessidade de adaptação dos métodos existentes (Muller, 2015, p. 7). Contudo, não há abordagem única definida como a melhor para isso, o que faz com que o debate entre os criadores desses índices seja frutífero para avançar (Pawlak, 2016).

Muller (2015) enumera alguns dos primeiros esforços, dos quais poucos foram escolhidos para representar, no presente trabalho, a dificuldade de construir ferramentas que auxiliem não só na avaliação de maturidade de segurança cibernética, mas também ajudem os Estados a priorizarem setores deficientes, indicando quais melhorias fazer. Esses instrumentos foram alguns dos primeiros criados, de forma que não foram utilizados no trabalho para avaliar o Brasil por já haver opções mais desenvolvidas de fazê-lo.

Um primeiro exemplo é o *Cyber Index,* do Instituto das Nações Unidas para Pesquisa sobre o Desarmamento, cujo objetivo é analisar as capacidades cibernéticas estatais de forma individual. Embora seja uma forma de analisar de forma individualizada – e, portanto, mais detalhadamente – as capacidades estatais, esse modelo não permitia a comparação entre países e é inflexível para eventuais melhorias que um país viesse a fazer: não se buscava, à época, ter uma visão evolutiva do processo de construção de capacidade dos países, o que limita sua utilidade para analisar a evolução das infraestruturas relevantes ao longo do tempo. Dessa forma, fica evidente a importância da adaptabilidade, em termos temporais, dos modelos internacionais, sob pena de terem sua utilidade minada.

Outro modelo descrito pela autora é o *Cyber Readiness Index 1.0*, desenvolvido pelo *Belfer Center,* na Universidade de Harvard. O modelo em questão analisa 35 países integrados às tecnologias disruptivas e aplica uma metodologia objetiva, de cinco elementos, para investigar a maturidade de cada um deles, bem como o comprometimento de cada um com a melhoria das condições de segurança cibernética. Apesar do esforço interessante, a amostra desse índice é limitada, dado o número crescente de países totalmente conectados às redes. Isso dificulta a identificação de padrões globais de segurança cibernética.

A autora apresenta, ainda, o modelo de mensuração da Organização dos Estados Americanos (OEA), em conjunto com a União Internacional de Telecomunicações (UIT) e a Parceria Multilateral Internacional Contra Ameaças Cibernéticas, que mede as capacidades de segurança cibernética de seus Estados-membros por meio de exercícios organizados de ataques cibernéticos. Assim, os

Estados podem compreender, na prática, em quais recursos precisam melhorar com urgência.

O lado negativo dessa estratégia é a dificuldade de atingir o setor privado, considerando que, como já explorado no presente trabalho, o setor privado e a sociedade civil são cruciais para manter a integridade das estruturas de segurança cibernética. A partir desses exemplos, compreende-se a dificuldade da tarefa, posto que a mensuração contínua de capacidades e a comparação entre países pode facilitar a identificação de lacunas ou padrões de comportamento dos Estados que podem ser úteis como instrumento auxiliar na tomada de decisão.

A partir desses índices, percebe-se a variação nas metodologias e ênfases em cada índice de mensuração de capacidades. Alguns são mais voltados à sociedade, outros ao setor privado, além daqueles focados no setor público e mesmo em recursos de poder. No presente trabalho, sem desconsiderar os desafios inerentes à mensuração de capacidade, três índices internacionais de capacidade cibernética foram utilizados. Esses serão detalhados no próximo capítulo, juntamente com a aplicação de cada um ao caso brasileiro, mas cabe citá-los aqui: o *Cyber Security Capability Maturity Model* (CMM), da Universidade de Oxford; o *National Cyber Power Index (NCPI)*, do *Belfer Center for Science and International Affairs*, no âmbito da *Harvard Kennedy School*; e, por fim, o *National Cyber Security Index (NCSI),* da *e-Governance Academy,* organização sem fins lucrativos concebida, em conjunto, pelo governo estoniano, pelo *Open Science Institute* e pelo Programa das Nações Unidas para o Desenvolvimento.

3.4 CONCLUSÕES DO CAPÍTULO

Este capítulo abordou conceitos fundamentais para o entendimento do ciberespaço como um espaço de projeção de poder para atingir os resultados preferíveis do Estado. A assimilação da terminologia pertinente e reflexão sobre o progresso do debate sobre capacidade cibernética se fez crucial para justificar a importância de discutir o progresso das capacidades cibernéticas no Brasil. O objetivo específico cumprido neste capítulo foi apresentar o conceito de capacidade cibernética e situar a segurança cibernética no contexto das relações internacionais como pré-requisito para desenvolvimento estatal, segurança e projeção de influência.

Ademais, buscou-se explorar a evolução do ciberespaço e sua importância crescente no cenário internacional. Destacou-se o modo como o ciberespaço desafia conceitos tradicionais, como soberania, fronteira e a relação entre Estado, entes subnacionais e indivíduos. Além disso, empreendeu-se contextualização do objeto de pesquisa como instrumento de poder brando e poder duro, uma vez que ele atinge aspectos políticos, militares e econômicos.

Outrossim, tratou-se da capacidade cibernética como parte essencial do poder a partir da Terceira Revolução Industrial, uma vez que as diversas funções estatais, bem como os processos produtivos, vêm sendo transportados para esse domínio – esses últimos, intrinsecamente relacionados à inserção internacional. Reconhece-se que a capacidade cibernética não se concretiza apenas pela capacidade de defender sistemas internos por meios computacionais. A construção de capacidade cibernética deve passar, necessariamente, pela posse de uma base material que permita que o Estado não dependa de redes externas e produza material necessário para o aprofundamento da Transformação Digital em território nacional. No capítulo seguinte, busca-se expor um histórico das capacidades cibernéticas brasileiras, além de tentativas de mensuração dessas capacidades por meio de índices internacionais.

4 CAPACIDADES CIBERNÉTICAS BRASILEIRAS: PANORAMA ATUAL E DESAFIOS

No presente capítulo, expõe-se um panorama do desenvolvimento das capacidades cibernéticas brasileiras. Em seguida, analisam-se as mensurações da capacidade cibernética brasileira realizadas por três modelos internacionais: o Modelo de Maturidade de Capacidade de Segurança Cibernética de Oxford (CMM), o *National Cyber Power Index* (NCPI) e o *National Cyber Security Index* (NCSI). Assim, busca-se compreender o estado atual das capacidades cibernéticas brasileiras.

4.1 CAPACIDADE CIBERNÉTICA BRASILEIRA: BREVE HISTÓRICO E PANORAMA DO DESENVOLVIMENTO

Nesta subseção, busca-se expor brevemente o histórico da construção de capacidades cibernéticas e recursos digitais no Brasil. O país, desde a década de 1990, tem se mostrado relativamene rápido na implementação das tecnologias da informação e comunicação. Diplomaticamente, tem buscado se projetar, há mais de uma década, como ator relevante no contexto da governança da internet em âmbito regional e global (Lobato, 2017). Nesse contexto, o país passa a se preocupar com o aprimoramento da segurança cibernética nacional, principalmente, a partir dos anos 2000.

Hurel (2021) destaca que o desenvolvimento dos recursos institucionais de segurança de redes e informação foi continuamente consistente em áreas ligadas ao sistema de inteligência brasileiro e à governança da internet. Órgãos específicos para o tema foram criados entre 1995 e 2005, como o Comitê Gestor da Internet (CGI), o Núcleo de Coordenação do ponto BR (NIC.br) e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br).

A disposição brasileira a aderir ao processo de digitalização já se fazia presente na década de 1990. Com as políticas de privatização observadas nesse período, surgiram vários provedores de acesso à internet, concomitantemente à ampliação do acesso mundial às redes e à telefonia móvel (Borne; Canabarro, 2013).

Todavia, a intensificação do uso dessas ferramentas não foi adequadamente seguida de políticas de segurança cibernética eficazes. Obstáculos notáveis para fornecer segurança digital são relacionados à falta de planejamento: os documentos que tratavam sobre o tema eram pouco articulados entre si e, até dezembro de 2023, não estavam ligados a uma política nacional formal de segurança cibernética (Hurel, 2021). Exemplo disso é que, por cinco anos a partir de sua instituição, a Política Nacional de Segurança da Informação, que dispõe sobre a governança da segurança da informação no âmbito da Administração Pública Federal, também compreendia a segurança cibernética, não havendo política própria para essa última.

Cabe aqui distinguir os dois conceitos. Segundo o Glossário de Segurança da Informação, segurança cibernética diz respeito a “ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis”. Por sua vez, o conceito de segurança da informação se refere a “ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações” (Brasil, 2021). Embora os dois conceitos estejam intrinsecamente relacionados, cada um possui seu próprio escopo, de forma que a articulação dos dois em um instrumento único pode comprometer sua implementação.

Outro desafio é o cibercrime, com o qual o Brasil sofre muito por ser grande usuário de recursos digitais e das redes (Instituto Igarapé, 2021). A implementação de meios eficazes para conter o crime cibernético é primordial para a manutenção da segurança cibernética, que, por sua vez, é um dos pilares da capacidade cibernética. Apesar disso, as primeiras leis específicas para esse tipo de crime só foram implementadas a partir de 2012 (PJERJ, 2019). Esse cenário tem se modificado conforme mais leis específicas para o cibercrime são instituídas, tipificando comportamentos antes não previstos. Além disso, iniciativas como o estabelecimento de delegacias especializadas e de centros de defesa cibernética em instituições da Administração Pública também representam avanços. Espera-se que evolua mais com a publicação do Decreto 11.856/2023, que institui a Política Nacional de

Cibersegurança e tem como um dos objetivos contribuir para o combate do cibercrime (Safernet, 2023; Brasil, 2023).

Contudo, a inicial falta de estratégia não se confunde com a ausência de esforços para desenvolver capacidades de segurança cibernética no Brasil. Aqui, cabe citar a Política Nacional de Defesa, instituída pelo Decreto n.º 5.484/2005, e a Estratégia Nacional de Defesa, aprovada pelo Decreto n.º 6.703/2008, que traziam a segurança cibernética em suas disposições num contexto em que outros países começavam a se atentar a essa questão. A Convenção de Budapeste fora estabelecida quatro anos antes, e os ataques cibernéticos à Estônia em 2007 culminariam na publicação do Manual de Tallinn em 2013 (Schmitt, 2013; Council Of Europe, 2001). Não se pode dizer, portanto, que o Brasil começou o desenvolvimento de capacidades de segurança cibernética tardiamente em relação a seus pares.

Oliveira (2020) destaca que o marco de institucionalização da defesa cibernética, no Brasil, deu-se com a criação da Estratégia Nacional de Defesa (END), em 2008, em que o domínio cibernético foi definido como setor estratégico para a Política Nacional de Defesa (PND) de 2005. Nos documentos estratégicos que se seguiram, o ciberespaço adquiriu, progressivamente, mais destaque. Mais tarde, a criação de órgãos, como o Centro de Defesa Cibernética (CDCiber), no âmbito do exército, que atuou na proteção dos eventos de grande porte ocorridos entre 2012 e 2016. Os megaeventos, juntamente com o caso Snowden – em que foram vazadas informações confidenciais sobre o monitoramento, pelo governo dos Estados Unidos, de diversos países, inclusive de conversas da então presidente Dilma Rousseff – suscitaram maior discussão a respeito da necessidade de garantir a proteção a infraestruturas cibernéticas brasileiras (Borne; Canabarro, 2013; Oliveira, 2020).

Contudo, há dúvidas sobre a eficiência das respostas brasileiras à questão da segurança cibernética. Borne e Canabarro (2013) argumentam que, inicialmente, a arquitetura de segurança cibernética do Brasil estabelecia competências claras para cada ator num campo que é, por natureza, mal definido. Por exemplo, os autores citam a Polícia Federal como agente responsável por cuidar da criminalidade comum e o exército como responsável por preparar para a guerra cibernética. Todavia, essa atribuição de responsabilidades não fica clara, uma vez que é difícil identificar os

autores e as origens de crimes cibernéticos, além de também ser possível que outros países contratem cibercriminosos. Isso pode dificultar a determinação do órgão competente para atuar em certas situações. Tal característica demonstra, mais uma vez, a natureza transcendental do espaço cibernético, em que a atuação dos diversos atores se confunde. A segurança desse domínio depende dessa ação conjunta, suscitando a necessidade de operações interagência – a exemplo da Operação Ágata[5]. Entretanto, a segurança cibernética exige iniciativa permanente; dessa forma, resta o Instituto do Consórcio. Aqui importa retomar a relevância dos instrumentos administrativos que possibilitam a criação de novos órgãos ou a atribuição de novas responsabilidades a órgãos já existentes.

Porém, apesar das lacunas existentes, o surgimento de instituições de segurança cibernética demonstra que o Brasil está atento à urgência do tema. Isso é visível no aparato de segurança cibernética do Brasil, que segue a abordagem adotada por outros países – a título de exemplo, o COMDCiber, semelhante ao *U.S. Cyber Command*, evidencia essa preocupação, apesar da diferença entre os contextos dos dois países e do orçamento disponibilizado a cada um deles (Devanny; Goldoni; Medeiros, 2022).

Diniz, Glenny e Muggah (2014) argumentam que essa abordagem não faria sentido para o Brasil, visto que as principais ameaças à segurança nacional não viriam, diretamente, de um ator externo, mas do próprio cibercrime (Diniz; Glenny; Muggah, 2014). Entretanto, o domínio cibernético e sua natureza global suscitam a necessidade de uma abordagem integrada para seu desenvolvimento. Considerando que um ataque poderia vir de qualquer lugar do mundo, as capacidades cibernéticas para os diversos contextos devem ser construídas em conjunto, não negligenciando um setor em favor do outro. Além disso, capacidades cibernéticas ofensivas e defensivas são importantes para os Estados responderem a ataques no próprio ciberespaço, reduzindo o risco de agravar conflitos e, ao mesmo tempo, mostrando descontentamento (Maness;

[5] A Operação Ágata, iniciada em 2011, é uma ação coordenada pelo Estado-Maior Conjunto das Forças Armadas (EMCFA) para fortalecer a segurança das fronteiras terrestres do Brasil, totalizando cerca de 17 mil quilômetros. Essa operação visa prevenir e reprimir atividades criminosas ao longo das fronteiras com os dez países sul-americanos. A Ágata envolve a colaboração de 12 ministérios e 20 agências governamentais, promovendo uma abordagem integrada e coordenação entre as Forças Armadas e os agentes de segurança pública em âmbitos federal, estadual e municipal (Brasil, 2013).

Valeriano, 2018; Devanny; Goldoni; Medeiros, 2022). Dessa forma, o desafio é encontrar uma forma de articular os agentes, considerando o contexto brasileiro, de modo que seja possível construir capacidades de segurança cibernética tanto para as Forças Armadas quanto para a Administração Pública e o setor privado.

Nesse sentido, a partir de 2018, evidencia-se um compromisso crescente com o estabelecimento de diretrizes para o desenvolvimento integrado das capacidades cibernéticas do Brasil. Esse esforço se iniciou com a instituição da Política Nacional de Segurança da Informação (PNSI) pelo Decreto n.º 9637/2018, que revogou a antiga Política de Segurança da Informação da Administração Pública Federal e ampliou seu escopo original para incluir temas de segurança cibernética (Brasil, 2018b). Posteriormente, a PNSI abarcaria apenas o âmbito da defesa cibernética e a Política Nacional de Cibersegurança (PNDCiber) seria responsável pela segurança cibernética.

Embora esse documento seja a primeira tentativa de incluir a segurança cibernética em forma de estratégia nacional, já havia legislação correlata. A título de exemplo, tem-se a Política Nacional de Segurança de Infraestruturas Críticas (Decreto n.º 9.573/2018) e a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) (Brasil, 2018a; Brasil, 2018c).

Nos anos que se seguiram, outros instrumentos político-estratégicos foram publicados, notadamente a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC) no Decreto n.º 10.569/2020, o Plano Nacional de Segurança de Infraestruturas Críticas (PNSIC) com o Decreto n.º 11.200/2022 e a Estratégia Nacional de Segurança Cibernética (E-Ciber) com o Decreto n.º 10.222/2020 (Brasil, 2020b; Brasil, 2022; Brasil, 2020a). O esforço de elaborar um projeto nacional de construção de capacidades cibernéticas culmina na publicação da PNDCiber, que se apresenta como iniciativa responsável por orientar o aprimoramento da segurança cibernética no país.

Se o arcabouço político-estratégico vem evoluindo, cabe analisar o desenvolvimento material das capacidades cibernéticas. Nesse sentido, interessa discutir as capacidades cibernéticas do ponto de vista material. Aqui cabe o conceito de Centro de Decisão Econômica, descrito por Celso Furtado como a capacidade de centralizar as decisões sobre atividade econômica no próprio território, incluindo a

posse de tecnologias fundamentais de cada ciclo econômico. Isso permite que o Estado controle internamente a produção e o mercado, tornando-se autossuficiente (Furtado, 1962). No caso da cibernética, o Centro de Decisão Econômica se baseia nos chips, cuja produção depende dos chips e da fibra óptica, primordialmente.

Filippin (2020) aponta que o Brasil possui longo histórico de iniciativas voltadas à indústria de semicondutores no país. As primeiras iniciativas brasileiras de incentivo a essa indústria datam da década de 1970, com a criação do Laboratório de Microeletrônica (LME) da Universidade de São Paulo (USP) em 1968. A autora também cita a experiência da Transit, o primeiro empreendimento brasileiro em semicondutores. Pretendia-se produzir chips com tecnologia nacional desenvolvida no âmbito do LME da USP. A Transit dominou a técnica de difusão do silício em escala industrial, crucial para a produção dos chips, mas suas operações só duraram dois anos. Por fim, a indústria de chips entrou na pauta governamental novamente nos anos 2000, quando o governo avaliou que ela era a lacuna do complexo eletrônico que mais afetava a competitividade da indústria brasileira.

Em 2007, por meio da Lei nº 11.484, o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores foi instituído com objetivo de promover a ampliação desse mercado, fomentando o desenvolvimento nacional de chips e favorecendo as exportações de componentes estratégicos (Brasil, 2007). O programa estabelecia isenção da alíquota do imposto de importação a fim de diminuir custos para adquirir insumos para produzir circuitos integrados e teria vigência até 2022.

Ainda sobre a indústria de semicondutores, há de se mencionar a CEITEC S.A., uma empresa pública criada para a produção de semicondutores – a única na América Latina capaz de realizar todas as etapas de produção do chip. A indústria brasileira, todavia, ainda é incipiente. Em 2021, o Brasil registrou um consumo de semicondutores avaliado em cerca de US$11 bilhões; contudo, apenas 8% dessa demanda foi suprida por empresas nacionais do setor (IPEA, 2023). O saldo da balança comercial brasileira, no setor de eletrônica, é consistentemente negativo, e o déficit vem aumentando (ABINEE, 2023; Peters, 2022). Outro indício das lacunas na indústria brasileira de chips foi o anúncio da liquidação e privatização da CEITEC em 2020. Contudo, o processo foi

interrompido pelo Tribunal de Contas da União (TCU) e a empresa agora se encontra excluída do Programa Nacional de Desestatização (Brasil, 2021b; Brasil, 2023aa)

Evidencia-se, aqui, a relevância de constituir uma indústria nacional que consiga suportar a demanda de um processo de transformação digital inserido na Terceira e na Quarta Revolução Industrial. Atualmente, há o Plano Brasil de Semicondutores, cujos objetivos são aumentar a participação do Brasil no mercado mundial de semicondutores de 2% para 4%, num prazo de até vinte anos. O plano ainda está por ser lançado (ABISEMI, 2022).

Portanto, observa-se que o Brasil, ao longo dos anos, vem progredindo no desenvolvimento de capacidades cibernéticas, ainda que de forma relativamente lenta. Na próxima seção, serão analisados os indicadores de segurança cibernética propostos por índices internacionais a fim de compará-los, criticá-los e obter uma visão própria a respeito dos obstáculos e avanços na construção de capacidade cibernética brasileira.

4.2 MENSURAÇÃO DA CAPACIDADE CIBERNÉTICA BRASILEIRA

Expostos os principais conceitos da cibernética e um breve histórico da capacidade cibernética brasileira, busca-se, nesta seção, investigar os indicadores de aspectos fundamentais da maturidade de infraestruturas do país no ciberespaço por meio de índices internacionais de segurança cibernética.

Aqui cabe apresentar a contribuição de Robert Cox: “toda teoria serve a alguém e a algum propósito” (Cox, 1981, p. 128). O autor defende que todas as teorias têm perspectivas, derivadas de uma posição no tempo e no espaço social e político. Essa constatação importa quanto aos índices porque esses possuem interpretações que derivam de uma posição de poder no tocante à segurança cibernética – interpretações essas que refletem nas análises.

Desde logo, cumpre notar que todos os modelos apresentados no trabalho são restritivos e tratam a segurança cibernética exclusivamente no âmbito do *software*. Essa delimitação não engloba o espaço cibernético em sua totalidade, conforme a definição adotada por este trabalho. Cabe retomar que o ciberespaço é entendido aqui como composto de dois âmbitos: o virtual, que diz respeito à esfera do *software*, e o físico, que se refere ao *hardware* e à infraestrutura física necessária para garantir o

funcionamento do ciberespaço – os cabos submarinos e chips. Ou seja, segurança cibernética também envolve prover meios de garantir esse acesso de forma autônoma. Conforme Cox, toda teoria adota uma visão de mundo

> "a partir de um ponto de vista definível em termos de nação ou classe social, de dominação ou subordinação, de poder ascendente ou declinante, de uma sensação de imobilidade ou de crise presente, de experiência e de expectativas e esperanças para o futuro" (COX, 1981, p. 128).

Ao excluir a segurança da esfera física do ciberespaço dos relatórios, os índices adotam uma perspectiva pertencente a uma posição dominante. Desconsideram, então, que os quesitos de segurança cibernética analisados por eles dependem da autonomia que necessariamente vem da posse do centro de decisão econômica.

Considerando disso, cabe recorrer também à contribuição de Bresser-Pereira sobre a importação de instituições: deve ocorrer cautelosamente, adaptando as instituições à realidade nacional, uma vez que uma instituição criada em determinado contexto nacional não se adaptará automaticamente a contextos diferentes (Bresser-Pereira, 2004). Isso é especialmente verdadeiro quando se trata de países com níveis diferentes de influência. A seguir, cabe analisar os relatórios dos índices internacionais de segurança cibernética a respeito do Brasil.

4.2.1 Modelo de Maturidade de Capacidade de Segurança Cibernética

O primeiro índice utilizado para mensurar a capacidade cibernética brasileira é o Modelo de Maturidade de Capacidade de Cibersegurança (CMM), desenvolvido no âmbito da Universidade de Oxford. Os resultados para o Brasil são expostos no relatório intitulado Revisão da Capacidade de Cibersegurança para o Brasil, e a pesquisa inicial foi realizada entre 2018 e 2020 (GCSCC, 2020).

Antes de abordar a análise feita do caso brasileiro, cumpre expor, brevemente, a metodologia utilizada pelo índice. O CMM trata a segurança cibernética por uma visão que se pretende holística. Isso é feito em cinco dimensões: política e estratégia de segurança cibernética; cultura e sociedade; capacitação e recursos humanos em segurança cibernética; criação de mecanismos legais; e, por fim, padrões técnicos e organizacionais para controle e mitigação de riscos (GCSCC, 2020). O índice utiliza metodologia de grupo focal, semelhante a entrevistas: os pesquisadores são responsáveis por facilitar discussões em grupos compostos por especialistas em

setores correspondentes às dimensões do índice. Com base nas respostas obtidas e nas evidências coletadas, cada dimensão é classificada em um de cinco níveis progressivos: (1) iniciante, (2) formativo, (3) consolidado, (4) estratégico e (5) dinâmico.

O iniciante é o estágio em que não existem ou existem pouquíssimos recursos para lidar com ameaças e desafios cibernéticos. O nível formativo possui estruturas específicas, ainda que descentralizadas e pouco funcionais. O nível consolidado possui instituições funcionais, mas não há priorização de objetivos e alocação eficiente de recursos. O nível estratégico, por sua vez, é aquele em que há priorização, mas ainda não se consegue alocar recursos de forma ágil. O nível dinâmico, por fim, é aquele no qual existem indicadores funcionais do estado da segurança cibernética, sendo possível alocar recursos de acordo com prioridades dinâmicas, que mudam conforme avaliação constante.

No momento da pesquisa inicial sobre o Brasil foi feita, não havia documento nacional que explicitasse, sistematicamente, os objetivos brasileiros de segurança cibernética. Contudo, em 2020, quando das atualizações concedidas pelo Governo Federal, o cenário já não era o mesmo, uma vez que a E-ciber já havia sido publicada. Por ser conduzido em conjunto com os governos dos países que requisitam a análise de suas capacidades cibernéticas de forma holística, é o mais detalhado relatório encontrado para o presente trabalho.

O modelo avalia a dimensão política e estratégica do Brasil como situada entre os estados formativo e consolidado. Cita a existência de documentos que estabelecem diretrizes de segurança cibernética, mas os considera pouco claros. Destaca a necessidade de orientações mais claras, metas definidas e inclusão abrangente da sociedade, incluindo parcerias público-privadas. Aponta que há vários documentos relacionados à defesa cibernética nacional, mas menos quando se trata de direitos individuais no ciberespaço. Exemplos desses últimos incluem o Marco Civil da Internet e a Lei de Crimes Cibernéticos, assim como a Lei Geral de Proteção de Dados (Brasil, 2014; Brasil, 2012; Brasil, 2018c).

Quanto à capacidade de resposta a incidentes, destaca a existência de várias Equipes de Resposta a Incidentes de Segurança Cibernética (CSIRTs) descentralizadas, público e privadas, com legislação que busca facilitar o

compartilhamento de informações e ameaças. Aponta o desafio de melhorar o tempo de resposta desde a detecção do incidente até a ação como uma área a ser aprimorada.

O relatório classifica o estágio de maturidade do Brasil em relação à proteção de infraestruturas críticas como consolidado, mas aponta para variações na capacidade de defesa dessas infraestruturas entre os setores público e privado. Destaca-se que o setor privado não é considerado parte integrante da estratégia nacional de defesa cibernética. Proteger o setor privado importa porque ataques a ele também podem afetar o setor público, mesmo que esse esteja protegido.

Entretanto, a estratégia vigente não só reconhece a relevância do setor privado para sua concretização, como também estabelece objetivos e ações voltadas à integração de empresas privadas à arquitetura de segurança cibernética do país. Isso pode ser visto em várias seções no documento, das quais se destacam algumas ações estratégicas que mencionam expressamente o setor privado: estabelecer fóruns de governança, controle de tratamento de informações, requisitos mínimos de segurança cibernética e padrões de desenvolvimento de produtos, compartilhamento de informações sobre incidentes e vulnerabilidades; v) exercícios cibernéticos com múltiplos atores, entre outros (Brasil, 2020a). Portanto, não há deliberada exclusão do setor privado na estratégia formal vigente.

Além disso, aponta que as capacidades e recursos cibernéticos na Administração Pública variam significativamente devido à falta de mecanismos para garantir a aplicação uniforme de políticas, falta de conhecimento especializado, financiamento inadequado e ausência de responsabilização e métricas para avaliar a conformidade (GCSCC, 2020).

Também se aponta que o governo não consegue identificar, eficientemente, as lacunas de maturidade de capacidade cibernética. A população enfrenta dificuldades em seguir boas práticas e se proteger de ataques cibernéticos, resultando em prejuízos para empresas e indivíduos, além da ausência de uma cultura de denúncia de crimes cibernéticos, levando muitos casos a ficarem sem resolução. Quanto a isso, cabe retomar o relativo ineditismo do tema, posto que se trata de uma realidade ainda emergente. A velocidade da transição que abrange a crescente capacidade

computacional e o desenvolvimento da inteligência artificial implica, naturalmente, a dificuldade de adaptação da sociedade civil de forma simultânea.

Em relação à segurança de serviços digitais, o relatório indica a falta de sistematização na detecção de violações em serviços governamentais online e escassez de profissionais especializados. As autoridades policiais enfrentam desafios relacionados à falta de recursos técnicos e financeiros, bem como à carência de sistematização na coleta de informações e evidências cibernéticas.

Outro ponto que o índice apresenta como lacuna é a diminuta cooperação internacional. Entretanto, é crucial notar que a cooperação não gera capacidade. Cumpre retomar as desvantagens da cooperação e a desconfiança quanto a um sistema global de governança da segurança cibernética. Um sistema como esse apenas favoreceria a projeção de influência dos Estados que já possuem capacidades consolidadas. Essa relevância se explica por uma possível preocupação dos Estados com os ganhos relativos provenientes da cooperação num cenário de transformação digital que conduzirá as próximas Revoluções Industriais e ditará a distribuição de poder no sistema internacional.

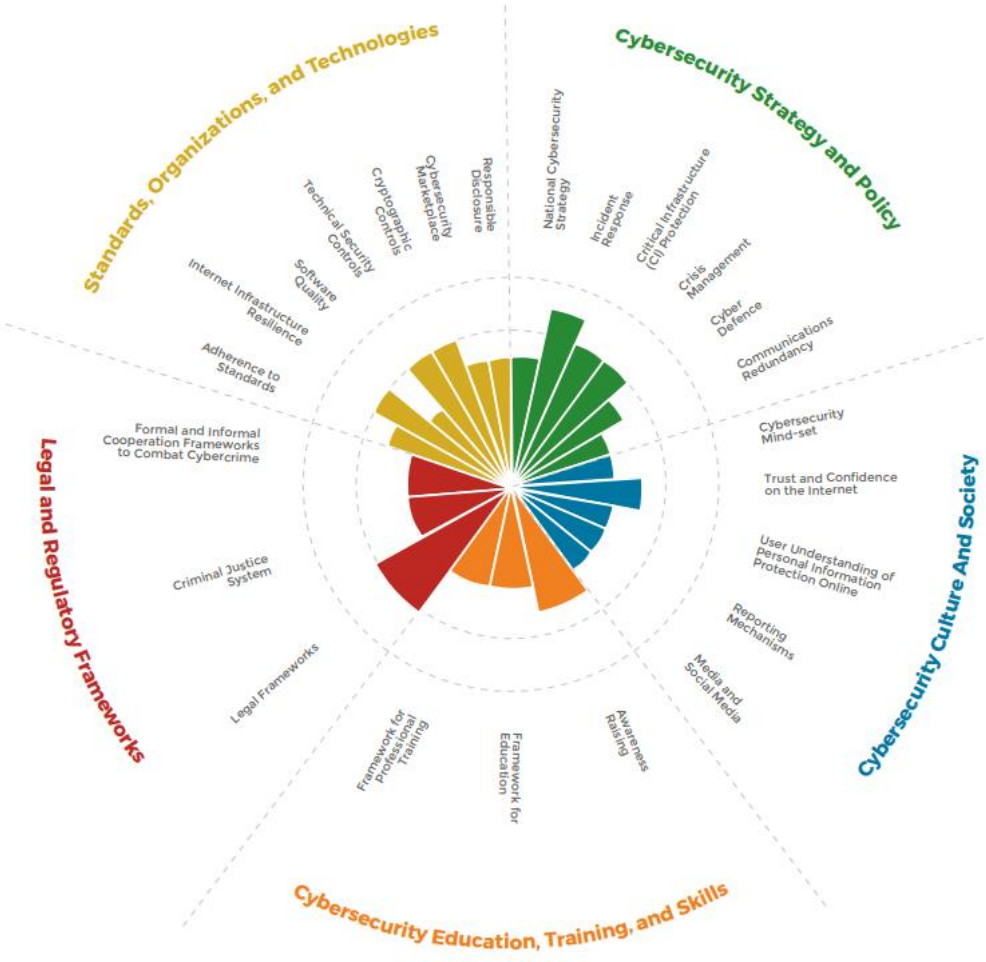
Aqui se questiona a cooperação internacional – em especial, aquela voltada ao estabelecimento de instituições internacionais – para a construção de capacidade. A adesão aos instrumentos cooperativos existentes representa a adesão a uma perspectiva cuja ênfase está, quase exclusivamente, na esfera virtual, que não gera capacidade se não aliada a uma base material para aumentar a competitividade e autonomia da indústria estatal. Cabe retomar a ideia de que toda teoria cumpre um objetivo. O reconhecimento da base material como elemento gerador de capacidade seria estímulo ao desenvolvimento de produtos essenciais para garantir autonomia produtiva de equipamentos e infraestruturas cruciais para o aprofundamento da Transformação Digital. Atualmente, poucos são os países que possuem capacidade de produzir essa base material – chips e fibra óptica – em escala, e esses ocupam uma posição de poder em relação aos outros, confinados à importação desses recursos.

Em geral, como se vê na Figura 1, o CMM considera que as dimensões com desenvolvimentos mais consistentes em segurança cibernética são a político-estratégica e a tecnológica-organizacional (no gráfico, respectivamente, em verde e em

amarelo). No primeiro item, entretanto, relata que a estratégia ainda é insuficiente. A dimensão tecnológica-organizacional, por sua vez, tem natureza técnica: diz respeito à adesão do país a padrões internacionais, resiliência da infraestrutura digital, qualidade de *software*, entre outros recursos específicos e fundamentais para o bom desenvolvimento da área. A dimensão regulatória da segurança cibernética no Brasil também se destaca nesse modelo: as leis relacionadas ao cibercrime estariam bem elaboradas, mas a implementação da legislação é apontada como uma área que precisa de atenção, e os esforços de treinamento e conscientização estão em fase de desenvolvimento.

De forma geral, o índice conclui que o país possui condições de aprimorar capacidades cibernéticas, mas precisa preencher lacunas que permitam o desenrolar do processo (GCSCC, 2020). Percebe-se, também, que o principal desafio observado pelo CMM é a implementação eficaz das leis e das diretrizes estratégicas elaboradas, além da conscientização da população.

Figura 1 - Representação geral da segurança cibernética no Brasil



Fonte: GCSCC (2020)

4.2.2 National Cyber Power Index

Outro índice que propõe uma visão a respeito das capacidades cibernéticas do Brasil é o *National Cyber Power Index* (NCPI), do *Belfer Center for Science and International Affairs*, no âmbito da *Harvard Kennedy School*. A última edição foi publicada em 2022. Embora esse modelo não disponibilize relatórios individuais de cada país, como o CMM, ele elabora *rankings* comparativos de 30 países com maior projeção de poder cibernético, com auxílio de fontes de dados externas de capacidade cibernética.

O *National Cyber Power Index* tem uma premissa diferente dos demais: aferir o poder cibernético. Nesse modelo, poder cibernético é descrito como a capacidade de

utilizar meios cibernéticos para atingir objetivos nacionais (Cassidy; Hemani; Voo, 2022). Medem-se estratégias, capacidades ofensivas e defensivas, alocação de recursos e capacidades de os Estados tomarem ações que para alcançar determinados resultados.

O índice busca determinar se o Estado consegue i) identificar e monitorar ameaças cibernéticas internas; ii) defender-se e desenvolver capacidades defensivas no ciberespaço, incluindo a habilidade de realizar operações defensivas, proteger infraestrutura e educar a população sobre riscos existentes; iii) controlar informação, inclusive propaganda governamental, dentro e fora do território, construindo uma narrativa que atenda aos interesses nacionais; iv) obter informações confidenciais de rivais por meio de elementos cibernéticos em prol do interesse nacional; v) desenvolver a indústria nacional de tecnologia ou outras indústrias nacionais por meios cibernéticos, utilizando-se de meios legais, como pesquisa e desenvolvimento de recursos humanos, ou meios ilegais, como espionagem para facilitar transferência de tecnologia – o índice não discute a abrangência do que define como indústria nacional de tecnologia; vi) destruir infraestruturas críticas de adversários; vii) definir normas internacionais e padrões técnicos para segurança cibernética; vii) extrair riqueza, inclusive por meio de operações agressivas, como ataques a instituições financeiras.

A coleta de dados vem primordialmente de duas fontes: o Cyber Operations Tracker, pelo Council of Foreign Relations, e do banco de dados de incidentes significativos do Centro de Estudos Estratégicos e Internacionais (CSIS). O índice procurar mensurar a intenção, por parte de cada Estado, de alcançar objetivos relativos aos indicadores escolhidos pelo modelo e, portanto, tornar-se uma potência cibernética. Por exemplo, se determinada área é menos desenvolvida, depreende-se que o Estado não atribui a ela prioridade (Cassidy; Hemani; Voo, 2022). Dessa forma, observam-se tanto as capacidades do país, distribuídas em oito objetivos, quanto sua intenção de desenvolvê-las.

Os objetivos de poder cibernético descritos pelo índice são oito: i) vigilância e monitoramento de grupos domésticos; ii) fortalecimento e aprimoramento das defesas nacionais cibernéticas; iii) controle e manipulação do ambiente de informações; iv) coleta de inteligência estrangeira para segurança nacional; v) crescimento da

competência nacional em segurança cibernética e tecnologia comercial; vi) destruição ou desabilitação da infraestrutura e capacidades de um adversário; vii) definição de normas e padrões técnicos cibernéticos internacionais; viii) acúmulo de riqueza e/ou extração de criptomoedas.

O Brasil, na edição de 2022, encontrava-se na trigésima posição geral em termos de poder cibernético. Conforme esse modelo, os aspectos mais avançados são os de defesa e de vigilância de grupos internos. Os elementos menos desenvolvidos para aquisição de poder cibernético são os de aquisição de riqueza, o de comércio e o de influência sobre o estabelecimento de normas internacionais. Praticamente não há intenção de desenvolver a capacidade de aquisição de riqueza por meios cibernéticos, conforme o modelo.

Aqui cabe ressaltar a delicadeza desse último tópico, posto que o modelo enquadra a aquisição de riqueza, principalmente, na extração de riqueza e criptomoedas. Esse quesito possui desafios próprios: a regulamentação das criptomoedas é recente e o assunto é complexo, de forma que a população não compreende plenamente o funcionamento dos criptoativos. Isso abre espaço para atividade ilegal envolvendo esses bens virtuais – a própria definição do NCPI de aquisição de criptomoedas enfatiza meios agressivos e ilegais no Brasil – a título de exemplo, o índice cita ataques do tipo *ransomware* e chantagem envolvendo informação obtida em vazamentos de dados.

Os outros três objetivos (inteligência, capacidade ofensiva e controle de informação) foram avaliados com notas baixas e muito aproximadas. A análise desse modelo argumenta, dessa forma, que o país não possui capacidades ofensivas significativas no ciberespaço – talvez por não ter interesse em se portar de forma potencialmente agressiva frente aos vizinhos, dado o tradicional posicionamento mediador do Brasil (Lobato, 2017).

O NCPI, ainda, considera a habilidade de vigilância de grupos internos relativamente avançada, tendo o Brasil uma nota de aproximados 40 pontos, do total de 100, no quesito capacidade de vigilância interna. Por outro lado, 40% de aproveitamento ainda é menos da metade dos pontos possíveis, o que indica que,

segundo esse modelo, mesmo as capacidades mais avançadas do país são insuficientes.

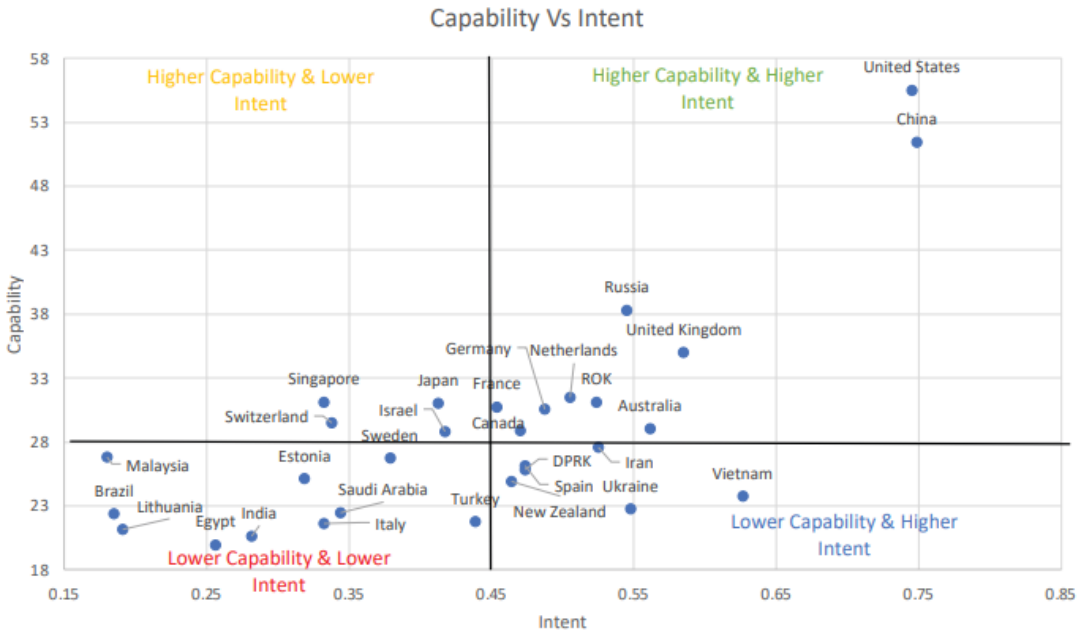
No que diz respeito à intenção de desenvolver capacidades, o índice indica que as prioridades do Brasil parecem ser o desenvolvimento de mecanismos de defesa, da indústria tecnológica e da capacidade de influenciar normas e padrões internacionais relativos à cibernética. Por não disponibilizar relatórios individuais, o índice não especifica a que se refere essa indústria, o que impossibilita análise detalhada. Contudo, o presente trabalho identifica os chips e a fibra óptica como principais elementos materiais da indústria tecnológica. Essa última, apesar de ter igual ou maior importância, será abordada de forma mais detalhada em trabalhos futuros. Essas prioridades estão de acordo com o que se viu na literatura até aqui, uma vez que o Brasil possui iniciativas para se projetar internacionalmente pelo tema do ciberespaço. Também vem modernizando seu ecossistema digital, além de buscar o desenvolvimento da defesa cibernética nacional.

O avanço da indústria tecnológica nacional também parece corresponder ao que é indicado por esse modelo. De fato, a indústria brasileira possui lacunas quanto à base material do ciberespaço. No entanto, como já exposto neste trabalho, possui programas de incentivo a essa indústria, além da única empresa pública produtora de semicondutores na América Latina, a CEITEC S.A., demonstrando seu progresso frente aos vizinhos. Portanto, o que o modelo indica é correto: esse setor é pouco desenvolvido, mas o progresso é promissor.

Em geral, o NCPI considera o Brasil um país de baixas capacidades cibernéticas e poucas intenções de tornar-se uma potência cibernética. Esse índice desconsidera, entretanto, que o poder cibernético está inserido num contexto mais amplo de transição tecnológica que vem alterando e continuará a alterar as relações sociais, econômicas e políticas. Dessa forma, enquanto semiperiferia, é urgente que o Brasil desenvolva os recursos necessários para se posicionar no ciberespaço e operar eficientemente nesse domínio. Dados os recentes desenvolvimentos normativo-estratégicos do país, compreende-se neste trabalho que o país está ciente dessa necessidade e busca superar os desafios que enfrenta. Resta saber se ocorrerá a materialização da

estratégia em sua forma material, o que depende de iniciativas que transcendem a esfera formal.

Figura 2 - Gráfico de dispersão de capacidade versus intenção



Fonte: Cassidy; Hemani; Voo (2022)

4.2.3 National Cyber Security Index

O terceiro e último índice utilizado é o *National Cyber Security Index* (NCSI), da e-Governance Academy em parceria com o governo estoniano, com o *Open Science Institute* e com o PNUD. O Brasil ocupa o 71º lugar nesse índice, e a última análise foi feita em agosto de 2022 (EGA, 2022). Esse modelo se propõe a medir a preparação dos países no que tange à prevenção de ameaças cibernéticas e gestão de incidentes. O NCSI é também uma base de dados com materiais disponíveis ao público e uma ferramenta para o reforço da capacidade nacional em matéria de segurança cibernética.

Os indicadores desse índice foram desenvolvidos com base em três tipos principais de ameaças cibernéticas: ataques de negação de serviço (impossibilidade de acessar serviços cruciais online), comprometimento da integridade de dados (modificação não autorizada de dados) e quebra da confidencialidade de dados. Para

esse índice, segurança cibernética indica proteção contra essas três categorias de ameaça.

A partir disso, o índice foi desenvolvido em cinco passos, sendo eles i) a identificação de ameaças cibernéticas a nível nacional e avaliação de capacidades de segurança cibernética; ii) seleção de aspectos importantes e mensuráveis de segurança cibernética – se há legislação específica, instituições, cooperação entre organizações (como grupos de pesquisa e comitês) e resultados alcançados (políticas, estratégias, entre outros exemplos; iii) desenvolvimento de indicadores específicos de segurança cibernética. Posteriormente, esses indicadores foram agrupados para uma análise abrangente do cenário de segurança cibernética. Em síntese, o índice identificou ameaças, apontou mecanismos capazes de lidar com essas ameaças e, a partir disso, desenvolveu indicadores próprios para medir o grau de consolidação desses mecanismos nos Estados.

O índice conta, ainda, com três categorias de análise: estratégica, preventiva e responsiva, tendo cada categoria quatro capacidades que se subdividem ainda mais, num total de 49 indicadores de segurança cibernética. A quantidade de indicadores torna inviável que todos sejam destrinchados no trabalho, de forma que se optou por observá-los de forma agrupada na análise feita sobre o Brasil. Em resumo, esse modelo verifica os instrumentos existentes, nos Estados, em cada uma das três categorias de análise: reportam os mecanismos estratégicos de desenvolvimento da segurança cibernética, além dos instrumentos de prevenção e de resposta a incidentes.

Quanto ao Brasil, o modelo apreende uma imagem de atributos de segurança cibernética em estágios de desenvolvimento muito discrepantes, como se pode ver na Figura 3. O índice considera satisfatório o desenvolvimento da política nacional de segurança cibernética, mas argumenta que não há plano de implementação da estratégia atual. A análise de ameaças cibernéticas também é considerada satisfatória, embora o índice considere a inexistência de relatórios anuais de riscos uma lacuna importante. De fato, a coleta de dados por meio de fontes oficiais é um desafio apontado pela literatura examinada (Instituto Igarapé, 2021).

O modelo também argumenta que a proteção dos serviços disponíveis à população deixa muito a desejar. Isso pode ser visto, principalmente, nos itens 5 e 6 da

Figura 3, mas também fica evidente em outros indicadores – o item 11, por exemplo, indica insuficiente atenção ao combate ao crime cibernético, o que também foi identificado, em maior ou menor medida, nos outros dois índices utilizados nessa pesquisa. A categoria Indicadores Básicos de Cibersegurança é a mais baixa. Ela diz respeito à segurança de serviços essenciais e digitais. Por outro lado, a indicador Proteção de Dados Pessoais recebeu nota máxima e se encontra nessa categoria.

As principais lacunas brasileiras, nesse sentido, diriam respeito à incapacidade do país de estabelecer padrões de segurança para os setores público e privado, além de não possuir uma autoridade supervisora de serviços essenciais e digitais que monitore riscos. O NCSI também aponta que as capacidades cibernéticas variam entre os setores público e privado. Essa constatação também foi feita pelo CMM. Contudo, esse fenômeno parece ser normal, uma vez que o setor privado não está sujeito aos mesmos padrões do setor público.

O índice também considera menos desenvolvida capacidade de responder a incidentes cibernéticos e gerenciar crises, a observar nos itens 9 e 10. Segundo o modelo, o país não estabelece a obrigatoriedade de reportar incidentes, não possui um plano de gerenciamento de crise nem realiza exercícios de resposta a incidentes (EGA, 2021).

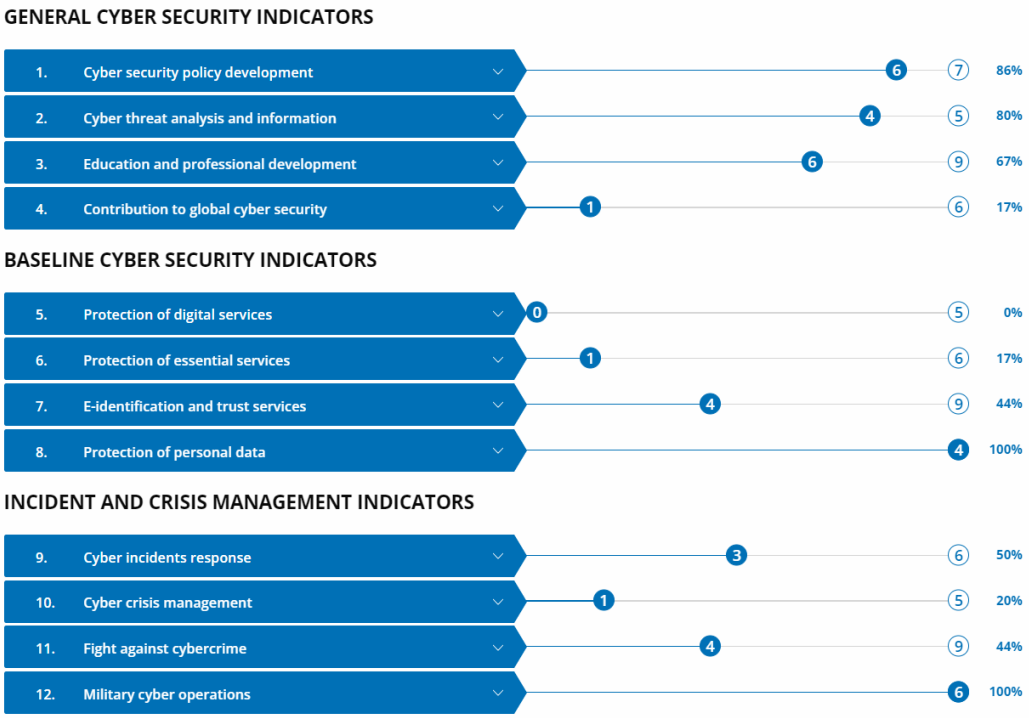
Em relação à projeção de poder no ciberespaço, a contribuição do Brasil à segurança cibernética global é tida como baixa. O Brasil não sedia organizações internacionais de segurança cibernética e não consegue financiar o desenvolvimento de capacidades cibernéticas de outros países, quesitos considerados por esse modelo. Consequentemente, a expressão de poder por meios cibernéticos do país seria limitada, segundo esse modelo. Aqui retorna-se à mesma questão das desvantagens da cooperação: ela não se constitui como forma de construção de capacidade.

Também é importante notar que as operações militares no ciberespaço mostram-se bem desenvolvidas e estabelecidas nesse modelo, como se pode observar no item 12. O índice atribui isso à existência de uma unidade voltada às operações cibernéticas e à realização de exercícios cibernéticos em âmbito doméstico e internacional. O NCSI não faz distinção entre capacidades ofensivas e defensivas; considera apenas se há

unidades especializadas em segurança cibernética e se as Forças Armadas do país realizam exercícios cibernéticos domésticos e internacionais rotineiramente.

Uma característica desse índice é que a pontuação em muitos de seus indicadores é pautada na existência de organismo formal relacionado ao atributo avaliado por cada item. Não há análise aprofundada da eficiência do aparato. Exemplo disso é o indicador 1, Desenvolvimento de Política de Cibersegurança, que só exigia a existência de instrumentos formais – como a estratégia atual, a E-Ciber – sem se preocupar com o estágio de implementação do instrumento. Essa característica pode distorcer os resultados, visto que não considera a dimensão material e prática de seus indicadores. Por outro lado, a existência de instituições representa um marco a partir do qual essas organizações podem evoluir, enquanto a ausência de instituições próprias de segurança cibernética impossibilita ações para o desenvolvimento desse escopo. Além disso, a definição de eficiência utilizada pelo índice poderia refletir, mais uma vez, a perspectiva restritiva que os três modelos analisados nesta pesquisa têm em comum.

Figura 3 - Indicadores de segurança cibernética



Fonte: EGA (2022)

4.3 COMPARAÇÃO DOS MODELOS E ANÁLISE DE CAPACIDADES

Nesta seção, inicialmente, pretende-se julgar os índices enquanto ferramentas de análise e tratar de como os modelos enxergam o Brasil, comparando-os. Em seguida, empreende-se esforço de análise pautada a partir dos dados e documentos oficiais expostos ao longo do trabalho para obter uma visão mais completa.

Quanto aos índices, cumpre evidenciar que a coleta de dados dos índices favorece uma perspectiva enviesada do cenário atual. O CMM, por exemplo, utiliza, majoritariamente, metodologia de grupo focal, baseada nas percepções dos entrevistados. Embora esses sejam em maioria servidores públicos ou especialistas em tecnologia, não necessariamente terão conhecimento do desenvolvimento geral dos recursos cibernéticos.

O NCSI, por sua vez, considera critérios objetivos importantes para a análise, como a existência de documentos estratégicos e legislação específica do cibercrime, mas não avalia a efetividade dos instrumentos. De fato, a existência de instrumentos específicos importa por indicar a condição que os Estados podem atingir com a evolução desses instrumentos, mas não é capaz de avaliar o estado atual das instituições.

O NCPI, por fim, admite a dificuldade de obter dados precisos sobre cada indicador proposto no índice, uma vez que muitas das informações necessárias para analisar poder cibernético no sentido admitido pelo modelo são confidenciais. Muitos dos dados são obtidos por fontes secundárias, o que põe em dúvida a confiabilidade desses. Novamente, ressalta-se a dificuldade de elaborar métricas de mensuração de capacidade; todas elas possuem limitações, mas isso não exclui por completo sua utilidade.

Por meio das análises, observou-se que os índices escolhidos são limitados em seus relatórios, uma vez que suas análises se restringem à capacidade de operação no âmbito virtual e desconsideram a capacidade material necessária para projetar influência e promover desenvolvimento no ciberespaço. Retomando-se o marco teórico do trabalho, identificam-se, pelo menos, cinco elementos essenciais para a construção de capacidade cibernética sobre os quais incidem decisões tomadas no âmbito

doméstico: (1) marco legal; (2) instrumentos administrativos; (3) instituições; (4) base material; e (5) educação. Os índices tratam apenas de três deles, sendo esses o marco legal, as instituições e a educação. Aqui resta avaliar como esses cinco elementos foram abordados nos índices.

Em relação ao marco legal, o CMM trata da existência de estratégia nacional de segurança cibernética e de legislação específica sobre crime cibernético; o NCPI não trata de legislação; e o NCSI aborda a existência de política e estratégia, além de plano de implementação e coordenação entre agências governamentais. O Brasil se encontra, em geral, em posição consolidada nesse quesito. Isso pode ser depreendido dos documentos oficiais abordados neste trabalho e os índices, de forma geral, também reconhecem isso.

Nenhum dos índices aborda profundamente os instrumentos administrativos, talvez por discrepâncias formais desses a depender do país. O CMM e o NCSI chegam a citar, por exemplo, o CDCiber e o COMDCiber, órgãos criados para assumir funções específicas no tocante à cibersegurança, mas não abordam a relevância dos documentos que efetuam o cumprimento da lei ao criarem essas instituições. No Brasil, a implementação da estratégia e do planejamento dependem diretamente dos instrumentos administrativos para definir responsabilidades específicas a entes existentes ou criar órgãos para assumir essas responsabilidades. Assim, esses são fundamentais para analisar a efetividade do marco legal, de modo que resta uma lacuna na análise dos índices.

As instituições são os pontos de maior atenção dos modelos. O CMM e o NCSI tratam de instituições técnicas governamentais para prevenção e resposta a incidentes, além daquelas constituídas para aprimorar capacidades defensivas e ofensivas do Estado e das instituições internacionais. O NCPI deixa implícita a relevância das instituições internas para atingir objetivos de poder cibernético, mas não as utiliza como critério de análise. Em vez disso, tem como critério a intenção e capacidade de influenciar normas e instituições internacionais.

A ênfase concedida às instituições em detrimento de outros elementos sugere uma interpretação pautada em uma configuração de influência que valoriza instituições em conformidade com padrões internacionais estabelecidos de acordo com

determinados interesses. O incentivo à cooperação internacional pode solucionar problemas técnicos no curto prazo, mas no longo prazo estabelece uma relação de dependência que dificulta que o Estado se coloque em posição de influência com base na capacidade cibernética.

A base material da capacidade cibernética poderia ser incluída no NCPI, que estabelece o desenvolvimento da indústria nacional de tecnologia como um dos atributos do poder cibernético. Entretanto, o modelo não se aprofunda nesse critério, que, apesar de ser composto por 10 quesitos, só relaciona três a uma concepção fracamente ligada à base material. Limita-se a reportar a existência de estratégias e parcerias público-privadas para ampliar a indústria e as cadeias de valor cibernéticas, bem como de esforços de pesquisa. Os outros quesitos desse critério são relacionados à adesão ou não do Estado a padrões internacionais de tecnologia. O CMM e o NCSI não abordam a base material. Isso suscita, mais uma vez, o exposto no parágrafo anterior. A base material é imprescindível para o Estado se posicionar de forma favorável na distribuição de poder do sistema internacional.

Por fim, o CMM e o NCSI tratam da educação na forma da conscientização e da difusão de boas práticas de segurança cibernética, incluindo a cultura de denúncias e a recusa em fornecer dados pessoais e sensíveis. Além disso, tratam da existência de treinamentos profissionais e existência de cursos de nível superior a fim de formar recursos humanos para desenvolver a área.

A análise isolada dos três índices leva a crer que a maturidade das capacidades cibernéticas do Brasil é, de fato, insuficiente em muitos sentidos. Os principais desafios identificados nos modelos dizem respeito à estratégia pouco coesa para o ciberespaço e sua implementação desorganizada; à dificuldade de enfrentamento do cibercrime e a pouca influência do país na criação de normas e estruturas internacionais de segurança cibernética. Conforme o NCSI, as principais lacunas diriam respeito à incapacidade de implementar uma autoridade supervisora de serviços essenciais e digitais que monitore regularmente os riscos e a infraestrutura de segurança cibernética.

Outras lacunas sobre as quais os índices concordam são a legislação penal relativa ao crime cibernético; os serviços governamentais disponibilizados à população,

que possuiriam falhas de segurança; por fim, a baixa capacidade brasileira de influenciar normas e estruturas no ciberespaço.

Os pontos fortes do país segundo esses relatórios parecem se centrar nos aspectos técnicos e nos militares, especialmente os de defesa. Aqui incluem-se apenas a esfera tática, referente à segurança de sistemas em rede. Os índices discordam a respeito da consolidação de padrões técnicos de segurança para os setores público e privado.

Os relatórios dos diferentes índices internacionais escolhidos sugerem a adesão ao modelo proposto por eles, pautado num conceito de capacidade cibernética restrito à segurança de *softwares*. Se apenas essa esfera for considerada, o Brasil continuará em situação de dependência, uma vez que não poderá centralizar a base material necessária para construir capacidade cibernética. Isso não os desqualifica por completo como instrumentos de análise. As avaliações objetivas proporcionadas por eles (a existência ou não de instituições para determinados fins, por exemplo) é um ponto de partida para tecer análises mais aprofundadas sobre as capacidades brasileiras. Não se pode, todavia, adotar esses relatórios como fontes últimas sem antes questionar suas perspectivas e até que ponto servirão como instrumentos de análise.

Ademais, a imagem que se tem por meio de outras fontes examinadas é outra. Compreende-se que o Brasil, apesar de ainda não se classificar como ator relevante no domínio cibernético, tem feito progresso contínuo e promissor. O país tem um arcabouço estratégico formal consolidado, instrumentos administrativos capazes de atribuir responsabilidades a órgãos existentes e novos, além de previsões constitucionais de instituições que podem dar suporte ao desenvolvimento de capacidade cibernética (aqui se encontra o Instituto do Consórcio). O desenvolvimento de capacidades cibernéticas ocorre no país desde a década de 1960, se forem considerados momentos como as primeiras iniciativas de produção de chips e, mais tarde, produtos de software.

O Brasil também está ciente da necessidade de desenvolver a base material da capacidade cibernética, a ver pelo PADIS, pela CEITEC, pelo Plano Brasil de Semicondutores, entre outras iniciativas que – apesar de não suficientemente expressivas – permitem o aprendizado organizacional necessário para

empreendimentos futuros. Aqui se identifica esse quesito como o mais importante, uma vez que a proteção do ciberespaço só pode ser desenvolvida com autonomia sobre a rede: o país precisa garantir o acesso doméstico aos recursos cibernéticos sem depender de fontes externas. Há necessidade de fortalecer essa indústria, bem como de formar recursos humanos para desenvolvê-la. A pesquisa indica que os meios institucionais e administrativos estão evoluindo de forma promissora. Entretanto, há obstáculos sistêmicos ao desenvolvimento dessas capacidades que também devem ser considerados – aqui se sugere proposta para trabalhos futuros.

Por fim, o crime cibernético, de fato, permanece um desafio para o país, considerando os números de crimes tentados e consumados nos últimos anos. A adoção de boas práticas de segurança cibernética pela população é importante para reduzir grande parte do número de ocorrências. Além disso, não se pode dizer que a legislação específica não vem evoluindo (ao contrário do que os índices sugerem), tendo em vista a lei penal específica que vem sendo publicada na última década, bem como o enquadramento de determinados crimes cibernéticos em legislação já existente.

Portanto, observa-se que o progresso brasileiro, quanto às capacidades cibernéticas, é promissor, apesar das lacunas existentes. Nesse sentido, o principal desafio é mobilizar-se internamente para superar a posição de dependência em que se encontra. Isso deve ser feito de maneira holística, ultrapassando a esfera estatal, de modo que se possa prover segurança cibernética como um todo e de forma autônoma.

4.4 CONCLUSÕES DO CAPÍTULO

O presente capítulo apresentou breve histórico evolutivo e o panorama atual da capacidade cibernética no Brasil. Buscou-se identificar avanços e obstáculos que o país enfrenta no processo de construção de capacidade cibernética. Para isso, utilizaram-se índices internacionais de segurança cibernética juntamente a literatura referente ao tema, de modo que fosse possível correlacionar os resultados proferidos nos índices com o que se observa na literatura examinada, em dados e nos documentos oficiais do governo brasileiro. Portanto, cumpriu-se o terceiro e último objetivo específico.

Nesse capítulo, concluiu-se que os índices internacionais são limitados em suas análises por excluírem aspectos importantíssimos da construção de capacidade cibernética, em especial a base material. Cabe retomar a noção de que esses modelos são elaborados com interesses específicos que não se alinham à posição que o Brasil ocupa quanto à capacidade cibernética e à distribuição de poder no sistema. Assim, ressalta-se, mais uma vez, a necessidade de adaptar instituições importadas à realidade doméstica, não as tomando como absolutas. A construção de capacidade cibernética brasileira depende da mobilização interna de modo a desenvolver os elementos que permitirão maior autonomia ao país.

5 CONCLUSÃO

Esta pesquisa buscou compreender os desafios para a construção de capacidade cibernética no Brasil. O objetivo central do trabalho foi identificar os desafios para a construção da capacidade cibernética do Brasil. Os objetivos específicos foram três: compreender como o Realismo Neoclássico poderia auxiliar a compreensão do objeto de estudo; apresentar o conceito de capacidade cibernética, situando a segurança cibernética no contexto das relações internacionais como pré-requisito para desenvolvimento estatal, segurança e projeção de influência; por fim, analisar a capacidade cibernética brasileira atual e identificar avanços e obstáculos enfrentados pelo país a partir de dados, documentos oficiais e índices internacionais de maturidade de capacidade cibernética.

Recapitulando, buscava-se compreender os principais desafios do Brasil para construir capacidade cibernética. Estabeleceu-se a seguinte hipótese de trabalho: a dificuldade de construir capacidade cibernética ocorreria devido à dificuldade de mobilizar recursos internos. Esse desafio se originaria pela inabilidade de conciliar os principais atores e suas respectivas responsabilidades e recursos em um arcabouço normativo passível de ser posto em prática. Dessa forma, o Estado não conseguiria mobilizar recursos eficazmente.

Durante a pesquisa, observou-se que, além da dificuldade em mobilizar recursos, há um desafio interno adicional e igualmente importante: a baixa produção doméstica da base material de capacidade cibernética, que coloca o país em posição de dependência externa. Não possuindo o centro de decisão econômica, o país precisa recorrer a outros a fim de abastecer a demanda local, sendo constrangido ao aprimoramento da segurança cibernética apenas na esfera tática. De fato, no âmbito doméstico, uma estratégia material e um planejamento são necessários para orientar a mobilização de recursos de construção de capacidade, notadamente os materiais. Contudo, o desafio da dependência limita as possibilidades do Brasil. Esse se constitui como obstáculo sistêmico. A hipótese, dessa forma, se confirma parcialmente, posto que o país possui dificuldades em mobilizar recursos para construir capacidade cibernética (especialmente a base material) mas a razão para tal é sistêmica.

O contexto em que surge a demanda pela construção de capacidade cibernética é o da Terceira Revolução Industrial, cujo advento dos chips – em que se baseia o Centro de Decisão Econômica – impulsionou significativamente as telecomunicações e a indústria. Tais mudanças suscitam a necessidade de adoção de abordagens inovadoras para a adaptação aos novos parâmetros produtivos. A necessidade de ter controle sobre a cadeia produtiva, ou seja, o centro de decisão econômica, será fundamental para o avanço brasileiro conforme se aproxima da Quarta Revolução Industrial.

Portanto, reconhece-se a necessidade de construir capacidades cibernéticas como parte da Transformação Digital no cenário em que as redes tornaram-se pilar indissociável das relações de produção e, consequentemente, de poder. O ciberespaço se coloca como domínio emergente cujo surgimento alterará fundamentalmente as relações internacionais, uma vez que sua natureza provoca tensões entre as fronteiras – antes bem definidas – de dimensões centrais do funcionamento do Estado – o público e o privado, o civil e o militar, os entes federativos e a própria federação.

O Realismo Neoclássico foi a teoria escolhida para tratar do objeto por considerar o ambiente interno como elemento fundamental para compreender o comportamento dos Estados e a distribuição de poder na perspectiva realista. Além disso, a teoria atenta mais ao processo de construção de capacidade em relação às outras vertentes do realismo, posto que as possibilidades de atuação dos Estados dependem de suas capacidades. Todavia, essa teoria reconhece os fatores sistêmicos tanto quanto todas as outras variantes do realismo.

Esse enfoque foi útil ao trabalho em razão de aqui se tratar dos desafios internos para a construção de capacidade cibernética, como a ausência de estratégia material para mobilização de recursos e a dificuldade de concentrar a produção de chips e fibra óptica própria em território brasileiro. Essa importa por ser componente essencial para a elaboração de uma rede interna e passível de controle pelo Brasil. Ou seja, o país poderia controlar o ciberespaço de fato – controlar quem atua nele, quais ações pode empreender, e mesmo a disponibilidade de acesso. Aqui, cabe retomar a natureza artificial do ciberespaço. O fato de o Brasil não ser um de seus artífices é um dos grandes entraves à capacidade cibernética. A mera capacidade de causar ataques

hacker ou defender de artifícios maliciosos não é de grande utilidade se o país não dispõe do controle de moldar o ciberespaço.

Os desafios expostos são desafios internos, mas a condição de dependência na qual o Brasil se encontra, no contexto das capacidades cibernéticas, é estrutural. Portanto, considera-se que o Realismo Neoclássico foi adequado para compreender lacunas referentes ao processo de construção de capacidade, posto que o Brasil não conseguiria mobilizar recursos de forma efetiva para responder às pressões sistêmicas; contudo, não se deve negligenciar o desafio imposto pela estrutura, sendo esse a posição de dependência em que o país se encontra em relação à base material de capacidade cibernética, o setor eletrônico – principalmente o de chips e fibra óptica, cujo estudo exige pesquisa própria futura. Assim, existem desafios a superar tanto em âmbito externo quanto em âmbito doméstico.

Depreende-se, dos índices internacionais, progresso insuficiente do Brasil no que diz respeito à segurança cibernética. No entanto, a análise proposta pelos índices teve utilidade limitada por considerar apenas a esfera tática, excluindo a logística. Essa se configura como fundamental por envolver o controle sobre as redes do país, que são, por sua vez, cruciais para a execução e o desenvolvimento de capacidades produtivas no contexto da Transformação Digital.

Um dos modelos analisados, o NCPI, aproxima-se dessa ideia. Inclui o desenvolvimento da indústria nacional de tecnologia, mas não a fibra óptica, como um dos fatores de poder cibernético. A presente pesquisa questiona essa perspectiva, uma vez que a fibra óptica, que compõe os cabos subterrâneos, é o que sustenta a conexão do país à rede mundial. Não possuindo capacidade de centralizar a produção dos recursos necessários para o desenvolvimento de capacidades cibernética, esse processo, no Brasil, fica limitado. Cumpre retomar Robert Cox e a ideia de que toda teoria cumpre um interesse específico. Aqui compreendem-se as análises dos modelos apresentados como parte de um cenário em que se busca enfraquecer a possibilidade de maior número de países centralizar recursos materiais de capacidade cibernética – deixando, portanto, a posição de dependência.

Considerando o exposto, cabe a ressalva de interpretar esses modelos criticamente, e não acatá-los como verdade única. Essa ressalva é especialmente

relevante quando se trata do ciberespaço, dado que é um domínio recente, diferente dos demais e cada vez mais importante para a produção (consequentemente, para angariar poder) à medida que se aprofundam a digitalização e digitização. A estratégia e o planejamento de construção de capacidade cibernética não podem se apoiar cegamente naquelas desenvolvidas por atores com interpretações, interesses e contextos opostos – especialmente os beneficiados pela atual distribuição de poder no sistema internacional. Num contexto pró-desenvolvimento nacional, se os índices forem adaptados a uma concepção doméstica de capacidade cibernética, podem constituir base para erigir parâmetros próprios de mensuração de capacidade cibernética além da esfera tática. Cumpre recuperar o pensamento de Bresser-Pereira sobre a importação de instituições: deve ocorrer de forma que elas sejam moldadas de acordo com o contexto doméstico.

No que diz respeito à concretização da estratégia, o conceito de centro de decisão econômica também é importante: precisa-se de autossuficiência para manter uma indústria produtiva de custos reduzidos que permita a atuação relevante no sistema internacional, obtendo os resultados preferidos por meio da combinação de recursos estatais – o poder inteligente. Por conseguinte, é crucial encontrar meios de construir capacidade em um domínio novo e fundamental para as transformações vindouras. Como apreendido da literatura examinada, a transição tecnológica traz urgência à construção de capacidades cibernéticas – não só pela aproximação da Quarta Revolução Industrial como também pelo aprofundamento da Terceira Revolução Industrial, que segue incompleta. A capacidade de atuar no ciberespaço e alcançar objetivos por meio de elementos desse domínio, o poder cibernético, é parte crucial disso, mas não é a única. O desafio, dessa forma, é a operacionalização da estratégia para que essa se materialize, de fato, em capacidade.

A extensão do desafio de concretizar o planejamento também se relaciona com a necessidade de desenvolver capacidade cibernética de maneira integrada, abrangendo múltiplos agentes de forma transversal. As demandas que surgem com o período suscitam a ação de um sujeito consubstanciado na integração dos diferentes componentes do Estado, não se restringindo à esfera estatal. A segurança cibernética, de fato, já é pré-requisito para o pleno desenvolvimento nesse cenário, mas se tornará

ainda mais imprescindível à medida que a automação passa a fazer parte do cotidiano da sociedade. Veem-se exemplos já materializados dessa nova realidade: *smart homes,* veículos autônomos, além de setores da economia em que a inteligência artificial já atua como auxiliar nas decisões humanas. Ademais, as redes só crescem em importância, com destaque para a comunicação sem fio e o advento das redes 5G.

Adicionalmente, observou-se a necessidade de um Estado que vá além dos limites tradicionais e estabeleça conexões práticas entre a esfera estatal, a sociedade civil e o setor privado. Trata-se da esfera pública não-estatal. Isso requer instituições adequadas para lidar com questões éticas e jurídicas à medida que a inovação se intensifica. Esses novos dilemas já existem: o debate entre proteção de dados e vigilância estatal, a consideração de armas autônomas, o transporte da dicotomia entre liberdade de expressão e discurso de ódio para as redes, entre outros exemplos que não caberiam neste trabalho. A ascensão do domínio cibernético e das capacidades cibernéticas como ferramenta de poder exigem respostas ágeis que preservem a autonomia dessas dimensões e, simultaneamente, permitam seu desenvolvimento integrado no ciberespaço, uma vez que a capacidade cibernética funcional deve envolver todas elas, retomando o conceito de *smart power*.

Um modo de possibilitar o desenvolvimento dessa esfera é o consórcio público-público. Como se observou no decorrer da pesquisa, um projeto nacional de segurança cibernética deve, necessariamente, envolver, além da norma, meios econômicos, burocráticos, diplomáticos e militares, uma vez que todos esses contribuem para a concretização da estratégia. Retomando o conceito de poder inteligente, a capacidade se consubstancia a partir da união das diferentes esferas: pública e privada, civil e militar. Esse é precisamente o papel que uma esfera pública não-estatal pode desempenhar: o de materialização da estratégia. Como visto, essa esfera é entendida como um dispositivo econômico e político necessário para o desenvolvimento de capacidades cibernéticas por estas não se circunscreverem à esfera estatal e dependerem de ação conjunta do Estado e outros agentes. Ela seria utilizada para atividades não exclusivas do Estado, mas de interesse público – caso do espaço cibernético, em que são necessárias proteções para a esfera privada que o Estado não pode prover completamente, além das atribuições exclusivas da Administração Pública.

A consolidação desse conceito, no contexto do ciberespaço, requer adaptação das normas vigentes de forma a lidar com questões sociais, econômicas e políticas no domínio cibernético, num arcabouço que segue se desenvolvendo.

Como exposto, as capacidades cibernéticas possibilitam a inovação e o desenvolvimento nacional no contexto da Terceira e da Quarta Revolução Industrial. Entretanto, a segurança cibernética é premissa fundamental para a consolidação dos instrumentos que darão forma ao aprofundamento desses processos. Premissa essa que só logrará efeitos significativos se todos os atores do processo assumirem o compromisso de mitigar riscos e executar estratégias bem construídas para a segurança digital.

É nesse sentido que se faz necessária uma Política Nacional de Segurança Cibernética que oriente não só a Administração Pública, mas também o setor privado e a sociedade civil. Essa política deve guiar o desenvolvimento de instrumentos administrativos, base material, educação e recursos humanos, além do marco legal e de instituições adaptadas aos novos desafios. A manutenção, no ciberespaço, de funções básicas do Estado e infraestruturas críticas, direitos individuais e garantias constitucionais, a produção e, por conseguinte, o desenvolvimento nacional, são elementos tão diversos quanto necessários para a consolidação do espaço cibernético. Não só isso, mas deve haver esforço significativo do país em superar a dependência no que se refere à base material da capacidade cibernética, o pilar de todos os outros elementos da expressão de capacidade no ciberespaço.

O Brasil demonstra estar ciente da importância das capacidades necessárias para o desenvolvimento, uma vez que se observam avanços em relação ao espaço cibernético, na legislação do país, há quase duas décadas. O futuro, portanto, parece promissor. Resta ao país encontrar meios próprios, além de operacionalizar os já existentes, para consolidar sua estratégia e aprimorar os recursos já em vigor para, de fato, construir capacidade cibernética.

REFERÊNCIAS

ABINEE (ASSOCIAÇÃO BRASILEIRA DA INDÚSTRIA ELÉTRICA E ELETRÔNICA). **Panorama econômico e setorial**, 2015a. Disponível em: http://www.abinee.org.br/programas/50anos/public/panorama/index.htm#7/z. Acesso em: 12 jan. 2024.

ABINEE (ASSOCIAÇÃO BRASILEIRA DA INDÚSTRIA ELÉTRICA E ELETRÔNICA). **Comportamento da Indústria Elétrica e Eletrônica em 2023**. Desempenho do setor – dados preliminares. Disponível em: http://www.abinee.org.br/abinee/decon/decon15.htm. Acesso em: 02 jan. 2024.

ANDRESS, Jason; WINTERFELD, Steve. **Cyber warfare: techniques, tactics and tools for security practitioners**. Waltham: Elsevier, 2014.

BORNE, Thiago; CANABARRO, Diego R.Brazil and the Fog of (Cyber)War. **NCDG Policy Working Paper**, n. 13-002, p. 1-12, mar. 2013. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3155500. Acesso em: 28 nov. 2023.

BRASIL. **Decreto nº 3.505, de 13 de junho de 2000**. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm. Acesso em: 01 nov. 2023.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 02 nov. 2023.

BRASIL. **Decreto nº 9.573, de 22 de novembro de 2018**. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 18 out. 2023.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação. Brasília, 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637 .htm. Acesso em: 05 jan. 2024.

BRASIL. **Decreto n° 11.200, de 15 de setembro de 2022**. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11200.htm. Acesso em: 20 out. 2023.

BRASIL**. Decreto Nº 11.478, de 6 de abril de 2023**. Exclui empresas do Programa Nacional de Desestatização e revoga a qualificação de empresas e ativos no âmbito do Programa de Parcerias de Investimentos da Presidência da República. 2023a. Disponível em: http://www.in.gov.br/web/dou/-/decreto-n-11.478-de-6-de-abril-de-2023-475785730. Acesso em: 07 dez. 2023.

BRASIL. **Decreto Nº 11.768, de 6 de novembro de 2023**. Autoriza a reversão do processo de dissolução societária da empresa pública Centro Nacional de Tecnologia Eletrônica Avançada S.A. - Ceitec. Brasília, 2023b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11768.htm. Acesso em: 29 dez. 2023.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, 2020a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/ D10222.htm. Acesso em: 15 jan. 2024.

BRASIL. **Decreto nº 10.569, de 9 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, 2020b. Disponível em: 206 http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm. Acesso em: 10 dez. 2023.

BRASIL. **Decreto N.º 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, 2023c. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 10 jan. 2023.

BRASIL**. Lei N.º 11.484, de 31 de maio de 2007**. Dispõe sobre os incentivos às indústrias de equipamentos para TV Digital, instituindo o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores. Brasília, 2007. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/lei/l11484.htm. Acesso em: 27 dez. 2023.

BRASIL. **Lei Nº 12.737, de 30 de novembro de 2012**. Disponivel em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em: 10 de ago de 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 set. 2023

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados (LGPD). Brasília, 2018c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 set. 2023.

BRASIL. Ministério da Defesa. **Operação Ágata**. 2013. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/exercicios-e-operacoes/operacoes-conjuntas/operacao-agata. Acesso em: 12 jan. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação**. Glossário de Segurança da Informação**. Brasília, 2021a. Disponível em: http://dsic.planalto.gov.br/arquivos/documentospdf/glossario_completo.pdf. Acesso em: 30 set. 2023.

BRASIL. Tesouro Nacional. Ministério da Fazenda. **SIAFI: História**. 2023. Disponível em: https://www.gov.br/tesouronacional/pt-br/siafi/historia-e-estrutura/historia. Acesso em: 16 jan. 2024.

BRASIL. Tribunal de Contas da União**. TC 020.973/2020-9**. Plenário. Relator: Walton Alencar Rodrigues. Sessão de 01/09/2021. 2021b. Disponível em: https://portal.tcu.gov.br/data/files/D1/D2/7B/BE/CD3AB710EA6C5BA7E18818A8/020.973-2020-9-AC-revisor%20-%20Ceitec.pdf. Acesso em: 01 dez. 2023.

BRESSER-PEREIRA, Luis Carlos; GRAU, Nuria Cunill. Entre o Estado e o mercado: o público não-estatal. In: BRESSER-PEREIRA, Luis Carlos; GRAU, Nuria Cunill (org.). O público não-estatal na reforma do Estado**. Rio de Janeiro**: Editora FGV, 1999.

BRESSER-PEREIRA, Luis Carlos. A reforma do Estado nos anos 90: lógica e mecanismos de controle. **Brasília**: Ministério da Administração Federal e Reforma do Estado, 1997a.

BRESSER-PEREIRA, Luiz Carlos. Instituições, bom Estado, e reforma da gestão pública. In: BIDERMAN, Ciro; ARVATE, Paulo (org.). Economia do Setor Público no Brasil. **São Paulo**: Campus Elsevier, 2004. p. 3-15. Disponível em: https://bresserpereira.org.br/papers/2004/556-Insts-BomEstado-Reforma95-98.pdf. Acesso em: 30 dez. 2022.

CALDERARO, Andrea; CRAIG, Anthony J.S.. Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. **Third World Quarterly**, v. 41, n. 6, p. 917-938, 2020.

CASSIDY, Daniel; HEMANI, Irfan; VOO, Julian. National Cyber Power Index 2022. **Cambridge**, MA, 2022. Disponível em: https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf. Acesso em: 7 nov. 2023

CISA (CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY). **Explore Terms: A Glossary of Common Cybersecurity Words and Phrases**. Disponível em: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c. Acesso em: 07 set. 2023.

COX, Robert. W. Social Forces, States and World Orders: Beyond International Relations Theory. Millennium, v. 10, n. 2, p. 126–155, 1 jun. 1981.

CRAIG, Anthony J. S.; VALERIANO, Brandon. Conceptualising cyber arms races. *In*: International Conference on Cyber Conflict: Cyber Power, 8., 2016, Tallinn. **Conference proceedings** [...]. Tallinn: NATO CCD COE Publications, 2016, v.1. 141–158. Disponível em: https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf. Acesso em: 01 jul. 2023.

CRAIG, Anthony J. S; VALERIANO, Brandon. Realism and cyber conflict: security in the digital age. *In*: Avgustin, J. R.; NURNUS, Max; ORSI, Davide. **Realism in practice: an appraisal**. Briston: E-International Relations, 2018. Disponível em: https://asutoshcollege.in/new-web/Study_Material/Realism_in_Practice_E_IR.pdf#page=100. Acesso em: 01 jul. 2023

CRANDALL, M. Soft Security Threats and Small States: the Case of Estonia. **Defence Studies**, v. 14, n.1, p. 30-55, 2014. doi: 10.1080/14702436.2014.890334.

CRANDALL, M., & ALLAN, C. Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms. **Contemporary Security Policy**, v. 36, n.2, p. 346-368, 2015. doi: 10.1080/13523260.2015.1061765.

CRAVO, Vanessa Copetti.. **Em busca de uma estratégia nacional de segurança cibernética**: marco legal e Autoridade Nacional de Segurança Cibernética. Tese (Doutorado em Estudos Estratégicos Internacionais) – Faculdade de Ciências Econômicas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023.

CREESE, S.; DUTTON, W. H.; ESTEVE-GONZÁLEZ, P.; SHILLAIR, P.; Cybersecurity capacity-building: cross-national benefits and international divides. **Journal of Cyber Policy**, v. 6, n. 2, p. 214-235, 2021. Disponível em: https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1979617. Acesso em: 05 ago. 2023.

DEVANNY, Joe; GOLDONI, Luiz Rogério Franco; MEDEIROS, Breno Pauli. The rise of cyber power in Brazil. **Revista Brasileira de Política Internacional**, v. 65, 2022.

DINIZ, Gustado; GLENNY, Misha; MUGGAH, Robert. Deconstructing Cyber Security in Brazil: Threats and Responses. **Instituto Igarapé**, artigo estratégico 11, dez. 2014. Disponível em: https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf. Acesso em: 28 nov. 2023.

DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. **São Paulo**: Editora Atlas, 2014.

DOMINGO, Francis Rico. **Small states and the strategic utility of cyber capabilities**. 2018. 288 p. Tese (Doutorado) – School of Politics and International Relations, University of Nottingham, Nottingham, 2018. Disponível em: https://eprints.nottingham.ac.uk/55316/. Acesso em: 28 nov. 2023.

E-GOVERNANCE ACADEMY. **National Cyber Security Index.** Tallinn, 2022. Disponível em: https://ncsi.ega.ee/country/br_2022/?allData=1. Acesso em: 7 nov. 2023

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). **ENISA Overview of cybersecurity and related terminology**. v. 1. Set. 2017. p. 8. Disponível em: https://www.enisa.europa.eu/publications/enisa-position-papers-andopinions/enisa-overview-of-cybersecurity-and-related-terminology. Acesso em: 01 jul. 2023.

FIFTH DOMAIN. **What is 'sovereignty' in cyberspace? Depends who you ask.** 2019. Disponível em: https://www.fifthdomain.com/international/2019/11/21/what-is-sovereignty-in-cyberspace-depends-who-you-ask/. Acesso em: 20 mar. 2023.

FILIPPIN, F. **Estado e desenvolvimento: a indústria de semicondutores no Brasil**. BNDES. 2020. Dissertação (Mestrado em Ciências Econômicas) – Programa de Pós-Graduação em Economia, Instituto de Economia, Universidade Estadual de Campinas, Campinas, 2020. Disponível em: https://web.bndes.gov.br/bib/jspui/bitstream/1408/19660/1/Premio37_Mestrado.pdf. Acesso em: 12 dez. 2020.

FORTINET. 1H 2023 FortiGuard Labs Threat Report, 2023. Disponível em: https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings-1h-2023. Acesso em: 7 nov. 2023.

FOULON, M. (2016). Neoclassical Realism: Challengers and Bridging Identities.

International Studies Review, v. 17, n. 4, p. 635-661, dez. 2015. Disponível em: https://www.jstor.org/stable/24758570. Acesso em: 28 nov. 2023

FRIEDMAN, Allan; SINGER, Peter Warren; **Cybersecurity and cyberwar: what everyone needs to know**. Oxford University Press, 2014.

FURTADO, Celso. A pré-revolução brasileira. Rio de Janeiro: Fundo de Cultura, 1962.

FURTADO, Celso. **Cultura e desenvolvimento em época de crise**. Rio de Janeiro: Paz e Terra, 1984.

GENRO FILHO, **Adelmo. Violência, política, poder e Estado: reflexões preliminares**. Florianópolis, UFSC, mimeo., 1984, 25 pp.

GHERNAOUTI, Solange. Cyber Power: Crime, Conflict and Security in Cyberspace. **Lausanne**: EPFL Press, 2013.

GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE – GCSC. **Advancing Cyberstability,** nov. 2019. Disponível em: https://cyberstability.org/report/. Acesso em: 28 mar. 2023.

GLOBAL CYBER SECURITY CAPACITY CENTRE – GCSCC. **Revisão da capacidade de cibersegurança da República Federativa do Brasil**. Disponível em: https://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf. Acesso em: 07 nov. 2023.

GODOY, Arnaldo Sampaio de Moraes. **A execução fiscal administrativa no direito tributário comparado**. 1ª Ed. Belo Horizonte: Fórum, 2009. p. 18.

HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. **Instituto Igarapé**, artigo estratégico v. 54, 2021. Disponível em: https://www.researchgate.net/publication/351098187_Ciberseguranca_no_Brasil_uma_Analis e_da_Estrategia_Nacional. Acesso em: 05 ago. 2023.

HUREL, Louise; LOBATO, Luisa Cruz. A Strategy for Cybersecurity Governance in Brazil. **Instituto Igarapé**, strategic note n. 30, 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf. Acesso em: 28 nov. 2023.

INSTITUTO IGARAPÉ. **Mapeamento deriscos digitais: uma agenda multissetorial para a segurança digital no brasil**, 2021. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/Agenda-Seguranca-Digital.pdf. Acesso em: 7 nov. 2023.

IPEA (INSTITUTO DE PESQUISA ECONÔMICA APLICADA). Países se articulam para diminuir dependência das cadeias globais de suprimento de chips. **Centro de Pesquisa em Ciência, Tecnologia e Sociedade**. 2023. Disponível em: https://www.ipea.gov.br/cts/pt/central-de-conteudo/artigos/artigos/348-paises-se-articulam-para-diminuir-dependencia-das-cadeias-de-suprimento-globais-de-semicondutores#:~:text=O%20consumo%20de%20semicondutores%20no,locais%20de%20semicondutores%20no%20passado. Acesso em: 02 jan. 2024.

KELLO, L. The Virtual Weapon and International Order. **London**: Yale University Press, 2017.

KUEHL, Daniel. From cyberspace to cyberpower: defining the problem. *In*: KRAMER, Franklin D.; STARR, Stuart H; WENTZ, Larry K. **Cyberpower and national security**. Dulles: Potomac Books, 2009. p. 24-42.

LÉVY, P. **A inteligência coletiva por uma antropologia do ciberespaço.** São Paulo: Loyola, 1998.

LIBICKI, Martin C. Cyberspace Is Not a Warfighting Domain. **A Journal of Law and Policy for the Information Society**, v. 8, n. 2, p. 325-340, 2012. Disponível em:

https://kb.osu.edu/bitstream/handle/1811/73111/1/ISJLP_V8N2_321.pdf. Acesso em: 01 jul. 2023.

LIBICKI, Martin C. **Cyberdeterrence and Cyberwar**. Santa Monica, 2009, California: RAND Corporation.

LIFF, A. P. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. **Journal of Strategic Studies**, v. 35, n. 3, p. 401-428, 2012. doi: 10.1080/01402390.2012.663252

LINDSAY, J. R; GARTZKE, E. Coercion through Cyberspace: The Stability-Instability Paradox. Kelly Greenhill and Peter Krause. (Eds.), **The Power to Hurt: Coercion in the Modern World**. Oxford: Oxford University Press, 2018.

LOBATO, Luisa Cruz. La política brasileña de ciberseguridad como estrategia de liderazgo regional. **URVIO Revista Latinoamericana de Estudios de Seguridad**, n. 20, p. 16-30, 2017. Disponível em: https://revistas.flacsoandes.edu.ec/urvio/article/view/2576. Acesso em: 01 jul. 2023.

LOBELL, Steven E.; RIPSMAN, Norrin M.; TALIAFERRO, Jeffrey W. **Neoclassical realist theory of International Relations**. New York: Oxford University Press, 2016.

MANESS, Ryan; VALERIANO, Brandon. **Cyber war versus cyber realities: cyber conflict in the International System**. New York: Oxford University Press, 2015.

MARTINS, José Miguel Quedi. **Prefácio**. In.: CRAVO, Vanessa Copettti. Em busca de uma estratégia nacional de segurança cibernética eletrônico: marco legal e autoridade nacional de segurança cibernética. Porto Alegre: Editora Fundação Fênix, 2023.

MAZANEC, Brian; WHYTE, Christopher. **Understanding cyber-warfare: politics, policy and strategy**. New York: Routledge, 2019.

MEARSHEIMER, John J. Structural realism. *In*: DUNNE, Tim; KURKI, Milja; SMITH, Steve. **International Relations theories**: discipline and diversity. Oxford: Oxford University Press, 2013, p. 77-93.

MILLER, Chris. **A Guerra dos Chips: a batalha pela tecnologia que move o mundo**. Rio de Janeiro: Globo Livros, 2023.

MOTTA, Fernando C. Prestes. **O que é burocracia**. 1ª Ed. São Paulo: Editota Brasiliense, 1981

MULLER, Lilly Pijnenburg. Cyber Security Capacity Building in Developing Countries: Challenge and Opportunities. **Norwegian Institute of International Affairs,** Oslo, n. 3, p. 2 - 23, 2015. Disponível em: https://nupi.brage.unit.no/nupi-

xmlui/bitstream/handle/11250/284124/NUPI+Report+03-15-Magatuller.pdf?sequence=3. Acesso em: 7 nov. 2023.

NYE, Jr., Joseph S. Soft Power. **Foreign Policy**. n. 80, p. 153-171, Fall 1990.

NYE, Jr., Joseph S. The future of power. **New York**: Public Affairs, 2011.

OLIVEIRA, B. T. (In)segurança digital: o sistema de ciberdefesa brasileiro. **O Cosmopolítico,** v. 7, n. 2, p. 142-148, 6 dez. 2021. Disponível em: https://periodicos.uff.br/ocosmopolitico/article/view/53880. Acesso em: 7 nov. 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. **United Nations system support for capacity-building**, E/2002/58. 14 maio, 2002. New York: United Nations.

PAWLAK, Patryk. Capacity building in cyberspace as an instrument of foreign policy. **Global Policy**, v. 7, n. 1, p. 83-92, 2016. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1111/1758-5899.12298. Acesso em: 7 nov. 2023.

PETERS, Michael A. Semiconductors, geopolitics and technological rivalry: The US CHIPS & Science Act. **Educational Philosophy and Theory**, 55:14, 1642-1646, 2022. DOI: 10.1080/00131857.2022.2124914. Acesso em: 12 jan. 2024.

PINTO, Daniela Jacon Ayres; GRASSI, Jéssica Maria; PINTO. A construção de capacidade cibernética na América do Sul. **Campos Neutrais-Revista Latino-Americana de Relações Internacionais**, v. 4, n. 2, p. 52-64, 2022. Disponível em: https://periodicos.furg.br/cn/article/view/14664. Acesso em: 01 jul. 2023.

PINTO, Danielle Jacon Ayres. Smart power: os pilares deste poder na política externa brasileira. **ENABRI**, n. 3, v. 1, 2011. Disponível em: http://www.proceedings.scielo.br/pdf/enabri/n3v1/a61.pdf. Acesso em: 09 jan. 2024.

PODER JUDICIÁRIO DO ESTADO DO RIO DE JANEIRO (PJERJ). **Crimes cibernéticos: evolução da legislação brasileira**, 2019. https://www.tjrj.jus.br/web/portal-conhecimento/noticias/noticia/-/visualizar-conteudo/5736540/6447772

POHLE, Julia; THIEL, Thorsten. Digital Sovereignty. **Internet Policy Review**: Journal on Internet Regulation, Berlim, v. 9, n. 4, p. 1-19, 17 dez. 2020. Disponível em: https://policyreview.info/pdf/policyreview-2020-4-1532.pdf. Acesso em: 20 mar. 2021.

PUYVELDE, Damien Van; BRANTLY, Aaron F. Cybersecurity: Politics, Governance and Conflict in Cyberspace. **Cambridge**: Polity Press, 2019.

RICCIARDI, Stéphane; SOUQUE, Cédric. Modern Electromagnetic Spectrum Battlefield: From EMS Global Supremacy to Local Superiority. **PRISM**, vol. 9, no. 3, 2021, pp. 122–

39. JSTOR. Disponível em: https://www.jstor.org/stable/48640750. Acesso em: 20 Jan. 2024.

ROSE, Gideon. Neoclassical realism and theories of foreign policy. **World Politics**, Cambridge, v. 51, n. 1, p. 144-172, 2011. Disponível em: https://www.cambridge.org/core/journals/world-politics/article/abs/neoclassical-realism-and-theories-of-foreign-policy/48B6DD61980E75A29672E8553D0F79E4. Acesso em: 05 ago. 2023.

SAFERNET. **Delegacias cibernéticas**, 2024. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 13 jan. 2024.

SALLES, Alexsandro Souza de. **Consórcio público: instrumento de capacidade estatal**. Dissertação (Mestrado em Estudos Estratégicos Internacionais), Programa de Pós-Graduação de Estudos Estratégicos Internacionais da Universidade Federal do Rio Grande do Sul. 2019.

SCHMITT, Michael N. (ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. **Cambridge**: Cambridge University Press, 2013. Disponível em: http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf . Acesso em 21 mar. 2021.

SCHWAB, Klaus. The Fourth Industrial Revolution: What it Means, How to Respond. **Japan Spotlight**, Tokyo, p. 3-5, Jul./Aug. 2016. Disponível em: https://www.jef.or.jp/journal/pdf/208th_Cover_01.pdf . Acesso em: 15 maio 2022.

SCHWELLER, Randall L. (2006). Unanswered Threats: Political Constraints on the Balance of Power. **Princeton**: Princeton University Press.

SHELDON, John B. Deciphering Cyberpower Strategic Purpose in Peace and War. **Strategic Studies Quarterly**, 2011. Disponível em: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-2/Sheldon.pdf. Acesso em: 7 nov. 2023

SHEN, Yi. Cyber Sovereignty and the Governance of Global Cyberspace. **Chinese Political Science Review**, v.1, n.1, p. 81-93, mar. 2016. Disponível em: https://doi.org/10.1007/s41111-016-0002-6. Acesso em: 7 nov. 2023.

SILVA, Ana Lucia Gonçalves da. **Indústria de componentes eletrônicos semicondutores: padrão de concorrência internacional e inserção do Brasil**. 1985. Dissertação (Mestrado em Ciências Econômicas) – Estadual de Campinas, Campinas, 1985. Disponível em: https://repositorio.unicamp.br/Acervo/Detalhe/28949. Acesso em: 20 jan. 2024.

SILVA, Taziane Mara da; TEIXEIRA, Talita de Oliveira; FREITAS, Sylvia Mara Pires de. Ciberespaço: uma nova configuração do ser no mundo. **Psicologia em Revista**, Belo Horizonte, v. 21, n. 1, p. 176-196, jan. 2015 . Disponível em:

http://pepsic.bvsalud.org/scielo.php?script=sci_abstract&pid=S1677-11682015000100012&lng=pt&nrm=iso . Acesso em 21 dez. 2023.

SNYDER, Jack. (1977). The Soviet Strategic Culture: Implications for Limited Nuclear Operations. **Santa Monica**: RAND Corporation.

SOLAR, Carlos. Cybersecurity and cyber defence in the emerging democracies. **Journal of Cyber Policy**, v. 5, n. 3, p. 392-412, 2020.

TALIAFERRO, Jeffrey W. State building for future wars: neoclassical realism and resource-extractive state. **Security Studies**, London, v. 15, n. 3, p. 464-495, 2006. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/09636410601028370. Acesso em: 05 ago. 2023.

UNGER, Roberto Mangabeira et al. Imaginação institucional: a vanguarda rebelde do pensamento brasileiro. **Revista de Ciências do Estado**, Belo Horizonte, v. 6, n. 2, p. 1–17, 2021. DOI: 10.35699/2525-8036.2021.35620. Disponível em: https://periodicos.ufmg.br/index.php/revice/article/view/e35620. Acesso em: 19 out. 2023

VAN EVERA, Stephen. Guía para estudiantes de ciencia política: métodos y recursos. **Barcelona**: Editorial Gedisa, 2002.

WALTZ, Kenneth. **O homem, o Estado e a guerra: uma análise teórica.** São Paulo: Martins Fontes, 2004.

WALTZ, Kenneth N. **Theory of international politics**. Menlo Park: Addison-Wesley Publishing Company, 1979.

WORLD ECONOMIC FORUM -- WEF. **The Global Risks Report 2023**, n. 18, 2023. Disponível em: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf?_gl=1*1avmt40*_up*MQ..&gclid=Cj0KCQjw4bipBhCyARIsAFsieCzDkud5IyTR72W2X8Sz5kgTvq626rRJ1sNxHG3Wxs-ECaSMgvajE2EaAsoHEALw_wcB. Acesso em: 7 nov. 2023.

ZAKARIA, Fareed. (1999). **From Wealth to Power: The Unusual Origins of America's World Role**. Princeton, New Jersey: Princeton University Press.