UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE FILOSOFIA E CIÊNCIAS HUMANAS
DEPARTAMENTO DE CIÊNCIA POLÍTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA POLÍTICA

RENATO VICTOR LIRA BRITO

SEGURANÇA CIBERNÉTICA COMPARADA:
O BRASIL E AS AMÉRICAS

RECIFE
2022

RENATO VICTOR LIRA BRITO

SEGURANÇA CIBERNÉTICA COMPARADA:
O BRASIL E AS AMÉRICAS

Dissertação apresentada como requisito obrigatório para a obtenção do grau de Mestre em Ciência Política, pelo Departamento de Ciência Política da Universidade Federal de Pernambuco.

Área de Concentração: Democracia e Instituições.

Orientador: Prof. Dr. Rafael Mesquita de Souza Lima.

RECIFE

2022

Catalogação na fonte
Bibliotecária Maria do Carmo de Paiva, CRB4-1291

B862s Brito, Renato Victor Lira.
Segurança cibernética comparada : o Brasil e as Américas / Renato Victor Lira Brito. – 2022.
182 f. : il. ; 30 cm.

Orientador: Prof. Dr. Rafael Mesquita de Souza Lima.
Dissertação (Mestrado) - Universidade Federal de Pernambuco, CFCH. Programa de Pós-Graduação em Ciência Política, Recife, 2022.
Inclui referências, apêndices e anexos.

1. Ciência Política. 2. Cibernética. 3. Segurança. 4. Crimes cibernéticos. I. Lima, Rafael Mesquita de Souza (Orientador). II. Título.

320 CDD (22. ed.) (BCFCH2022-059)

RENATO VICTOR LIRA BRITO

SEGURANÇA CIBERNÉTICA COMPARADA:
O BRASIL E AS AMÉRICAS

Dissertação apresentada como requisito obrigatório para a obtenção do grau de Mestre em Ciência Política, pelo Departamento de Ciência Política da Universidade Federal de Pernambuco.

Área de Concentração: Democracia e Instituições.

Aprovada em: 24/02/2022.

BANCA EXAMINADORA

Prof. Dr. Rafael Mesquita de Souza Lima (Orientador)
Universidade Federal de Pernambuco

Prof. Dr. Marcos Aurelio Guedes de Oliveira (Examinador Interno)
Universidade Federal de Pernambuco

Prof. Dr. Gills Vilar Lopes (Examinador Externo)
Universidade da Força Aérea

"Quem falou de primavera sem ter visto o teu sorriso, falou sem saber o que era (...)"

(Cecília Meireles, Onda)

Dedico esta obra à improbabilidade da vida no universo, que possibilitou a existência da mente, sistema essencial para se pensar sobre questões como incerteza, epistemologia, propósito e eventos raros, como a bela história do ser humano que é o meu tio-avô, **Marcos Fernando de Souza Lira** (*in memoriam*). Com o seu sorriso, ele abraçou o mundo.

AGRADECIMENTOS

Sopesando a aparentemente solitária disciplina do ofício do pesquisador, a condição tênue do fazer científico dos indivíduos das classes menos abastadas, ou seja, dos cientistas pobres, é essencial e inescapavelmente social. **Mercedes Sosa** cantava "*traigo un pueblo en mi voz*". A criação mais fidedigna, entretanto, foi proposta por **João Cabral de Melo Neto**, meu conterrâneo:

"Um galo sozinho não tece uma manhã:
ele precisará sempre de outros galos.
De um que apanhe esse grito que ele
e o lance a outro; de um outro galo
que apanhe o grito que um galo antes
e o lance a outro; e de outros galos
que com muitos outros galos se cruzem
os fios de sol de seus gritos de galo,
para que a manhã, desde uma teia tênue,
se vá tecendo, entre todos os galos.
E se encorpando em tela, entre todos,
se erguendo tenda, onde entrem todos,
se entretendendo para todos, no toldo
(a manhã) que plana livre de armação.
A manhã, toldo de um tecido tão aéreo
que, tecido, se eleva por si: luz balão."
(João Cabral de Melo Neto, Tecendo a Manhã)

Desse modo, é certo que não há agradecimento suficiente pelas escolhas, ações, presenças e ausências das pessoas, raízes minhas, que me conduziram e acompanharam, até o momento, as nossas discretas conquistas. Sabendo disso, ainda assim, agradeço. O primeiro fio de luz acadêmico e formativo me foi trazido pelo meu tio-avô, **Marcos Lira** (*in memoriam*), que é a força inquebrantável da certeza frente às dúvidas e que acreditou em mim e no meu potencial mais até do que eu mesmo. Minha mãe, **Karine Lira**, me proporcionou a existência e contribuiu preponderantemente para a arquitetura do meu caráter e à minha busca pela verdade e pela justiça. Atualmente, ela divide comigo o dia a dia acadêmico, onde eu aprendo muito sobre o seu encantamento com os Direitos Humanos e ensino um pouco da efervescência da Ciência Política que permeia a minha curiosidade. **Glória Lira**, minha avó, sempre foi o meu exemplo familiar da preponderância do humano sobre qualquer adversidade. Esse enfrentamento destemido das causas perdidas, e a descoberta - através da experiência - da possibilidade de realização do que era considerado impossível, são parte fulcral da minha herança. Nas minhas visitas ao seu ofício de Diretora de Cultura no município de Paulo Afonso, onde havia uma biblioteca, tive acesso à maior parte dos livros

que constituem o que eu sou, marcas indeléveis, memória. O meu avô, **Evandro Lira** (*in memoriam*), com quem convivi até a adolescência, trouxe luz e alegria à minha infância. Passei com ele as melhores férias da minha vida. Talvez seja ele a pessoa mais inteligente que já conheci. Não apenas inteligente em termos formais, daqueles que geram diplomas uma vez ou outra, mas de forma substantiva, singular. A música que ele ouvia criou raízes e se multiplicou na minha formação. **Ana Cecília**, minha irmã a quem eu dei o nome, renova a cada dia a minha crença no futuro e gera alegria por onde passa. Ela é parte da solução que a humanidade necessita. **Edson Lira**, meu tio-avô, realça e dá sofisticação ao brilhantismo característico da família. Com o seu exemplo, aprendi o potencial que uma mente disciplinada tem. Além disso, compartilhamos o gosto pela música dos baluartes **Frank Sinatra** e **Tony Bennett**. **Fátima Couto Guedes** e **Marconi Guedes**, meus tio-avós, me receberam em sua casa durante o bacharelado, participaram e continuam participando das minhas invenções de peças, shows e momentos culturais. Tio Marconi é o mestre do meu barco. Artista por excelência, tem o perfeccionismo digno de um ourives bilaquiano. Tia Fátima é o coração da família, a voz que agrega e aglutina todos ao redor de uma mesa, transmutando solidões e estabelecendo um lar. São delas as mãos que servem, curam e zelam. É dela a práxis sagrada. **Ângela Lira**, minha tia-avó, me hospedou nos primeiros meses da graduação e, desde então, tem acompanhado o meu desenvolvimento acadêmico e intercedido por mim. A sua fé arrebatadora e a sua presença na vida de todos da família dão a sustentação necessária para que tudo o mais permaneça em equilíbrio. **Mercedes Lira** (*in memoriam*), minha tia-avó, com sua máxima "é pra frente que se anda", é o meu exemplo de perspectiva, de perseverança e de sabedoria. É a manifestação de que não é necessário dividir para conquistar. **Gorette Guedes**, minha tia-avó e madrinha, com quem aprendo a vida nos seus interlúdios e desimportâncias, detalhes que constituem matéria-prima para bons observadores. **Anderson Lira**, meu tio, com quem passei o período de transição entre a Bahia e Pernambuco, que me apresentou o Recife e que me ajudou em diversos momentos durante esses anos em que vivo no Recife. **Marcelo Couto Guedes**, meu primo, com as suas sagacidade e catilogência embebidas no mais alto grau da inteligência irônica, abriga em si, ao mesmo tempo, um humanismo assustadoramente simples. A Profª. **Lívia Couto Guedes**, minha prima, presenciou e muito contribuiu para o meu crescimento acadêmico, sendo uma excelente companhia para o debate intelectual e as conversas sobre o estado das coisas, além de ser um exemplo de que a simplicidade é o ápice da sofisticação. **Nadine Bovet**, minha namorada, amiga e companheira, que compartilha comigo os momentos, as vitórias e os desafios, encarnando a citação do **Guimarães Rosa**, em Grande Sertão: Veredas, do amor como "um pouquinho de saúde, um descanso na loucura" e

uma composição da **Sueli Costa** e do **Cacaso**, do amor e do mar como complexa e irretocável calmaria. Com ela, o belo é possível e a vida persiste. Agradeço a **Valdomiro Matias** e a **Laurinete Lins**, bem como à toda família Matias, por toda hospitalidade e pela convivência vivificante, que foram salutares durante a minha seleção para o doutorado e trouxeram leveza ao que é e deve ser, de fato, leve. Dentre as minhas amigas e os meus amigos, principio agradecendo a **Carolina Dolléans**, cujos apoio, conversa e companhia tornaram o percurso do mestrado muito mais otimista e possível. Além de tudo, ela é a pesquisadora mais generosa que conheço. **Gabriela Vilela Lyra**, de quem eu e Carolina fomos coautores na nossa primeira inveteração nos periódicos, é de uma grandeza e de uma sensatez admiráveis, além de ser a amiga que esteve comigo durante o período mais difícil da pandemia. As duas perpassaram o tempo, estão entre as descobertas da minha vida. **Thays Oliveira**, minha amiga, com quem também participei de eventos e coordenei Grupos de Trabalho, tem em si uma fonte inesgotável de determinação. Com empenho e tempo, o horizonte desfaz os limites. Profª. **Anahí Barbosa**, minha amiga, é a pessoa com quem converso sobre os mistérios da vida, do universo e tudo mais, e integra o conjunto das pessoas que gosto desde que conheci, sem explicações e de graça. Agradeço a **Luiza Marriely**, que enquanto médica é de um profissionalismo ímpar porque humano, e como amiga tem sido um dos motivos pelos quais o tempo e a pandemia não me soterraram. **Fernanda Negromonte**, minha amiga, vivenciou comigo alguns dos maiores desafios durante o bacharelado e, assim como eu, perseverou e finalizou etapas. Ela é corresponsável por algumas das minhas melhores decisões e acrescenta referências musicais preciosas à minha vida. Conclamo **Daniel Barreto Ferreira**, meu primeiro amigo, porque é ele e porque sou eu. Nele, a ideia de "páreo nisso tudo deste mundo" se torna inescapavelmente real, a contragosto da álvara destinação do Pessoa. São dele algumas das frases mais inteligentes e outras tantas das mais equivocadas que ouvi na vida. E isso é maravilhoso. **Railda Freitas**, minha amiga, com quem criei projetos culturais, participei da elaboração de documentos institucionais, e que foi a pessoa que ratificou a minha capacidade de liderança, não reconhecida, até então, por mim. Ela tem lugar cativo no meu coração, sendo uma extensão do mesmo onde ela estiver. E ela sabe disso. **Ju Velloso**, minha mais recente amiga atemporal, oferece ao mundo sempre o melhor que há em si e propaga boas ações e um sorriso belo por onde passa. Algumas das respostas da vida podem ser facilmente encontradas nesse comportamento altivo porque generoso. Profº. **Rafael Mesquita**, meu orientador, com quem aprendo todos os dias a poderosa força da disciplina, da humildade e da diligência, características que o fazem ser o exemplo de pessoa e intelectual que almejo ser. Prof. **Marcos Guedes**, meu orientador no bacharelado, que me acolheu no

Núcleo de Estudos Americanos - NEA, no Grupo de Pesquisa “O Brasil e as Américas” e na Rede CTIDC, proporcionando oportunidades muito relevantes para a minha carreira. Agradeço ao Prof. **Rodrigo Albuquerque**, de quem sou coautor junto ao Prof. **Rafael Mesquita**, e que chancelou, com o bom humor que lhe é característico, a ideia do Triplo-R. Agradeço também ao Prof. **Dalson Figueiredo**, Coordenador do PPGCP/UFPE, que ministrou a disciplina Seminário de Dissertação com maestria, e com quem participei da coordenação do Grupo de Trabalho “Show me the data: potenciais metodológicos para políticas públicas baseadas em evidências”, ao Prof. **Davi Moreira**, que aceitou integrar a proposta de estudo sobre a CPI da COVID-19 e convidou a mim e a **Carolina Dolleáns** para participar do projeto Retórica Parlamentar, ao Prof. **Ricardo Borges**, por muito humanamente ter se disponibilizado a se reunir comigo ainda no bacharelado e conversar sobre o meu tema na época, tirando dúvidas e indicando referencial teórico, ao Prof. **Gills Vilar Lopes**, cujos trabalhos lançaram as bases que possibilitaram a existência desta dissertação, e cujas generosidade e disponibilidade se materializaram em um acervo inestimável de referências para a área, que ele compartilha com todos que o procuram. Os seus comentários e sugestões na minha qualificação também conduziram ao aprofundamento desta dissertação. A Prof.ª **Andrea Steiner** foi a primeira entusiasta da progressão dos meus estudos, de estudo de caso para teoria de médio porte e, finalmente, um estudo sobre o mundo. Nela, encontrei uma confirmação da validade desse movimento e um reflexo da curiosidade científica. Agradeço, ainda, ao Prof. **Leon Queiroz**, ao Prof. **Marcelo Medeiros**, à Prof.ª **Olívia Perez**, uma vez mais ao Prof. **Rafael Mesquita** e, *last but not least*, ao Prof. **Ranulfo Paranhos**, integrantes da Comissão Avaliadora da Seleção do Doutorado 2022 - PPGCP/UFPE, pelas integridade e lisura com as quais conduziram o referido concurso. Participar desse processo sendo avaliado por profissionais tão empenhados nas suas respectivas áreas trouxe um significado a mais para a experiência. Encerrando esta colcha de homenagens aos integrantes do caminho causal que conduz a minha vida acadêmica, agradeço aos leitores, que poderão replicar, discutir e citar esta obra, fincando raízes minhas e perpetuando o impacto social do investimento proporcionado pela Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco - FACEPE.

Quando a pátria que temos não a temos
Perdida por silêncio e por renúncia
Até a voz do mar se torna exílio
E a luz que nos rodeia é como grades
(Sophia de Mello Breyner Andresen, Exílio)

(...) Neste retiro em que me não conhecem.
Nem só lodos se arrastam, nem só lamas,
Nem só animais bóiam, mortos, medos,
Túrgidos frutos em cachos se entrelaçam
No negro poço de onde sobem dedos.
Só direi, crispadamente recolhido e mudo,
Que quem se cala quando me calei
Não poderá morrer sem dizer tudo.
(José Saramago, Poema à boca fechada)

Apesar das ruínas e da morte,
Onde sempre acabou cada ilusão,
A força dos meus sonhos é tão forte,
Que de tudo renasce a exaltação
E nunca as minhas mãos ficam vazias.
(Sophia de Mello Breyner Andresen,
Apesar das ruínas e da morte)

Olhando o tempo passar carcará não caça
Mas eu sei que o tempo passa e o dia há de chegar
De alguém vir me avisar carcará mandou recado
Está mais velho e mais cansado e a voz mais rouca e mais feio
Saiu pra dar um passeio, tá todo mundo assombrado
(Siba, Carcará de Gaiola)

Esta é a madrugada que eu esperava
O dia inicial inteiro e limpo
Onde emergimos da noite e do silêncio
E livres habitamos a substância do tempo
(Sophia de Mello Breyner Andresen, 25 de Abril)

RESUMO

Quais fatores explicam o nível de comprometimento com a Segurança Cibernética no continente americano? Esta pesquisa busca responder a essa questão a partir de uma análise configuracional-qualitativa dos 35 países americanos listados no *Global Cybersecurity Index* (GCI) para o ano-referência de 2018. Como condições explicativas do modelo, utilizamos: a) Securitização; b) Despesas Militares; c) Ocorrência de eventos raros em Segurança Cibernética; d) Tempo do marco jurídico-institucional do setor cibernético; e) Militarização do Espaço Cibernético; f) Desenvolvimento econômico. Metodologicamente, este trabalho é estruturado na Análise Qualitativa Comparativa, *Qualitative Comparative Analysis* (QCA), seguida pela realização de um estudo aprofundado, e orientado por mecanismos causais, do caso brasileiro. Dessa maneira, o desenho resultante consiste em uma pesquisa com caráter metodológico misto em relação à análise e à coleta dos dados. Detalhadamente, buscamos identificar quais conjuntos de configurações explicam o nível de comprometimento com a Segurança Cibernética nos países do continente americano em 2018. De maneira complementar, realizamos um estudo de caso para explicar, através de mecanismos causais, como as condições/fatores explicativos se configuram no contexto nacional. Os principais resultados da pesquisa apontam para a identificação de três caminhos causais para o maior comprometimento com a Segurança Cibernética: 1) Despesas Militares associadas ao Desenvolvimento Econômico (Estados Unidos, Canadá, Chile e Uruguai); 2) Despesas Militares e Tempo do Marco Jurídico-Institucional (Cuba); 3) Militarização do Espaço Cibernético e Desenvolvimento Econômico (Brasil e Colômbia). As condições que explicam esses caminhos conjunturalmente foram identificadas como do tipo INUS. O estudo do contexto brasileiro apontou como mecanismo causal o histórico de militarização de setores no país explicado pelos jogos institucionais de barganha orçamentária e pela busca de legitimação dos militares frente à sociedade civil. Como consequência do caminho percorrido pelo país, elencamos alguns problemas: 1) o desvio da função do setor; 2) a ineficiência na resolução de problemas reais da sociedade, como os crimes cibernéticos. Por fim, são discutidas as limitações do trabalho e disponibilizados o repositório dos dados da pesquisa e o código para replicação.

Palavras-chave: Segurança Cibernética Comparada; Américas; Brasil; QCA; Estudo de Caso.

ABSTRACT

What factors explain the level of commitment to Cybersecurity on the American continent? This research seeks to answer this question from a configurational-qualitative analysis of the 35 American countries listed in the Global Cybersecurity Index (GCI) in 2018. As explanatory conditions of the model, we used: a) Securitization; b) Military Expenditure; c) Occurrence of rare events in Cybersecurity; d) Time of the Legal-Institutional Framework; e) Militarization of the Cyberspace; f) Economic Development. Methodologically, this work is structured in Qualitative Comparative Analysis (QCA), followed by an in-depth study, guided by causal mechanisms, of the Brazilian case. Thus, the resulting design consists of a research with a mixed methodological character in relation to data analysis and collection. In detail, we sought to identify which sets of configurations explain the level of commitment to Cybersecurity in the countries of the American continent in 2018. In a complementary way, we carried out a case study to explain, through causal mechanisms, how the explanatory conditions/factors are configured in the national context. The main results of this study lead to the identification of three causal pathway towards a greater commitment with Cybersecurity: 1) Military Expenditure associated to Economic Development (United States, Canada, Chile and Uruguay); 2) Military Expenditure and Time of the legal-institutional framework (Cuba); 3) Militarization of the Cyber Space and Economic Development (Brazil and Colombia). Conditions that explain these pathways, in a conjunctural nature, were identified as type INUS. The study of the Brazilian case showed, as causal mechanisms, the history of militarization of sectors in the country explained by institutional games of budget bargain and by the investigation/search of legitimization of the military towards the civil society. As a consequence of the pathway traveled by the country, we raise some issues: 1) the deviation of the sector's function; 2) the inefficiency in the resolution of real social problems, like cybercrimes. Finally, the limitations of the work are discussed and the repository of research data and the code for replication are made available.

Keywords: Comparative Cybersecurity; Americas; Brazil; QCA; Case Study.

RESUMEN

¿Qué factores explican el nivel de compromiso con la Ciberseguridad en el continente americano? Esta investigación busca responder a esta pregunta a partir de un análisis configuracional-cualitativo de los 35 países americanos listados en el *Global Cybersecurity Index* (GCI) para el año de referencia 2018. Como condiciones explicativas del modelo se utilizaron: a) Securitización; b) Gastos militares; c) Ocurrencia de eventos raros en Seguridad Cibernética; d) Tiempo del Marco Jurídico-Institucional del sector Cibernético; e) Militarización del Ciberespacio; f) Desarrollo Económico. Metodológicamente, este trabajo se estructura en el Análisis Comparativo Cualitativo, *Qualitative Comparative Analysis* (QCA), seguido de un estudio en profundidad, guiado por mecanismos causales, del caso brasileño. De esta forma, el diseño resultante consiste en una investigación de carácter metodológico mixto en lo que se refiere al análisis y la recogida de datos. En detalle, buscamos identificar qué conjuntos de configuraciones explican el nivel de compromiso con la Ciberseguridad en los países del continente americano en 2018. De manera complementaria, realizamos un estudio de caso para explicar, a través de mecanismos causales, cómo las condiciones explicativas/factores se configuran en el contexto nacional. Los principales resultados de la investigación apuntan a la identificación de tres caminos causales para un mayor compromiso con la Ciberseguridad: 1) Gastos Militares asociados al Desarrollo Económico (Estados Unidos, Canadá, Chile y Uruguay); 2) Gastos Militares y Tiempo del Marco Jurídico-Institucional (Cuba); 3) Militarización del Ciberespacio y Desarrollo Económico (Brasil y Colombia). Las condiciones que explican estos caminos fueron identificadas como del tipo INUS. El estudio del contexto brasileño señaló como mecanismo causal la historia de militarización de sectores en el país, explicada por los juegos institucionales de negociación presupuestaria y la búsqueda de legitimación de los militares frente a la sociedad civil. Como consecuencia del camino recorrido por el país, enumeramos algunos problemas: 1) el desvío de la función del sector; 2) ineficiencia en la solución de problemas reales de la sociedad, como los delitos cibernéticos. Finalmente, se discuten las limitaciones del trabajo y se ponen a disposición el repositorio de datos de investigación y el código para la replicación.

Palabras clave: Ciberseguridad Comparativa; Américas; Brasil; QCA; Estudio de Caso.

RÉSUMÉ

Quels sont les facteurs qui expliquent le niveau d'engagement envers la sur le continent américain? Cette recherche a pour but de répondre à cette question à partir d'une analyse configurationnelle-qualitative des 35 pays américains listés dans le *Global Cybersecurity Index* (GCI), pour l'année de 2018. Comme conditions explicatives du modèle, nous utilisons: a) Sécuritisation; b) Dépenses Militaires; c) Occurrence d'évènements rares; d) Temps du Cadre Juridico-Institutionnel du Secteur Cybernétique; e) Militarisation de l'Espace Cybernétique; f) Développement Économique. Méthodologiquement, ce travail est structuré par l'Analyse Qualitative Comparative, *Qualitative Comparative Analysis* (QCA), suivi par la réalisation d'une étude approfondie, et orientée par des mécanismes causaux, du cas brésilien. De cette façon, le plan de recherche résultant possède un caractère méthodologique mixte par rapport à l'analyse et la collecte des données. Plus précisément, nous cherchons à identifier quels sont les ensembles de configurations qui expliquent le niveau d'engagement envers la cybersécurité dans les pays du continent américain en 2018. De manière complémentaire, nous réalisons une étude de cas pour expliquer, à travers des mécanismes causaux, comment les conditions/facteurs explicatifs se configurent dans le contexte national. Les principaux résultats de la recherche permettent l'identification de trois chemins causaux menant à un engagement plus important envers la Sécurité Cybernétique: 1) Dépenses Militaires associées au Développement Économique (Etats-Unis, Canada, Chile, Uruguay); 2) Dépenses Militaires et le Temps du Cadre Juridico-Institutionnel (Cuba); 3) Militarisation de l'Espace Cybernétique et le Développement Économique (Brésil et Colombie). Les conditions qui expliquent ces chemins de manière conjoncturelle ont été identifiées comme étant du type INUS. L'étude du contexte brésilien a révélé, comme mécanisme causal, l'historique de militarisation de secteurs dans le pays expliqué par les jeux institutionnels de négociation budgétaire et par la recherche de légitimation des militaires par rapport à la société civile. En conséquence du chemin parcouru par le pays, nous recensons quelques problèmes: 1) le détournement de la fonction du secteur; 2) l'inefficience dans la résolution de problèmes réels de la société, comme les crimes cybernétiques. Enfin, nous examinons les limitations du travail et disponibilisons la banque de données de la recherche et le code qui sert à la réplication.

Mots-clés: Cybersécurité Comparative; Amériques; Brésil; QCA; Étude de cas.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS

AGESIC	*Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento*
BID	Banco Interamericano de Desenvolvimento
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CCDCOE	Centro de Excelência Cooperativa de Defesa Cibernética da Organização do Tratado do Atlântico Norte
CDCiber	Centro de Defesa Cibernética
CERT.br	Centro de Estudos de Resposta e Tratamento de Incidentes de Segurança para a Internet Brasileira
CERTs	*Computer Emergency Response Teams*
CIA	*Central Intelligence Agency*
CIRTs	*Computer Incident Response Teams*
CISA	*Cybersecurity and Infrastructure Security Agency*
CMDT-17	Conferência Mundial de Telecomunicações em 2017
CMSI	Cúpula Mundial sobre a Sociedade da Informação
CNUDS	Conferência das Nações Unidas sobre Desenvolvimento Sustentável
COMDCIBER	Comando de Defesa Cibernética
CONPES 3854	*Política Nacional de Seguridad Digital - Consejo Nacional de Política Económica y Social*
CPRI	Ciência Política e Relações Internacionais
CSIRTs	*Computer Security Incident Response Teams*
CSIS	*Center for Strategic & International Studies*
csQCA	*Crisp-set QCA*
DoS	*Distributed Denial of Service*
ECEME	Escola de Comando e Estado-Maior do Exército
END	Estratégia Nacional de Defesa
ESMC	Espectro da Securitização Militar do Ciberespaço
FACEPE	Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco
fsQCA	*Fuzzy-set QCA*
GCA	*Global Cybersecurity Agenda*
GCI	*Global Cybersecurity Index*

GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IDH	Índice de Desenvolvimento Humano
INUS	*Insufficient but Necessary part of a condition which is itself Unnecessary but Sufficient for the result*
IPdDC	Índice de Politização Documental da Defesa Cibernética
IPiDC	Índice de Politização Institucional da Defesa Cibernética
IPvDC	Índice de Politização Virtual da Defesa Cibernética
IT	*Information Technology*
ITU	União Internacional de Telecomunicações
KKV	King, Keohane e Verba
LAI	Lei de Acesso à Informação
LNA	*Large-N analysi*
MCI	Marco Civil da *Internet*
MEC	Ministério da Educação
mvQCA	*multi-value Qualitative Comparative Analysis*
NSA	Agência de Segurança Nacional
OEA	Organização dos Estados Americanos
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
OTSC	Organização do Tratado de Segurança Coletiva
OWID	*Our World in Data*
PIB	Produto Interno Bruto
PIPEDA	*Personal Information Protection and Electronic Documents Act*
PNSI	Política Nacional de Segurança da Informação
PND	Política Nacional de Defesa
PNUD	Programa das Nações Unidas pelo Desenvolvimento
PPGCP/UFPE	Programa de Pós-Graduação em Ciência Política da Universidade Federal de Pernambuco
QCA	*Qualitative Comparative Analysis*
REMJA	*Reuniones de Ministros de Justicia y otros Ministros y Fiscales Generales de las Américas*
SCADA	Sistema de Supervisão e Aquisição de Dados
SUIN	*Sufficient but Unnecessary part of a factor that is Insufficient but Necessary for an outcome*

TIC	Tecnologias da Informação e Comunicação
UE	União Europeia
UFPE	Universidade Federal de Pernambuco
UFSC	Universidade Federal de Santa Catarina
UNIDIR	Instituto das Nações Unidas para Pesquisa de Desarmamento

LISTA DE ABREVIATURAS

cf. *confer*.

e. g. *exempli gratia*.

et al. *et alia.*

LISTA DE SÍMBOLOS

$\cap$	Interseção.
+	Adição, ou positivo.
-	Subtração, ou negativo.

SUMÁRIO

1 INTRODUÇÃO

"Whereas science elicits changes in order to know, technology knows in order to elicit changes." (Mario Bunge)

A Revolução Digital proporcionou uma realidade na qual as noções de fronteira e espaços instam por uma nova definição (LÉVY, 1997). Os territórios antes analisados em suas dimensões marítima, aérea, espacial e terrestre se complexificam com o surgimento de uma infraestrutura material capaz de criar flutuações de informação desconstituídas de geografia estática.

O espaço cibernético não é apenas mais uma divisão geográfica do território, mas uma divisão sobreposta a todas as possibilidades de divisão territorial, como em um nó intrincado de circuitos virtualizados. Sua estrutura cibernética pode funcionar em uma rede fechada, restrita ou em hiperconexão - como a rede mundial de computadores. Ele é, portanto, um território deslocalizado, embora não rompa absolutamente com as relações espaciais tradicionais, uma vez que requer servidores físicos para sua virtualização (GUEDES DE OLIVEIRA; PORTELA, 2017). Nesse sentido, denota-se a importância mundial da Segurança Cibernética como objeto de estudo, uma vez que a mesma engloba discussão tão ou mais urgente quanto os debates fronteiriços ao seu tema, como os de Segurança Pública, Defesa e Defesa Cibernética.

Não obstante, com a popularização do caso Snowden[1] , ocorrido em 2013, instaurou-se uma agenda de pesquisa sobre as ameaças emergentes, especificamente as mais midiatizadas como os terrorismo e espionagem cibernéticos. Em tempo, os Estados passaram a perceber a necessidade do fortalecimento das suas políticas de Segurança e Defesa Cibernéticas, bem como do investimento em alta tecnologia e recursos humanos especializados. Essa questão também se tornou patente por causa da ocorrência de eventos raros na área, que demonstraram a vulnerabilidade dos países envolvidos em relação à Segurança Cibernética.

A União Internacional de Telecomunicações (ITU), agência que integra a Organização das Nações Unidas (ONU), foi fundada há 156 anos e tem seu *framework* voltado a temas de Tecnologias da Informação e Comunicação (TICs), aspirando a cooperação internacional na área de satélites orbitais e atuando no estabelecimento de normas mundiais em agendas como

[1] Edward Joseph Snowden, ex-administrador de sistemas da Central Intelligence Agency (CIA) que tornou públicos arquivos referentes ao sistema de vigilância global da NSA.

as de mudanças climáticas, acessibilidade e fortalecimento da segurança cibernética[2].

Nesse contexto, as metas estabelecidas no marco da Cúpula Mundial sobre a Sociedade da Informação (CMSI) e as Iniciativas Regionais adotadas durante a Conferência Mundial de Telecomunicações em 2017 (CMDT-17) são referências para a ITU, que busca conectar o mundo por meio da mobilização de recursos humanos, técnicos e financeiros.

A partir dessas contribuições, foi criado o Índice Global de Segurança Cibernética (*Global Cybersecurity Index* - GCI). Ele é resultado dos questionários elaborados pela ITU e desenvolvidos ao longo dos anos, sendo o seu objetivo mensurar o comprometimento dos Estados-membros da ONU em relação à Segurança Cibernética, com o intuito de aumentar a conscientização sobre a temática no mundo. Participam do Índice 193 Estados-membros, além do Estado da Palestina, totalizando 194 países avaliados. No entanto, apenas 54% deles responderam ao inquérito em 2015, 69% em 2017, e cerca de 80% em 2018. Nesta última versão, dos 194 casos, o índice de 2018 contou com 155 respondentes (ITU, 2019). No entanto, mesmo sem os questionários respondidos pelos responsáveis nos países, os especialistas da ITU buscam aproveitar ao máximo as informações, através de fontes primárias e secundárias, de maneira que o número de casos com dados disponíveis representa a totalidade dos países analisados.

De acordo com a União Internacional de Telecomunicações (2019), o GCI é um índice composto por 25 indicadores agrupados nos 5 pilares da *Global Cybersecurity Agenda* (GCA), que são: a) Legal; b) Técnico; c) Organizacional; d) Capacitação; e) Cooperação.

O eixo Legal é formado por três indicadores que mensuram a existência de instituições jurídicas referentes à Segurança Cibernética e aos crimes cibernéticos, enquanto o Técnico é composto a partir de seis indicadores relacionados à presença de estruturas técnicas na área.

O pilar Organizacional é constituído por três indicadores que avaliam a coordenação de políticas e estratégias para o desenvolvimento da Segurança Cibernética em nível nacional, enquanto o eixo de Capacitação consiste em sete indicadores que verificam a realização de programas de pesquisa e desenvolvimento, educação e treinamento, de profissionais certificados, bem como de agências do setor público que promovam a capacitação destes.

Por último, o eixo de Cooperação mensura, a partir de seis indicadores, a existência de parcerias, quadros cooperativos e redes de compartilhamento de informações (ITU, 2019). O Quadro 1 sumariza essas informações.

---

[2] Disponível em: https://www.itu.int/en/about/Pages/default.aspx. Acesso em: 12 de fev. de 2021.

Quadro 1 - Pilares do Índice Global de Segurança Cibernética (GCI).

PILARES DO GCI	INDICADORES
LEGAL	1) Legislação sobre crimes cibernéticos; 2) Regulamentação da Segurança Cibernética; 3) Legislação para contenção de *spam*.
TÉCNICO	1) Existência, a nível nacional, regional e setorial de *Computer Emergency Response Teams* (CERTs), *Computer Security Incident Response Teams* (CSIRTs) e *Computer Incident Response Teams* (CIRTs); 2) Estrutura de implementação de padrões de Segurança Cibernética para organizações; 3) Existência de um órgão de padronização; 4) Mecanismos técnicos e recursos para lidar com *spam*; 5) Uso da nuvem para fins de cibersegurança; 6) Mecanismos de proteção online para crianças.
ORGANIZACIONAL	1) Existência de Estratégia Nacional; 2) Agência designada responsável pelo setor; 3) Métricas/parâmetros de Segurança Cibernética.
CAPACITAÇÃO	1) Campanhas públicas de conscientização; 2) Padrões na Segurança Cibernética e na certificação de profissionais; 3) Cursos de treinamento profissional em Segurança Cibernética; 4) Programas nacionais de educação e currículos acadêmicos em Segurança Cibernética; 5) Programas de Pesquisa e Desenvolvimento (R&D) em Segurança Cibernética; 6) Mecanismos de incentivo no setor; 7) Indústria de Segurança Cibernética nacional.
COOPERAÇÃO	1) Acordos bilaterais; 2) Acordos multilaterais; 3) Participação em fóruns e associações internacionais na área; 4) Parcerias público-privadas; 5) Parcerias inter-agências e intra-agências; 6) Aplicação das melhores práticas em Segurança Cibernética.

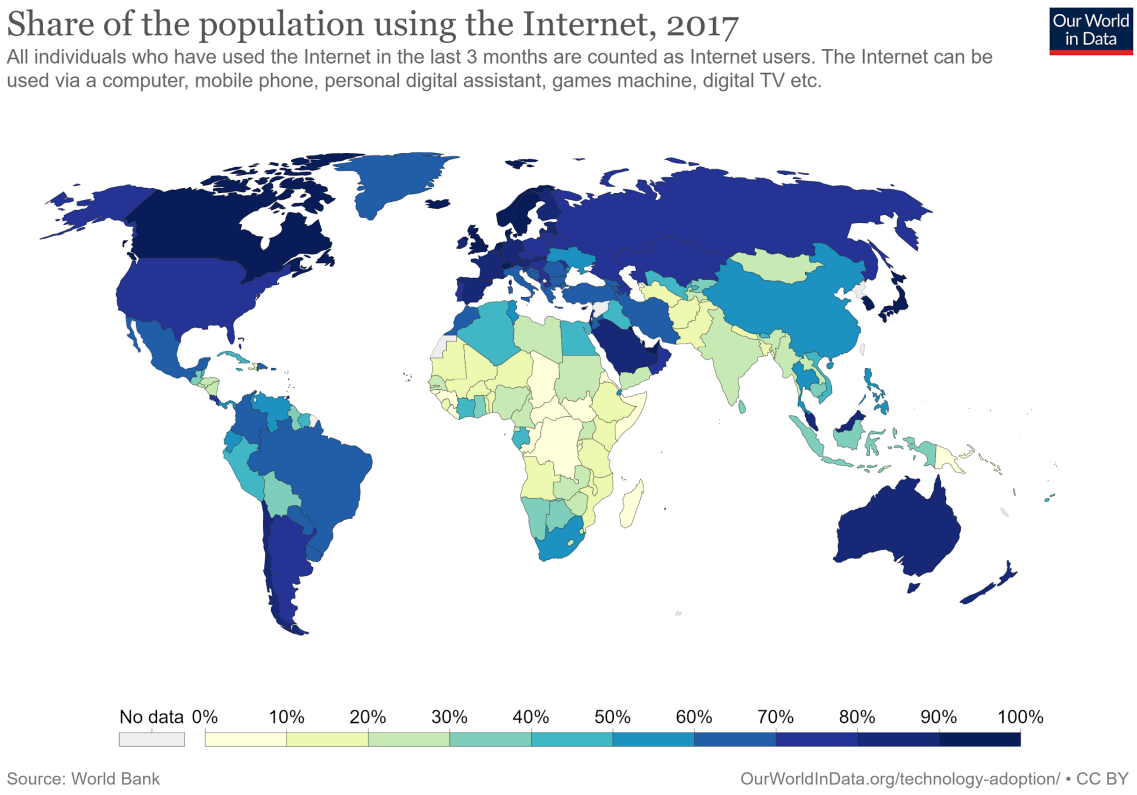
Fonte: ITU (2019) e Lira-Brito (2021). Adaptação do autor.

Quando observado a partir da Segurança Cibernética, o continente americano, dividido entre as regiões América do Norte, América Central e América do Sul, apresenta, em seus 35 países, alta variabilidade na pontuação do Índice Global de Segurança Cibernética (GCI), garantindo uma distribuição que abrange tanto casos entre as melhores (Estados Unidos, 1º lugar no ranque regional e 2º lugar no mundial, 0,926) quanto entre as piores (Comunidade da Dominica, 33º lugar no ranque regional e 172º lugar no mundial, 0,019)

pontuações no ranque global, que são considerados *outliers*, além de exemplos dos casos considerados mais comuns, ou próximos à mediana (0,440), como o Chile (9º lugar no ranque regional e 83º no mundial, 0,470).

No ano de 2020, com cerca de 784 milhões de usuários na *Internet* e taxa de penetração em torno de 80%[3], o continente americano se posicionou em segundo lugar em relação ao quantitativo de usuários em sua população, sucedendo apenas o continente asiático e precedendo os continentes europeu, africano e Oceania. Além disso, dois países do Continente, Estados Unidos e Canadá, integraram a seleção dos 5 Estados com maior número de usuários da *Internet* em 2017. Na Figura 1, apresentamos um mapa mundial que representa a taxa de usuários da *Internet* distribuída espacialmente, tendo os países como unidade observada.

Figura 1 - Usuários da *Internet* por país em 2017.



Fonte: Our World in Data - OWID[4].

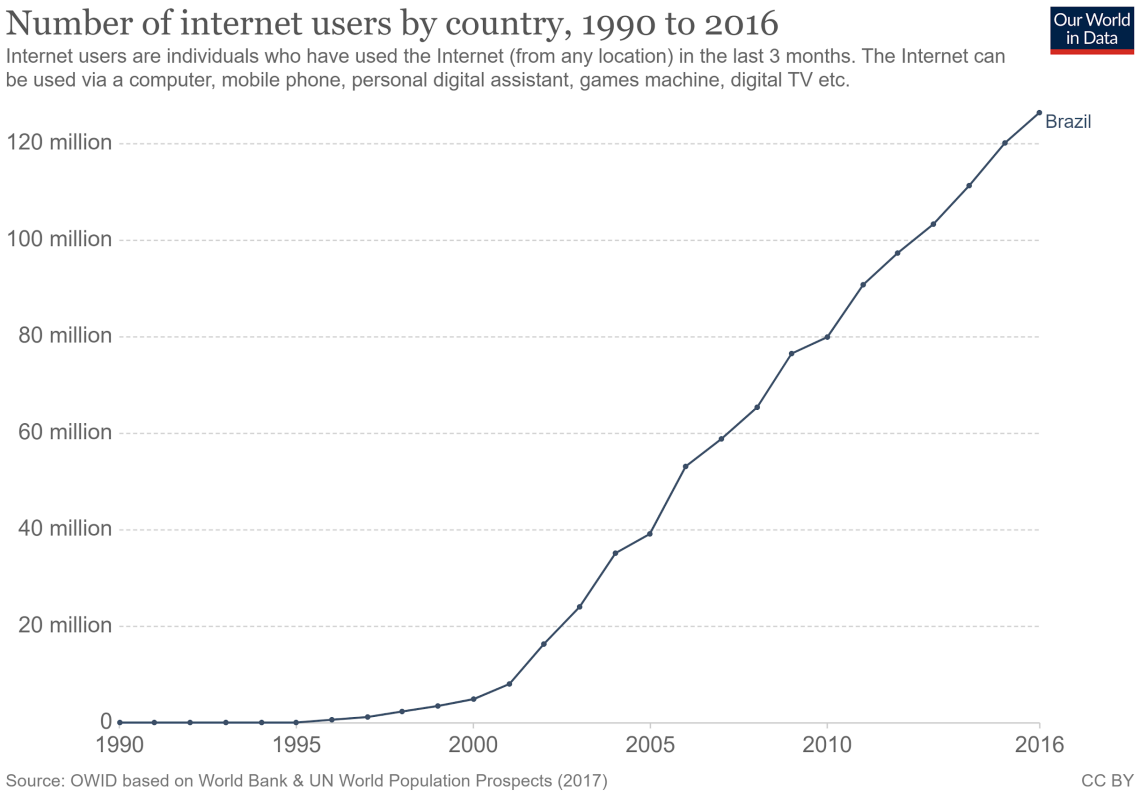
Como a Figura 1 evidencia, no continente americano há poucos Estados com menos de 60% de taxa de penetração da *Internet*. Essa informação, aliada aos dados sobre a região

[3] Disponível em: https://www.internetworldstats.com/stats2.htm. Acesso em 15 de fev. de 2021.
[4] Disponível em: https://ourworldindata.org/internet. Acesso em 10 de fev. de 2021.

no Índice Global de Segurança Cibernética, reforça a necessidade da realização de pesquisas empíricas sobre o comprometimento dos países americanos no que concerne à Segurança Cibernética e aos fatores que podem explicá-lo.

Além disso, no ano de 2019, com uma população de mais de 210 milhões de habitantes, o Brasil já registrava a marca de 150 milhões de usuários, com cerca de 257 milhões de aparelhos celulares[5]. Como pode ser observado na Figura 2, grande parte do crescimento substancial no número de usuários na *Internet* no País ocorreu do ano de 2000 até o ano de 2016, saltando de cerca de 10 milhões de usuários para mais de 120 milhões, fato que situou o País entre as maiores populações virtualizadas, transpondo as suas proporções continentais também para o espaço cibernético.

Figura 2 - Brasil: número de usuários no período 1990 - 2016.



Fonte: Our World in Data - OWID.

Nessa perspectiva, as informações levantadas pelo Centro de Estudos de Resposta e Tratamento de Incidentes de Segurança para a Internet Brasileira (CERT.br) revelaram que,

[5] Disponível em: https://www.internetworldstats.com/. Acesso em: 10 de fev. de 2021.

desde o início do seu período de análise, o País presenciou um salto considerável de 3.000 ataques registrados no ano de 1999 para 675.000 no ano de 2018[6].

Além disso, no mesmo ano, quase 78% dos incidentes reportados ao CERT.br tiveram como origem o solo brasileiro. Dessa maneira, é pungente a relevância desse País como objeto de estudo no âmbito da Segurança Cibernética, considerando a quantidade de usuários, os incidente reportados e o fato de que a maior parte dos mesmos são oriundos do seu território[7]. A pontuação do Brasil (0,577) no GCI classifica-o em sexto lugar no ranque regional, que é liderado pelos Estados Unidos, e septuagésimo no ranque global, consistindo em um exemplo de país com nível médio (0,669 - 0,340) de comprometimento com a Segurança Cibernética.

1.1 PERGUNTA DE PESQUISA

Quais fatores explicam o nível de comprometimento com a Segurança Cibernética nas Américas? Esta pesquisa objetiva responder a essa pergunta através da identificação dos conjuntos de condições que explicam o nível de comprometimento com a Segurança Cibernética no continente americano para o ano-referência de 2018.

1.2 HIPÓTESES

As hipóteses desta pesquisa consistem em uma hipótese central, **H1**, e seis hipóteses secundárias, **H1.1**, **H1.2**, **H1.3**, **H1.4**, **H1.5**, **H1.6**. Há uma hierarquia de nível entre a primeira e as consecutivas porque estas últimas estão circunscritas pela hipótese basilar, ou seja, a rejeição da hipótese nula de todas elas implica a rejeição da hipótese nula da primeira.

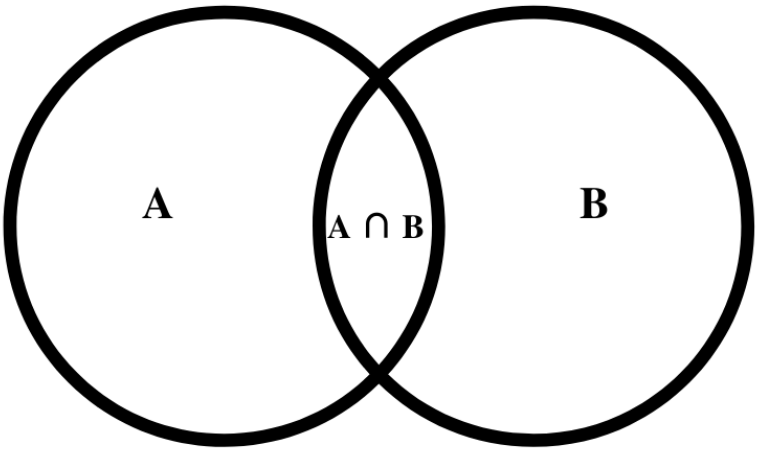
Nas seis hipóteses secundárias, argumentamos pela possibilidade de confirmação das mesmas caso sejam observadas a necessidade ou a suficiência da condição (SCHNEIDER, 2018), de forma a alcançar o maior horizonte de possibilidades, como pode ser observado na Figura 3.

---

[6] Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 10 de fev. de 2021.

[7] Disponível em: https://www.cert.br/stats/incidentes/2018-jan-dec/top-cc.html. Acesso em: 11 de fev. de 2021.

Figura 3 - Conjuntos Necessidade, Suficiência e a sua Interseção.



Fonte: Banco de dados da pesquisa. Elaboração do autor.

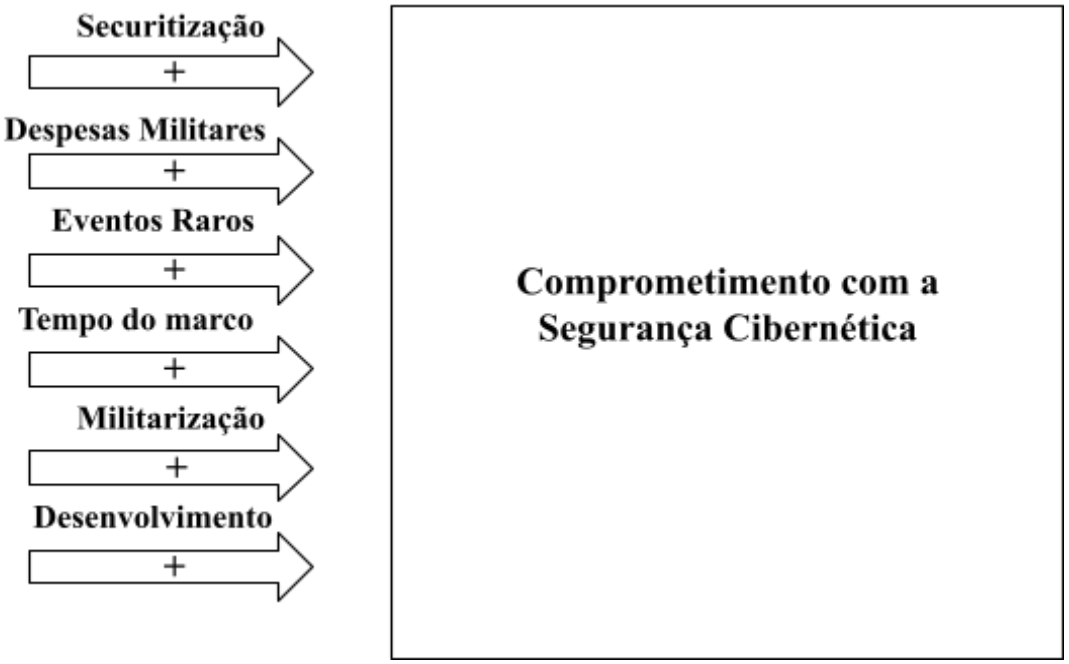
Na Figura 3, o conjunto denominado **A** se refere à necessidade, agregando as condições necessárias para que algum fenômeno ocorra. Paralelamente, o conjunto **B** é relativo à suficiência, ou seja, reúne as condições que são suficientes para o acontecimento do fenômeno observado. A interseção entre eles, **A∩B**, abarca as condições que são, ao mesmo tempo, necessárias e suficientes.

A assunção presente em **H1**, de que as condições 1) Securitização da Segurança Cibernética, 2) Despesas Militares, 3) Ocorrência de Eventos Raros, 4) Tempo do Marco Jurídico-institucional, 5) Militarização da Segurança Cibernética, e 6) Desenvolvimento Econômico, explicam conjunturalmente o comprometimento com a Segurança Cibernética nos países do continente americano, é a hipótese basilar desta pesquisa. A hipótese nula é a de que as referidas condições não explicam conjunturalmente o comprometimento com a Segurança Cibernética nos Estados das Américas.

Deriva-se dela as seguintes hipóteses de que a **Securitização** (**H1.1**), as **Despesas Militares** (**H1.2)**, a **Ocorrência de Eventos Raros** (**H1.3**), o **Tempo do Marco Jurídico-institucional** (**H1.4**), a **Militarização da Segurança Cibernética** (**H1.5**) e o **Desenvolvimento Econômico** (**H1.6**) são condições necessárias e/ou suficientes para explicar

o comprometimento com a Segurança Cibernética nos países do continente americano. Em seguida, na Figura 4, representamos a síntese das relações que esperamos observar na realidade empírica.

Figura 4 - Síntese das Relações Esperadas.



Fonte: Banco de dados da pesquisa. Elaboração do autor.

Na Figura 4, apresentamos um resumo das relações esperadas entre as condições explicativas e o objeto do estudo. Dessa forma, a expectativa teórica é de que a securitização do setor, as despesas militares, a ocorrência de eventos raros, o tempo do marco jurídico institucional, a militarização da Segurança Cibernética e o desenvolvimento econômico são determinantes para a explicação do comprometimento com Segurança Cibernética nos países americanos para o ano-referência de 2018. Na primeira seção deste estudo, discorremos mais detalhadamente sobre as relações esperadas entre as condições e o fenômeno observado, além da conceituação.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Explicar o nível de comprometimento com a Segurança Cibernética no continente americano no ano de 2018.

1.3.2 Objetivos Específicos

1. **Analisar** de maneira exploratória a pontuação dos países americanos no *score* do *Global Cybersecurity Index* em 2018;
2. **Mensurar** as condições, para os países americanos: a) securitização; b) despesas militares; c) ocorrência de eventos raros; d) tempo do marco jurídico-institucional; e) militarização do setor de Segurança Cibernética; e f) desenvolvimento econômico;
3. **Testar** quais conjuntos de configurações explicam o nível de comprometimento com a Segurança Cibernética nos países do continente americano em 2018;
4. **Identificar os mecanismos causais** para o comprometimento com a Segurança Cibernética no contexto brasileiro.

1.4 JUSTIFICATIVA

Como enunciam King, Keohane e Verba (1994), “um projeto de pesquisa deve propor uma questão que é importante no mundo real” e “deve fazer uma contribuição específica para a produção acadêmica da área, aumentando a capacidade coletiva de construir explicações científicas verificadas de um certo aspecto do mundo” (p. 15, tradução livre). Assim, especificamos, a seguir, quais são as principais contribuições sociais e científicas deste trabalho, bem como as áreas disciplinares contempladas pelo aporte mobilizado na pesquisa.

Nesse âmbito, um dos principais problemas do mundo real a que esta pesquisa está alinhada no horizonte de soluções é o crescimento exponencial dos crimes cibernéticos no mundo. Essa questão, vale ressaltar, é comumente vista como a pedra angular de todo o debate sobre Segurança Cibernética, enquanto a guerra cibernética constitui esse mesmo papel no campo da Defesa Cibernética.

Ademais, mesmo havendo uma grande variedade de formas de analisar a capacidade e o investimento de um país ou de alguma organização em termos de Segurança Cibernética, via de regra, a ocorrência dos crimes cibernéticos é um dos principais fatores considerados quando essas análises e pesquisas são feitas. Esse conceito pode ser operacionalizado tanto em relação à quantidade de crimes ou eventos significativos ocorridos em um período e lugar, como também pode colaborar com outros tipos de conceitos e condições explicativas, com o exemplo do construto legal e jurídico sobre crimes cibernéticos.

A fronteira de abordagens mencionada é apenas uma entre as numerosas interseções em que esta pesquisa se posiciona (VILAR-LOPES, 2016). Dentro de uma área primordialmente estudada pelas Relações Internacionais, a proposta da obra é mais

direcionada ao aparato metodológico da Ciência Política e à visão de condicionantes domésticos e de políticas públicas para um fenômeno como o comprometimento com a Segurança Cibernética, que é normalmente tratado como uma resultante de variáveis exógenas. Dentro desse debate, esse trabalho está concentrado na linha de pesquisa de Política Comparada, tratando da temática utilizando os arcabouços *mainstream* e emergente da área. As condições utilizadas, sobre as quais realizamos um amplo levantamento de informações, tipificam os países americanos de acordo com várias categorias importantes para o entendimento da região, de modo que a construção e sistematização desses dados também representa uma contribuição específica deste estudo. Metodologicamente, apresentamos um desenho de pesquisa não usual nos trabalhos da área, construindo um modelo original, a partir da Análise Qualitativa Comparativa (QCA), e complementando as inferências com um estudo de como o caso brasileiro pode ser explicado pelo modelo a partir da identificação de mecanismos causais, tornando a metodologia da pesquisa de caráter misto. Portanto, esperamos, com essa iniciativa, apresentar um exemplo de como a produção científica sobre o tema pode integrar teorias de médio porte robustas a um arcabouço metodológico sofisticado.

Estima-se que o custo das atividades criminosas no espaço cibernético representa pelo menos 1% do Produto Interno Bruto (PIB) global[8], o que indica uma necessidade urgente da abordagem devida da questão, ancorada em políticas públicas eficientes e empiricamente orientadas para o combate e a repressão dos crimes cibernéticos. No entanto, para que isso seja feito, é preciso que se busque, primeiramente, uma padronização dos conceitos abrangidos no debate. Assim, neste trabalho, utilizamos a tipologia proposta por Muggah, Glenny e Diniz (2014) para a classificação dos crimes cibernéticos:

1) Crime cibernético convencional;

2) Crime cibernético complexo; e

3) Ameaças emergentes.

Segundo os referidos autores, o crime cibernético convencional "trata-se das formas mais difundidas no mundo de infrações cibernéticas" (MUGGAH; GLENNY; DINIZ, 2014, p. 78). Algumas das ações tipificadas nessa área são a pornografia infantil, o discurso de ódio, a fraude bancária e a interceptação de dados. Essa última apresentou um aumento de 108%[9] durante o ano de 2020, que foi marcado pela emergência da pandemia do novo coronavírus,

[8] Disponível em: https://www.istoedinheiro.com.br/cibercrimes-terao-impacto-de-mais-de-us-1-trilhao-na-economia-global-em-2020/. Acesso em: 10 de mar. de 2021.

[9] Disponível em: https://www.cnnbrasil.com.br/tecnologia/2020/06/17/roubo-de-dados-aumenta-108-durante-a-pandemia-saiba-como-se-proteger. Acesso em: 10 de mar. de 2021.

que resultou em uma crise sanitária mundial e ampliou os impactos das atividades criminosas no espaço cibernético[10].

Em seguida, a noção de crime cibernético complexo, no entanto, "leva em conta e amplia a definição da ITU de infrações cibernéticas complexas ou combinadas, as que se enquadram em mais de uma categoria do cibercrime convencional" (MUGGAH; GLENNY; DINIZ, 2014, p. 78), tendo como exemplos as ações dos *hackers*, os ataques, a espionagem e o terrorismo cibernéticos.

As ameaças emergentes, em vista disso, representam as novas ameaças que não se enquadram necessariamente nas definições vigentes. Um dos exemplos dessa classificação no Brasil é a recente assimilação do espaço cibernético pelo crime organizado como uma forma de blindagem das suas atividades, uma vez que esses tipos de crimes são difíceis de rastrear e a repressão do Estado aos mesmos é menos eficiente do que em relação ao que ocorre com os crimes convencionais (MUGGAH; GLENNY; DINIZ, 2014, p. 78; LIRA-BRITO, 2020, p. 31).

Entretanto, mesmo exemplificando e demonstrando a validade deste estudo com base nos seus efeitos e no seu diálogo com a realidade explícita do mundo, acreditamos também na necessidade da colaboração com a sociedade, considerando que pesquisas científicas devem apresentar em seu núcleo um impacto social nítido.

Amparado nessa lógica, o Grupo de Trabalho Impacto e Relevância Econômica e Social, vinculado ao Ministério da Educação (MEC) e à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), que "foi composto para analisar conceitos e propor indicadores para avaliação do Impacto e Relevância Econômica e Social" (BRASIL, 2020, p. 3), oferece uma possibilidade de classificação das contribuições dos trabalhos, tendo em vista os seus impactos nas esferas econômica e social. A partir dessa visão, esta pesquisa integra o campo dos impactos científicos instrumentais e conceituais, que:

> Redundam em ferramentas seja de trabalho científico, seja de intervenção na sociedade (por exemplo, publicações e redes científicas no primeiro caso; políticas e legislação no segundo), conceituais, quais sejam os que geram uma transformação nos modos de se conceber atividades, permitindo sua reelaboração (maneiras de pensar, novas teorias, no caso dos científicos; modos de compreender e propor ações de intervenção social no caso dos segundos) (BRASIL, 2020, p. 12).

Com base nessa definição do que são os impactos científicos e conceituais, este trabalho pode ser considerado como pertencente ao campo, uma vez que:

---

[10] Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/aumento-dos-crimes-ciberneticos-com-a-pandemia-da-covid-19/. Acesso em: 10 de mar. de 2021.

1) Propõe novas teorias na Segurança Cibernética; e

2) Colabora com a transformação social e a intervenção social.

A propositura de teorias originais a partir de uma análise sistemática, no âmbito da Segurança Cibernética Comparada, de fatores explicativos para o comprometimento com Segurança Cibernética no continente americano, oferece uma contribuição ao conhecimento científico e proporciona o estabelecimento de um paradigma científico em uma área na qual a maior parte da produção com alto impacto ainda é recente (KUHN, 1962).

Por conseguinte, em relação às transformações e intervenções na sociedade, trabalhos como este podem servir de fonte e referência para mudanças significativas na legislação sobre os crimes cibernéticos e para reivindicações dos movimentos sociais (por uma regulamentação padronizada da Segurança Cibernética e pela desmilitarização do setor, por exemplo), além de impulsionar a formulação e implementação de políticas públicas empiricamente orientadas na área.

No entanto, Gustafsson e Hagström (2018) ressaltam que preencher lacunas do conhecimento sobre o tema, responder a questões e problemas do mundo real, e apresentar rigor metodológico, não são, por si só, justificativas para a necessidade de uma pesquisa. Com esse enunciado, eles defendem que os "problemas de pesquisa são mais úteis para esclarecer a natureza e a importância de uma contribuição para as pesquisas existentes, e, com isso, consistem em uma forma preferível de justificar novos trabalhos" (GUSTAFSSON; HAGSTRÖM, 2018, tradução livre).

À vista desse argumento, esta pesquisa contribui para a literatura na área à medida que busca analisar empiricamente o que explica o comprometimento com a Segurança Cibernética, respondendo a um problema real (KING; KEOHANE; VERBA, 1994), que é a necessidade de aprimoramento desse setor na maioria dos países do mundo. Além disso, a escolha metodológica da análise integrativa, utilizando QCA e estudo de caso, representa um avanço incremental em relação ao referencial teórico na Política Comparada (e.g. KIRTILLI, 2019; ELAMIRYAN; BOLGOV, 2018; SOLAR, 2020; STITILIS; PAKUTINSKAS; MALINAUSKAITE, 2017) e nos estudos de caso (e.g. AUSTIN, 2018; BAUMARD, 2017; OPPERMANN, 2010; SCHALLBRUCH; SKIERKA, 2018). No Quadro 2, apresentamos uma relação de trabalhos de Política Comparada na área, além das suas respectivas perguntas de pesquisa metodologias.

Quadro 2 - Perguntas de Pesquisa e o Estado da Arte na Segurança Cibernética.

PESQUISA	PERGUNTA	METODOLOGIA
Kirtilli, 2019.	Qual o impacto do nível de desenvolvimento econômico na implementação de políticas de Segurança Cibernética?	Quantitativa: regressão linear múltipla.
Elamiryan; Bolgov, 2018.	Como o regime político dos Estados membros da Organização do Tratado do Atlântico Norte (OTAN) e da Organização do Tratado de Segurança Coletiva (OTSC) influencia as prioridades das estratégias cibernéticas nacionais?	Qualitativa: análise documental.
Stitilis; Pakutinskas; Malinauskaite, 2017.	Como as estratégias cibernéticas dos Estados membros da União Europeia (UE) e da OTAN correspondem às políticas de Segurança Cibernética dessas organizações?	Qualitativa: análise documental.
Vilar-Lopes, 2014.	Como ocorreu a securitização do Espaço Cibernético nos Estados Unidos, no Brasil e no Canadá?	Métodos Mistos: análise quantitativa de dados qualitativos.
Oppermann, 2010.	Quais são as principais ameaças cibernéticas e os ataques virtuais contra as principais redes político-econômicas na China e na Rússia?	Qualitativa: estudo de caso.
Tatar et al., 2014.	Quais fatores afetam as estratégias nacionais de Segurança Cibernética na França, Alemanha, Holanda, Reino Unido, Estados Unidos e Turquia?	Qualitativa: análise documental.
Barbas; Sancho Hirane, 2018.	Quais são as principais características e os desafios das políticas de Segurança Cibernética no Chile e em Portugal?	Qualitativa: estudo de caso.
Solar, 2020.	Como, em se tratando de Segurança e Defesa Cibernéticas, se pode ir além do que se sabe sobre democracias avançadas?	Qualitativa: estudo de caso.
Calderaro; Craig, 2020.	Quais são os fatores determinantes da capacitação em Segurança Cibernética em todo o mundo?	Quantitativa: regressão linear múltipla.
Souza Junior; Streit, 2017.	Como as políticas de Segurança Cibernética brasileiras se relacionam com as diretrizes internacionais para o setor?	Qualitativa: estudo de caso.

Fonte: Banco de dados da pesquisa. Elaboração do autor.

Como evidenciado no Quadro 2, uma parte considerável da produção científica na área se concentra na lógica qualitativa, especificamente em estudos de caso e/ou análises dos

documentos oficiais de Estados nas áreas de Segurança e Defesa Cibernéticas. Há produção quantitativa, mas totalmente direcionada à utilização de regressões multivariadas, em detrimento de outras técnicas. Também imperam desenhos de pesquisa de teor descritivo, uma vez que a temática é recente.

No entanto, não identificamos uma representação expressiva de estudos com métodos qualitativos-configuracionais, que dialogam em certa medida com as lógicas quantitativa e qualitativa, como a Análise Qualitativa Comparativa (QCA). Nesse âmbito, o nosso trabalho contribui discutindo as questões concernentes à Segurança Cibernética a partir de um desenho de pesquisa envolvendo métodos mistos e utilizando QCA, método que, injustificadamente, não integra o cânone na área, mas que pode representar avanços significativos na formulação de teorias e no teste de hipóteses em Política Comparada.

Dessa forma, partindo do arcabouço teórico-metodológico supracitado, o *puzzle* desta pesquisa se relaciona com o potencial de identificação de fatores explicativos para o comprometimento com a Segurança Cibernética em regiões, lidando, assim, com um contexto de causalidade complexa e equifinalidade, apresentando, de maneira sistemática e original, um modelo explicativo baseado nas configurações de condições que explicam o fenômeno observado.

Por fim, buscando o impacto prático do conhecimento científico na sociedade, e considerando os padrões de *open science*, *open data,* transparência e replicabilidade das Ciências Sociais (CRÜWELL et al., 2019; MIGUEL et al., 2014; ROHLFING et al., 2021; DAFOE, 2014), esta dissertação incorrerá em três produtos, a saber: 1) Repositório com os códigos da pesquisa para replicação; 2) Modelo de classificação dos países americanos com base nas condições explicativas mobilizadas e no GCI; 3) Repositório com os documentos oficiais e dados analisados sobre os países das Américas

1.5 ESTRUTURA DA DISSERTAÇÃO

Este trabalho, buscando responder à pergunta de pesquisa e atender aos objetivos da mesma, é dividido em três seções, categorizadas da seguinte maneira:

1) Revisão da Literatura e Metodologia;
2) Segurança Cibernética Comparada: o Brasil e as Américas;
3) Limitações, Agenda da Pesquisa e Considerações Finais.

No Quadro 3, estão reunidas as informações sobre a estrutura desta dissertação e, em seguida, apresentamos uma síntese do que será discutido em cada parte deste estudo.

Quadro 3 - Estrutura da Dissertação.

CAPÍTULOS	DESCRIÇÃO
1 INTRODUÇÃO	Breve apresentação do tema estudado, do problema de pesquisa, das hipóteses, dos objetivos do estudo e da justificativa.
2 REVISÃO DA LITERATURA: CONCEITUAÇÃO E OPERACIONALIZAÇÃO	Conceituação e operacionalização do fenômeno de interesse e das condições mobilizadas na pesquisa.
3 METODOLOGIA	Definição do desenho de pesquisa, bem como dos métodos utilizados.
4 ANÁLISE QUALITATIVA COMPARATIVA DOS PAÍSES AMERICANOS	Análise, utilizando a QCA, de como as condições utilizadas no trabalho se configuram nos Estados do continente americano.
5 SEGURANÇA CIBERNÉTICA NO BRASIL	Observação e análise em profundidade do caso brasileiro, de maneira a apreender as suas peculiaridades pensando em mecanismos causais.
6 LIMITAÇÕES E AGENDA DE PESQUISA	Sumarização das principais limitações do trabalho e prospectos para a agenda de pesquisa na área
7 CONSIDERAÇÕES FINAIS	Últimas considerações do trabalho, oferecendo uma síntese dos principais pontos discutidos na dissertação e as conclusões.

Fonte: Plano da Dissertação. Elaboração do autor.

A primeira seção é constituída por dois capítulos: Capítulo 2 - Revisão da Literatura: conceituação e operacionalização, e Capítulo 3 - Metodologia.

No segundo capítulo, mobilizamos e definimos os conceitos de comprometimento com a Segurança Cibernética - fenômeno observado - e, securitização, despesas militares, ocorrência de eventos raros, tempo do marco jurídico-institucional, militarização e desenvolvimento econômico - condições explicativas. Para tanto, identificamos as teorias sob as quais esses conceitos se organizam e, amparados na expectativa teórica, propomos a operacionalização dos referidos conceitos.

No terceiro capítulo, apresentamos a metodologia utilizada para a satisfação dos objetivos da pesquisa. Ela é dividida em duas etapas:

1) a Análise Qualitativa Comparativa dos países americanos; e

2) o estudo do caso brasileiro.

Assim, a estrutura metodológica da pesquisa consiste em uma abordagem de métodos mistos, como é evidenciado no final do capítulo.

A segunda seção abrange dois capítulos: Capítulo 4 - Análise Qualitativa Comparativa dos Países Americanos, e 5 - Segurança Cibernética no Brasil. Ela é a pedra angular da dissertação, pois, é nessa seção onde ocorrem o desenvolvimento e a análise dos dados deste estudo.

O quarto capítulo consiste na análise qualitativa comparativa (QCA) dos fatores explicativos para o comprometimento com a Segurança Cibernética nas Américas, onde há o teste das hipóteses e a discussão dos resultados.

No quinto capítulo, realizamos o estudo do caso brasileiro, de maneira a observar em profundidade como os fatores explicativos estão relacionados com o comprometimento com a Segurança Cibernética no País, buscando contribuir para o estado da arte na área identificando mecanismos causais, e, assim, robustecendo o aporte teórico do modelo.

A terceira seção está dividida em dois capítulos: 6 - Limitações e Agenda de Pesquisa, e 7 - Considerações Finais. É nela onde ocorre a delimitação do estudo em relação às suas limitações teórico-metodológicas e às suas fronteiras inferenciais e onde apresentamos as últimas considerações da nossa pesquisa.

2 REVISÃO DA LITERATURA: CONCEITUAÇÃO E OPERACIONALIZAÇÃO

"The essence of life is statistical improbability on a colossal scale." (Richard Dawkins)

Neste capítulo, apresentamos, primeiramente, os conceitos referentes ao fenômeno de interesse (mensurado a partir do GCI) e aos fatores explicativos utilizados nesta pesquisa, a saber: 1) Securitização do setor de Segurança Cibernética; 2) Despesas Militares; 3) Ocorrência de Eventos Raros; 4) Tempo do marco jurídico-institucional; 5) Militarização do Espaço Cibernético; e 6) Desenvolvimento econômico. Adicionalmente, explanamos como esses conceitos são operacionalizados neste trabalho e quais teorias são mobilizadas para tanto.

2.1 COMPROMETIMENTO COM A SEGURANÇA CIBERNÉTICA

2.1.1 Segurança Cibernética: conceitualização e operacionalização

Segundo o Glossário das Forças Armadas, a Segurança Cibernética pode ser definida como a "arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas" (BRASIL, 2015, p. 249).

Entretanto, buscando uma conceituação mais apropriada, e tendo em vista o amplo debate sobre a esfera essencialmente civil da Segurança Cibernética, alinhamos-nos ao conceito utilizado pelo Glossário de Segurança da Informação (BRASIL, 2019), que a considera como:

> Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (BRASIL, 2019, *online*).

Dessa forma, o comprometimento com a Segurança Cibernética refere-se a quando os Estados desenvolvem ações para a garantia da existência da sociedade da informação e também para a proteção do espaço cibernético, de forma a proteger a integridade e a confidencialidade dos dados e orientado pela lógica liberal da garantia dos direitos e liberdades civis. A partir dessa conceituação mínima, esta pesquisa utiliza o Índice Global de Segurança Cibernética (GCI), produzido pela *International Telecommunication Union* (ITU), e o principal no grupo dos índices que avaliam países. Segundo a ITU:

> Os índices para avaliar os países foram desenvolvidos por organizações internacionais e *think tanks*, muitas vezes em parceria com organizações do setor privado. No nível mais alto, esses índices examinam aspectos políticos e regulatórios, medidas organizacionais, estratégias nacionais e esforços cooperativos, entre outros. Alguns índices simplesmente comparam e contrastam as medidas entre os países, enquanto outros fornecem uma pontuação de índice com base em indicadores. Outros ainda fornecem classificações com base na pontuação. Todos oferecem informações valiosas sobre práticas de segurança cibernética e lacunas a nível nacional (ITU, 2015, p. 1, tradução livre).

O Índice dos Índices de Segurança Cibernética (ITU, 2015), além de categorizar e apresentar as diferenças e semelhanças entre os índices na área, reúne informações essenciais sobre o que integra cada um deles e para que tipo de análise eles são indicados.

Segundo Troein e Acayo (2020), o GCI foi elaborado para incentivar a conscientização sobre Segurança Cibernética no mundo, promover a capacitação dos países membros da ITU, garantindo, assim, o aumento da capacidade geral no que tange à Segurança Cibernética, e também se apresentando como uma fonte de compartilhamento das melhores práticas na temática. Na Tabela 1, apresentamos a classificação dos índices que utilizam os países como unidade observada, com base na quantidade de Estados participantes e de indicadores, além das fontes de dados utilizados.

Tabela 1 - Índices de Segurança Cibernética.

ÍNDICE	PAÍSES	DADOS	INDICADORES
Global Cybersecurity Index	194	Primários e secundários	25
Cyber Readiness Index 2.0	125	Primários e secundários	7
The Cyber Index: International Security Trends and Realities	114	Secundários	0
EU Cybersecurity Dashboard	28	Secundários	25
Cybersecurity: The Vexed Question of Global Rules	23	Primários	10
Cyber Power Index	19	Secundários	39
Cyber Maturity in the Asia-Pacific Region	16	Secundários	9
Cybersecurity Policy Making at a Turning Point	10	Primários e secundários	10

Fonte: ITU (2015). Adaptação do autor.

O GCI é o mais abrangente dos índices mencionados na Tabela 1, utilizando também fontes de dados mistas, tanto primárias quanto secundárias, e tendo uma das maiores quantidades de indicadores em sua composição. Além disso, o Índice Global de Segurança Cibernética também apresenta mil, trezentos e cinquenta (1.350) menções[11] em produções acadêmicas, avaliadas pela ferramenta do *Google Scholar*, o que denota a sua ampla utilização, assim como a sua aceitação pela comunidade científica mundial.

2.1.2 Índice Global de Segurança Cibernética (GCI)

A ITU (2019) classifica o comprometimento com a Segurança Cibernética dos países a partir de três níveis - alto, médio e baixo, que são avaliados pelo Índice Global de Segurança Cibernética (GCI). O GCI, por sua vez, é formado por 5 pilares (Legal, Técnico, Organizacional, Capacitação e Cooperação) que agregam informações, a partir de 25 indicadores, para analisar e categorizar 194 Estados.

Dessa forma, neste trabalho, aplicamos a referida tipologia, de maneira a considerar o discernimento dos países do continente americano entre alto (pontuações entre 1 e 0,670), médio (pontuações entre 0,669 e 0,340) e baixo (pontuações entre 0,339 e 0,000) comprometimento com a Segurança Cibernética (ITU, 2019). No entanto, posteriormente, reavaliamos a mensuração de forma a diferenciar os países de acordo com um maior (X > 0,450) ou menor (X igual ou < 0,450) comprometimento com a Segurança Cibernética. Esse novo modelo de classificação nos permite isolar comparativamente quais os conjuntos de condições explicativas que propiciam o fenômeno analisado. A Tabela 2 apresenta a distribuição, com base nos lugares ocupados nos ranques regional e global, dos Estados americanos no GCI e as suas respectivas regiões.

Tabela 2 - Distribuição dos Países Americanos no GCI.

PAÍS	REGIÃO	PONTUAÇÃO NO GCI	RANQUE REGIONAL	RANQUE GLOBAL
Estados Unidos	Am. do Norte	0,926 (alto)	1	2
Canadá	Am. do Norte	0,892 (alto)	2	9
Uruguai	Am. do Sul	0,681 (alto)	3	51
México	Am. do Norte	0,629 (médio)	4	63

[11] Disponível em: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=%22Global+Cybersecurity+Index%22&btnG=. Acesso em: 30 de out. de 2021.

Paraguai	Am. do Sul	0,603 (médio)	5	66
Brasil	Am. do Sul	0,577 (médio)	6	70
Colômbia	Am. do Sul	0,565 (médio)	7	73
Cuba	Am. Central	0,481 (médio)	8	81
Chile	Am. do Sul	0,470 (médio)	9	83
República Dominicana	Am. Central	0,430 (médio)	10	92
Jamaica	Am. Central	0,407 (médio)	11	94
Argentina	Am. do Sul	0,407 (médio)	11	94
Peru	Am. do Sul	0,401 (médio)	12	95
Panamá	Am. Central	0,369 (médio)	13	97
Equador	Am. do Sul	0,367 (médio)	14	98
Venezuela	Am. do Sul	0,354 (médio	15	99
Guatemala	Am. Central	0,251 (baixo)	16	112
Antígua e Barbuda	Am. Central	0,247 (baixo)	17	113
Costa Rica	Am. Central	0,221 (baixo)	18	115
Trindade e Tobago	Am. Central	0,188 (baixo)	19	123
Barbados	Am. Central	0,173 (baixo)	20	127
São Vicente e Granadinas	Am. Central	0,169 (baixo)	21	129
Bahamas	Am. Central	0,147 (baixo)	22	133
Granada	Am. Central	0,143 (baixo)	23	134
Bolívia	Am. do Sul	0,139 (baixo)	24	135
Guiana	Am. do Sul	0,132 (baixo)	25	138
Nicarágua	Am. Central	0,129 (baixo)	26	140
Belize	Am. Central	0,129 (baixo)	26	140
El Salvador	Am. Central	0,124 (baixo)	27	142

Suriname	Am. do Sul	0,110 (baixo)	28	144
Santa Lúcia	Am. Central	0,096 (baixo)	29	149
São Cristóvão e Névis	Am. Central	0,065 (baixo)	30	157
Haiti	Am. Central	0,046 (baixo)	31	164
Honduras	Am. Central	0,044 (baixo)	32	165
Dominica	Am. Central	0,019 (baixo)	33	172

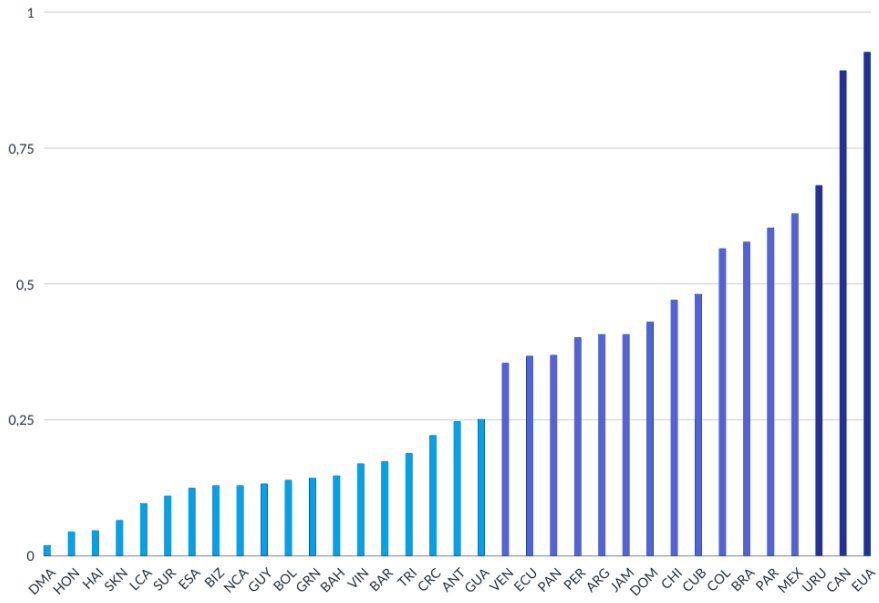
Fonte: ITU (2019). Adaptação do autor.

O Gráfico 1 representa as informações que constam na tabela anterior. De acordo com a ITU (2019), como pode ser observado no Gráfico 1, dos 35 países do continente americano, 03 demonstram alto nível (de 0,670 a 1) de comprometimento com a Segurança Cibernética, apresentando coloração azul escuro, enquanto 13 têm um nível mediano (de 0,340 a 0,669), apresentando coloração azul, e 19 um nível baixo (de 0,339 a 0,000), apresentando coloração azul claro. No entanto, considerando o estilo *case-oriented* e a exigência de que o fenômeno explicado pela técnica escolhida precisa ser dicotômico (embora as condições explicativas possam apresentar outros valores), na Análise Qualitativa Comparativa, estabelecemos 0,450 como um limite entre o maior (>0,450) e o menor (<0,450) comprometimento com a Segurança Cibernética. Dessa maneira, dividimos os países em dois grupos

Grupo 1 (Maior Comprometimento): Estados Unidos da América, Canadá, Uruguai, México, Paraguai, Brasil, Colômbia, Cuba, Chile.

Grupo 2 (Menor Comprometimento): República Dominicana, Jamaica, Argentina, Peru, Panamá, Equador, Venezuela, Guatemala, Antígua e Barbuda, Costa Rica, Trindade e Tobago, Barbados, São Vicente e Granadinas, Bahamas, Granada, Bolívia, Guiana, Nicarágua, Belize, El Salvador, Suriname, Santa Lúcia, São Cristóvão e Névis, Haiti, Honduras, Dominica.

Gráfico 1 - O Continente Americano no Índice Global de Segurança Cibernética.



Fonte: ITU (2019). Elaboração do autor.

Os cinco líderes no ranque regional são: 1º lugar - Estados Unidos (América do Norte); 2º lugar - Canadá (América do Norte); 3º lugar - Uruguai (América do Sul); 4º lugar - México (América do Norte); e 5º lugar - Paraguai (América do Sul). Os últimos colocados, segundo o Índice, são: 33º lugar - Dominica (América Central); 32º lugar - Honduras (América Central); 31º lugar - Haiti (América Central); 30º lugar - São Cristóvão e Névis (América Central); e 29º lugar - Santa Lúcia (América Central).

Nos próximos subcapítulos, apresentaremos a conceituação, a expectativa teórica e a operacionalização das condições explicativas mobilizadas no nosso modelo, a saber: 1) Securitização da Segurança Cibernética; 2) Despesas Militares; 3) Ocorrência de Eventos Raros; 4) Tempo do Marco Jurídico-institucional; 5) Militarização da Segurança Cibernética; e 6) Desenvolvimento Econômico.

2.2 SECURITIZAÇÃO DA SEGURANÇA CIBERNÉTICA

2.2.1 Securitização: conceitos e expectativa teórica no campo da Segurança Cibernética

Uma das principais contribuições da Escola de Copenhague, cujos expoentes são Buzan, Waever e Wilde (1998), para os estudos de Segurança Internacional foi entender as questões de segurança como essencialmente discursivas, ou seja, argumentando que a

securitização de um setor dá-se uma vez que há a construção discursiva daquele setor como algo que representa ameaça existencial para os Estados (BUZAN, WAEVER, WILDE, 1998; TANNO, 2003). Diante disso, eles ampliaram o debate, lançando as bases para a diferenciação entre os conceitos de politização e securitização, de onde, no decorrer deste trabalho, utilizamos a tricotomia tradicional "não-politizado, politizado, securitizado". De acordo com os referidos autores:

> 'Securitizar' se refere ao movimento que conduz a política além das regras estabelecidas no jogo e enquadra a questão como um tipo especial de política ou acima da política. A securitização pode, portanto, ser vista como uma versão mais extrema do que a politização. Em teoria, qualquer questão pública pode ser localizada no espectro que vai desde não-politizado (ou seja, quando o estado não lida com isso e de nenhuma outra forma tornou isso uma questão de debate público e decisão), passando a ser politizado (o que significa que a questão é parte de política pública, exigindo decisão governamental e alocação de recursos ou, mais raramente, alguma outra forma comum de governança) até ser securitizado (ou seja, quando o problema é apresentado como uma ameaça existencial, exigindo medidas de emergência e justificando ações fora dos limites normais do procedimento político). Em princípio, a localização de questões nesse espectro é aberta: dependendo das circunstâncias, qualquer problema pode terminar em qualquer parte do espectro. Na prática, a localização varia substancialmente de Estado para Estado (e também ao longo do tempo). Alguns estados politizaram a religião (Irã, Arábia Saudita, Birmânia) e outros não (França, Estados Unidos). Alguns irão securitizar a cultura (a ex-URSS, Irã) e outros não (Reino Unido, Holanda). No caso de questões (notadamente o meio ambiente) que se moveram dramaticamente para fora da categoria não politizada, enfrentamos a dupla questão de se elas foram meramente politizadas ou também securitizadas. Essa ligação entre politização e securitização não implica que a securitização sempre passe pelo Estado; a politização, bem como a securitização, podem ser promulgadas em outros fóruns também. (BUZAN, WAEVER, WILDE, 1998, p. 23-24, tradução livre)

Hansen e Nissembaum (2009) contribuem com esse debate, quando buscam analisar como esses caminhos teóricos se desdobram no caso do setor de Segurança Cibernética dos países. Sob o argumento de que os indivíduos e suas relações em rede estão intrincados em relação ao Estado, elas desenvolvem uma gramática própria para a área, apresentando os conceitos de hipersecuritização, práticas cotidianas de segurança e tecnificação, que acabam representando especificamente o que ocorre no espaço cibernético (HANSEN, NISSEMBAUM 2009). Conduzidos por essa discussão e objetivando compreender como ela se desenvolve nas produções acadêmicas empíricas e quais os problemas atuais dentro do tema, Silva e Pereira (2019), a partir da análise de 276 periódicos entre os conceitos Qualis A e B, identificaram 30 artigos que utilizaram o conceito de securitização de alguma forma, classificando-os como: "1) estudos que problematizam ou criticam a teoria de securitização; 2) estudos que articulam a teoria de securitização a outros referenciais teóricos; e 3) estudos que aplicam a teoria em análises empíricas".

Para exemplificar a terceira possibilidade mencionada, ressaltamos o trabalho de

Vilar-Lopes (2014), que analisou comparativamente os casos dos Estados Unidos, Brasil e Canadá, sob o argumento de que os casos escolhidos integravam o grupo das dez primeiras economias mundiais à época, além do fato de que esses Estados estão situados em um mesmo continente e representam as principais forças estatais no setor cibernético.

Esse estudo objetivou identificar as ameaças cibernéticas predominantes nos setores militares desses países. Para isso, Vilar-Lopes (2014) desenvolveu o *framework* denominado Espectro da Securitização Militar do Ciberespaço (ESMC), com base em três índices:

1) Índice de Politização Virtual da Defesa Cibernética (IPvDC);

2) Índice de Politização Documental da Defesa Cibernética (IPdDC);

3) Índice de Politização Institucional da Defesa Cibernética (IPiDC).

O IPvDC foi criado para responder a seguinte pergunta: "no século XXI, é possível constatar um aumento do interesse militar pelas ameaças cibernéticas, tendo como plataforma o próprio ciberespaço?" (VILAR-LOPES, 2014, p. 120). Dessa forma, utilizando técnicas quantitativas para atender a esse objetivo, o autor realizou buscas sistematizadas de menções aos temas referentes à Defesa Cibernética nos *sites* oficiais do Ministério da Defesa e das Forças Armadas de cada um desses países.

A análise quantitativa de dados qualitativos, que se relaciona com a utilização do texto como dado (*text as data*), é uma das contribuições que o autor traz para o tema estudado, representando também, sabendo ser esse um trabalho baseado em um desenho de pesquisa que integra métodos mistos tanto na coleta quanto na análise dos dados, um avanço em direção à sofisticação das pesquisas sobre Defesa Cibernética.

Embora não esteja ancorado diretamente a uma pergunta ou problema específico, o IPdDC é igualmente importante para a análise de Vilar-Lopes (2014). Esse índice é mensurado a partir de técnica qualitativa, consistindo a sua amostra na reunião de documentos oficiais de cada país sobre Defesa Cibernética, que podiam ter sido produzidos pelo Ministério da Defesa, pelas Forças Armadas, ou destinados aos mesmos. Como o IPdDC apresenta proposta semelhante à que desenvolvemos neste trabalho, escolhemos nos ater mais a como se dá a categorização dele. Sobre o IPdDC, Vilar-Lopes (2014) ressalta que:

> Três critérios são assegurados: possuir documento oficial nacional de defesa que abarque, ainda que de maneira geral, o tema em tela (2 pontos); possuir documento oficial nacional de defesa cibernética que inclua medidas extraordinárias, como criação de instituições e delegação de poder nessa área (3 pontos); e conter, no corpo textual de tal(is) documento(s), referência a armas cibernéticas – como o Stuxnet – e a ataques cibernéticos por parte de países estrangeiros, com o fito de potencializar a dramatização (1 ponto) (VILAR-LOPES, 2014, p. 126).

De acordo com essas informações e essa categorização, a politização documental da Defesa Cibernética nos Estados pode ser avaliada e, consequentemente, é originada uma métrica que possibilita a comparação deles que, associada aos outros índices, compõe a principal resultante da pesquisa de Vilar-Lopes (2014), que é o Espectro da Securitização Militar do Ciberespaço.

O IPiDC parte do argumento de que é possível que a securitização ocorra de maneira institucionalizada a partir de uma situação que demande resposta com urgência (BUZAN, WAEVER, WILDE, 1998; VILAR-LOPES, 2014). Dessa forma, o IPiDC mensura, a partir de documentos oficiais nos países estudados, a existência de órgãos institucionalmente centralizadores ou forças singulares quando o assunto abordado é Defesa Cibernética.

2.2.2 Tipologia Tripartite da Securitização

Nesta pesquisa, intencionamos aplicar a Teoria de Securitização à análise empírica dos trinta e cinco países do continente americano, através de uma replicação parcial das categorizações de Vilar-Lopes (2014) e Silva e Pereira (2019), consistindo a contribuição na Tipologia Tripartite da Securitização.

Com base nos documentos oficiais de cada Estado das Américas (América do Norte, América Central e América do Sul), intencionamos apresentar como resultante a classificação de cada um desses casos de acordo com uma adaptação dos seguintes níveis: a) não politizado; b) politizado; e c) securitizado (SILVA, PEREIRA, 2019).

O Quadro 4 apresenta a operacionalização do conceito de securitização, de acordo com Silva e Pereira (2019).

Quadro 4 - Securitização: operacionalização do conceito.

CONTINUUM	CARACTERÍSTICAS
Não Politizado	1 - Estado não é envolvido; 2 - Não existe debate ou decisão pública.
Politizado	1 - Há uma política pública; 2 - Há decisões governamentais; 3 - Há discurso sobre o tema.
Securitizado	1 - É uma ameaça existencial; 2 - Exige uma medida de emergência;

	3 - Justifica ações fora dos procedimentos políticos normais.

Fonte: Silva e Pereira (2019).

De maneira análoga, apresentaremos um modelo original mínimo, cujas bases são pautadas na ideia da existência de uma "Estratégia Nacional de Segurança Cibernética". Esse elemento, argumentamos, representa a materialização do posicionamento do Estado em relação à noção de que a Segurança Cibernética significa uma ameaça existencial à nação, demandando uma atenção especial, em termos de políticas públicas e estratégias, em detrimento dos outros campos (BUZAN; WAEVER; WILDE, 1998; HANSEN; NISSEMBAUM, 2009). A categorização, que implica na Tipologia Tripartite da Securitização, pode ser vista no Quadro 5, a seguir.

Quadro 5 - Tipologia Tripartite da Securitização.

CLASSIFICAÇÃO	DEFINIÇÃO
NÃO SECURITIZADO (0)	Não há uma Estratégia Nacional de Segurança Cibernética no país.
EM SECURITIZAÇÃO (1)	O Estado está em processo de desenvolvimento de uma Estratégia Nacional de Segurança Cibernética.
SECURITIZADO (2)	O país possui uma Estratégia Nacional de Segurança Cibernética, além de uma agência responsável pelo setor, com atribuições específicas.

Fonte: Elaboração do autor.

Para classificar os países do continente americano com base nesses pressupostos, utilizamos os dados do relatório do Banco Interamericano de Desenvolvimento (BID) e da Organização dos Estados Americanos (OEA), intitulado "Cibersegurança: riscos, avanços e caminho a seguir na América Latina e Caribe" (BID; OEA, 2021).

Uma das principais contribuições desse relatório é a apresentação do Modelo de Maturidade das Capacidades de Cibersegurança, onde é apresentado um perfil sobre cada um dos países da região no que concerne às dimensões: "(i) Política e estratégia de cibersegurança; (ii) Cibercultura e sociedade; (iii) Educação, capacitação e competências; (iv)

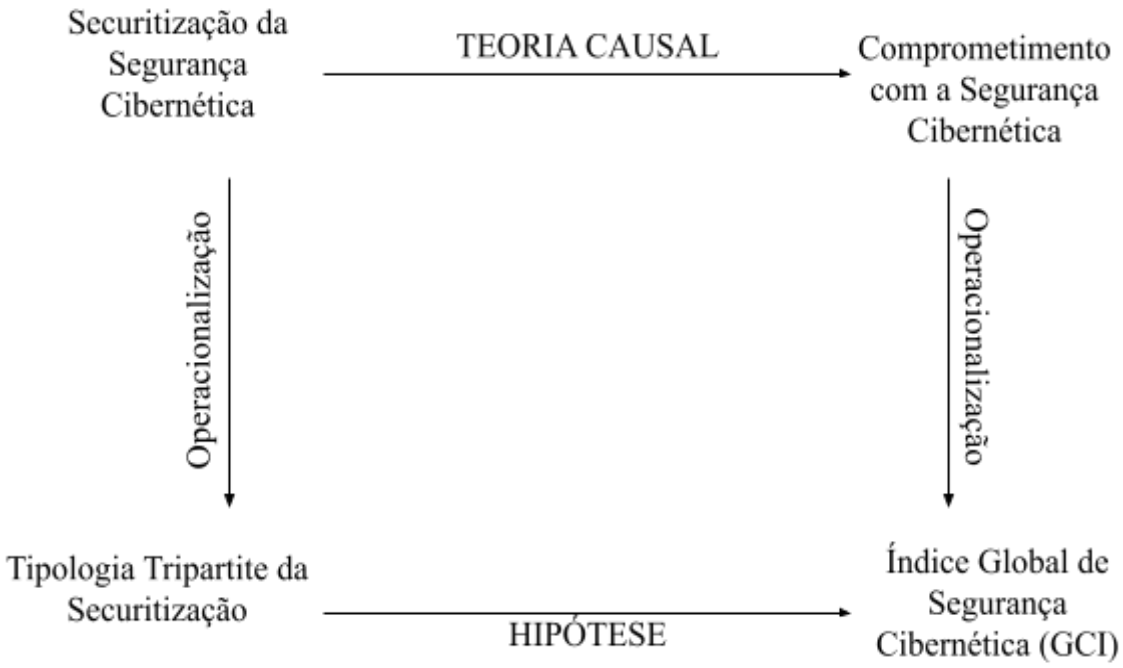
Marcos legais e regulatórios; e (v) Normas, organizações e tecnologias" (BID; OEA, 2021). Dentro do eixo de Política e Estratégia sobre Segurança Cibernética, coletamos os dados acerca do *status* atual dos países em relação à criação de uma Estratégia Nacional de Segurança Cibernética.

Além disso, as informações faltantes foram complementadas a partir de uma segunda fonte, o *Cyber Policy Portal* (2021) do Instituto das Nações Unidas para Pesquisa de Desarmamento (UNIDIR). Nesse portal, a UNIDIR arregimenta os perfis de cada Estado a partir de quatro seções: 1 - Políticas de Segurança Cibernética; 2 - Estrutura; 3 - *Framework* Legal; 4 - Cooperação.

Os resultados esperados, em consonância com a expectativa teórica, apontam para a identificação de uma relação positiva entre a existência da securitização do setor de Segurança Cibernética, que neste modelo se apresenta como a Estratégia Nacional de Segurança Cibernética, e o maior comprometimento com a Segurança Cibernética nos países, uma vez que a securitização desse assunto representa o grau extrapolado da politização do mesmo, garantindo, assim, que o assunto está sendo tratado como de importância extrema porque representa ameaça existencial para o Estado.

Tendo como base a tipologia tripartite supracitada, e levando em consideração modelo de Kellstedt e Whitten (2013), a Figura 5 representa a operacionalização da teoria e de qual é a relação esperada entre a condição analisada e o fenômeno observado.

Figura 5 - Securitização: operacionalização da teoria.



Fonte: Adaptação do autor a partir do modelo de Kellstedt e Whitten (2013).

Como visto no modelo representado na Figura 5, este trabalho busca testar a hipótese **H1.1**, a derivação que argumenta que a **Securitização** do setor de Segurança Cibernética é uma condição necessária e/ou suficiente para o comprometimento da Segurança Cibernética no continente americano.

Dessa forma, poderemos avaliar, a partir da Tipologia Tripartite da Securitização, se essa condição integra um conjunto explicativo para o fenômeno de interesse, podendo lançar luz sobre o entendimento de como países onde a Segurança Cibernética é securitizada, ou seja, onde há uma Estratégia Nacional de Segurança Cibernética, alcançam um maior comprometimento com a Segurança Cibernética.

2.3 DESPESAS MILITARES

2.3.1 Despesas Militares como uma medida de Segurança Cibernética

As despesas militares compreendem um parâmetro importante para entender o comprometimento dos Estados com o setor. Intencionamos mensurar essa condição a partir do Índice de Despesas Militares, calculado a partir da porcentagem do Produto Interno Bruto (PIB), de 0% a 100%, que os países destinam às Forças Armadas, sendo também uma medida da capacidade militar desses Estados (BANCO MUNDIAL, 2020). Kumar (2020) faz uma breve síntese sobre o assunto, quando afirma que

> Military expenditure is an input measure, which is not directly related to the output of military activities, such as military capability or strength, while there may be other political or economic motivations, the primary reason of the countries carrying out military expenditure is to achieve military capability of one sort or other, as many other factors contribute to build military capability.

Em sua pesquisa, Berg (2014) intencionou explicar o desenvolvimento de políticas no âmbito da Segurança Cibernética a partir de um *framework* dividido nas seções:

a) Cooperação Internacional;

b) Fundamento Legal;

c) Responsabilidade da Agência.

Derivados dessas divisões, os fatores explicativos mobilizados no estudo foram o desenvolvimento tecnológico, a implementação da Convenção de Budapeste, a taxa de penetração da *Internet* e as despesas militares. A população analisada foram os Estados membros do Centro de Excelência Cooperativa de Defesa Cibernética da Organização do Tratado do Atlântico Norte (CCDCOE), totalizando 23 países.

Berg (2014) argumentou que a Segurança Cibernética consiste em um novo patamar de dilema de segurança, uma vez que é difícil discernir se as despesas no setor cibernético e o investimento estão sendo conduzidos para uma lógica ofensiva ou defensiva. Dessa maneira, as despesas militares compreendem uma parcela substancial do potencial explicativo na sua pesquisa, principalmente, por ter sido essa variável a melhor preditora para o desenvolvimento de políticas no âmbito da Segurança Cibernética nos países membros do CCDCOE.

Watanabe (2020), por sua vez, desenvolveu um modelo para aplicar a teoria da dissuasão, tradicional nas Relações Internacionais, para o entendimento sobre as questões envolvendo a Segurança Cibernética. O seu argumento é de que os crimes e os ataques cibernéticos representam uma grande ameaça aos países e uma forma de entender o combate aos mesmos se dá a partir do princípio de que os Estados buscam expandir o poder militar cada vez mais.

A partir de uma regressão multivariada para mais de 200 casos, o autor pode inferir que, entre outras variáveis, as despesas militares importam para explicar a ocorrência de crimes e ataques cibernéticos (WATANABE, 2020).

Mesmo objetivando entender qual o impacto do nível de desenvolvimento econômico na implementação de políticas de Segurança Cibernética, Kirtilli (2019) utilizou as despesas militares como uma variável no modelo multivariado e inferiu que o desenvolvimento econômico apresenta uma relação com a variável resposta, avaliada a partir do GCI, e que as

despesas militares atuam nessa relação como uma variável mediadora (KIRTILLI, 2019). Como argumenta Kirtilli (2019):

> The military capacity is likely to have an impact on cybersecurity policy outcomes. If a country is investing in its military, it is also investing in its defensive and offensive forces and, indirectly, on cybersecurity (KIRTILLI, 2019, p. 50).

Os argumentos apresentados nessas considerações são de patente importância, considerando que poderão ser corroborados nesta pesquisa, a partir de uma estrutura de métodos mistos e com enfoque na causalidade complexa.

Paralelamente, Elamiryan e Bolgov (2018) buscaram responder à questão "como o regime político dos Estados membros da Organização do Tratado do Atlântico Norte (OTAN) e da Organização do Tratado de Segurança Coletiva (OTSC) influencia as prioridades das estratégias cibernéticas nacionais?", a partir de metodologia qualitativa que teve a análise documental como sua principal técnica. Um dos achados mais significativos tem relação com a identificação de que um grande obstáculo para a implementação de políticas e das estratégias cibernéticas nacionais era o fato de o orçamento militar de alguns países membros da OTAN ser bem reduzido. No âmbito da inovação, que compartilha as fronteiras da Segurança Cibernética, Jia (2014) ressalta que:

> the positive impact of military spending on the society can also be seen from the trend of innovation. Comparing to traditional military development, which merely brings more casualties and disasters, modern military development brings more positive contributions to human civilization. In the past two centuries, the military has initiated many state of the art innovations, which fundamentally changed modern civilization (JIA, 2014, p. 5-6).

Com base nessas discussões, como evidenciado anteriormente, utilizamos a medida do Índice de Despesas Militares, organizado pelo Banco Mundial (2020). Segundo a Instituição:

> Military expenditure (% of GDP). Military expenditures data from SIPRI are derived from the NATO definition, which includes all current and capital expenditures on the armed forces, including peacekeeping forces; defense ministries and other government agencies engaged in defense projects; paramilitary forces, if these are judged to be trained and equipped for military operations; and military space activities. Such expenditures include military and civil personnel, including retirement pensions of military personnel and social services for personnel; operation and maintenance; procurement; military research and development; and military aid (in the military expenditures of the donor country). Excluded are civil defense and current expenditures for previous military activities, such as for veterans' benefits, demobilization, conversion, and destruction of weapons. This definition cannot be applied for all countries, however, since that would require much more detailed information than is available about what is included in military budgets and off-budget military expenditure items. (For example, military budgets might or might not cover civil defense, reserves and auxiliary forces, police and paramilitary forces, dual-purpose forces such as military and civilian police, military

> grants in kind, pensions for military personnel, and social security contributions paid by one part of government to another). (BANCO MUNDIAL, 2020).[12]

Dessa maneira, poderemos avaliar como os países do continente americano - América do Norte, América Central e América do Sul - estão distribuídos em termos de despesas militares e se o Índice de Despesas Militares participa conjunturalmente de uma configuração explicativa para o comprometimento com a Segurança Cibernética, avaliado pelo GCI.

Observando a descrição dos pilares técnico e de capacitação no Índice Global de Segurança Cibernética, identificamos que os mesmos, de maneira indireta, podem sofrer influência desse fator explicativo, de maneira que é esperada uma relação positiva entre essa condição e o fenômeno de interesse.

Na seção a seguir, apresentaremos brevemente a métrica utilizada para a categorização dos casos analisados na Análise Qualitativa Comparativa.

2.3.2 Classificação das Despesas Militares na QCA

Em observância da distribuição dos países americanos no Índice de Despesas Militares, atribuímos classes a eles, dividindo-os em três categorias. Essa seleção ocorreu a partir da constatação, como pode ser avaliado no Apêndice III, de que os limiares 1% e 2% - e os seus interlúdios - garantem que, mesmo havendo uma grande quantidade de *missing data*, seja possível a obtenção de informação útil sobre as despesas militares no continente americano.

A primeira (0) reúne os *missing data*, uma vez que essa variável não abrange, para o ano de 2018, todos os casos que o GCI analisa. Também estão presentes os países que apresentam Índice de Despesas Militares baixo, ou seja, que destinam menos de 1% do seu PIB para essa área. A segunda (1) agrega os Estados que destinam entre 1% e 2% do PIB para as despesas militares, tendo um desempenho médio no Índice. Por último, na terceira classe (2), estão os países que despendem mais de 2% do seu PIB nesse setor. Essas informações estão sistematizadas no Quadro 6.

Quadro 6 - Despesas Militares: classificação.

CLASSIFICAÇÃO	DEFINIÇÃO
Índice de Despesas Militares baixo e N/A **(0)**	N/A ou < 1% do PIB do país;
Índice de Despesas Militares médio **(1)**	Entre 1% e 2% do PIB do país;

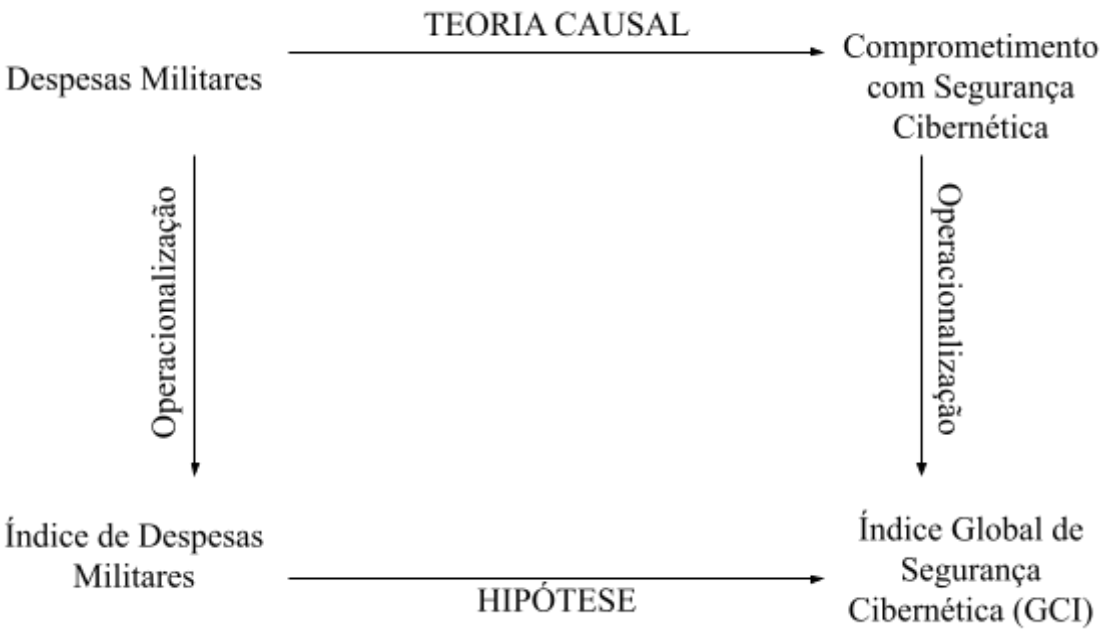
[12] Disponível em: https://qog01-p.gu.gu.se/shiny/users/xalvna/qog/map2/. Acesso em: 18 de dez. de 2021.

Índice de Despesas Militares alto **(2)**	> 2% do PIB do país.

Fonte: Elaboração do Autor com base nos dados da pesquisa.

Nesse sentido, representamos, na Figura 6, a operacionalização da teoria a partir do que foi idealizado por Kellstedt e Whitten (2019).

Figura 6 - Despesas Militares: operacionalização da teoria.



Fonte: Adaptação do autor a partir do modelo de Kellstedt e Whitten (2013).

A Figura 6 sintetiza o que é pretendido nesta seção, que é testar a hipótese **H1.2**, ou seja, verificar se as **Despesas Militares** constituem condição necessária e/ou suficiente para o comprometimento com a Segurança Cibernética nos países do continente americano.

2.4 EVENTOS RAROS

2.4.1 O Problema da Indução e as Raízes Epistemológicas dos Eventos Raros

A conceituação do que consideramos como eventos raros remete à noção de Taleb (2010) sobre cisnes negros, que são acontecimentos ou fenômenos altamente improváveis, mas que representam um impacto estratosférico quando ocorrem. O autor parte de uma analogia para o esclarecimento da ideia: até a Austrália ter sido descoberta, acreditava-se que só existia cisnes brancos no mundo.

Essa história faz alusão a uma questão central na filosofia e na teoria do conhecimento, que é o problema da indução (DUTRA, 2010; MALDONADO, 2016; TALEB, 2010). O problema da indução coloca em xeque a legitimidade, e até mesmo a viabilidade, de

generalização do conhecimento gerado a partir de um conjunto finito de observações. Nesse sentido, ao analisarmos o exemplo histórico dos cisnes negros, podemos notar os riscos oferecidos pela ilusão da continuidade e da generalização sem consideração da contingência do fenômeno estudado.

Essa discussão não escapou a Popper (1959), que apresentou esse problema secular e introduziu as suas ideias de verificação e de falseabilidade. Dessa maneira, a confiabilidade das teorias científicas, em Popper (1959), está submetida à possibilidade, não só da verificação - positiva - dos pressupostos, mas da falseabilidade - negativa - dos mesmos. Assim, a sua contribuição nesse debate está centrada no argumento de que teorias devem ser passíveis de refutação e não apenas de confirmação.

Popper (1959) ainda defende a falseabilidade como uma forma válida de demarcação da ciência e do conhecimento empírico. Seguindo essa lógica, a teoria de que só existem cisnes brancos representaria um sistema científico circunstancial e falseável, uma vez que, ao serem acrescentadas maiores informações, incluindo a da existência de cisnes negros na Austrália, a teoria daria lugar a outra mais adequada e também passível de refutação.

No entanto, mesmo estabelecendo formas de tornar a ciência mais sensível à realidade empírica com o caráter da falseabilidade das teorias, essa resposta ao problema da indução não abrange totalmente o questionamento levantado sobre o impacto do imprevisível ou altamente improvável (TALEB, 2010; MALDONADO, 2016). King e Zeng (2001) também contribuem com essa discussão, constatando que “a maioria dos eventos mais significativos nas Relações Internacionais - guerras, golpes, revoluções, depressões e choques econômicos - são eventos raros” (KING, ZENG, 2001, p. 693, tradução livre), o que denota a relevância e a necessidade de estudos direcionados especificamente para tratar essas questões.

A partir do crescimento exponencial das informações disponíveis na era marcada pelo Big Data, e considerando que o fazer científico e o estado das coisas da realidade atuais se mostram cada vez mais contraintuitivas, Maldonado (2016) argumenta por uma epistemologia da complexidade pautada em quatro aspectos:

1) Observar o inobservado;

2) Pensar o inesperado;

3) Ver o que - ainda - não existe; e

4) Abranger o possível e o aparentemente impossível.

A ideia essencial desses quatro pontos parte do pressuposto de que o conhecimento pela experiência e a criação de modelos com base no probabilisticamente esperado

simplificam a realidade, o que, em média, é eficiente, necessário e não causa maiores problemas.

Entretanto, como também afirmam Hochtl, Parycek e Schollhammer (2015), o risco de se discutir essa questão em termos probabilísticos implica na ilusão de que o impacto de uma análise equivocada - porque orientada pela média - dos fenômenos pode ser mensurado sob uma lógica de diferenças quantitativas. A realidade empírica, pelo contrário, aponta para abismos qualitativos entre os impactos mensurados dos eventos esperados e os dos fenômenos altamente improváveis.

Pensando sobre essa lacuna, Taleb (2010) ressalta a importância do desenvolvimento de ferramental analítico e metodológico para abordar de maneira acertada os eventos raros. Nessa perspectiva, reside o argumento do salto paradigmático do conhecimento, uma vez que a ocorrência desses eventos raros, ou cisnes negros, muitas vezes coloca em xeque tudo o que se sabe sobre determinado assunto. Por isso, é incentivado o seu estudo em Política Comparada e através de estudos de caso (REZENDE, 2011). Como defende Rezende (2011, p. 321): “os eventos singulares e não apenas as regularidades importam de forma significativa para a produção de inferências causais”.

2.4.2 A Segurança Cibernética e o Xadrez

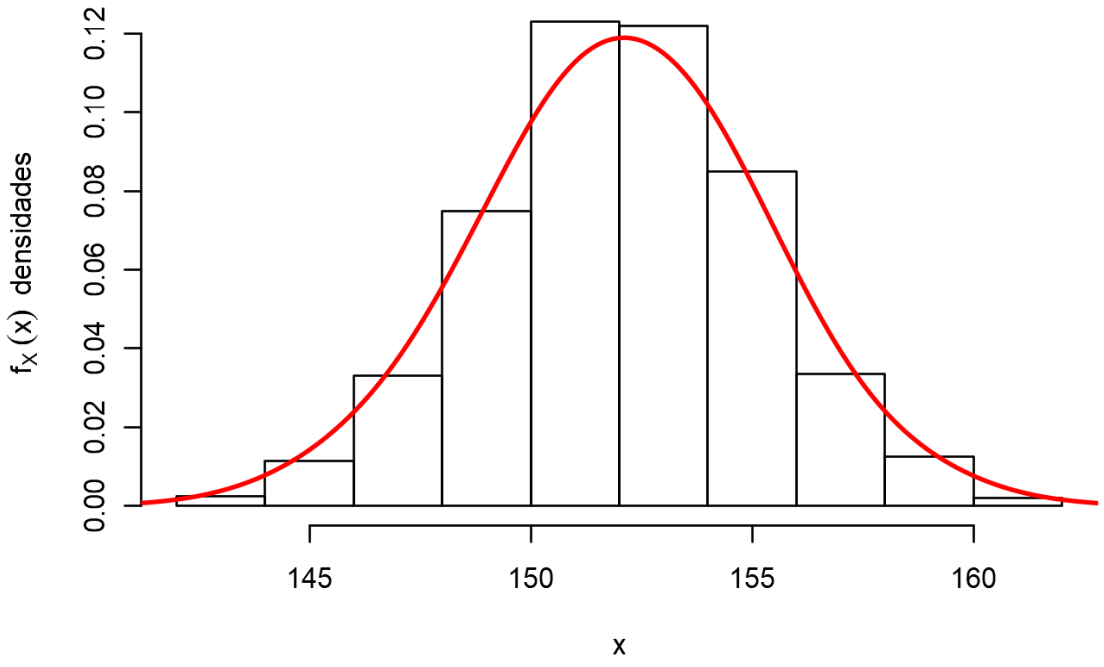
Nesta seção, de forma complementar ao discutido, apresentaremos uma analogia que representa minimamente o problema dos cisnes negros e da produção do conhecimento: a comparação entre Segurança Cibernética e o xadrez. Esse jogo milenar de estratégia e tomada de decisão elucida satisfatoriamente o que observamos e queremos demonstrar no que tange à Segurança Cibernética.

A grande maioria da população de enxadristas apresenta performance baixa ou medíocre nesse esporte, de maneira que a lógica da estimação de efeitos médios e da observação sobre o todo da população nesse caso produziria informação e dados referentes a esse grupo, o que na prática teria pouca utilidade substancial para o conhecimento empírico.

Na verdade, os fenômenos que são importantes no xadrez são os eventos raros ambulantes, indivíduos como Bobby Fischer (1943-2008), Garry Kasparov (1963-) e, mais recentemente, Magnus Carlsen (1990-), mestres do xadrez mundial. São esses esportistas de alta performance que concentram a grande maioria do potencial de aprendizado e das informações sobre teoria dos jogos, modelos computacionais e lógica probabilística, entre outros campos.

Mais recentemente, e a partir do que foi apreendido com a observação de fenômenos improváveis como o desempenho de Kasparov contra o computador, e a sua posterior derrota, a tecnologia de criação dos algoritmos apresentou um avanço gigantesco, passando a prepará-los para fazer cálculos de probabilidades de jogadas por amostragem e para "aprender a aprender a jogar", desbravando, assim, um universo de possibilidades de jogadas consideradas ineficientes até para os mestres enxadristas, mas que, se analisadas a partir de uma quantidade substancial de jogadas e a longo prazo, se tornavam imbatíveis. Nesse quesito, os eventos raros proporcionados pelas mentes humanas serviram de base para o desenvolvimento de algoritmos que, atualmente, se distanciam qualitativamente dos primeiros (LAUNAY, 2019). Na Figura 7, apresentamos um exemplo de uma distribuição normal.

Figura 7 - Representação de uma Distribuição Probabilística Normal.



Fonte: Moodle UFSC[13].

As distribuições probabilísticas normais, também chamadas de curvas gaussianas, são utilizadas para os mais variados tipos de estudos, desde pesquisas sobre eleições majoritárias, onde a informação acerca do eleitor mediano determinará a tônica dos resultados (DOWNS,

[13] Disponível em: https://www.inf.ufsc.br/~andre.zibetti/probabilidade/normal.html. Acesso em: 05 de mai. de 2021.

1999), até análises contabilísticas de distribuições de números suspeitas de fraude, já que tendem a emular a curva gaussiana como padrão de gastos e ideal de homogeneidade, quando, na verdade, a maioria dos gastos e representações numéricas se apresenta de maneira heterogênea e com probabilidades significativamente desiguais de aparecimento de cada decimal, sendo guiados pela Lei de Benford (LAUNAY, 2019).

Nesse sentido, Taleb (2010) e Maldonado (2016) argumentam que há urgência na observação da importância não apenas do centro de uma distribuição gaussiana, mas também, e principalmente, para os extremos dessa curva. É neles que podemos encontrar os chamados eventos raros.

Mesmo que de relevância probabilística quase nula, esses fenômenos representam um impacto consideravelmente maior do que os contidos no centro da distribuição, de maneira que há o entendimento de que uma epistemologia da complexidade precisa conceber e lidar com objetos de estudo que apresentam impacto inversamente proporcional à sua proximidade do centro da curva, ou à sua previsibilidade.

Os cisnes negros da Segurança Cibernética são comparáveis aos do xadrez, já que são eles que expandem as fronteiras do conhecimento na área através do salto paradigmático que proporcionam com as inovações e o impacto que causam.

Assim como os mestres enxadristas são os fenômenos que mais concentram informações e possibilidades de aprendizado no referido jogo, os grandes ataques, incidentes e escândalos ocorridos na Segurança Cibernética consistem em fonte valiosa para o avanço da tecnologia na área. Consequentemente, eles podem contribuir qualitativamente para o acúmulo de conhecimento empírico e, através da adaptação dos Estados às novas ideias apreendidas, os eventos raros podem conduzi-los ao aumento do comprometimento com a Segurança Cibernética.

Enxadristas de alta performance procuram os pontos fracos de jogadas amplamente acreditadas como melhores, inclusive as de maior complexidade, executadas por outros campeões mundiais. Dessa forma, eles encontram as fragilidades no encadeamento das decisões e nas estratégias, objetivando a redução total do ruído (KAHNEMAN, SLOVIC, TVERSKY, 1982) que pode ser produzido nas tomadas de decisão, enquanto os jogadores medianos apenas operam com a lógica da curva de sino, de que em média, estratégia *X* é aceitável como uma forma defensiva de se ganhar no xadrez.

De maneira semelhante, os sistemas e as redes, assim como as infraestrutura críticas, que concernem à Segurança Cibernética de determinado país, devem ser administrados e projetados a partir de um modelo que funcione com lógica semelhante à exemplificada acima,

onde seja prezada a complexidade e a atitude preventiva em relação aos eventos raros, em detrimento do foco nas ações reativas que normalmente fazem parte dos protocolos na área.

Um potencial exemplo dessa relação é o caso da Estônia. Em 27 de Abril de 2007, a Estônia foi vítima de ataques cibernéticos do tipo *Distributed Denial of Service* (DoS), que deixaram sites governamentais fora do ar. Posteriormente, o país investiu massivamente no setor de Segurança Cibernética e, com base no levantamento do ano de 2018, passou a figurar entre os cinco países com maior comprometimento com Segurança Cibernética no mundo, segundo o Índice Global de Segurança Cibernética (ITU, 2019).

Outro exemplo conhecido é o do *Stuxnet*, que foi descoberto em meados de 2010. Considerado uma das primeiras armas cibernéticas, e um argumento contundente da sobreposição do espaço cibernético em relação aos outros territórios, o *Stuxnet* consistiu em um *malware* que foi utilizado para o ataque ao Sistema de Supervisão e Aquisição de Dados - SCADA, que servia para o controle de centrífugas em uma área de enriquecimento de urânio no Irã[14].

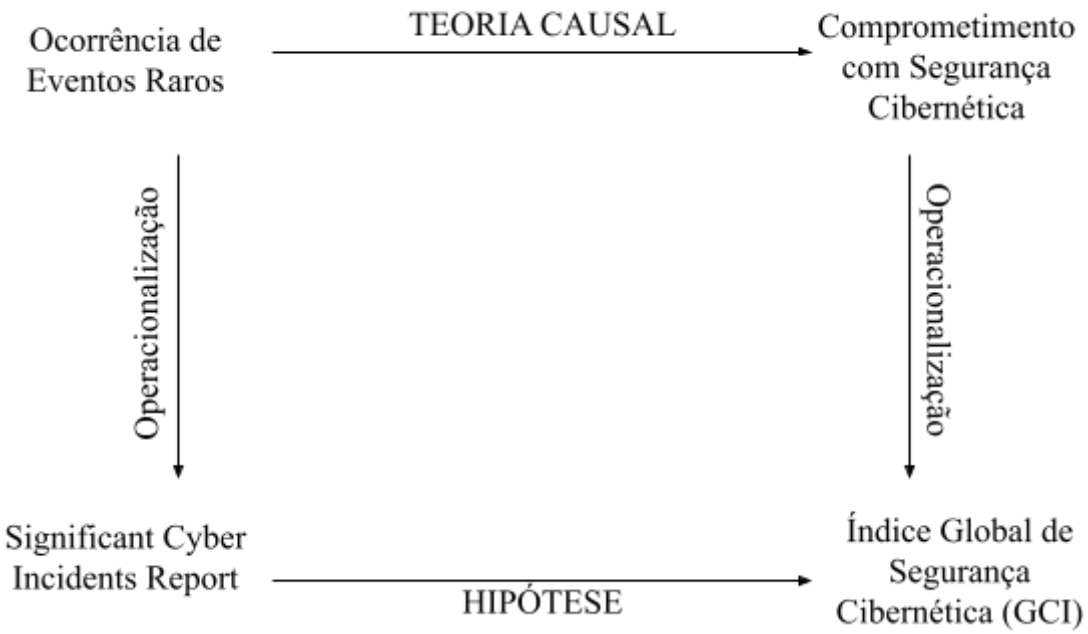
Dessa forma, nesta pesquisa, intencionamos mensurar esses eventos a partir de uma classificação minimalista e original, contabilizando a ocorrência a partir dos incidentes de alta significância reportados pelo Center for Strategic & International Studies (CSIS, 2020).

O resultado esperado, a partir desse parâmetro teórico, é uma relação positiva entre a ocorrência de eventos raros na área e o maior nível de comprometimento com a Segurança Cibernética dos Estados, uma vez que o alto impacto desses acontecimentos expõe as fragilidades e a vulnerabilidade dos países, influenciando-os a direcionar esforços para melhorar a sua condição na área.

Dessa maneira, na Figura 8, podemos observar a síntese representativa da operacionalização da teoria.

[14] Segundo o *report* do CSIS: “October 2010 - Stuxnet, a complex piece of malware designed to interfere with Siemens Industrial Control Systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program.” (CSIS, 2020, p. 57)

Figura 8 - Ocorrência de Eventos Raros: operacionalização da teoria.



Fonte: Adaptação do autor a partir do modelo de Kellstedt e Whitten (2013).

Tendo em vista o que foi proposto na Figura 8, buscamos testar a hipótese **H1.3**, de que **Ocorrência de Eventos Raros** é uma condição necessária e/ou para a explicação conjuntural do comprometimento com a Segurança Cibernética nos países do continente americano para o ano-referência de 2018. O Quadro 7 apresenta a classificação dos Estados com base nos dados sobre essa variável.

Quadro 7 - Categorização dos Estados a partir da Ocorrência de Eventos Raros.

CLASSIFICAÇÃO	DEFINIÇÃO
Ausência de Eventos Raros **(0)**	N/A;
Evento raro Isolado **(1)**	Pelo menos 1 evento raro no país;
Presença de Eventos raros **(2)**	> 2 eventos raros no país

Fonte: Elaboração do autor com base nos dados da pesquisa.

Como representado no Quadro 7, cada caso será avaliado de acordo com a seguinte classificação: 0 - ausência de eventos raros no país; 1 - Presença de pelo menos um evento de alta significância no país; 2 - Mais de 2 eventos raros de alta significância no Estado. Dessa maneira, mensuramos desde a não ocorrência desses acontecimentos de alta significância,

categoria (0), até a ocorrência ostensiva, que é o valor máximo atribuído a essa variável, categoria (2).

2.5 TEMPO DO MARCO JURÍDICO-INSTITUCIONAL

2.5.1 O Conceito de Marco Jurídico-Institucional

A noção de marco jurídico-institucional pressupõe o entendimento do que são as instituições (NORTH, 1990; CAVALCANTI, 2012; IMMERGUT, 1992; HALL, TAYLOR, 2003). Nesta pesquisa, utilizamos a definição de North (1990) de instituições, como destacamos no trecho abaixo:

> As instituições são as regras do jogo em uma sociedade ou, mais formalmente, são as restrições concebidas humanamente que moldam a interação dos indivíduos. Consequentemente, elas estruturam incentivos nas trocas humanas, sejam políticas, sociais ou econômicas. A mudança institucional molda a forma como as sociedades evoluem ao longo do tempo e, portanto, é a chave para a compreensão da mudança histórica (NORTH, 1990, p. 3, tradução livre).

Dessa maneira, o marco jurídico-institucional em relação à Segurança Cibernética pode ser entendido como o primeiro esforço tangível legal e institucionalmente, consistindo em uma política pública na medida em que entendemos a mesma como:

> Um curso de inação ou ação, escolhido por autoridades públicas para focalizar um problema que é expresso no corpo das leis, regulamentos, decisões e ações de governo. A política pública está relacionada com as intenções que determinam as ações de um governo; com o que o governo escolhe fazer ou não fazer; com as decisões que têm como objetivo implementar programas para alcançar metas em uma determinada sociedade; com a luta de interesses entre o governo e sociedade; ou ainda, com atividades de governo, desenvolvidas por gestores públicos ou não, que têm uma influência na vida de cidadãos (CAVALCANTI, 2012, p. 13).

Nesse contexto, o continente americano abrange 35 países com características diferentes quanto aos regime político, desenvolvimento econômico e processo histórico. Além disso, no que concerne à Segurança Cibernética, esses Estados podem ser comparados levando em consideração o tempo desde a primeira legislação na área, ou o marco institucional.

A ideia central desse argumento é que o tempo referente ao marco jurídico-institucional no setor proporciona a maturação institucional desse campo nos países, se relacionando positivamente com o comprometimento com a Segurança Cibernética, uma vez que um dos pilares do GCI mensura a existência de legislação sobre o tema.

A inclusão dessa condição contribui para o debate à medida em que analisa o tempo e, consequentemente, a maturação, diferenciando-se da mera observação da existência de leis sobre Segurança Cibernética, que já está incluída no Índice Global de Segurança Cibernética

(ITU, 2019), e evitando o problema da dependência causado pela circularidade entre o fenômeno analisado e a condição que o explica (GERRING, 2005). Diante disso, a expectativa teórica é de que países que apresentam maior amadurecimento institucional também tenham um melhor desempenho no GCI.

2.5.2 Operacionalização do Conceito.

A definição de como a condição envolvendo maturidade da legislação em Segurança Cibernética está classificada foi realizada a partir dos dados disponibilizados pela UNIDIR - no *Cyber Policy Portal* - e pela OEA - no *Portal Interamericano de Delitos Cibernéticos*. Essas duas instituições estão comprometidas com a sistematização de informações sobre os países em matéria de Segurança Cibernética, enfatizando também a estrutura do setor cibernético nesses países e a cooperação com outros Estados e organizações. De acordo com a UNIDIR:

> The UNIDIR Cyber Policy Portal is an online reference tool that maps the cybersecurity and cybersecurity-related policy landscape. Through concise and comprehensive profiles, it provides a rigorous, accessible and up-to-date overview of the cyber capacity of UN Member States and a select group of intergovernmental organisations (UNIDIR, 2021).

Paralelamente, o *Portal Interamericano de Delitos Cibernéticos*, além do Grupo de Trabalho responsável pela reunião das informações no Portal são alguns dos principais *"resultados del proceso de las Reuniones de Ministros de Justicia y otros Ministros y Fiscales Generales de las Américas* (REMJA) *con el objetivo de fortalecer la cooperación hemisférica en la investigación y juzgamiento de estos crímenes"* (OEA, 2021). Como atribuições do Grupo de Trabalho das REMJA, a OEA (2021) estabelece:

> Promueve la adopción o actualización de legislaciones nacionales y medidas procesales necesarias para la persecución efectiva de los delitos cibernéticos; reglamentaciones para que los proveedores de servicios aseguren la preservación y recuperación de la información almacenada y de tránsito; la adhesión de los Estados al Convenio de Budapest; e impulsando a los Estados al desarrollo de estrategias nacionales que incluyan esfuerzos para prevenir, investigar y procesar los delitos cibernéticos (OEA, 2021).

A partir dessas considerações, e com base nos dados levantados, no Quadro 8, apresentamos a categorização da condição mobilizada nesta pesquisa.

Quadro 8 - Operacionalização do Tempo do Marco Jurídico Institucional.

CLASSIFICAÇÃO	DEFINIÇÃO
Marco jurídico-institucional Inexistente **(0)**	Não possui legislação (N/A);

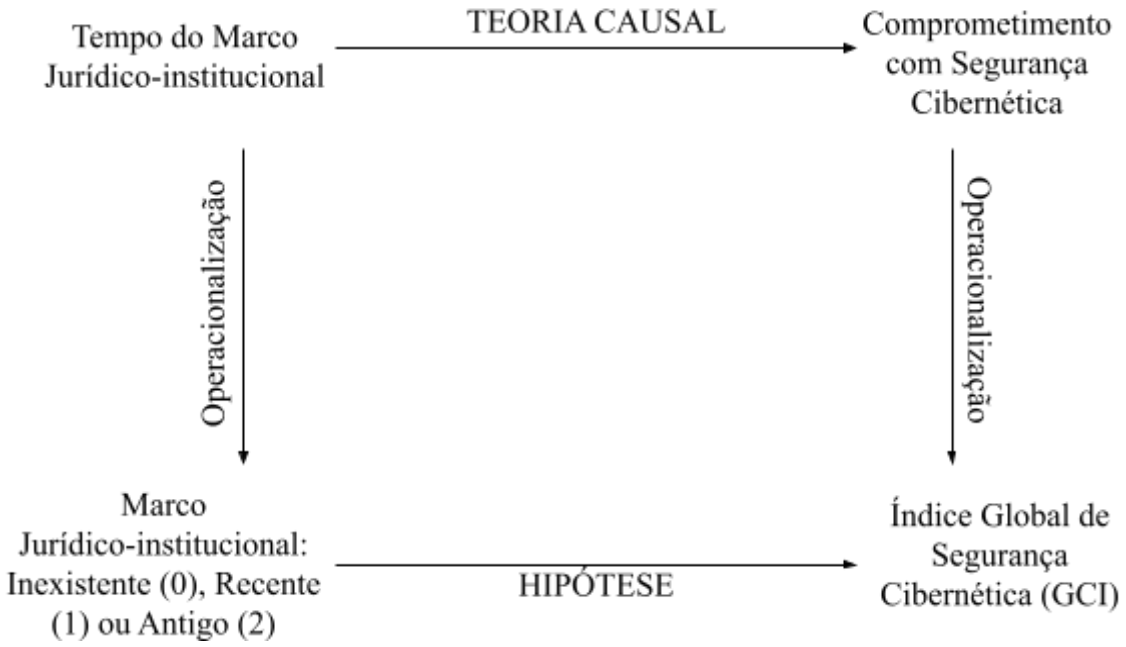
Marco jurídico-institucional recente **(1)**	Entre 1 e 15 anos de marco jurídico-institucional;
Marco jurídico-institucional antigo **(2)**	16 anos ou mais desde o marco jurídico-institucional.

Fonte: Elaboração do Autor.

A distribuição dos países americanos em relação ao Tempo do Marco Jurídico-Institucional apresentou os mais variados valores, desde datas mais recentes de marco até legislações com mais de 20 anos desde a sua criação. Com isso em mente, estabelecemos uma métrica para a classificação dos referidos Estados, considerando também uma tendência internacional referente à existência de tratados internacionais nesse âmbito, como a Convenção de Budapeste sobre o Cibercrime. Esse tratado, por exemplo, estabeleceu grande parte das premissas para os futuros frameworks de países em todo o mundo. Nesse sentido, classificamos os países com marco temporal antigo no limiar do surgimento da referida Convenção, de modo que grande parte dos países com marco recente tenha compartilhado direta ou indiretamente o *Zeitgeist* propiciado pela Convenção de Budapeste. Os Apêndices VI e VII detalham essa classificação.

Os Estados que não possuem legislação sobre Segurança Cibernética foram classificados como N/A, assumindo um valor (0), enquanto os casos que têm legislações datadas de 1 a 15 anos foram classificados na categoria (1), representando o período recente do marco. Por fim, os casos com legislação datada há 16 anos ou mais assumiram um valor (2), sendo a categoria que significa o valor máximo de amadurecimento em termos institucionais e de legislação na área. Na Figura 9, está definida a relação entre a condição explicativa e o fenômeno observado, através da teoria causal e da hipótese da pesquisa.

Figura 9 - Tempo do marco Jurídico-institucional: representação da teoria.



Fonte: Adaptação do autor a partir do modelo de Kellstedt e Whitten (2013).

Como pode ser observado a partir da representação na Figura 9, intencionamos testar a hipótese **H1.4**, de que o **Tempo do Marco Jurídico-institucional** é uma condição necessária e/ou suficiente para o comprometimento com a Segurança Cibernética nos países do continente americano.

Com isso, argumentamos que a maturação da legislação em matéria de Segurança Cibernética importa para a explicação conjuntural do comprometimento dos países das Américas na área. Para comprovar essa hipótese, precisamos identificar o **Tempo do Marco Jurídico-institucional** como uma condição que integra os conjuntos de possíveis caminhos para o maior comprometimento com a Segurança Cibernética.

2.6 MILITARIZAÇÃO DO ESPAÇO CIBERNÉTICO

2.6.1 O Estado e a Segurança Cibernética

A ideia de militarização pressupõe uma discussão anterior sobre como a Segurança Cibernética, desde a sua origem até então, tem sido abordada como um assunto dos Estados (cf. CAVELTY; EGLOFF, 2019; FARIA, 2016; OLSZEWSKI, 2016; KREMER, 2014). Essa visão conduz ao cerne do problema atual no debate sobre a militarização do setor. Como afirmado por Cavelty e Egloff (2019), nos países democráticos, os limites da participação

estatal nas diversas áreas da sociedade é algo a ser questionado e analisado com ponderação. A partir dessa perspectiva, os autores desenvolvem em seu estudo uma estruturação do que eles entendem como os três níveis de apresentação do assunto:

1) A partir da revisão da literatura sobre Segurança Cibernética;

2) Com base na realidade das políticas desenvolvidas pelos países, discutindo, assim, qual o papel que o Estado exerce na prática;

3) Debatendo, amparados na expectativa teórica, o que os autores entendem como o papel do Estado no setor de Segurança Cibernética e em que isso diverge em relação ao que tem sido apresentado empiricamente até então (CAVELTY; EGLOFF, 2019).

Nesse sentido, o que normalmente é vivenciado pelos países em todo o mundo é o que Kremer (2014) indica como uma predominância da mentalidade militar nos assuntos de Segurança Cibernética. Ele afirma que as abordagens nessa área podem ser classificadas como pertencentes a uma mentalidade militar ou a uma mentalidade liberal, ressaltando também que o próprio conceito pode implicar em várias possibilidades de interpretação:

> A maneira como conceituamos o termo segurança determina fortemente a forma como entendemos e resolvemos os problemas de segurança. Portanto, falar sobre a segurança estratégica de um estado implica a articulação de diferentes estratégias e de resoluções de problemas divergentes dos que são necessários quando falamos sobre segurança alimentar para os seres humanos nos países menos desenvolvidos. Torna-se claro que segurança pode significar muitas coisas (KREMER, 2014, p. 221, tradução livre).

Na perspectiva da Segurança Cibernética, que dialoga com a primeira noção de segurança supracitada, as mentalidades liberal e militar agrupam as possibilidades de tomadas de decisão e de formulação de políticas públicas, fazendo mister a sua explanação mais detalhada.

Enquanto a mentalidade militar na Segurança Cibernética preza pela formulação de políticas e estratégias nacionais tendo como mote as ameaças emergentes, a ideia de guerra cibernética, os ataques de caráter internacional e a própria noção de defesa nacional, a mentalidade liberal está alinhada ao que pode ser entendido como um direcionamento mais civil da questão, que consiste na defesa do debate legal sobre os limites e as fronteiras do espaço cibernético, a regulamentação da legislação na área, principalmente direcionada ao combate aos crimes cibernéticos. Além disso, o construto liberal nessa temática pressupõe também a necessidade da proteção e da privacidade de dados, bem como o zelo pelos direitos humanos, pela liberdade e pelo que deve ser entendido como o bem da sociedade civil. No Quadro 9, apresentamos as principais divergências entre as mentalidades liberal e militar na Segurança Cibernética.

Quadro 9 - Atributos das Mentalidades na Segurança Cibernética.

Mentalidade Militar	Mentalidade Liberal
A ideia de ameaça é direcionada a uma comunidade ou às suas partes existenciais;	A ideia de ameaça é direcionada aos indivíduos;
A ameaça vem de um inimigo;	A ameaça vem de indivíduos;
Há ênfase na proteção da comunidade;	Há ênfase na proteção dos indivíduos contra danos;
Os meios e métodos priorizados são os militares, táticos e estratégicos;	Os meios e métodos priorizados são baseados no policiamento com justificativa e balanceamento de poder;
Foco no combate às ameaças;	Foco na regulamentação das ameaças;
Defesa de meios excepcionais para o combate às ameaças existentes;	Os meios excepcionais de combate às ameaças podem existir, mas precisam ser justificados pelos marcos legais;
Cenários de ameaça exagerados.	Cenários de ameaça moderados.

Fonte: Kremer (2014). Tradução do autor.

Como o Quadro 9 evidencia, as divergências entre as mentalidades militar e liberal no que concerne à Segurança Cibernética são várias e se entrelaçam institucionalmente, abrangendo os mais diversos aspectos. Há diferença não apenas no modo de se entender o conceito de Segurança Cibernética, mas também no modo em que se operacionaliza o conceito e que são formuladas estratégias e políticas públicas para o combate do que é entendido como a ameaça (e.g. guerras cibernéticas para o ideal militar e crimes cibernéticos para o liberal).

Dessa forma, a militarização demonstra ser um fator importante para o entendimento da Segurança Cibernética como campo de estudo, e também das políticas públicas na área, considerando que o debate sobre a presença do Estado e dos militares no espaço cibernético é recente e demanda maiores contribuições para o conhecimento científico, com o exemplo de trabalhos empíricos.

2.6.2 Militarização: conceito, expectativa teórica e operacionalização

A nossa pesquisa adere à definição de Zaverucha (2008) para o conceito de militarização, que é entendido como “o processo de adoção de modelos, conceitos, doutrinas,

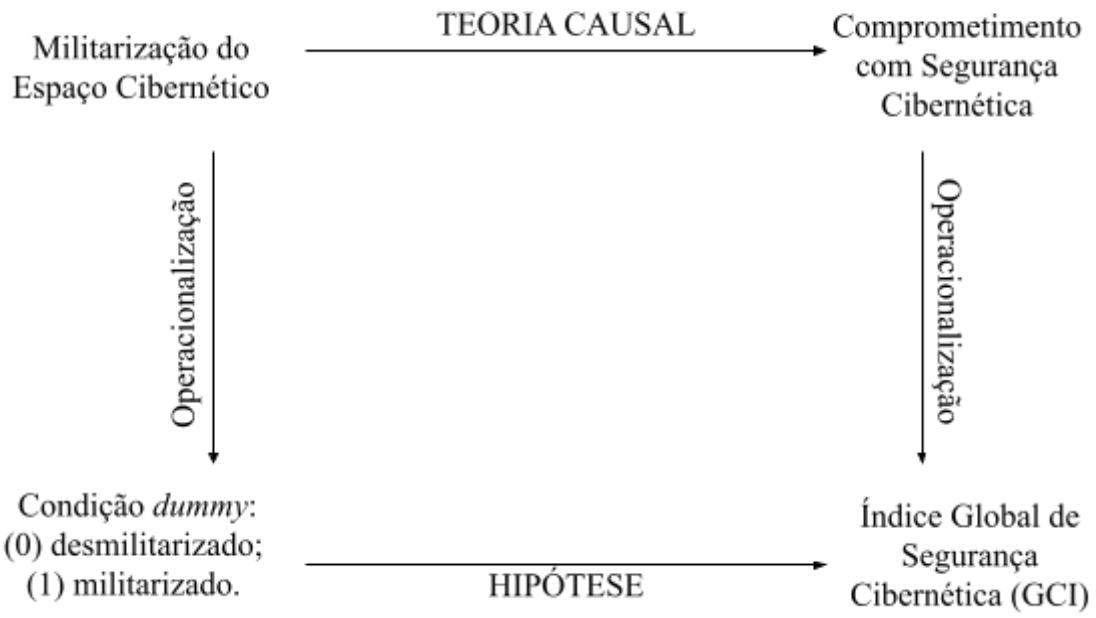
procedimentos e pessoal militares em atividades de natureza civil, dentre elas a segurança pública" (ZAVERUCHA, 2008).

Dessa maneira, argumenta-se que a militarização do espaço cibernético (CAVELTY, 2012) está negativamente relacionada com a utilização dessa estrutura militar para fins essencialmente civis, como a Segurança Pública Cibernética (LIRA-BRITO, 2020). Segundo a literatura da área, a determinação desse setor como de domínio militar, como acontece no Brasil (NOBREGA JUNIOR, 2010; HUREL, 2018), representa problemas para os Estados, uma vez que pode ocorrer um desvio nos procedimentos, doutrinas e modelos, de maneira a submeter a Segurança Cibernética à Defesa Cibernética e à noção do espaço cibernético como um território que deve ser controlado por atores estatais, ao invés de entender e respeitar o seu caráter civil e a centralidade que a economia e as soluções baseadas na cooperação entre os Estados devem ter (CAVELTY, 2012).

Com base no que foi exposto, esperamos confirmar a expectativa teórica de que, no entanto, a militarização do espaço cibernético está positivamente relacionada com o comprometimento com a Segurança Cibernética nos países americanos, considerando que, mesmo que os casos onde há a militarização do espaço cibernético tendam a utilizar ferramental e estrutura institucional diferentes dos necessários para a efetivação da Segurança Pública Cibernética e o estabelecimento da cooperação entre os Estados, a militarização do setor integra um contexto conjuntural que potencializa o comprometimento com a Segurança Cibernética.

Na Figura 10, apresentamos a aplicação do modelo de Kellstedt e Whitten à teoria aqui mobilizada.

Figura 10 - Militarização do Espaço Cibernético: operacionalização da teoria.



Fonte: Adaptação do autor a partir do modelo de Kellstedt e Whitten (2013).

Como explicitado acima e ilustrado na Figura 10, buscamos testar a hipótese **H1.5**, de que a **Militarização** da Segurança Cibernética é condição necessária e/ou suficiente para o comprometimento com a Segurança Cibernética dos países americanos.

Quadro 10 - Classificação dos Países Americanos segundo a Militarização.

CATEGORIA	DESCRIÇÃO
Não militarizado (0)	Não possui um setor cibernético militarizado, ou seja, a agência responsável pelo setor não é de caráter militar;
Militarizado (1)	O setor cibernético do país é militarizado, estando sob responsabilidade institucional dos militares.

Fonte: Elaboração do autor com base nos dados da pesquisa.

Como pode ser observado no Quadro 10, os casos das Américas serão avaliados de acordo com o caráter da agência responsável pelo setor de Segurança Cibernética, para a classificação dos Estados. Dessa maneira, países onde a agência responsável é de origem civil, ligada, por exemplo, a ministérios como o da Ciência e Tecnologia, são analisados como não militarizados (0) nesse aspecto. Por outro lado, os países onde o setor está estruturado a

partir de uma agência militar são categorizados como militarizados (1) em relação ao setor de Segurança Cibernética.

2.7 DESENVOLVIMENTO ECONÔMICO

2.7.1 Desenvolvimento Econômico e Segurança Cibernética

Os estudos sobre desenvolvimento econômico são uma constante na Ciência Política contemporânea, abrangendo desde análises sistemáticas sobre regimes políticos e a sua relação com o desenvolvimento econômico, utilizando o método comparativo, até pesquisas sobre as transições democráticas, a importância das instituições e da cultura, bem como o modo como esses processos ocorreram nas últimas décadas (e.g. PRZEWORSKI et al., 2000; NORTH, 1990; PUTNAM, 1996; SUMNER; TRIBE, 2008; MARQUES, 2018).

Em observância desse debate, a condição desenvolvimento econômico integra o conjunto de fatores explicativos analisados nesta pesquisa, uma vez que, considerando o fenômeno do comprometimento com a Segurança Cibernética (ITU, 2019) a partir de uma lógica multicausal, torna-se indispensável a inserção desta condição (cf. VASIU; VASIU, 2018), pois, o continente americano apresenta uma distribuição heterogênea e repleta de *outliers* em relação ao desenvolvimento econômico, podendo ser observada um desnível entre as regiões das Américas (América do Norte, América do Sul, América Central). Esse fato, argumentamos, pode ser equiparado à irregularidade na distribuição dos países americanos no Índice Global de Segurança Cibernética (GCI).

2.7.2 Índice de Desenvolvimento Humano

Com base nos argumentos apresentados, faz-se mister dissociar conceitualmente a noção de desenvolvimento econômico da ideia de crescimento econômico. Dessa forma, o primeiro difere do segundo na medida em que é entendido como o "melhoramento dos padrões de vida, da educação, da assistência médica e da proteção ambiental" (SUMNER; TRIBE, 2008, p. 7, *apud* KIRTILLI, 2019, p. 48), não se resumindo simplesmente ao Produto Interno Bruto (PIB) e ao crescimento da economia (SOUZA; SPINOLA, 2017).

A partir dessa definição, decidimos utilizar o Índice de Desenvolvimento Humano (IDH), desenvolvido pelo Programa das Nações Unidas pelo Desenvolvimento (PNUD), como medida de desenvolvimento econômico pela sua capacidade de abranger outros aspectos que "mensuram a satisfação das necessidades humanas básicas e as liberdades substantivas" (SOUZA; SPINOLA, 2017, p. 78), o que representa uma complementaridade

em relação aos outros fatores explicativos do estudo. Os referidos autores assim complementam:

> O IDH é calculado anualmente e se apresenta como uma medida agregada e sintética do desenvolvimento, uma alternativa de medição do bem-estar humano, passível de comparação entre países e contraponto às medidas de desenvolvimento que se centram exclusivamente em indicadores monetários e na dimensão econômica. Simboliza uma mudança na forma de mensuração do desenvolvimento, porém captura apenas uma parte daquilo que o desenvolvimento humano representa. SOUZA; SPINOLA, 2017, p. 97)

Muller (2015) vislumbra o desenvolvimento humano como uma importante medida para o eixo da capacitação em Segurança Cibernética nos países emergentes. Com a popularização do acesso à *Internet*, promoveu-se a inserção de uma maioria ao espaço cibernético sem ter sido propiciadas as mínimas condições para que esse acesso fosse seguro. Dessa forma, além das contribuições em relação ao desenvolvimento econômico, o IDH fornece aparato para se avaliar aspectos básicos do acesso humano à educação e ao exercício de liberdade, que são as premissas para a potencial formação em termos de Segurança Cibernética para o dia a dia.

No Brasil, por exemplo, há uma iniciativa intitulada *Cyber-Cid* - os desafios da cidadania cibernética na era da informação, do Projeto "Ciência, Tecnologia e Inovação em Defesa: cibernética e defesa nacional", coordenado pelo Professor Doutor Marcos Aurélio Guedes de Oliveira. Esse projeto proporciona formação básica, em escolas públicas do município de Recife/PE, sobre as questões inerentes à proteção contra os crimes cibernéticos e sobre as melhores práticas para o exercício da cidadania no espaço cibernético.

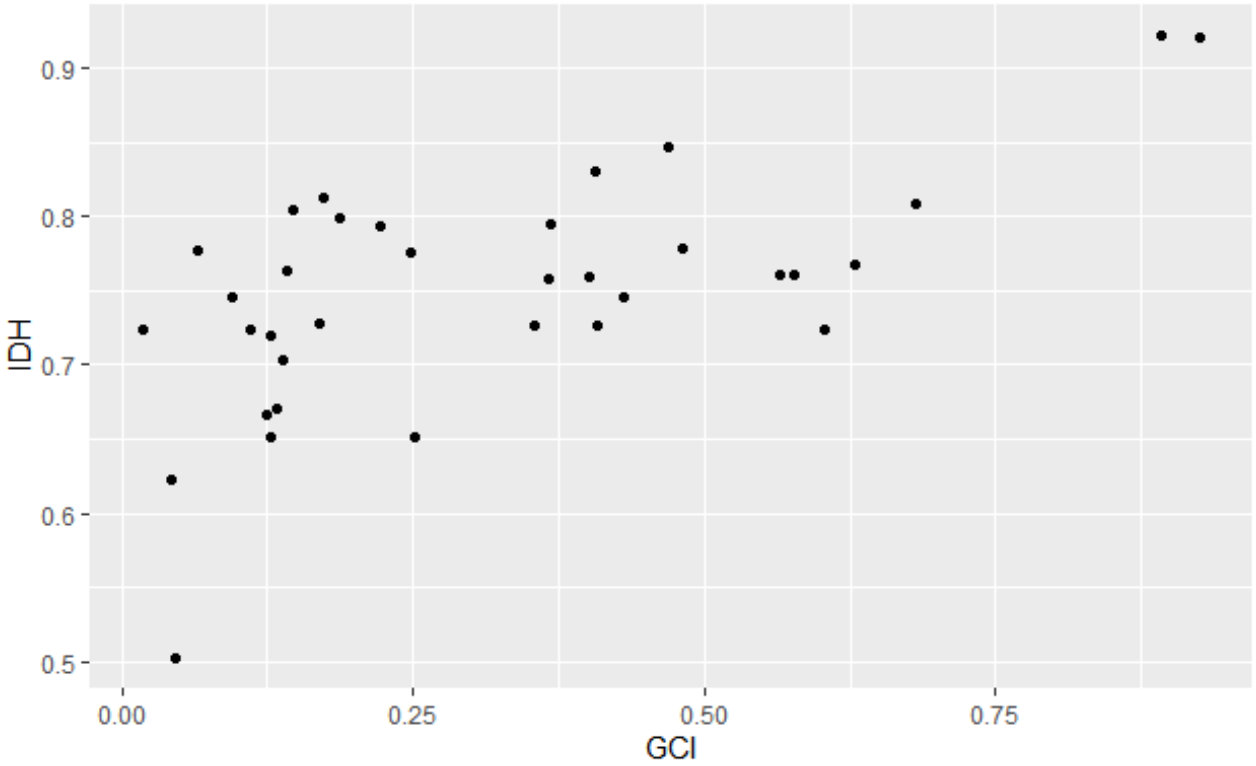
Diferentemente de Kirtilli (2019), que buscou através de análises quantitativa e qualitativa, identificar a relação entre desenvolvimento econômico e elaboração de políticas públicas na Segurança Cibernética em países desenvolvidos, emergentes e em desenvolvimento, utilizando o Produto Interno Bruto (PIB) como variável independente, a nossa pesquisa intenciona analisar os Estados do continente americano a partir do Índice de Desenvolvimento Humano (IDH).

Apenas no último ano, de 2020 até então, o *Google Scholar* já registrou em torno de 19 mil e 300 (19.300) menções[15] ao IDH em sua plataforma, o que ressalta a importância e a ampla aplicabilidade desse índice nas pesquisas científicas.

---

[15] Disponível em: https://scholar.google.com/scholar?as_ylo=2020&q=%22Human+Development+Index%22+&hl=en&as_sdt=0,5 Acesso em: 02 de nov. de 2021.

Gráfico 2 - Distribuição do IDH em Relação ao GCI nos Países Americanos - 2018.



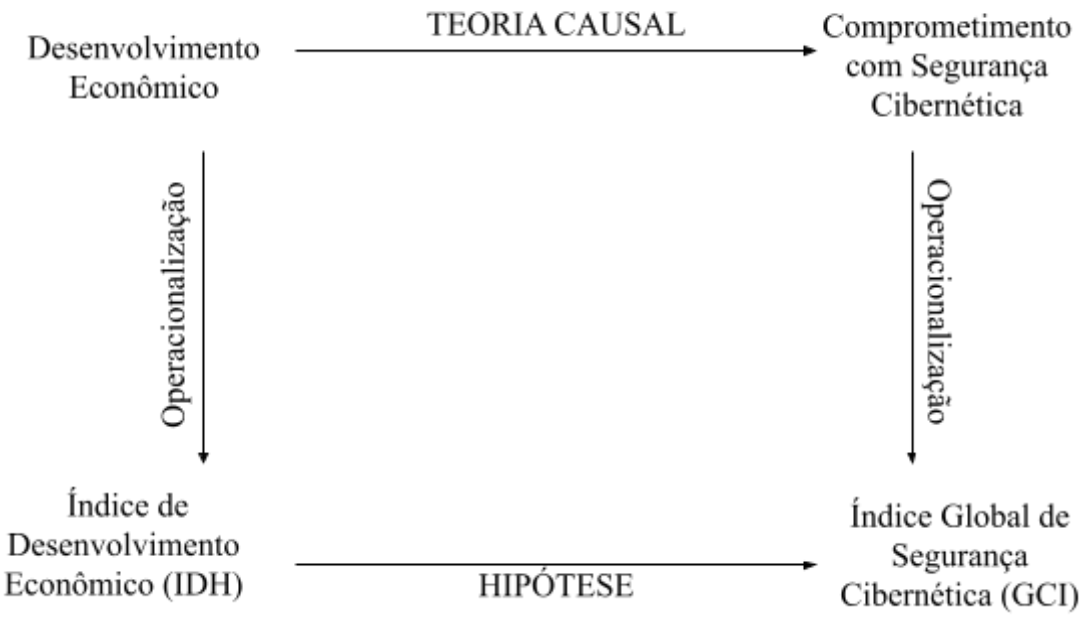
Fonte: ITU (2019) e PNUD[16]. Elaboração do autor.

No Gráfico 2, com base no teste de correlação de Pearson entre o IDH e o GCI, que apresentou p-valor estatisticamente significante (0,00005), intervalo de confiança não incluindo o 0, e uma correlação positiva de 63% (considerada moderada), confirmamos a necessidade de um estudo mais detalhado sobre o tema, discutindo a relação entre os dois índices e como o Índice de Desenvolvimento Humano pode integrar o conjunto de fatores que determinam o comprometimento com Segurança Cibernética nos Estados das Américas, avaliado pelo GCI.

No entanto, considerando o tamanho da população analisada e a irregularidade da distribuição (como pode ser observado no Gráfico 2), que dificultam a possibilidade de uma abordagem quantitativa, decidimos pela inclusão do IDH no modelo da Análise Qualitativa Comparativa (QCA). Na Figura 11, apresentamos a operacionalização do conceito para fins de aplicação nesta pesquisa.

[16] Disponível em: http://hdr.undp.org/en. Acesso em 20 de mar. de 2021.

Figura 11 - Desenvolvimento Econômico: operacionalização da teoria.



Fonte: Adaptação do autor a partir do modelo de Kellstedt e Whitten (2013).

Direcionados pelo modelo representado na Figura 11, pretendemos testar a hipótese **H1.6**, de que o **Desenvolvimento Econômico** constitui uma condição necessária e/ou suficiente para explicar conjunturalmente o comprometimento com a Segurança Cibernética nos países do continente americano. Nesse ínterim, em termos de operacionalização do conceito de Desenvolvimento Econômico, como mencionado, utilizaremos o desempenho dos países no Índice de Desenvolvimento Humano como a materialização da condição supracitada. No Quadro 11, apresentamos as classificações.

Quadro 11 - Categorização do Desenvolvimento Econômico nas Américas.

CATEGORIA	DEFINIÇÃO
IDH baixo ou médio (0)	Estados com o IDH inferior a 0,699.
IDH Elevado (1)	Estados com o IDH entre 0,700 e 0,799.
Muito Elevado (2)	Estados com o IDH igual ou superior a 0,800.

Fonte: Elaboração do autor com base nos dados da pesquisa.

A partir das informações disponibilizadas pelo PNUD (2019), adaptamos a tipologia dos países em três dimensões, como pode ser observado no Quadro 11, onde os Estados com IDH inferior a 0,699 passam a ter o valor (0). Por sua vez, os países com IDH elevado - entre

0,700 e 0,799 - passam a ser representados pela categoria (1). Os casos com IDH muito elevado - igual ou superior a 0,800 -, por fim, são classificados com valor (2) nesta pesquisa.

3 METODOLOGIA

"The motto of science is not just Pauca but rather Plurima ex paucissimis – the most out of the least." (Mario Bunge)

A presente pesquisa se insere no campo da Política Comparada à medida que, através de metodologias qualitativa e qualitativa-configuracional, intenciona identificar os fatores que explicam o nível de comprometimento com a Segurança Cibernética nos países do continente americano em 2018, que é avaliado a partir do Índice Global de Segurança Cibernética (GCI), consistindo em um estudo observacional com corte transversal. Segundo Barberia (2019):

> Estudos observacionais de corte transversal são realizados quando comparamos diferentes unidades de análise em um determinado ponto no tempo. As unidades espaciais costumam ser definidas em termos geográficos: distritos, bairros, municípios, regiões, estados, países ou mesmo continentes. (BARBERIA, 2019, p.7)

King, Keohane e Verba (KKV), na obra seminal *Designing Social Inquiry: Scientific Inference in Qualitative Research*, ressaltaram o papel do rigor metodológico tanto nas pesquisas qualitativas quanto nas quantitativas, buscando enfatizar a necessidade da cautela para a elaboração de desenhos de pesquisa. Os autores argumentam que, mesmo havendo uma separação histórica entre as duas vertentes, há unicidade lógica entre as culturas metodológicas, uma vez que elas estariam buscando, cada uma a seu modo, gerar inferências causais válidas, produzir teorias falseáveis operacionalizadas em hipóteses claras (KING; KEOHANE; VERBA, 1994).

Após uma década do lançamento do trabalho de KKV, em *Rethinking Social Inquiry: Diverse Tools, Shared Standards*, cujos editores são Brady e Collier (2004), cientistas sociais apresentaram uma série de ressalvas contundentes aos principais argumentos de KKV.

Para aqueles, a ideia de unificação metodológica presente na obra foi pautada numa lógica quantitativa de pesquisa. Eles frisaram também o valor das tipologias e classificações nos estudos com viés qualitativo, que não necessariamente consistem em geração de hipóteses e inferência causal (BRADY; COLLIER, 2004).

Nesse decurso, Goertz e Mahoney (2012), em *A Tale of Two Cultures: Contrasting Quantitative & Qualitative Research in the Social Sciences*, defenderam que os métodos quantitativos e qualitativos constituem duas culturas diferentes, cada uma com paradigmas, práticas, e técnicas dessemelhantes.

O enfoque dos autores são as diferenças entre essas culturas, que são consideráveis nas pesquisas nas Ciências Sociais. Mas eles, para além do estudo das diferenças entre os métodos quantitativos e qualitativos, buscam promover entre os pesquisadores das duas

culturas uma prática de tolerância, tendo em vista as possibilidades de aprendizado que cada cientista social pode ter ao não reduzir as suas fronteiras a uma dessas culturas (GOERTZ; MAHONEY, 2012).

3.1 DESENHO DA PESQUISA

A metodologia desta pesquisa está configurada em duas etapas vinculadas: o método para realização da primeira parte da pesquisa tem caráter qualitativo-configuracional, consistindo a coleta de dados em análise documental acerca dos 35 países do continente americano e no acesso às informações contidas no GCI. Complementarmente, a segunda parte do trabalho consiste em um estudo de caso sobre o Brasil, sendo a sua coleta de dados também uma análise documental. No Quadro 12, apresentamos a estrutura metodológica desta pesquisa.

Quadro 12 - Desenho da Pesquisa.

DESCRIÇÃO	ESTUDO COMPARATIVO	ESTUDO DE CASO
Pergunta	Quais fatores explicam o nível de comprometimento com a Segurança Cibernética no continente americano em 2018?	Como os conjuntos de condições que explicam o nível de comprometimento com a Segurança Cibernética se relacionam no caso brasileiro?
Tipo de Método	Qualitativo-configuracional.	Qualitativo.
Coleta de Dados	Análise documental.	Análise documental.
Análise de Dados	Análise Qualitativa Comparativa.	Análises Qualitativa e Quantitativa.
Ferramenta de Análise	R, RStudio e Tosmana.	R, RStudio e Tosmana.
Recorte Temporal	2018.	2004 - 2018.
Condições	a) securitização, b) despesas militares, c)	a) securitização, b) despesas militares Cibernética, c)

	ocorrência de eventos raros, d) tempo do marco jurídico-institucional, e) militarização do espaço cibernético; f) desenvolvimento econômico.	ocorrência de eventos raros, d) tempo do marco jurídico-institucional, e) militarização espaço cibernético; f) desenvolvimento econômico.
Fonte	Índice Global de Segurança Cibernética (GCI), legislação e políticas de segurança cibernética dos 35 casos analisados.	Índice Global de Segurança Cibernética (GCI), legislação e políticas de segurança cibernética no Brasil.

Fonte: Banco de dados da pesquisa. Elaboração do autor.

No Quadro 12, apresentamos a estrutura do desenho desta pesquisa, que tem caráter misto e se divide nas duas etapas complementares. Na QCA, a pergunta que mobiliza a pesquisa é "Quais fatores explicam o nível de comprometimento com a Segurança Cibernética no continente americano em 2018?", enquanto no estudo de caso a questão que intencionamos responder é "Como os conjuntos de condições que explicam o nível de comprometimento com a Segurança Cibernética se relacionam no caso brasileiro?".

Para tanto, estabelecemos as técnicas da Análise Qualitativa Comparativa e do estudo de caso, com coleta de dados quantitativos e qualitativos, através da análise documental. Na primeira etapa, o recorte temporal é referente ao ano de 2018. Na segunda etapa, no entanto, para acompanhar o desenvolvimento do contexto brasileiro, o recorte temporal abrange o período de 2004 a 2018, buscando identificar os mecanismos causais para o comprometimento com a Segurança Cibernética no país.

Como condições explicativas, consideramos: 1) securitização; 2) despesas militares; 3) ocorrência de eventos raros; 4) tempo do marco jurídico-institucional; 5) militarização do espaço cibernético; e 6) desenvolvimento econômico. A principal fonte da pesquisa é o *Global Cybersecurity Index* (ITU, 2019), no entanto também utilizamos outras fontes, como os portais eletrônicos da UNIDIR (2021) e da OEA (2021), que sistematizam grande parte das informações necessárias para o desenvolvimento desta pesquisa.

3.1.1 Método Comparativo

O Método Comparativo possui um lugar canônico na Ciência Política e nas Relações Internacionais, sendo a estrutura metodológica de uma grande parte das obras renomadas nessas áreas (PUTNAM, 1996; HAGGARD; MCCUBBINS, 2001; MAINWARING, 1993; SHUGART; CAREY, 1992; SKOCPOL, 1979; PRZEWORSKI et al., 2000). O próprio fazer científico e a construção do conhecimento, sob uma lógica estrutural, pressupõem a ideia comparação. Mas essa ideia permeia o campo teórico-metodológico de maneira mais profícua. Como argumenta Landman (2008), a comparação de países em Ciência Política e Relações Internacionais (CPRI) pode ter inúmeras vantagens, desde a possibilidade de classificação e teste de hipóteses com uma maior amplitude até a capacidade de predição de fenômenos políticos. Além disso, a Política Comparada também está inserida nas áreas em transformação devido às recentes modificações em CPRI na direção do ajuste para a geração de inferências causais (REZENDE, 2017).

Em Política Comparada, também têm sido debatidas as possibilidades explicativas em termos de suficiência e necessidade. Devido à escassez de estudos com essa orientação metodológica na área de Segurança Cibernética, buscamos ampliar o horizonte em direção a desenhos metodológicos semelhantes em outras áreas. Um dos estudos exemplares nessa seara é a obra de Immergut (1992). A autora tem desenvolvido, ao longo de sua carreira, pesquisas abordando temas como: o impacto da competição eleitoral e política nas reformas do estado de bem-estar social; políticas de saúde na Europa e as consequências do populismo de direita para as políticas sociais. Nesse sentido, o referido trabalho alinha-se ao neoinstitucionalismo histórico com arcabouço metodológico da Política Comparada e parte das seguintes questões:

> se as instituições devem ter uma espécie de capacidade de permanência, como as mesmas instituições podem explicar tanto a estabilidade quanto a mudança? Se as instituições limitam o escopo da ação que parece possível aos diferentes atores, por que estes podem às vezes escapar dessas restrições? (IMMERGUT, 1992, p. 1).

Dessa forma, Immergut (1992) contribui com a discussão neoinstitucionalista histórica apresentando, a partir de casos de países europeus (Suécia, França e Suíça), como as mesmas instituições podem servir para explicar tanto a mudança como a permanência de políticas. Ela seleciona o seguro nacional de saúde como política analisada e observa como *inputs* e *outputs* se relacionam de formas diferentes a depender do sistema político de cada país, o que, segundo a autora, rompe com a noção usual de explicação por correlações.

Mesmo não utilizando necessariamente as técnicas de pesquisa da Análise Qualitativa Comparativa (QCA), a autora se utiliza de uma lógica de necessidade e suficiência que dialoga com o modo como o Método Comparativo em si é pensado, apresentando casos que, tudo o mais constante, divergiam unicamente, ou quase isso, em como as regras do jogo, que consistiam nos poderes de veto dos atores políticos, estavam distribuídas no sistema político de cada país, chegando a três tipos de resultados diferentes: no primeiro, o seguro nacional de saúde foi implementado perfeitamente; no segundo, foi instaurado de maneira quase satisfatória; e, no último, o seguro de saúde não foi aprovado como política pública no país.

Dessa maneira, os resultados da autora apresentam as condições do posicionamento estratégico das regras do jogo como necessárias e suficientes para que a política em questão ocorresse. Nesse sentido, é necessário o entendimento de como o Método Comparativo pode se ramificar para a sua aplicação na QCA, buscando a identificação da necessidade e da suficiência.

Para melhor apresentar os limites e possibilidades desse tipo de lógica para a análise de fenômenos, utilizaremos o exemplo de Mackie (1965) sobre o incêndio. A princípio, hipoteticamente, sabe-se que houve um incêndio em uma casa específica causado por um curto-circuito em determinado cômodo.

O curto-circuito é uma condição necessária para a ocorrência do evento? Mackie (1965) argumenta que não. Esse mesmo *outcome* poderia ter sido alcançado de diversas formas diferentes, desde vazamento de gás até curtos-circuitos em casas vizinhas. Seria, então, o curto-circuito uma condição suficiente para o incêndio? O autor responde que não, uma vez que, além do curto-circuito, o fenômeno necessitava da presença de materiais inflamáveis próximos ao local, garantindo, assim, que o curto-circuito tomasse a proporção de um incêndio.

A partir dessa problematização, Mackie (1965) aponta como o exemplo dialoga com a questão da causação: a causa do incêndio implica o entendimento do mesmo a partir de um conjunto de condições, ou uma condição complexa, para a sua ocorrência (MACKIE, 1965).

Por conseguinte, como derivação desse problema para uma maior adaptabilidade do poder explicativo à realidade empírica, acrescenta-se duas outras possibilidades para as condições: INUS e SUIN.

1) **INUS:** "***I****nsufficient but* ***N****ecessary part of a condition which is itself* ***U****nnecessary but* ***S****ufficient for the result"* (MACKIE, 1965, p. 245).

2) **SUIN:** "***S****ufficient but* ***U****nnecessary part of a factor that is* ***I****nsufficient but* ***N****ecessary for an outcome*" (MAHONEY, 2008, p. 419).

O exemplo desenvolvido confirma-se, então, como uma condição INUS, uma vez que, segundo Mackie (1965):

> O curto-circuito que se diz ter causado o incêndio é, portanto, uma parte indispensável de uma condição complexa suficiente (mas não necessária) do incêndio. Nesse caso, então, a chamada causa é, e sabe-se que é, uma parte insuficiente, mas necessária, de uma condição que é ela própria desnecessária mas suficiente para o resultado (MACKIE, 1965, p. 245, tradução livre).

Substantivamente, nesta pesquisa, o potencial de classificação dos casos a partir da ideia de necessidade, suficiência e, quando devido, INUS e SUIN, bem como a possibilidade de realização de teste de teorias, constituem a base para as próximas seções.

Em seguida, apresentamos a Análise Qualitativa Comparativa, seu conceito, suas categorias, pressupostos e consequências. Essa técnica será utilizada para avaliar como os 35 países americanos podem ser considerados em termos de Securitização, Ocorrência de Eventos Raros, Militarização do setor cibernético, Desenvolvimento Econômico, Tempo do Marco Jurídico-Institucional e Despesas Militares, e de como essas condições se configuram em conjuntos para explicar os casos de maior desempenho no que tange ao comprometimento com a Segurança Cibernética, medido pelo GCI.

3.1.2 Análise Qualitativa Comparativa (QCA)

A Análise Qualitativa Comparativa (QCA) baseia-se no método booleano proposto por Ragin (1987). Além disso, nos anos consecutivos, o referido autor acrescentou uma nova contribuição metodológica, ao propor maior flexibilidade aos valores e condições na QCA, passando a pensá-la através do modelo *fuzzy* (RAGIN, 2000).

Nesse ínterim, considerando o número de casos da amostra e a quantidade de informação de cada caso que deve ser preservada, optou-se pela utilização do tipo de análise *multi-value Qualitative Comparative Analysis* (mvQCA), que permite a categorização não-dicotômica de variáveis, sem precisar migrar para a lógica *fuzzy*.

Um dos principais aspectos que diferenciam a QCA de técnicas quantitativas tradicionais, segundo Hudson e Kühner (2013), é a sua independência em relação à natureza da amostragem, se aleatória ou não, e da distribuição dos casos, se homogênea ou heterogênea.

Dessa maneira, a Análise Qualitativa Comparativa é especialmente indicada para pesquisas que lidam com a presença de casos extremos e com uma distribuição heterogênea

(HUDSON; KÜHNER, 2013), sendo também preponderante em um contexto de multicolinearidade, onde há a dificuldade, por parte das técnicas quantitativas mais utilizadas, de isolar o efeito das variáveis.

Nesse sentido, Figueiredo Filho et al. (2021) ressaltam que, "por meio da QCA, acaba sendo possível analisar também o contexto e verificar situações envolvendo a interação de diversas variáveis na produção de um determinado *outcome*, permitindo identificar quais as condições necessárias e suficientes para obtenção de um resultado X". Além disso, como Betarelli Júnior e Ferreira (2018) afirmam:

> A abordagem de QCA, ao contrário das ferramentas estatísticas e econométricas tradicionais, possibilita a identificação de mais de um único caminho para um determinado resultado de política, pois mais de uma combinação de condições pode conduzir a um determinado resultado político. (BETARELLI JUNIOR; PEREIRA, 2018, p. 29).

Essa possibilidade mencionada é caracterizada pela causalidade complexa, que está intrinsecamente relacionada aos conceitos de equifinalidade, situação na qual trajetórias variadas podem conduzir à ocorrência de um evento, e multicausalidade conjuntural, que se refere "às combinações de vários conjuntos ou condições únicas que podem exibir efeitos sobre o resultado de interesse da pesquisa" (BETARELLI JUNIOR; PEREIRA, 2018, p. 17).

Não obstante, um dos avanços representados pela QCA é justamente a forma como os casos são tratados seguindo uma lógica configuracional. Dessa forma, por exemplo, cada país analisado neste trabalho é observado a partir do seu contexto configuracional, sendo classificado com base nas informações obtidas para cada condição explicativa. Diante disso, há como se maximizar as diferenças e observar em quais configurações de condições explicativas o fenômeno de interesse ocorre. De acordo com Sandes Freitas e Bizarro Neto (2015):

> O método de Ragin foi pensado como uma forma de realizar análises comparativas, buscando associações entre determinadas condições e o outcome, levando em conta o conjunto de configurações dos casos e não somente o efeito particular de uma variável sobre o outcome. Devido a esta particularidade, este tipo de análise é também denominado de método configuracional, tendo sido inicialmente desenvolvido para o estudo de um número pequeno ou intermediário de casos. Este método de comparação dos casos permite sistematizar, operacionalizar as variáveis ou configurações, possibilitando a análise cross-case, a partir de uma determinada teoria sobre o fenômeno em análise. Permite a comparação, guardando a complexidade dos casos (within-case). Além disso, com esse método, é possível ir além da descrição, realizando "generalizações modestas", mas com limitações temporais (SANDES FREITAS; BIZARRO NETO, 2015).

Dessa maneira, com a aplicação dessa técnica, o pesquisador pode aprofundar o detalhamento sobre os casos sem perder tanto o potencial explicativo em relação aos métodos

quantitativos em geral. Além disso, a possibilidade de se analisar as configurações das condições explicativas em uma conjuntura de causalidade complexa permite uma discussão mais pormenorizada em relação ao contexto de cada país e dos vários caminhos para o comprometimento com a Segurança Cibernética.

Betarelli Junior e Ferreira (2018), a partir do que foi enunciado sobre QCA por Rihoux e Ragin (2009) e Ragin (1987), representaram em um quadro, apresentado neste estudo como Quadro 13, as principais diferenças entre as técnicas quantitativas e a Análise Qualitativa Comparativa, que discutiremos abaixo.

Quadro 13 - Principais Diferenças entre a QCA e Técnicas Quantitativas.

TÉCNICAS QUANTITATIVAS TRADICIONAIS	ANÁLISE QUALITATIVA COMPARATIVA
Variáveis	Conjuntos
Variável Dependente	Resultado
Variáveis independentes	Condições
Correlações	Relações entre conjuntos
Matriz de correlação	Tabela Verdade
Efeitos líquidos das variáveis	Caminhos causais
Relações de aditividade e lineares	Relações não aditivas
Causalidade múltipla ou singular	Causalidade conjuntural múltipla
Causalidade simétrica	Causalidade assimétrica
Análise dos efeitos das variáveis	Análise dos efeitos das configurações

Fonte: Adaptado por Betarelli Junior e Ferreira (2018) de Rihoux e Ragin (2009) e Ragin (1987).

Como pode ser observado no Quadro 13, enquanto as técnicas tradicionais nos métodos quantitativos se utilizam de variáveis independentes e dependentes para explicar correlações, a QCA interpreta a realidade a partir de condições explicativas sob as quais um fenômeno pode ocorrer, a partir da relação de conjuntos.

Além disso, o que quantitativamente é proporcionado através de uma matriz de correlação, na QCA é interpretado tendo como fonte a tabela-verdade, que sistematiza as possibilidades lógicas encontradas nos dados levantados.

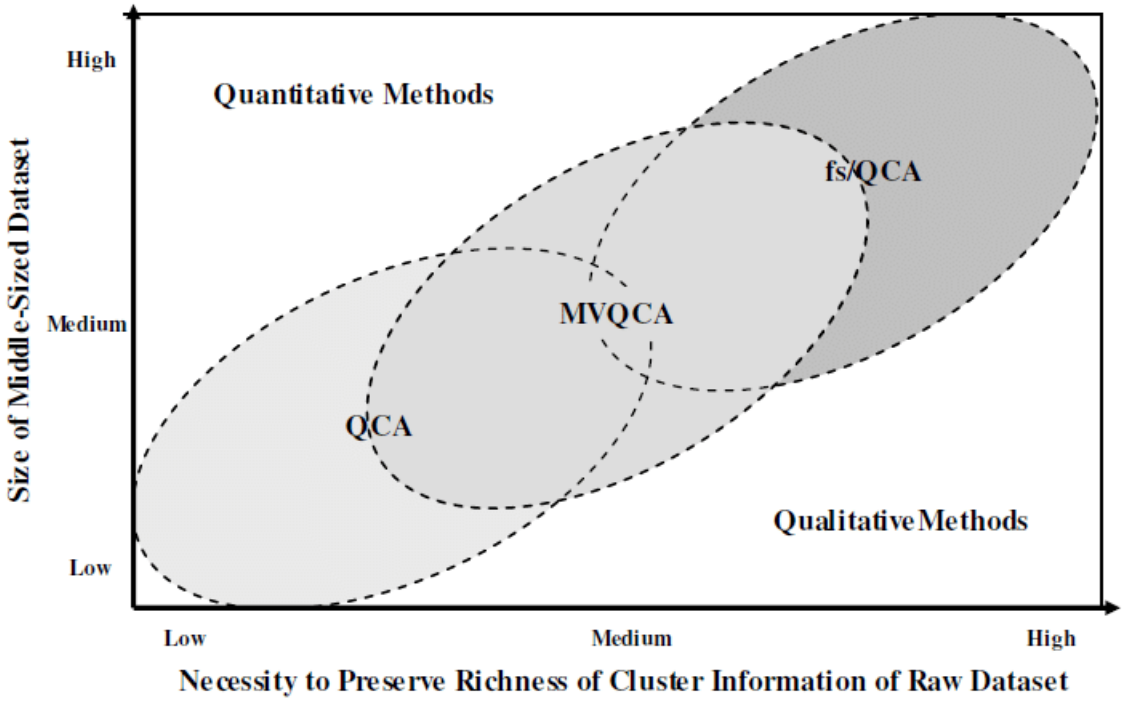
De modo semelhante, a Análise Qualitativa Comparativa busca identificar os caminhos causais para a ocorrência de um evento, diferente dos modelos quantitativos, que estimam os efeitos líquidos das variáveis explicativas sobre a variável resposta. Assim, essas últimas operam a partir de relações lineares e com a noção aditiva dos efeitos, enquanto a primeira funciona de maneira não linear e com base em diferenças qualitativas de categorias.

A essas questões, soma-se o fato de, na QCA, a lógica de causalidade ser direcionada a partir da ideia de causalidade conjuntural múltipla, o que não é observado na contraparte das técnicas quantitativas tradicionais, nas quais o que pode haver é a causalidade múltipla ou a causalidade singular, sem a inserção da noção de conjuntos na análise. Por isso, enquanto uma observa os efeitos de variáveis, a outra explica os efeitos dos conjuntos de condições.

A simetria é outra qualidade que diferencia a técnica utilizada nesta pesquisa de outras técnicas *mainstream* na Ciência Política, uma vez que a QCA não incorpora a possibilidade de causalidade simétrica em suas análise, enquanto as outras técnicas normalmente operam sob esse tipo de pressuposto. Nesse sentido, as conjunturas causais complexas que explicam o maior comprometimento com a Segurança Cibernética podem não explicar o seu menor comprometimento, não sendo possível aplicar o que foi inferido sobre as condições da ocorrência de um fenômeno para discussões acerca da não ocorrência do referido evento. Para tanto, seria necessária a identificação de possíveis condições, baseadas na expectativa teórica, para o menor comprometimento com a Segurança Cibernética e depois a realização de novos testes de hipóteses.

Dentre os tipos de classificações da Análise Qualitativa Comparativa, a *Multi-value QCA* (mvQCA) se apresenta como uma forma intermediária entre os modelos *Crisp-set QCA* (csQCA) e *Fuzzy-set QCA* (fsQCA), uma vez que oferece uma resposta ao problema da dicotomização no primeiro, assumindo mais valores para as classificações, sem necessariamente aderir à lógica de graus de pertencimento do segundo. Além disso, como ponderam Sandes Freitas e Bizarro Neto (2015), a mvQCA é especialmente indicada em pesquisas que apresentam pequeno ou médio número de casos, garantindo um detalhamento maior dos mesmos em relação ao modelo csQCA (SANTOS; BOTELHO, 2018; PÉREZ-LIÑÁN, 2010). A Figura 12 sistematiza algumas das divergências e convergências entre os tipos de Análise Qualitativa Comparativa, garantindo a comparabilidade para a escolha mais acertada.

Figura 12 - Comparação entre os modelos de QCA.



Fonte: HERRMANN, CRONQVIST (2006).

Como ilustrado acima por Herrmann e Cronqvist (2006), a mvQCA se apresenta de maneira intermediária entre a fsQCA e a csQCA, quando são considerados os aspectos de tamanho da base de dados e aprofundamento e preservação da riqueza de informações sobre os casos analisados, permanecendo também idealmente entre as culturas qualitativa e quantitativa. Os autores afirmam, ainda, que:

> mvQCA is the most appropriate method for analysing a genuinely middle-sized dataset which requires the retention of some raw-data information. On the one hand, and in contrast to fsQCA, mvQCA succeeds in revealing all causal conditions which lead to the observed outcome (HERRMANN; CRONQVIST, 2006, p. 15).

Portanto, em observância dessas questões, optamos pela utilização da mvQCA, que, além de tudo o que foi exposto, apresenta soluções para as contradições lógicas tão presentes na csQCA (RIHOUX; RAGIN, 2009). Nesse âmbito, analisaremos os países do continente americano a partir de um modelo nem dicotômico, nem diretamente *fuzzy*, proporcionando a assunção de categorias com valores (0), (1) e (2) para as condições explicativas do comprometimento com a Segurança Cibernética. De forma complementar, como uma forma de aprofundamento teórico-metodológico e integração em um desenho de pesquisa de métodos mistos, optamos por realizar um estudo de caso, que será apresentado a seguir.

3.1.3 Estudo de Caso

Em *The Case Study: What it is and What it Does*, Gerring (2007) recupera a definição de estudo de caso sob o enfoque da sua relação com a sua utilização na Política Comparada. Nesse sentido, esta pesquisa se utiliza do entendimento do referido autor de que esse método consiste em um estudo intensivo de um único caso com o intuito de contribuir para o conhecimento de uma população (GERRING, 2007). Como principais características e vantagens da utilização dos estudos de caso, Pasquarelli (2014) menciona que:

> Os estudos de caso são fortes principalmente nas áreas onde o método estatístico encontra problemas. Existem, então, quatro tipos de vantagens desse tipo de método. Em primeiro lugar, em razão da validade conceitual, identifica e mede indicadores que representam os conceitos teóricos – sem se expor ao estreitamento conceitual (conceptual stretching) ao colocar casos semelhantes e diferentes em uma mesma amostragem. Em segundo lugar, os estudos de caso têm procedimentos para identificar novas hipóteses e variáveis por meio de casos desviantes, desenvolvendo novas teorias que podem ser testadas através de evidências que não haviam sido examinadas. Em terceiro lugar, como não omite fatores contextuais, o método permite examinar o papel hipotético de mecanismos causais e de variáveis intervenientes inesperadas em casos individuais. Por fim, aborda a complexidade causal – como a equifinalidade, os efeitos de interação complexos e a path dependency (PASQUARELLI, 2014, p. 29-30).

Complementarmente, Sátyro e D'Albuquerque (2020) diferenciam os estudos de caso das técnicas qualitativas no Método Comparativo, porquanto os primeiros intencionam principalmente a análise em profundidade do caso em questão em detrimento do potencial de comparação dos resultados obtidos. Esse *trade-off* entre profundidade e riqueza das informações e abrangência da explicação (SÁTYRO; D'ALBUQUERQUE, 2020) é experienciado de forma oposta quando utilizamos a Análise Qualitativa Comparativa, o que acaba por balancear os fatores positivos e negativos das técnicas mencionadas quando observadas a partir de um desenho de pesquisa de caráter metodológico misto.

Sobre as razões emergentes para a utilização dos estudos de caso na Ciência Política e as suas relações com a validade no Método Comparativo, Rezende (2011), na mesma direção de Pasquarelli (2014), defende que:

> O núcleo argumentativo básico (*core*) se constitui por três explicações ou razões consideradas fundamentais para validar os estudos de caso. O primeiro deles está diretamente ligado à equifinalidade (*equifinality*) dos fenômenos políticos. O segundo argumento essencial considera a análise de processos causais, utilizando-se das metodologias de process-tracing como razão básica para validar as metodologias de caso na pesquisa histórico-comparada. Por fim, as escolhas metodológicas por estudos de caso se tornam válidas quando os analistas se voltam para a produção de explicações centradas em mecanismos causais. (REZENDE, 2011, p. 302).

Ao realizar um estudo de como as condições analisadas se configuram no contexto brasileiro, esperamos apresentar um prognóstico sobre qual é o caminho causal para o maior

comprometimento com a Segurança Cibernética no Brasil. Esse tipo de informação contribui para o estudo detalhando aspectos contextuais sobre o país analisado e acerca da capilaridade da teoria proposta para casos específicos, de modo a acrescentar profundidade explicativa ao modelo proposto nesta pesquisa.

Com o exemplo do caso brasileiro, estabelecemos não só uma aplicação das teorias mobilizadas para a realidade empírica - o que já é satisfeito na Análise Qualitativa Comparativa -, mas também o entendimento do papel do contexto para a avaliação do comprometimento com a Segurança Cibernética em cada caso. Sobre a possibilidade de realização de estudo de caso com base na observação e na explicação de mecanismos causais, Rezende (2011) argumenta que:

> Quando compreendida a partir dos mecanismos causais, a análise comparada deve se voltar para compreender como estes operam, abrindo diversas possibilidades pelas quais variáveis independentes se articulam e produzem o comportamento da variável dependente, em um conjunto específico de condições. Num sentido mais amplo, as explicações causais nas ciências sociais (e na ciência política) podem apenas ocorrer quando os analistas conferem substancial atenção aos processos de interação entre mecanismos causais e o contexto específico em que elas ocorrem. É exatamente pelo fato de se considerar a dependência do contexto combinada à coexistência de múltiplos processos causais operando sobre as mesmas variáveis, em diferentes contextos, que torna rica a necessidade de mergulhar com maior intensidade nas análises por mecanismos. Longe de buscar generalizações, os cientistas políticos devem estar voltados para construir teorias de médio alcance e penetrar de forma mais aguda nos mecanismos específicos que produzem fenômenos de interesse ao pesquisador (REZENDE, 2011, p. 326).

Dessa maneira, o estudo do caso brasileiro intenciona analisar em profundidade como as condições securitização, despesas militares, ocorrência de eventos raros, tempo do marco jurídico-institucional, militarização do espaço cibernético e desenvolvimento se configuram no contexto do Brasil, com base em uma abordagem a partir da identificação dos mecanismos causais.

3.1.4 Métodos Mistos

O desenho de pesquisa que estrutura este estudo integra a Análise Qualitativa Comparativa do comprometimento com a Segurança Cibernética nos países do continente americano à realização de um estudo de como o caso brasileiro pode ser explicado a partir da identificação dos mecanismos causais no seu contexto. Essencialmente, então, esta pesquisa integra uma minoria de trabalhos que utilizam métodos mistos em Ciência Política e Relações Internacionais (MEDEIROS et al., 2016; SOARES, 2005; BARBERIA; DE GODOY; BARBOZA, 2014; FIGUEIREDO FILHO et al., 2021).

Derivam desse fato algumas dificuldades centrais do fazer científico nesse contexto, sendo uma delas a escassez - com a exceção de alguns estudos, principalmente de autores como Dalson Britto Figueiredo Filho e Ranulfo Paranhos - de trabalhos introdutórios sobre aplicações práticas de estudos com metodologia mista, restando aos pesquisadores brasileiros a utilização dos manuais tradicionais e artigos internacionais, sendo esta a solução encontrada para esta pesquisa.

Em *Nested Analysis as a Mixed-Method Strategy for Comparative Research*, Lieberman argumenta em favor de uma abordagem resultante da combinação de análises *large-N* e *small-N*, de forma a oferecer uma alternativa sistemática para o Método Comparativo. Além disso, ele pondera que a Análise Qualitativa Comparativa pode ser uma substituta adequada das tradicionais análises de regressão na etapa LNA, ou *large-N analysis* (LIEBERMAN, 2005, p. 437).

Paralelamente, Small (2011), através de uma análise da literatura recente sobre métodos mistos e as suas aplicações, classifica os estudos a partir de dois tipos de combinação entre as lógicas quantitativa e qualitativa, participando esta pesquisa da categoria de *mixed data-collection studies,* uma vez que coleta e sistematiza tanto dados qualitativos como quantitativos. Além disso, o caráter metodologicamente misto não consiste apenas na sua coleta de dados, mas também na análise deles, já que são utilizadas duas técnicas diferentes, mesmo que dentro de uma só cultura - a qualitativa. Nesse ínterim, Creswell (2009) argumenta que a:

> Integration of the two types of data might occur at several stages I the process of research: the data collection, the data analysis, interpretation, or some combination of places. Integration means that the researcher "mixes" the data. For example, in data collection, this "mixing" might involve combining open-ended questions on a survey with closed-ended questions on the survey. Mixing at the stage of data analysis and interpretation might involve transforming qualitative themes or codes into quantitative numbers and comparing that information with quantitative results in an "interpretation" section of a study. The place in the process for integration seems related to whether phases (a sequence) or a single phase (concurrent) of data collection occurs (CRESWELL, 2009, p. 243).

Paranhos et al. (2016) argumentam sobre a utilidade dos métodos mistos, no que tange às suas possibilidades: 1 - confirmatória; e 2 - de complementaridade. Enquanto na primeira o objetivo é inserir cada vez mais informações e análises a partir de diversas técnicas, com o objetivo de robustecer e confirmar os resultados encontrados, na segunda a ideia é de promover o balanceamento do desenho de pesquisa, ponderando os pontos fortes e os pontos fracos de técnicas diferentes e assimilando as vantagens delas, de maneira que o desenho resultante suplanta desvantagens e potencializa as qualidades.

A partir desse parâmetro, nesta pesquisa, a Análise Qualitativa Comparativa do nível de comprometimento com a Segurança Cibernética nos países do continente americano, associada ao estudo do caso brasileiro, pode ser considerada como um exemplo do que Small denomina como análise integrativa, que ocorre quando "duas ou mais abordagens analíticas ou técnicas diferentes são mescladas em um só estudo" (SMALL, 2011, p.76, tradução livre).

Portanto, a ideia deste estudo é de complementaridade entre métodos, de forma que a vinculação da Análise Qualitativa Comparativa ao estudo do caso brasileiro proporciona o balanceamento entre as técnicas e a preservação da maior quantidade de informações possível, além de representar uma aplicação prática das teorias mobilizadas a um determinado contexto.

4 ANÁLISE QUALITATIVA COMPARATIVA DOS PAÍSES AMERICANOS

4.1 OS PAÍSES AMERICANOS E A SEGURANÇA CIBERNÉTICA: UMA ANÁLISE DESCRITIVA

Nesta seção, apresentaremos, inicialmente, um prospecto descritivo dos principais resultados sobre a categorização dos países do continente americano em relação às condições mobilizadas na pesquisa e ao fenômeno observado, que é o comprometimento com a Segurança Cibernética, avaliado pelo GCI (ITU, 2019). Como mencionado nos capítulos anteriores, considerando o caráter *case oriented* - "*QCA should fundamentally be considered as case oriented, rather than as some middle way between caseoriented and variable-oriented analysis*" (RIHOUX; LOBE, 2009, p. 222) -, fez-se mister o estabelecimento de alguns critérios para a preservação da riqueza informacional sobre os países e as condições explicativas.

Sobre a securitização os valores atribuídos aos países, segundo a classificação do *Cyber Policy Portal* (UNIDIR, 2021) e a análise documental, foram: 0 - não possui estratégia nacional sobre Segurança Cibernética; 1 - não possui estratégia nacional sobre Segurança Cibernética, mas está desenvolvendo; 2 - possui estratégia nacional sobre Segurança Cibernética.

Em relação ao Tempo do Marco Jurídico-Institucional, dividimos os Estados a partir destas classificações: 0) não possui legislação; 1) a legislação tem entre 1 e 15 anos de marco jurídico-institucional; 2) o marco possui 16 anos ou mais desde o marco jurídico-institucional.

Levando em consideração a Ocorrência de Eventos Raros, cada caso foi avaliado de acordo com as seguintes dimensões: 0 - Ausência de eventos raros no país; 1 - Presença de pelo menos um evento de alta significância no país; 2 - Mais de dois eventos raros de alta significância no Estado.

Paralelamente, a classificação dos países de acordo com as suas Despesas Militares ocorre desta forma: 0) N/A e < 1%; 1) 1% < X < 2%; 2) > 2%. Assim, os *missing case* e os países com despesas militares abaixo de 1% do PIB integram a primeira categoria (0). Em seguida, estão relacionados os países que possuem despesas militares entre 1% e 2% do PIB. Por último (2), estão representados os países com despesas militares acima de 2% do PIB.

De acordo com o PNUD (2019), os valores do IDH são diferenciados a partir dos graus: 1) Muito Elevado (igual ou superior a 0,800); 2) Elevado (Entre 0,700 e 0,799); 3) Médio (Entre 0,550 e 0,699); e 4) Baixo (inferior a 0,550). Para a pesquisa, consideramos as

classes “Baixo” e “Médio” como uma só categoria. Assim, chegamos a estes resultados: 0 - baixo ou médio IDH; 1 - IDH elevado; 2 - IDH muito elevado.

Em termos de Militarização do Setor Cibernético, os valores atribuídos aos países, segundo a classificação da UNIDIR e a análise documental, foram: 0 - não possui um setor cibernético militarizado, ou seja, a agência responsável pelo setor não é de caráter militar; 1 - o setor cibernético do país é militarizado, estando sob responsabilidade institucional de agência sob a supervisão dos militares. Em seguida, na Tabela 3, identificamos como cada um dos casos pode ser classificado de acordo com as condições mobilizadas neste estudo e em observância das regras acima.

Tabela 3 - Categorização dos Países das Américas em relação às Condições Explicativas.[17]

PAÍS	SECU.	DESP.	EVEN.	TEMP.	MILI.	DESE.	GCI
Estados Unidos	**2**	**2**	**2**	**2**	**0**	**2**	**1**
Canadá	**2**	**1**	**2**	**2**	**0**	**2**	**1**
Uruguai	**0**	**1**	**0**	**1**	**0**	**2**	**1**
México	**2**	**0**	**0**	**1**	**0**	**1**	**1**
Paraguai	**2**	**0**	**0**	**2**	**0**	**1**	**1**
Brasil	**1**	**1**	**1**	**1**	**1**	**1**	**1**
Colômbia	**2**	**2**	**0**	**1**	**1**	**1**	**1**
Cuba	**0**	**2**	**0**	**1**	**0**	**1**	**1**
Chile	**2**	**1**	**1**	**2**	**0**	**2**	**1**
República Dominicana	**2**	**0**	**0**	**1**	**0**	**1**	**0**
Jamaica	**2**	**1**	**0**	**1**	**0**	**1**	**0**
Argentina	**1**	**0**	**0**	**1**	**0**	**2**	**0**
Peru	**1**	**1**	**0**	**1**	**0**	**1**	**0**
Panamá	**2**	**0**	**0**	**1**	**0**	**1**	**0**
Equador	**1**	**2**	**0**	**2**	**0**	**1**	**0**

[17] Os dados desagregados e mais detalhados estão disponíveis nos Apêndices.

Venezuela	**0**	**0**	**0**	**2**	**0**	**1**	**0**
Guatemala	**2**	**0**	**0**	**2**	**0**	**0**	**0**
Antígua e Barbuda	**0**	**0**	**0**	**1**	**0**	**1**	**0**
Costa Rica	**2**	**0**	**0**	**2**	**0**	**1**	**0**
Trindade e Tobago	**2**	**0**	**0**	**0**	**0**	**1**	**0**
Barbados	**1**	**0**	**0**	**1**	**0**	**2**	**0**
São Vicente e Granadinas	**0**	**0**	**0**	**1**	**0**	**1**	**0**
Bahamas	**1**	**0**	**0**	**0**	**1**	**2**	**0**
Granada	**0**	**0**	**0**	**1**	**0**	**2**	**0**
Bolívia	**0**	**1**	**0**	**1**	**0**	**1**	**0**
Guiana	**1**	**1**	**0**	**0**	**0**	**0**	**0**
Nicarágua	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Belize	**1**	**1**	**0**	**2**	**0**	**1**	**0**
El Salvador	**0**	**1**	**0**	**1**	**0**	**0**	**0**
Suriname	**1**	**0**	**0**	**1**	**0**	**1**	**0**
Santa Lúcia	**0**	**0**	**0**	**1**	**0**	**1**	**0**
São Cristóvão e Névis	**0**	**0**	**0**	**1**	**0**	**1**	**0**
Haiti	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Honduras	**0**	**1**	**0**	**1**	**0**	**0**	**0**
Dominica	**0**	**0**	**0**	**0**	**0**	**1**	**0**

Fonte: elaboração do autor, a partir do banco de dados da pesquisa.

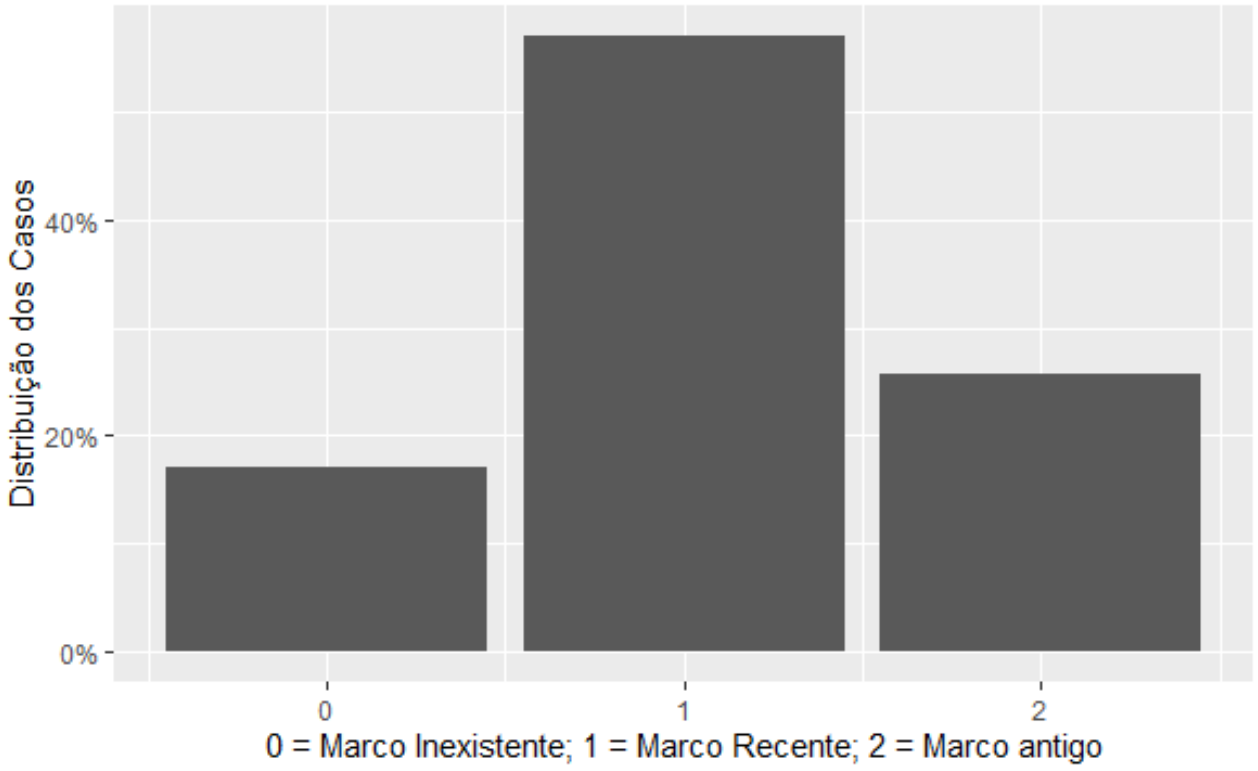
4.1.1 Tempo do Marco Jurídico-Institucional

Como evidenciado na Tabela 3 e ilustrado abaixo, no Gráfico 3, a maioria (>50%) dos países americanos possui uma legislação com marco jurídico-institucional recente, ou seja, com no máximo 15 anos de existência. Por conseguinte, cerca de 25% dos casos apresenta um marco antigo, tendo um maior nível de maturidade institucional.

Os casos menos frequentes, com quase 20% de abrangência, são os Estados que não possuem legislação significativa que possa constituir um marco jurídico-institucional em Segurança Cibernética.

O marco mais antigo está circunscrito no *Penal Code* da Guatemala, datado de 1973, enquanto o marco mais recente é o de Honduras, também originado no *Penal Code* do Estado, só que datado de 2017.

Gráfico 3 - Tempo do Marco Jurídico-Institucional: distribuição dos casos.



Fonte: Elaboração do autor com base nos dados da pesquisa.

Nesse sentido, os países das Américas distribuem-se dessa forma, de acordo com os conjuntos estipulados:

(0) Marco Inexistente: Bahamas, Dominica, Guiana, Haiti, Nicarágua, Trindade e Tobago.

(1) Marco Recente: Antígua e Barbuda, Argentina, Barbados, Bolívia, Brasil, Colômbia, Cuba, El Salvador, Granada, Honduras, Jamaica, México, Panamá, Peru, República Dominicana, São Cristóvão e Névis, Santa Lúcia, São Vicente e Granadinas, Suriname, Uruguai.

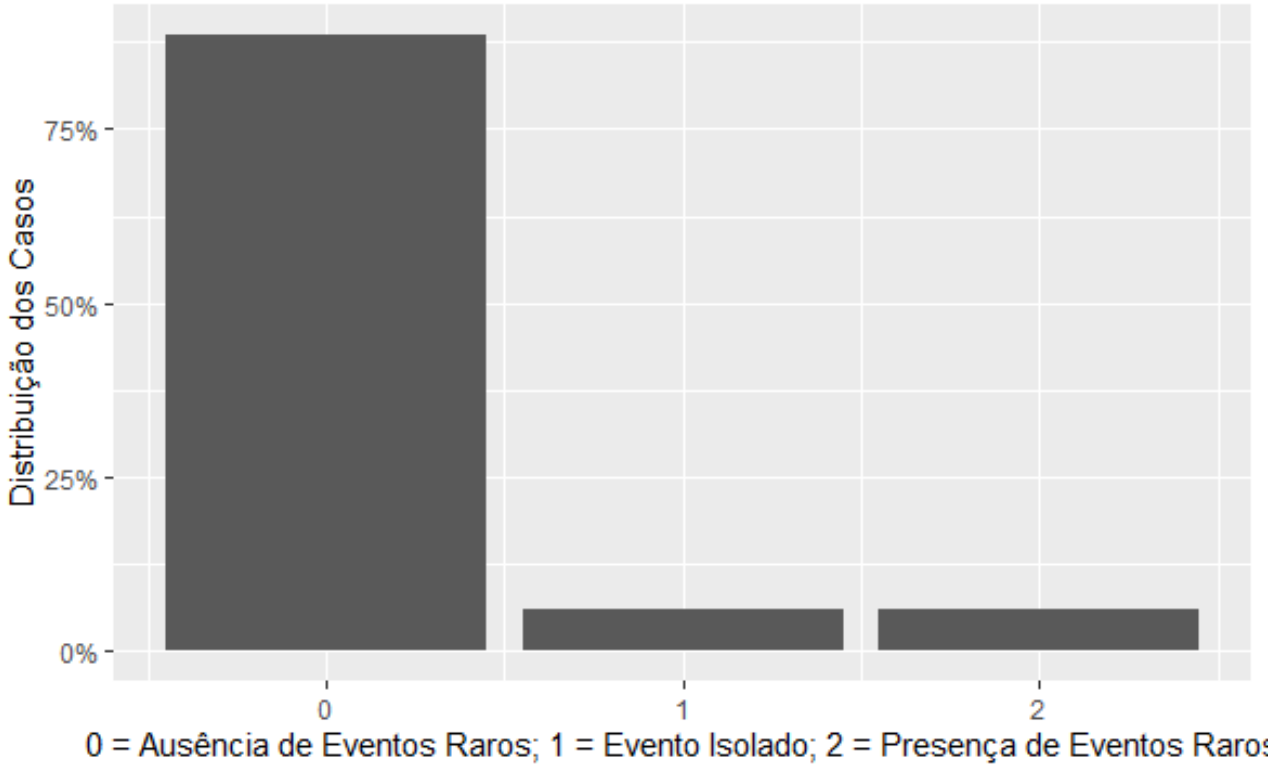
(2) Marco Antigo: Belize, Canadá, Chile, Costa Rica, Equador, Estados Unidos da América, Guatemala, Paraguai, Venezuela.

4.1.2 Ocorrência de Eventos Raros

A ocorrência de eventos raros foi uma das condições com maior quantidade de *missing cases*, devido também à raridade da existência desses tipos de eventos, que são caracterizados pelos seus altíssimos significância e impacto. Mais detalhadamente, em cerca de 90% dos países, os eventos altamente significativos foram considerados como ausentes.

Em torno de 6% dos casos, observamos a ocorrência de evento isolado, mas com altíssimo impacto. Igualmente em 6% dos Estados, foram identificados múltiplos eventos raros. O Gráfico 4 a seguir sistematiza essas informações. Dentre os casos positivos para a ocorrência desses fenômenos, ressaltamos os Estados Unidos, que foram palco de mais de setenta eventos de altíssima significância. Em seguida, deve-se mencionar o Canadá, que registrou a existência de quatro desses acontecimentos.

Gráfico 4 - Ocorrência de Eventos Raros: distribuição dos casos.



Fonte: Elaboração do autor com base nos dados da pesquisa.

A partir do Gráfico 4 e dos dados da pesquisa, sistematizamos os casos a partir das seguintes dimensões:

(0) Ausência de Eventos Raros: Antígua e Barbuda, Argentina, Bahamas, Barbados, Belize, Bolívia, Colômbia, Costa Rica, Cuba, Dominica, El Salvador, Equador, Granada, Guatemala, Guiana, Haiti, Honduras, Jamaica, México, Nicarágua, Panamá, Paraguai, Peru, República Dominicana, São Cristóvão e Névis, Santa Lúcia, São Vicente e Granadinas, Suriname, Trindade e Tobago, Uruguai, Venezuela.

(1) Evento Isolado: Brasil, Chile.

(2) Múltiplos Eventos: Canadá, Estados Unidos da América.

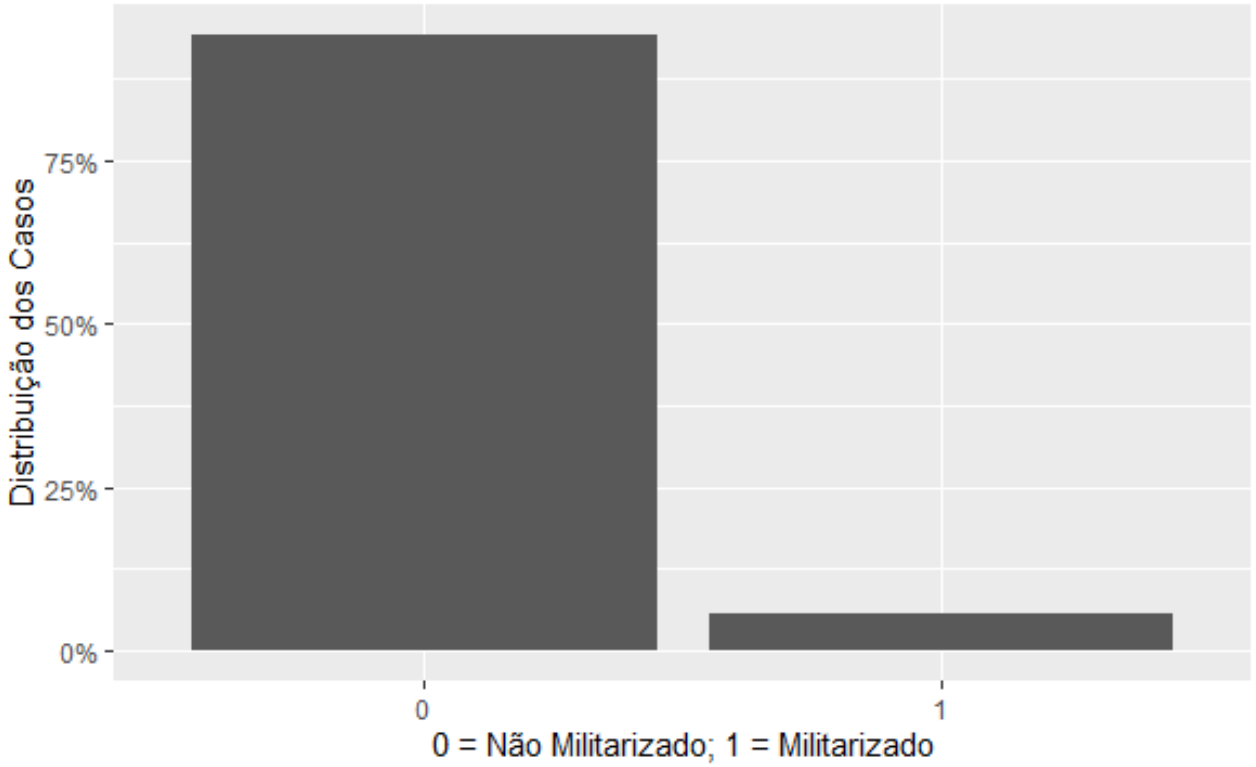
4.1.3 Militarização da Segurança Cibernética

A condição Militarização, referente ao setor cibernético, foi a única que apresentou mais dados em negativa do que a condição Ocorrência de Eventos Raros, apresentando apenas 6% de casos em que havia um setor cibernético militarizado (Brasil e Colômbia), enquanto em torno de 94% dos países possuem um setor cibernético não militarizado, estruturado a

partir da direção de uma agência ligada a setores civis do Estado. Diferente das outras condições mobilizadas na pesquisa, a Militarização da Segurança Cibernética apresenta uma categorização dicotômica pautada, principalmente, na origem da instituição responsável pelo setor cibernético.

No Gráfico 5, em seguida, está representada a distribuição desses países de acordo com as suas classificações em termos de Militarização da Segurança Cibernética.

Gráfico 5 - Militarização: distribuição dos casos.



Fonte: Elaboração do autor com base nos dados da pesquisa.

De maneira complementar ao exposto no Gráfico 5, elencamos, abaixo, quais são os países classificados de acordo com essa condição. Dentre eles, vale ressaltar o Brasil, que foi escolhido para o estudo de caso realizado nesta pesquisa e que integra um dos possíveis caminhos causais para o comprometimento com a Segurança Cibernética, que serão apresentados no próximo capítulo.

(0) Setor Cibernético não militarizado: Antígua e Barbuda, Argentina, Bahamas, Barbados, Belize, Bolívia, Canadá, Chile, Costa Rica, Cuba, Dominica, El Salvador, Equador, Estados Unidos da América, Granada, Guatemala, Guiana, Haiti, Honduras, Jamaica, México, Nicarágua, Panamá, Paraguai, Peru, República Dominicana, São Cristóvão e Névis, Santa Lúcia, São Vicente e Granadinas, Suriname, Trindade e Tobago, Uruguai, Venezuela.

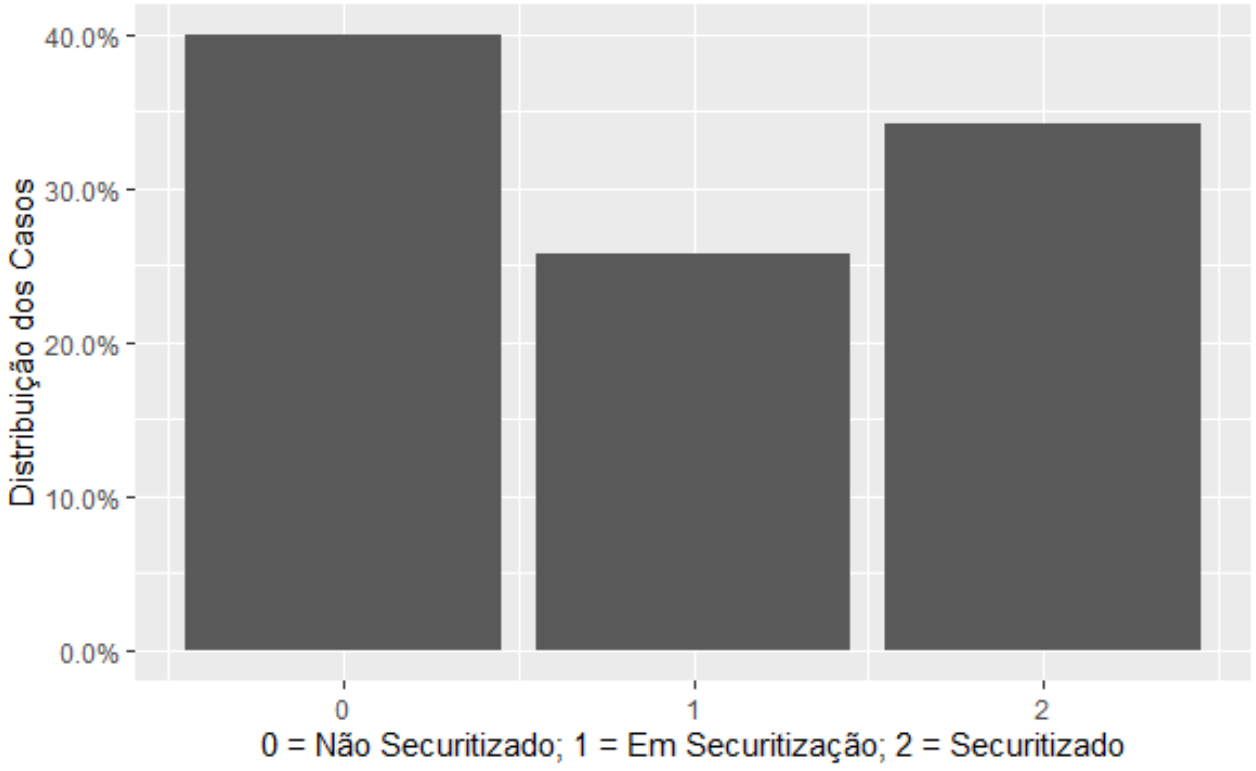
(1) Setor Cibernético Militarizado: Brasil, Colômbia.

Nesse aspecto, o Brasil e a Colômbia são dois casos especiais. O Brasil tem o seu setor cibernético associado ao Comando de Defesa Cibernética (COMDCIBER), enquanto a Colômbia atribui essa seara para o *Comando Conjunto Cibernético*. Mesmo a área de Segurança Cibernética tendo sido originada com base em uma discussão majoritariamente sobre Defesa Cibernética, o que observamos é que a imensa maioria dos países não submete os seus setores cibernéticos a uma instituição militar.

4.1.4 Securitização da Segurança Cibernética

Para mensurar a Securitização, utilizamos como objeto central as Estratégias Nacionais de Segurança Cibernética dos países do continente americano, sob o argumento de que esses documentos representam uma materialização do Estado como ator securitizador, implicando também em políticas públicas inerentes ao tema. Nesse sentido, podemos observar que em torno de 35% dos casos estão representados na categoria Securitizado (2), enquanto cerca de 25% está em processo de securitização, com Estratégias Nacionais na área ainda em desenvolvimento (1) (tendo o ano de 2018 como referência). Os Estados desprovidos desses documentos, por outro lado, constituem por volta de 40% da população. No Gráfico 6, apresentamos esses dados.

Gráfico 6 - Securitização: distribuição dos casos.



Fonte: Elaboração do autor com base nos dados da pesquisa.

Levando em consideração as categorias atribuídas na pesquisa, apresentamos, a seguir, a distribuição de cada país de acordo com a tipologia desenvolvida:

(0) Não Securitizado: Antígua e Barbuda, Bolívia, Cuba, Dominica, El Salvador, Granada, Haiti, Honduras, Nicarágua, São Cristóvão e Névis, Santa Lúcia, São Vicente e Granadinas, Uruguai, Venezuela.

(1) Em Securitização: Argentina, Bahamas, Barbados, Belize, Brasil, Equador, Guiana, Peru, Suriname.

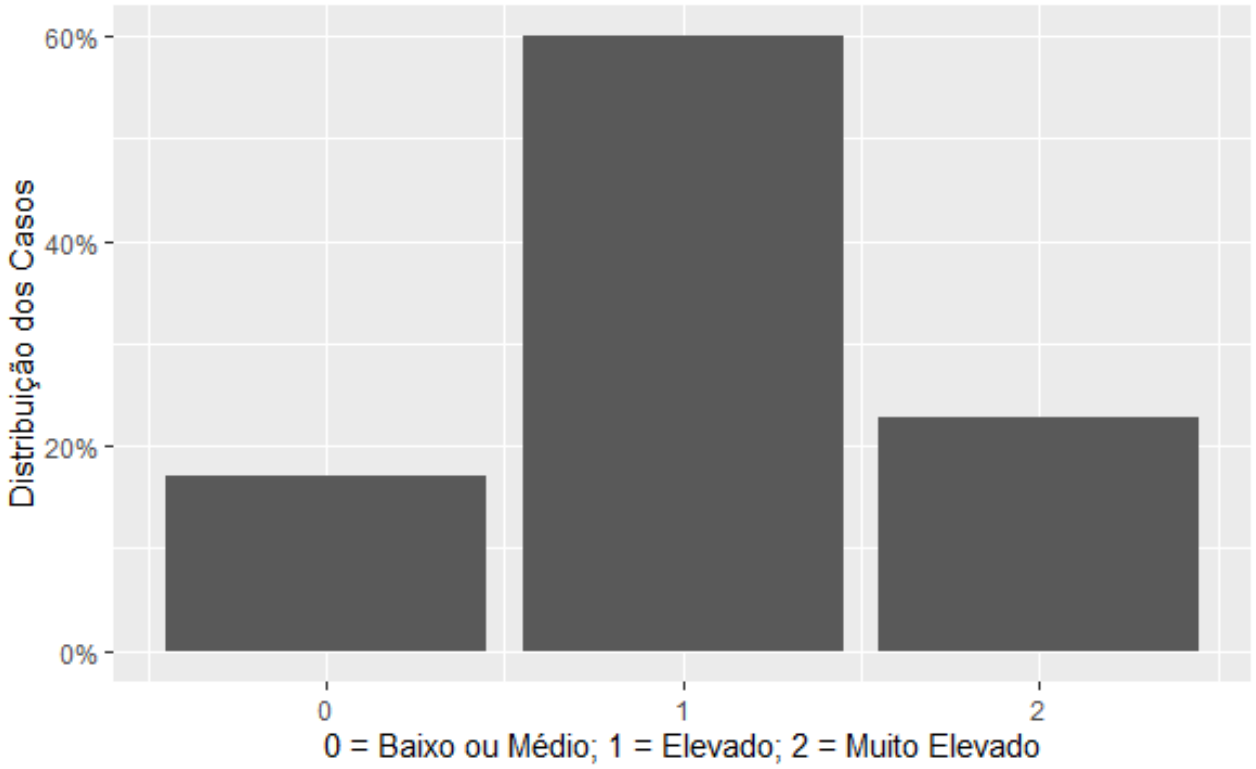
(2) Securitizado: Canadá, Chile, Colômbia, Costa Rica, Estados Unidos da América, Guatemala, Jamaica, México, Panamá, Paraguai, República Dominicana, Trindade e Tobago.

4.1.5 Desenvolvimento Econômico

O Desenvolvimento Econômico, neste estudo, é avaliado a partir do Índice de Desenvolvimento Humano. Nesse âmbito, os países americanos, em sua maioria (60%), estão abrangidos pela categoria referente ao IDH elevado (1). A segunda classe (2) com maior

quantidade de casos (cerca de 23%) agrega os países com IDH considerado muito elevado. Por último, na classificação (0) de IDH baixo ou médio, estão inseridos em torno de 17% dos Estados do continente americano. Em toda a população, apenas um país foi considerado como tendo IDH baixo (Haiti). Em seguida, no Gráfico 7, estão representadas essas informações.

Gráfico 7 - Índice de Desenvolvimento Humano: distribuição dos casos.



Fonte: Elaboração do autor com base nos dados da pesquisa.

Os dados ilustrados no gráfico acima correspondem a seguinte distribuição dos países, em termos de Índice de Desenvolvimento Humano:

(0) IDH Baixo ou Médio: El Salvador, Guatemala, Guiana, Haiti, Honduras, Nicarágua.

(1) IDH Elevado: Antígua e Barbuda, Belize, Bolívia, Brasil, Colômbia, Costa Rica, Cuba, Dominica, Equador, Granada, Jamaica, México, Panamá, Paraguai, Peru, República Dominicana, São Cristóvão e Névis, Santa Lúcia, São Vicente e Granadinas, Suriname, Trindade e Tobago, Venezuela.

(2) IDH Muito Elevado : Argentina, Bahamas, Barbados, Canadá, Chile, Estados Unidos da América, Uruguai.

4.1.6 Despesas Militares

Como apresentado nos capítulos anteriores, intencionando avaliar a condição Despesas Militares, utilizamos o Índice de Despesas Militares, proporcionado pelo Banco Mundial (2020). A partir dessa medida, classificamos os casos, obtendo os seguintes resultados:

1 - Cerca de 60% dos países utilizaram menos de 1% do PIB com despesas militares ou não declararam os seus gastos nesse aspecto;

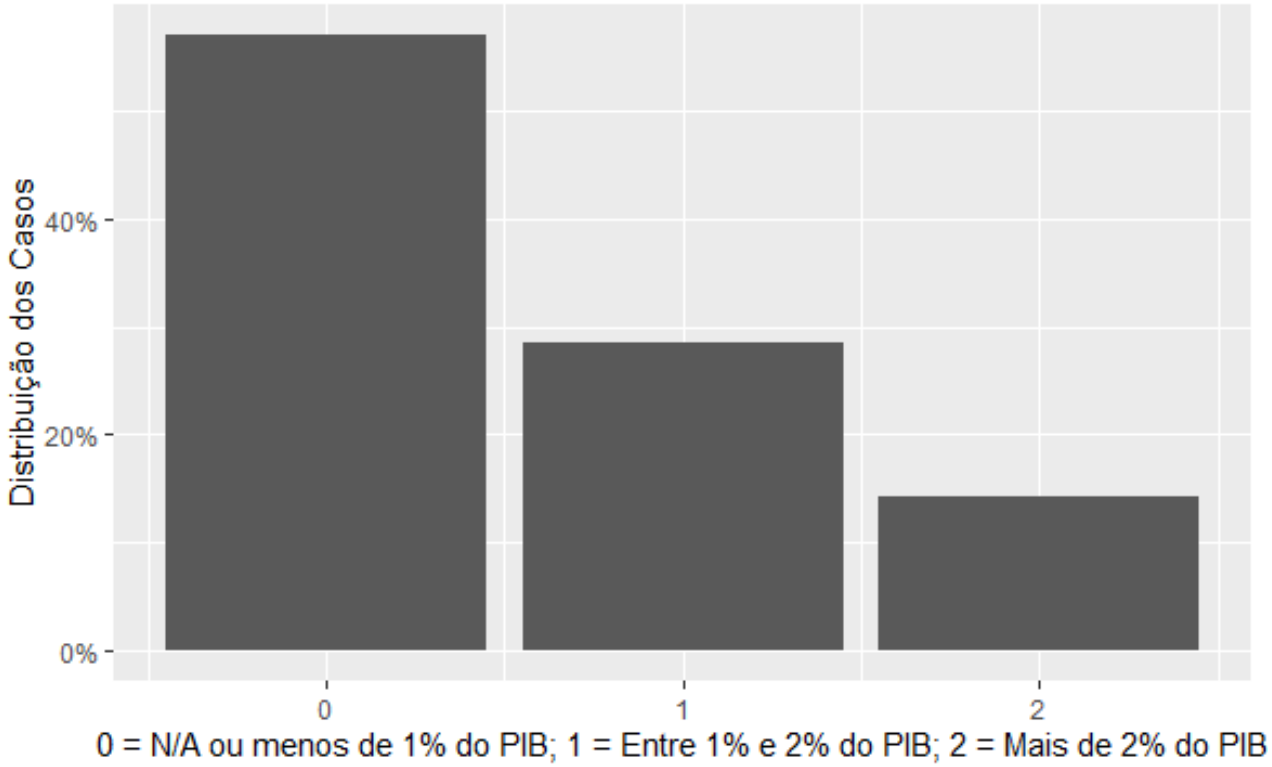
2 - Dos Estados do continente americano, pelo menos 29% tiveram entre 1% e 2% do seu PIB destinado às despesas militares;

3 - Apenas 14% dos casos apresentaram despesas militares acima de 2% do PIB do Estado.

Dentre esses países, a Costa Rica figura no extremo inferior, apresentando 0% de Despesas Militares em relação ao seu PIB. No extremo superior, observamos os Estados Unidos, que destinam cerca de 3,32% do PIB a Despesas Militares.

No Gráfico 8, abaixo, podemos conferir essas informações. Em seguida, serão apresentadas as classificações dos países - caso a caso - em relação a essa condição, agrupando-os em suas devidas dimensões.

Gráfico 8 - Despesas Militares: distribuição dos casos.



Fonte: Elaboração do autor com base nos dados da pesquisa.

(0) Índice de Despesas Militares Baixo ou N/A: Antígua e Barbuda, Argentina, Bahamas, Barbados, Costa Rica, Dominica, Granada, Guatemala, Haiti, México, Nicarágua, Panamá, Paraguai, República Dominicana, São Cristóvão e Névis, Santa Lúcia, São Vicente e Granadinas, Suriname, Trindade e Tobago, Venezuela.

(1) Índice de Despesas Militares Médio: Belize, Bolívia, Brasil, Canadá, Chile, El Salvador, Guiana, Honduras, Jamaica, Peru.

(2) Índice de Despesas Militares Alto: Colômbia, Cuba, Equador, Estados Unidos da América, Uruguai.

4.2 ANÁLISE QUALITATIVA COMPARATIVA DA SEGURANÇA CIBERNÉTICA NAS AMÉRICAS

O modelo da pesquisa, analisado a partir da QCA, permitiu a identificação dos conjuntos - ou caminhos - causais para o comprometimento com a Segurança Cibernética no continente americano. Além dos valores apresentados no subcapítulo anterior, foi necessário

assumir como ponto de corte a pontuação 0,450 no GCI (ITU, 2019) para a consideração do que vem a ser um "maior comprometimento com a Segurança Cibernética". De acordo com essa fronteira, chegamos a nove casos caracterizados de acordo com essa observação: Estados Unidos, Canadá, Uruguai, México, Paraguai, Brasil, Colômbia, Cuba e Chile.

Em observância do protocolo da Análise Qualitativa Comparativa, apresentamos, primeiramente, os resultados iniciais da *truth-table*, ou tabela-verdade, na Tabela 4.

Tabela 4 - Tabela-Verdade da Análise Qualitativa Comparativa.

ID	SEC	DESP	EVE	TEM	MIL	DESE	GCI	CASOS	CON[18]
(1)	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**Nicarágua e Haiti**	**–**
(2)	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**Dominica**	**–**
(3)	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**Antígua e Barbuda, São Vicente e Granadinas, Santa Lúcia, São Cristóvão e Névis**	**–**
(4)	**0**	**0**	**0**	**1**	**0**	**2**	**0**	**Granada**	**–**
(5)	**0**	**0**	**0**	**2**	**0**	**1**	**0**	**Venezuela**	**–**
(6)	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**El Salvador e Honduras**	**–**
(7)	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**Bolívia**	**–**
(8)	**0**	**1**	**0**	**1**	**0**	**2**	**1**	**Uruguai**	**1**
(9)	**0**	**2**	**0**	**1**	**0**	**1**	**1**	**Cuba**	**1**
(10)	**1**	**0**	**0**	**0**	**1**	**2**	**0**	**Bahamas**	**–**
(11)	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**Suriname**	**–**
(12)	**1**	**0**	**0**	**1**	**0**	**2**	**0**	**Argentina e Barbados**	**–**
(13)	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**Guiana**	**–**
(14)	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**Peru**	**–**
(15)	**1**	**1**	**0**	**2**	**0**	**1**	**0**	**Belize**	**–**

[18] Consistência.

(16)	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**Brasil**	**1**
(17)	**1**	**2**	**0**	**2**	**0**	**1**	**0**	**Equador**	**–**
(18)	**2**	**0**	**0**	**0**	**0**	**1**	**0**	**Trindade e Tobago**	**–**
(19)	**2**	**0**	**0**	**1**	**0**	**1**	**C[19]**	**México(1), República Dominicana(0)e Panamá(0)**	**0,33**
(20)	**2**	**0**	**0**	**2**	**0**	**0**	**0**	**Guatemala**	**–**
(21)	**2**	**0**	**0**	**2**	**0**	**1**	**C[20]**	**Paraguai(1) e Costa Rica(0)**	**0,5**
(22)	**2**	**1**	**0**	**1**	**0**	**1**	**0**	**Jamaica**	**–**
(23)	**2**	**1**	**1**	**2**	**0**	**2**	**1**	**Chile**	**1**
(24)	**2**	**1**	**2**	**2**	**0**	**2**	**1**	**Canadá**	**1**
(25)	**2**	**2**	**0**	**1**	**1**	**1**	**1**	**Colômbia**	**1**
(26)	**2**	**2**	**2**	**2**	**0**	**2**	**1**	**Estados Unidos**	**1**

Fonte: Elaboração do autor, utilizando o *Tosmana*, a partir do banco de dados da pesquisa.

Analisando a Tabela 4, simplificamos os resultados encontrados, que têm boa parte de combinações que não geram o maior comprometimento com a Segurança Cibernética. Também eliminamos as contradições, ou seja, as combinações que não geram resultados consistentes: a - Paraguai (1) e Costa Rica (0); b - México (1), República Dominicana (0) e Panamá (0). De uma forma geral, as contradições indicam que a referida conjuntura causal não necessariamente é o contexto decisivo para que seja alcançado o comprometimento com a Segurança Cibernética, uma vez que nem todos os países abrangidos por essas categorias atingem o resultado esperado.

A Tabela 5 sistematiza os resultados positivos, descartadas as contradições, as negativas e os remanescentes lógicos.

[19] C = Contradição.
[20] C = Contradição.

Tabela 5 - Casos Positivos da Tabela-Verdade.

ID	SEC	DESP	EVE	TEM	MIL	DESE	GCI	CASOS
(8)	**0**	**1**	**0**	**1**	**0**	**2**	**1**	**Uruguai**
(9)	**0**	**2**	**0**	**1**	**0**	**1**	**1**	**Cuba**
(16)	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**Brasil**
(23)	**2**	**1**	**1**	**2**	**0**	**2**	**1**	**Chile**
(24)	**2**	**1**	**2**	**2**	**0**	**2**	**1**	**Canadá**
(25)	**2**	**2**	**0**	**1**	**1**	**1**	**1**	**Colômbia**
(26)	**2**	**2**	**2**	**2**	**0**	**2**	**1**	**Estados Unidos**

Fonte: elaboração do autor, utilizando o *Tosmana*, a partir do banco de dados da pesquisa.

A partir da Tabela 5, podemos identificar as combinações de condições e contextos apresentados abaixo:

(8) Uruguai: setor não securitizado (0); índice de despesas militares médio (1); ausência de eventos raros (0); marco temporal recente (1); setor cibernético não militarizado (0); IDH muito elevado (2).

(9) Cuba: setor não securitizado (0); índice de despesas militares alto (2); ausência de eventos raros (0); marco temporal recente (1); setor cibernético não militarizado (0); IDH elevado (1).

(16) Brasil: setor em securitização (1); índice de despesas militares médio (1); evento raro isolado (1); marco temporal recente (1); setor cibernético militarizado (1); IDH elevado (1).

(23) Chile: setor securitizado (2); índice de despesas militares médio (1); evento raro isolado (1); marco temporal antigo (2); setor cibernético não militarizado (0); IDH muito elevado (2).

(24) Canadá: setor securitizado (2); índice de despesas militares médio (1); múltiplos eventos raros (2); marco temporal antigo (2); setor cibernético não militarizado (0); IDH muito elevado (2).

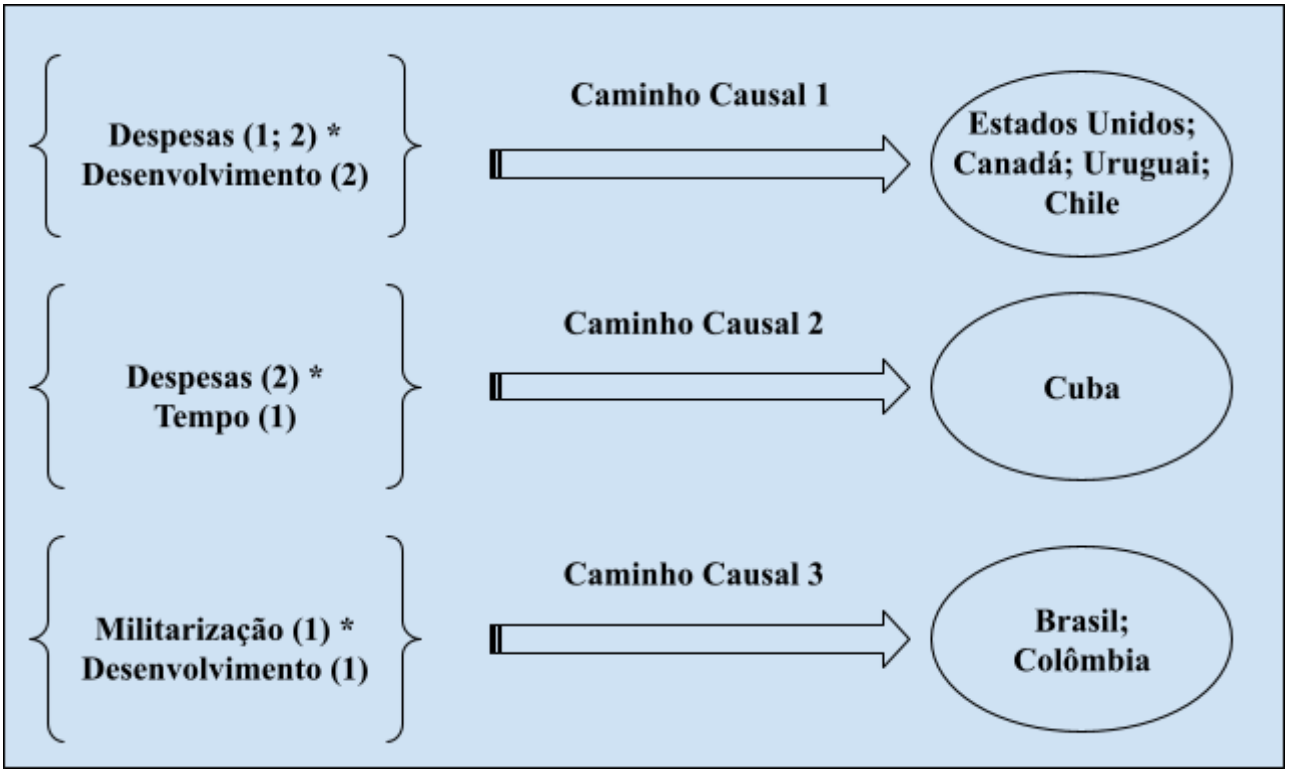
(25) Colômbia: setor securitizado (2); índice de despesas militares alto (2); ausência de eventos raros (0); marco temporal recente (1); setor cibernético militarizado (1); IDH elevado (1).

(26) Estados Unidos: setor securitizado (2); índice de despesas militares alto (2); múltiplos

eventos raros (2); marco temporal antigo (1); setor cibernético não militarizado (0); IDH muito elevado (2).

Por conseguinte, realizamos a minimização lógica, que tem o intuito de determinar, utilizando uma redução seguindo a lógica booleana, quais são as soluções com maior cobertura dos casos e mais parcimoniosas (RAGIN, 1987). Dessa forma, obtivemos as seguintes soluções ilustradas na Figura 13:

Figura 13 - Resultados da Análise Qualitativa Comparativa: caminhos causais.



Fonte: Elaboração do autor a partir dos dados da pesquisa.

Como evidenciado na Figura 13, três foram as soluções para o comprometimento com a Segurança Cibernética nos países americanos, cobrindo um total de 7 dos 9 casos afirmativos (2 deles incorreram em contradições). Dentre eles, 4 são da América do Sul - Brasil, Chile, Colômbia e Uruguai -, 2 da América do Norte - Estados Unidos e Canadá - e 1 da América Central - Cuba.

4.2.1 Caminho Causal 1: Estados Unidos, Canadá, Chile e Uruguai

A primeira categoria, denominada genericamente como **Caminho Causal 1**, foi a que abrangeu a maior quantidade de casos - cobrindo as configurações (8), (23), (24) e (26). Os países nela incluídos (Estados Unidos, Canadá, Uruguai e Chile) tiveram a sua pontuação no

GCI determinada, principalmente, pelas despesas militares superiores a 1% do PIB e pelo IDH muito elevado.

Dessa maneira, identificamos que as condições Despesas Militares e Desenvolvimento Econômico constituem condições **INUS**, ou seja, "***I**nsufficient but **N**ecessary part of a condition which is itself **U**nnecessary but **S**ufficient for the result"* (MACKIE, 1965, p. 245). Nesse sentido, as duas não são suficientes, mas são necessárias quando incluídas em uma conjuntura causal suficiente para a explicação do comprometimento com a Segurança Cibernética nos Estados Unidos, no Canadá, no Chile e no Uruguai. Houve casos, por exemplo, em que uma condição estava presente mas a outra estava ausente (e.g., Argentina, Barbados e Guiana) e o *outcome*, comprometimento com a Segurança Cibernética, não ocorria.

Nesse ínterim, essa conjuntura explicativa também confirma as hipóteses **H1.2** e **H1.6** da pesquisa, de que, respectivamente as Despesas Militares e o Desenvolvimento Econômico são condições necessárias e/ou suficientes para explicar o comprometimento com a Segurança Cibernética nos países do continente americano. Em seguida, apresentaremos algumas informações sobre esses Estados.

Quadro 14 - Contextos dos países do Caminho Causal 1.

PAÍS	SEC	DESP	EVE	TEM	MIL	DESE
EUA	Securitizado	Índice Alto	Múltiplos Eventos	Marco Antigo	Não Militarizado	Índice Muito Elevado
CAN	Securitizado	Índice Médio	Múltiplos Eventos	Marco Antigo	Não Militarizado	Índice Muito Elevado
CHI	Securitizado	Índice Médio	Evento Isolado	Marco Antigo	Não Militarizado	Índice Muito Elevado
URU	Não Securitizado	Índice Médio	Ausência de Evento	Marco Recente	Não Militarizado	Índice Muito Elevado

Fonte: Elaboração do autor a partir dos dados da pesquisa.

4.2.1.1 Estados Unidos

Localizados na América do Norte, os Estados Unidos ocupam o 1º lugar no ranque regional e o 2º lugar no ranque global do GCI (ITU, 2019), com uma pontuação de 0,926. Esse fato os posiciona como um ator demasiadamente importante no desenvolvimento em relação à Segurança Cibernética nas Américas.

A sua classificação como securitizado na condição Securitização se justifica porque há uma Estratégia Nacional na área nesse Estado, a *National Cyber Strategy of the United States of America*, que é definida pela UNIDIR (2021) como:

> Structured around four pillars of the National Security Strategy: 1 - Protect the American people, homeland, and the American way of life; 2 - Promote American prosperity; 3 - Preserve peace through strength; 4 - Advance American influence (UNIDIR, 2021)

Além disso, o País também é referência em termos de Índice de Desenvolvimento Humano, pontuando 0,920, o que é considerado como muito elevado, o parâmetro mais alto. Outro fator relevante que constitui a conjuntura explicativa desse caso são as Despesas Militares, que o alçam entre os países que mais gastam neste setor, o equivalente a 3,32% do seu PIB. Os Estados Unidos, também se destacam em relação à ocorrência de eventos raros, tendo registrado mais de 70 eventos de altíssimo impacto, com o exemplo do caso ocorrido entre abril e outubro de 2008 envolvendo o *Wikileaks* (CSIS, 2020):

> A State Department cable made public by WikiLeaks reported that hackers successfully stole “50 megabytes of email messages and attached documents, as well as a complete list of usernames and passwords from an unspecified (U.S. government) agency.” The cable said that at least some of the attacks originated from a Shanghai-based hacker group linked to the People’s Liberation Army’s Third Department (CSIS, 2020).

No que concerne ao Tempo do Marco Jurídico-Institucional, vale ressaltar que os Estados Unidos apresentam um dos marcos mais antigos da base de dados, sendo a legislação-referência o *Computer Fraud and Abuse Act - 18 USC § 1030*, datada de 1986, que “proíbe o acesso a um computador sem autorização, ou excedendo o seu tipo de autorização” (UNIDIR, 2021, tradução livre). Por último, mas igualmente importante, esse País integra a grande maioria da população, que tem o setor cibernético não militarizado, sendo a sua agência responsável na área a *Cybersecurity and Infrastructure Security Agency* (CISA).

4.2.1.2 Canadá

O Canadá, país da região da América do Norte, está posicionado em 2º lugar no

ranque regional e, além de ser o 9º lugar no ranque global, com um GCI de 0,892. Diferentemente dos Estados Unidos, essa País tem aproximadamente 1,326% destinado a Despesas Militares. Além disso, o segundo ultrapassa o primeiro em termos de Índice de Desenvolvimento Humano, pontuando 0,922 e ocupando o 13º lugar mundial.

Em relação à ocorrência de eventos raros, ele integra o grupo a categoria com múltiplos acontecimentos de altíssimo impacto. Como exemplo, apresentamos o ocorrido em janeiro de 2011, e descrito pelo CSIS (2020):

> The Canadian government reported a major cyberattack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the internet. Canadian sources attribute the attack to China (CSIS, 2020).

Nesse sentido, o marco jurídico-institucional do País remonta ao ano de 2000, o constituindo como da categoria de marco antigo. A legislação em questão é a *Personal Information Protection and Electronic Documents Act* (PIPEDA), que garante que se mantenham os registros, incluindo o setor privado, de todas as violações contra a privacidade dos dados (UNIDIR, 2021).

A nível de Estratégia Nacional como uma materialização do Estado como agente securitizador, o Canadá possui a *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*, do ano de 2018, que é definida como uma:

> Strategy to strengthen three pillars: Security and resilience; Cyber Innovation; and Leadership and Collaboration through an approach rooted in a sustained commitment to: 1) Protect the safety and security of Canadians and our critical infrastructure; 2) Promote and protect rights and freedoms online; 3) Encourage cyber security for business, economic growth, and prosperity; 4) Collaborate and support coordination across jurisdictions and sectors to strengthen Canada's cyber resilience; 5) Proactively adapt to changes in the cyber security landscape and the emergence of new technology. (UNIDIR, 2021).

Por sua vez, a agência responsável pela Segurança Cibernética, a *Canadian Centre for Cyber Security*, não incorre em uma militarização do setor.

4.2.1.3 Chile

Pertencente ao grupo de países da América do Sul que possuem um maior comprometimento com a Segurança Cibernética, o Chile, com GCI de 0,470, ocupa o 9º lugar no ranque regional e 83º lugar no ranque global. Ele também se destaca em relação ao Índice de Desenvolvimento Humano, a medida da pesquisa para Desenvolvimento Econômico, pontuando 0,847 no IDH, o que lhe garante o 42º lugar no mundo.

Ele é um dos poucos casos reportados pelo CSIS como alvos de eventos de altíssimo

impacto e rara frequência, tendo registrado um evento raro isolado em seu território em dezembro de 2018.

Segundo o CSIS (2020), nessa data, "*North Korean hackers targeted the Chilean interbank network after tricking an employee into installing malware over the course of a fake job interview*". No âmbito de um marco temporal, esse Estado apresenta a Lei 19.223, de 1993, se posicionando como um dos casos com marco jurídico-institucional antigo. De acordo com a UNIDIR (2021), ela "*sets out specific criminal definitions describing non-authorised access, theft and destruction of information systems*", o que constitui um diferencial dentre a legislação na área.

Além disso, o Chile é classificado no nosso modelo como securitizado em relação ao tema, uma vez que possui uma *National Cybersecurity Policy*, do ano de 2017, que:

> Identifies public policy measures for 2017-2018, and identifies the national standards and institutions involved in cybersecurity; Provides a risk and threat overview; Identifies the following policy objectives to reach by 2022:
> 1) Robust and resilient information infrastructure, prepared to face and recover from cybersecurity incidents, under a risk management approach; 2) Protection of people's rights in cyberspace; 3) Development of a cybersecurity culture based on education, good practices and accountability in the management of digital technologies; 4) Cooperation actions with other stakeholders in the field of cybersecurity and active participation in international forums and discussions; 5) Promoting the development of a cybersecurity industry serving its strategic objectives (UNIDIR, 2021).

Por último, o setor está constituído sob a jurisdição do *Interministerial Committee on Cyber Security*, de modo que o Estado integra a grande maioria dos países que não são considerados militarizados em termos de Segurança Cibernética.

4.2.1.4 Uruguai

Localizado na América do Sul, o Uruguai possui uma das maiores pontuações da região no GCI, especificamente 0,681, de maneira a alçá-lo ao 3º lugar no ranque regional, sendo também o 51º no ranque global. Essa posição de destaque também é notada em relação ao Índice de Desenvolvimento Humano, onde o País ocupa o 57º lugar mundial com o valor de 0,808 no índice.

De forma análoga ao que ocorre nos Estados Unidos, o Uruguai apresenta um Índice de Despesas Militares substancial, representando cerca de 2,13% do Produto Interno Bruto do Estado. Nesse sentido, a conjuntura de altas despesas militares associadas a um nível muito elevado de desenvolvimento humano se mostra frutífera para a explicação do contexto desse país.

Para além dessas questões, observamos o tempo do marco jurídico-institucional, que

nesse caso tem como origem o ano de 2009, com o *Presidential Decree* 452/009, que, entre outros fatores, "requires public administration bodies adopt an information security policy" (UNIDIR, 2021). No que se refere à securitização do setor, no entanto, a partir do nosso modelo, classificamos esse Estado como não securitizado, uma vez que ele não possui uma Estratégia Nacional de Segurança Cibernética.

Em se considerando a condição da militarização do setor cibernético, esse caso integra a grande maioria dos países que não têm o setor sob jurisdição de uma instituição essencialmente militar, ficando a cargo da *Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento* (AGESIC) a coordenação da área. A Agência, por sua vez, segundo a UNIDIR (2021), "Leads the development of the digital government and the information and knowledge society in Uruguay".

4.2.2 Caminho Causal 2: Cuba

A segunda categoria, entendida neste estudo como o **Caminho Causal 2**, é determinada por despesas militares acima de 2% do PIB e pelo marco jurídico-institucional recente, explicando 1 dos casos, a configuração (9): Cuba.

Com base nesses dados, inferimos que as condições Despesas Militares e Tempo do Marco Jurídico-Institucional constituem condições **INUS**, de forma que as duas mesmo não sendo suficientes, ainda assim são necessárias integrando uma conjuntura causal suficiente para explicar o maior comprometimento com a Segurança Cibernética em Cuba.

Dessa maneira, a conjuntura explicativa também confirma as hipóteses **H1.2** e **H1.4** do trabalho, ou seja, as Despesas Militares e o Tempo do Marco Jurídico-Institucional são condições necessárias e/ou suficientes para explicar o comprometimento com a Segurança Cibernética nos países do continente americano. Abaixo, perfilamos esse Estado de acordo com os dados da pesquisa.

Quadro 15 - Contexto do país do Caminho Causal 2.

PAÍS	SEC	DESP	EVE	TEM	MIL	DESE
CUB	Não Securitizado	Índice Alto	Ausência de Evento	Marco Recente	Não Militarizado	Índice Elevado

Fonte: Elaboração do autor a partir dos dados da pesquisa.

4.2.2.1 Cuba

Figurando como único país da América Central com um maior comprometimento com a Segurança Cibernética e explicado pelo modelo, Cuba ocupa o 8º lugar no ranque regional e 81º lugar no ranque global, com uma pontuação 0,481 no GCI. O seu marco jurídico-institucional recente se refere ao *Agreement 6058,* de 2007, que posteriormente foi revogado pelo Decreto Ley N. 370, de 2019, mas que, considerando o escopo temporal da pesquisa, se apresenta como ponto de referência em termos de legislação. Foi essa lei que lançou as bases para o melhoramento e a implementação das tecnologias de segurança da informação (UNIDIR, 2021).

Complementarmente, a conjuntura causal específica para a Segurança Cibernética nesse Estado implica em um Índice de Despesas Militares alto, totalizando em torno de 2,88% do PIB do país. Mesmo em um contexto com despesas militares elevadas, o setor cibernético não é militarizado, ficando sob o comando do *Centro de Seguridad del Ciberespacio*, ligado ao Ministério das Comunicações, a sua estruturação. Como definição do órgão, a UNIDIR (2021) especifica:

> Specialized structure designed to strengthen security in the Cuban cyberspace by promoting cooperation among all factors involved in cybersecurity nationwide and enhancing international cooperation in this area; Meant to contribute to the strengthening of security in the Cuban cyberspace and to effectively coordinate the management of cyber events with an impact on national cybersecurity; Tasked with, inter alia, proposing policies, strategies and technological security measures of national scope, to pursue the response cycle to cyber events with an impact on natinoal security, to make comprehensive analysis of the information obtained from cyberspace security events, to promote coordination, cooperation and information sharing among the various actors in charge of securing the country's cyberspace security UNIDIR (2021).

Por último, em contraponto à média dos países do continente, Cuba ainda não possui nem está desenvolvendo - tendo 2018 como ano de referência - uma Estratégia Nacional de Segurança Cibernética.

4.2.3 Caminho Causal 3: Brasil e Colômbia

A terceira categoria, considerada como o **Caminho Causal 3**, reúne os casos do Brasil - que vamos estudar mais detidamente no próximo capítulo - e da Colômbia. Eles são representados pelas configurações (16) e (25). Esses países são caracterizados principalmente pela militarização do setor cibernético. Vale ressaltar que, entre todos os casos avaliados na pesquisa, eles são os únicos com o setor sob jurisdição dos militares. Além da militarização

do setor, o desenvolvimento econômico, mensurado a partir do IDH, também é relevante para o resultado desses Estados, sendo o IDH deles classificado como elevado.

Nesse sentido, observamos que as condições Militarização e Desenvolvimento Econômico também operam como condições **INUS** para o maior comprometimento com a Segurança Cibernética nas Américas, integrando uma conjuntura suficiente para a ocorrência do fenômeno, mesmo que não sejam suficientes individualmente. Levando em consideração esse fato, a conjuntura explicativa também confirma as hipóteses **H1.5** e **H1.6** do estudo, de que, a Militarização e o Desenvolvimento Econômico são condições necessárias e/ou suficientes para explicar o comprometimento com a Segurança Cibernética nos países do continente americano. A seguir, discorreremos mais detalhadamente acerca desses Estados.

Quadro 16 - Contextos dos países do Caminho Causal 3.

PAÍS	SEC	DESP	EVE	TEM	MIL	DESE
BRA	Em Securitização	Índice Médio	Evento Isolado	Marco Recente	Militarizado	Índice Elevado
COL	Securitizado	Índice Alto	Ausência de Evento	Marco Recente	Militarizado	Índice Elevado

Fonte: Elaboração do autor a partir dos dados da pesquisa.

4.2.3.1 Brasil

Tendo posição de destaque na região da América do Sul, o Brasil ocupa o 6º lugar no ranque regional e o 70º lugar no ranque global do GCI, com uma pontuação igual a 0,577. Como mencionado, o caminho causal seguido pelo país para o comprometimento com a Segurança Cibernética é primordialmente representado pela militarização do setor, que fica sob a jurisdição do Comando de Defesa Cibernética (COMDCIBER), que, de acordo com a UNIDIR (2021), é uma unidade pertencente ao Exército do Brasil e que, majoritariamente é composta pelos representantes das Forças Armadas, tendo a responsabilidade de estruturar todo o ordenamento institucional, o que incorre em planejamento e coordenação das operações cibernéticas, mas sob o enfoque da Defesa.

O Índice de Desenvolvimento Humano é a outra medida explicativa da conjuntura brasileira. Nele, o País se posiciona em 79º lugar no mundo, com uma pontuação de 0,761, considerada elevada para os parâmetros do PNUD (2019). Vale ressaltar que o Brasil é um dos poucos países que presenciaram a ocorrência de eventos raros, tendo sido registrado um evento isolado em outubro de 2016. De acordo com o CSIS (2020), nesse período *"hackers*

gained control of a major Brazilian bank's Domain Name System addresses and seized the bank's entire online footprint for several hours".

No Índice de Despesas Militares, o Brasil está entre os Estados medianos, gastando em torno de 1,51% do seu Produto Interno Bruto nessa área. Paralelamente, no ano de 2018 ainda não havia uma Estratégia Nacional de Segurança Cibernética no país, mas já havia uma mobilização institucional e um planejamento para tal. Como marco jurídico-institucional do Brasil, podemos ressaltar a Lei 12.965, também conhecida como o Marco Civil da Internet, que, segundo a UNIDIR (2021) "estabelece princípios, garantias, direitos e obrigações para o uso da *Internet* no Brasil, e orienta as ações da União, dos Estados, do Distrito Federal e dos municípios nesse sentido".

4.2.3.2 Colômbia

A Colômbia integra, da mesma forma que o Brasil, o grupo de países da América do Sul representados nesta pesquisa. O seu GCI é de 0,565, garantindo-lhe o 7º lugar no ranque regional e o 73º lugar no ranque global. Nesse âmbito, o seu comprometimento com a Segurança Cibernética é explicado pela conjuntura que implica na militarização do setor cibernético associada a um Índice de Desenvolvimento Humano elevado (0,761, ocupando o 79º lugar). A instituição responsável por coordenar as ações referentes à Segurança Cibernética na Colômbia é o *Comando Conjunto Cibernético*, que, segundo a UNIDIR (2021), foi:

> Established by CONPES 3701, strengthened by CONPES 3854; Tasked with strengthening the technical and operational capabilities of the country to enable it to confront computer threats and cyber attacks through the implementation of protection measures, as well as introduction of cyberdefense protocols; Protects critical infrastructure, reducing the computer risks to the country's startegic information; Tasked with developing neutralization and response capabilities for dealing with computer incidents and attacks against the country's security and defense (UNIDIR, 2021).

Nesse ínterim, a *Política Nacional de Seguridad Digital - Consejo Nacional de Política Económica y Social*, mencionada como CONPES 3854, constitui a materialização da securitização da Segurança Cibernética no país, de acordo com o modelo estruturado nesta pesquisa. Segundo a UNIDIR (2021), essa política pública projeta:

> Five core areas of action, comprising Action and Follow-up Plan: 1) Establishment of a clear institutional framework around digital security; 2) Creation of conditions allowing stakeholders to manage digital security risk in their activities; 3) Strengthen the security of individuals and the State in a digital environment at national and transnational levels; 4) Strengthening national defense and security with a risk-management approach; 5) Creation of permanent mechanisms to promote cooperation, collaboration and assistance in digital security (UNIDIR, 2021).

Outro fator importante no contexto desse país é a ausência de eventos raros, característica que o diferencia do seu paralelo no caminho causal, o Brasil. Em se considerando o tempo do marco jurídico-institucional, a legislação de referência é o *Criminal Code*, de 2009, que estabelece os seguintes artigos sobre crimes cibernéticos:

> Article 192: Unlawful interception of communications; Article 269A: Illegal access to an information system; Article 269B: Illegitimate obstruction of information systems or telecommunication networks; Article 269C: Data interception; Article 269D: Unauthorised destruction, damaging, deleting, deteriorating, altering or suppression of data, or a data processing system, or its parts or components; Article 269E: Use of malicious software; Article 269F: Violation of personal data; Article 269G: Impersonation of websites to obtain personal data; Article 269H: Aggravating circumstances; Article 269I: Theft by computer and similar means; Article 269J: Unauthorised transfer of assets (UNIDIR, 2021).

Em relação às Despesas Militares, a Colômbia apresenta um dos índices mais altos, totalizando 3,1% do PIB do país destinados a esses tipos de gastos, o que se relaciona fortemente também com a militarização do setor cibernético nesse caso.

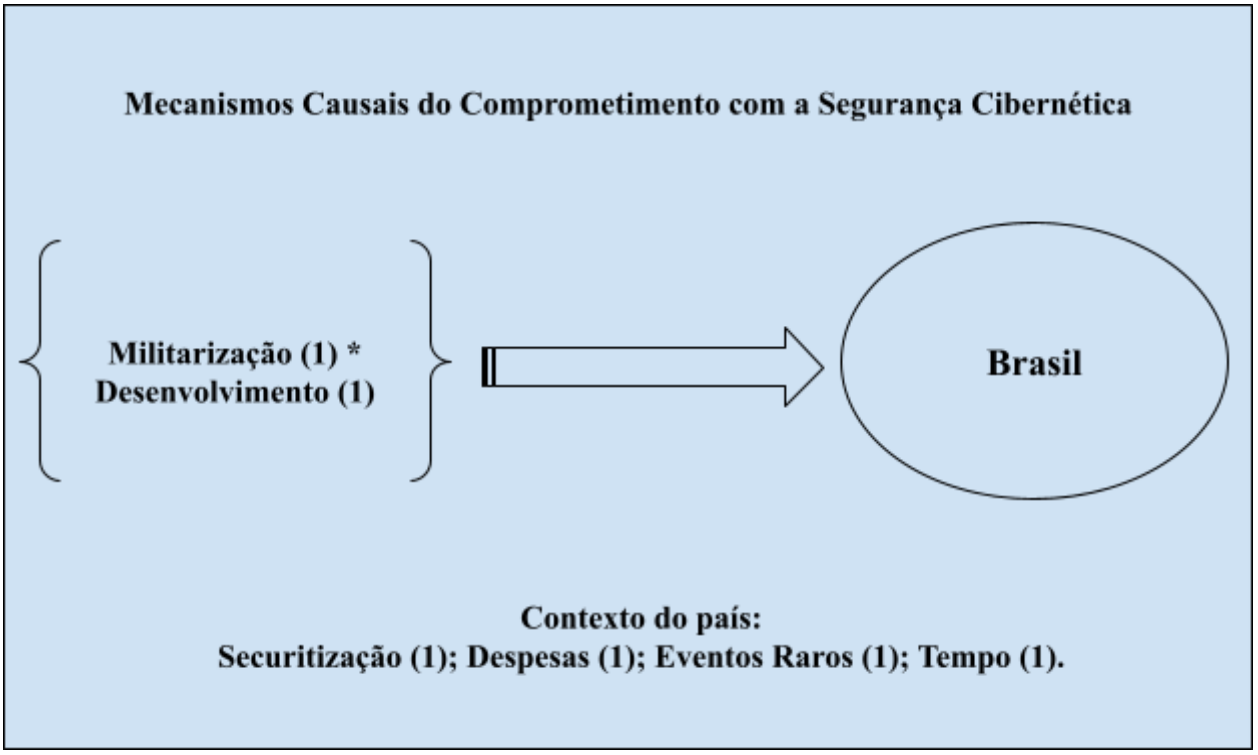
No próximo capítulo, realizaremos o estudo do caso brasileiro, na intenção de buscar a complementaridade em relação às inferências geradas neste capítulo da Análise Qualitativa Comparativa. Nesse sentido, o nosso intuito é robustecer o modelo apresentando uma aplicação prática para ele e buscando entender como o caminho causal opera em um contexto específico.

5 SEGURANÇA CIBERNÉTICA NO BRASIL

"Quis custodiet ipsos custodes?" (Juvenal)

Neste capítulo, realizamos um estudo de caso sobre o Brasil e o seu comprometimento com a Segurança Cibernética, buscando identificar mecanismos causais para o caminho pelo qual esse país atingiu a sua pontuação no *Global Cybersecurity Index*. Como representado na Figura 14, os dois principais fatores determinantes foram a militarização do setor cibernético e o nível elevado de desenvolvimento humano na sociedade brasileira.

Figura 14 - Comprometimento com a Segurança Cibernética: o caminho causal do Brasil.



Fonte: Elaboração do autor a partir dos dados da pesquisa.

Em seguida, apresentaremos uma discussão mais aprofundada sobre as condições explicativas e como elas estão relacionadas com o contexto do Estado brasileiro.

5.1 DETERMINANTES DO DESEMPENHO DO BRASIL NO GCI: UM ESTUDO DE CASO

5.1.1 As Raízes Institucionais da Militarização da Segurança Cibernética no Brasil

Partindo do conceito de militarização como "o processo de adoção de modelos, conceitos, doutrinas, procedimentos e pessoal militares em atividades de natureza civil, dentre

elas a segurança pública" (ZAVERUCHA, 2008, p. 178), faz-se mister o entendimento estrutural de como a militarização do setor cibernético no Brasil remonta e se associa à própria história recente desse país, que é marcado de forma muito específica pelas instituições militares (ZAVERUCHA, 2008; 1994; 2005; 2003; 2004; SCHWARCZ; STARLING, 2015; SCHWARCZ, 2019).

Nesse âmbito, a identificação de que o comprometimento com a Segurança Cibernética no Brasil trilha caminhos complementares à militarização patente no setor cibernético direciona essa pesquisa para um debate sobre relações civis-militares, controle social dos militares pela sociedade civil e, por conseguinte, teoria democrática. A experiência democrática recente do Brasil, que a expectativa teórica define como sendo de uma frágil democracia (ZAVERUCHA, 2000) ou até de período democrático tutelado, é marcada, principalmente, pela presença massiva dos militares nos governos eleitos democraticamente. Dessa maneira, argumenta-se que o período de transição da ditadura militar brasileira (1964 - 1985) para o ressurgimento dos governos democráticos foi tangenciado pela manutenção de prerrogativas militares que tornaram o País um *outlier* nesse quesito.

Como Zaverucha e Rezende (2009) argumentam:

> In Brazil, the return to democracy did not cause the military to reduce their levels of spending either during the regime of Fernando Henrique Cardoso (FHC) or, thus far, under that of Luís Inácio da Silva (Lula). Comparative empirical data on budgets at the ministerial level for these two administrations provide strong support for the argument that Brazil is an outlier. In fact, the military continued to expand its expenditures vigorously following the return to democracy (ZAVERUCHA; REZENDE, 2009, p. 407).

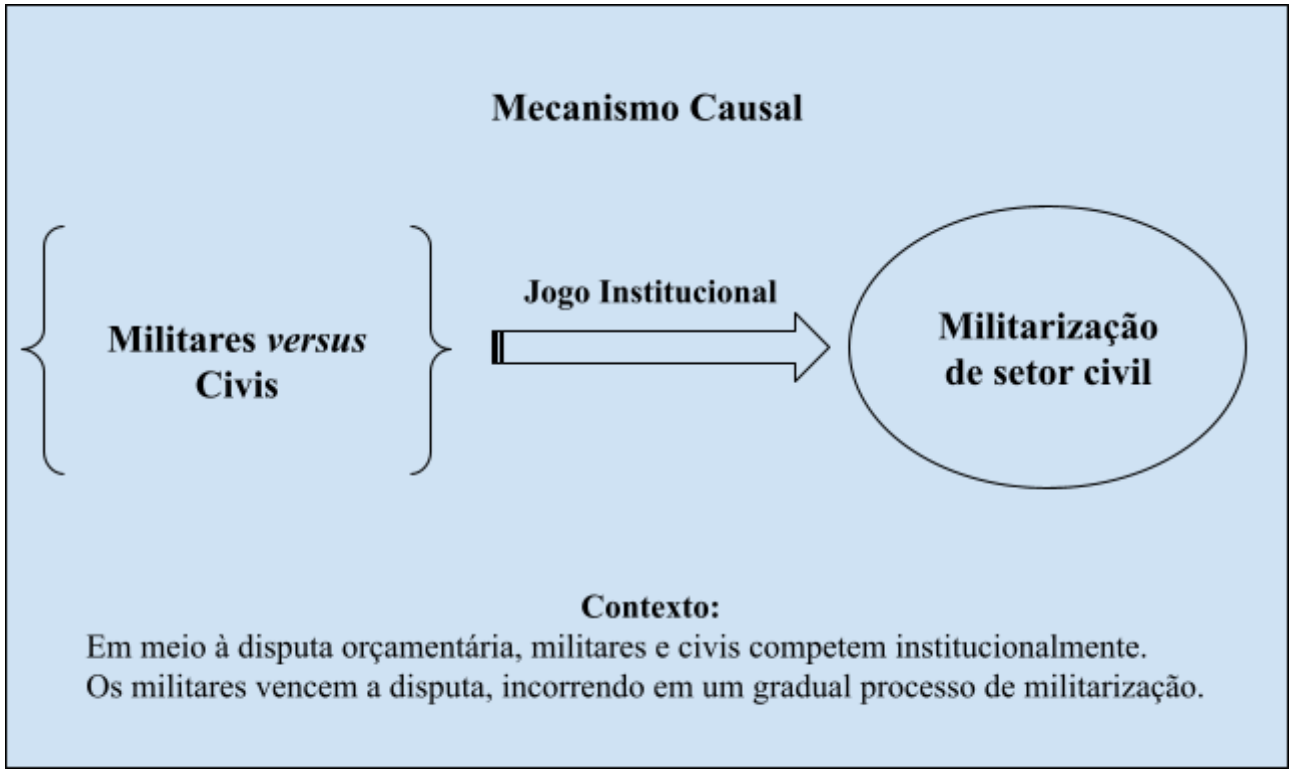
A partir do que foi apresentado durante este estudo, podemos identificar o princípio do que é denotado como uma das raízes da militarização do setor cibernético. Levando em consideração a atuação dos militares no jogo de barganha orçamentária na história democrática recente no Brasil, Zaverucha e Rezende (2009) reforçam o papel do País como um *outlier* também no que concerne às possibilidades de justificações para a expansão das despesas militares, uma vez que, ao contrário de outros países em desenvolvimento, o Brasil não sofreu influência relevante de fatores internacionais e da existência de conflitos regionais. Dessa forma, eles prosseguem:

> To justify their budgetary resources under democratic conditions, they have to perform internal roles such as policing, drug traffic control, commercial aviation control, merchant marine control, road construction, etc. The fact is that around 75% of the military budget is spent on personnel and salaries. Given that external factors do not play a considerable role in explaining military expenditure, examining the way the military strategically deals with politics and politicians offers greater explanatory power. (...) Brazil does not follow the path of civil–military relationship suggested by Feaver (2005). He makes the claim that civilian agencies may punish

> military ones by cutting the budget. In the case of Brazil, given the strategic exchange between the President, Congress and the military, politicians do not have the clout to shrink military expenditure, mainly for fear of the outcome of a political equilibrium breakdown. Instead, they have rewarded the military as the "guardians" either by maintaining their budgetary level or by expanding it. (ZAVERUCHA; REZENDE, 2009, p. 421).

Dessa maneira, argumentamos que essa atuação - e como ela incorreu em uma militarização do setor cibernético - pode ser explicada a partir do construto endógeno e institucionalista de Zaverucha e Rezende (2009), como evidenciado na Figura 15. Apresentamos essa ideia à revelia da ausência de possibilidades de explicação exógenas para o papel e o tamanho do aparato militar no Brasil.

Figura 15 - Explicação Institucionalista para a Militarização.



Fonte: Elaboração do autor a partir dos dados da pesquisa.

Outro aspecto relevante para a análise é a observação de que o Brasil possui uma dupla especificidade, sendo um *outlier* tanto em relação ao geral esperado nos países avaliados pela ITU, quanto no que concerne ao padrão das Américas. Enquanto um histórico ditatorial recente é raro em países com um maior comprometimento com a Segurança Cibernética, o contexto brasileiro o torna *sui generis* até quando comparado aos outros Estados do continente americano.

Após a terceira onda de democratização (HUNTINGTON, 1994), uma grande parte dos países latinoamericanos que passaram por períodos ditatoriais puniu as instituições

militares e revogou as suas prerrogativas. Nesse sentido, o Brasil fez o oposto: não só anistiou os antigos algozes, como também garantiu-lhes prerrogativas que foram expandidas nas décadas posteriores.

Por que os militares comumente ganham essas disputas institucionais? Diante da complexidade do fenômeno, encontramos respostas apenas na literatura interdisciplinar, tendo como exemplos trabalhos e modelos de outras áreas, como os estudos de debates legislativos. Bawn e Koger (2008) desenvolveram um modelo estratégico para o comportamento político, priorizando a análise das decisões legislativas, mas contribuindo com outros objetos de estudo. Segundo os autores, o resultado de um processo decisório vai depender especificamente das preferências dos atores envolvidos, dos custos de oportunidades para as suas decisões, das possibilidades de recompensas e, principalmente, do quanto esses grupos se esforçam para atingir a sua meta original.

Na disputa institucional, a possibilidade de *accountability*, a chance de externalidades eleitorais e o próprio esforço para o alcance dos pontos ideais de posicionamento, são algumas das diferenças entre os grupos militares e civis que tornam a relação no jogo institucional assimétrica.

Como os custos de oportunidade nas pautas entre civis e militares podem representar risco - mesmo que não incorrendo em um risco real - de desestabilização do argumentado equilíbrio entre as instituições na democracia, os atores políticos têm muito menos incentivos para buscar os seus pontos ideais em pautas envolvendo prerrogativas militares ou mesmo a expansão da sua influência. Além disso, o possível retorno eleitoral desse tipo de disputa é escasso, pois o eleitor mediano (DOWNS, 1999) de um país com um histórico de autoritarismo (SCHWARCZ; STARLING, 2015; SCHWARCZ, 2019) não escolhe recompensar os políticos com base nos seus posicionamentos acerca dos militares, mas sim em relação a questões mais inerentes ao cotidiano percebido pela população.

A partir desse contexto, os ganhos dos grupos militares no jogo institucional são mais previsíveis. O setor cibernético, instituído pela Estratégia Nacional de Defesa (END), é um exemplo de setor designado para a jurisdição dos militares, ficando a cargo, primordialmente, do Comando de Defesa Cibernética (COMDCIBER). Nesse sentido, historicamente, a área da Segurança Cibernética teve origem em um setor militarizado e com uma estrutura centrada na preocupação com a Defesa Cibernética, como evidenciado no Quadro 17.

Quadro 17 - Setor Cibernético e CDCiber.

PREMISSAS DO SETOR CIBERNÉTICO	OBJETIVOS DO CDCIBER
Contemplar multidisciplinaridade e dualidade das aplicações;	Melhoria da capacitação dos recursos humanos e a proteção contra ataques cibernéticos;
Fomentar a base industrial de defesa;	Atualização doutrinária;
Induzir a indústria nacional a produzir sistemas inovadores;	Fortalecimento da segurança;
Produzir componentes críticos nacionais.	Respostas a incidentes de redes;
	Incorporação de lições aprendidas;
	Proteção contra ataques cibernéticos.

Fonte: Adaptação de Lira-Brito (2020) do Livro Branco de Defesa Nacional (BRASIL, 2012a).

Para garantir que as premissas do setor cibernético, enunciadas no Livro Branco (BRASIL, 2012a), sejam atendidas, o Centro de Defesa Cibernética (CDCiber) coordena e integra a área, sendo uma das instituições relevantes na área.

No Quadro 18, apresentamos como a discussão sobre a Segurança Cibernética foi direcionada a partir de uma estrutura de políticas públicas e decisões institucionais voltadas para o caráter militar do setor cibernético e a sua preocupação com a Defesa Cibernética.

Quadro 18 - Gerações das Políticas de Defesa e Segurança Cibernéticas no Brasil.

GERAÇÃO	POLÍTICAS
PRIMEIRA GERAÇÃO	1. Política de Guerra Eletrônica de Defesa (2004); 2. Política de Defesa Nacional (2005); 3. Estratégia Nacional de Defesa (2008); 4. Instrução Normativa GSI/PR nº 1, de 13 de junho (2008); 5. Livro Verde: Segurança Cibernética no Brasil (2010).
SEGUNDA GERAÇÃO	1. Política Nacional de Defesa (2012); 2. Estratégia Nacional de Defesa (2012); 3. Livro Branco de Defesa Nacional (2012);

	4. Política Cibernética de Defesa (2012).
TERCEIRA GERAÇÃO	1. Doutrina Militar de Defesa Cibernética (2014); 2. Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública (2015); 3. Estratégia Nacional de Defesa (2016); 4. Política Nacional de Defesa (2016); 5. Livro Branco de Defesa Nacional (2016).

Fonte: Tipologia de Lira-Brito (2020).

Segundo a Tipologia Lira-Brito, originada a partir de classificações anteriores, as políticas de Defesa e Segurança Cibernéticas se dividem em três gerações, havendo, ainda, uma presença de novas versões de políticas anteriores de uma geração para a outra.

Para além de uma estrutura de políticas que se apresentam como um reflexo do setor militarizado, observamos a divisão dos níveis de decisão nesse setor, disponíveis na Política Nacional de Defesa (PND) e na Estratégia Nacional de Defesa, segundo os quais a Segurança Cibernética integra o nível político de decisão, ficando a cargo do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). O Quadro 19 sistematiza essas informações.

Quadro 19 - Níveis de Decisão do Setor Cibernético (PND/END).

NÍVEL DE DECISÃO	DESIGNAÇÃO	ESTRUTURA
POLÍTICO	Segurança Cibernética	Gabinete de Segurança Institucional
ESTRATÉGICO	Defesa Cibernética	Ministério da Defesa
OPERACIONAL	Guerra Cibernética	Componentes das Forças Armadas
TÁTICO	Guerra Cibernética	Componentes das Forças Armadas

Fonte: Lira-Brito (2020), adaptando a Política Nacional de Defesa (BRASIL, 2012c) e a Estratégia Nacional de Defesa (BRASIL, 2012b).

Essa subdivisão incentiva conclusões intuitivas de que não necessariamente a Segurança Cibernética está fadada a sofrer as influências da militarização do setor cibernético. No entanto, o histórico recente de Ministros-Chefes de Segurança Institucional do Brasil lança luz sobre essas questões, como evidenciado no Quadro 20.

Quadro 20 - Relação dos Ministros-Chefes de Segurança Institucional do Brasil.

PERÍODO	GOVERNO	MINISTRO-CHEFE
1985 - 1990	Governo Sarney	Rubens Bayma Denys (General de Exército)
1990 - 1992	Governo Collor	Agenor Francisco Homem de Carvalho (General de Divisão)
1992 - 1994	Governo Itamar Franco	Fernando Cardoso (General de Brigada)
1995 - 2002	Governo FHC	Alberto Mendes Cardoso (General de Exército)
2003 - 2010	Governo Lula	Jorge Armando Felix (General de Exército)
2011 - 2015	Governo Dilma	José Elito Carvalho Siqueira (General de Exército)
2015 - 2016	Governo Dilma	Marcos Antonio Amaro dos Santos (General de Exército)
2016 - 2019	Governo Temer	Sérgio Etchegoyen (General de Exército)

Fonte: Elaboração do autor com base nos dados da pesquisa.

Como pode ser observado, o Gabinete de Segurança Institucional, que já teve o nome de Casa Militar e também de Gabinete Militar, tem uma longa história de Ministros-Chefes de origem militar, não havendo na relação apontada algum civil nessa posição de autoridade, ficando a cargo de generais o comando do referido Gabinete.

Em suma, para além das questões institucionais envolvidas, a militarização do setor cibernético, que ocorre devido a jogos de barganhas orçamentárias, acaba por implicar em um maior comprometimento com a Segurança Cibernética, de acordo com o que foi registrado pelo GCI (ITU, 2019). Essa relação, argumentamos, ocorre porque, à guisa do embate nas relações civis-militares, esses últimos também buscam uma forma de legitimar a sua atuação

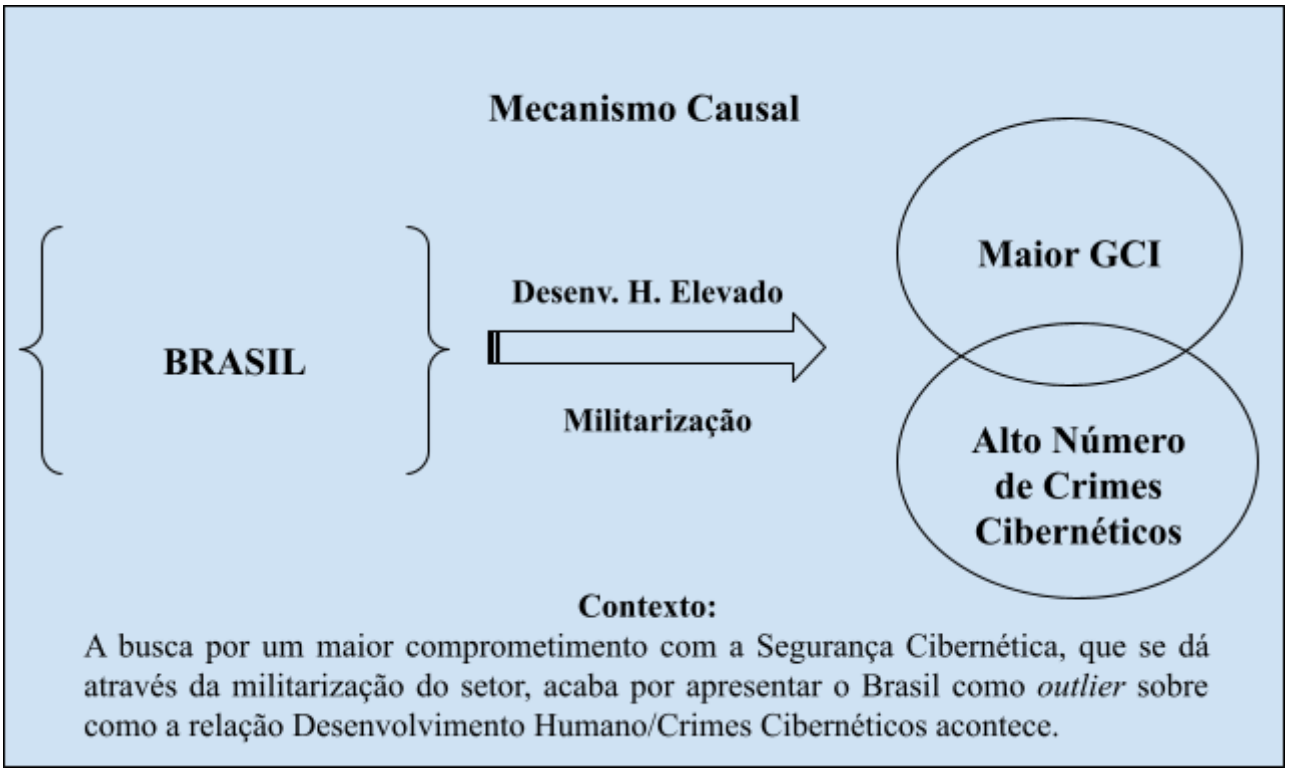
na democracia brasileira, de maneira que o cumprimento dos pilares do *Global Cybersecurity Index* proporciona um argumento de que a militarização do setor pode estar positivamente relacionada ao comprometimento com a Segurança Cibernética. No entanto, ressaltamos, as dimensões mensuradas pelo GCI não apresentam capilaridade sobre alguns dos fenômenos importantes para a realidade empírica brasileira, como a alta ocorrência de crimes cibernéticos à revelia do maior comprometimento com a Segurança Cibernética no País, como apresentamos, a seguir, no próximo subcapítulo.

5.1.2 O Desenvolvimento Econômico no Brasil e os Crimes Cibernéticos

O Desenvolvimento Econômico, entendido neste estudo a partir da sua perspectiva humana e mensurado pelo Índice de Desenvolvimento Humano, é uma das condições determinantes que explicam o maior comprometimento com a Segurança Cibernética no Brasil. Muller (2015) considera essa como uma condição essencial para a capacitação no que se refere à Segurança Cibernética. De forma semelhante, Kirtilli (2019) buscou identificar o impacto que o desenvolvimento econômico tem no desenvolvimento de políticas de Segurança Cibernética, inferindo, por sua vez, que o PIB per capita tem um impacto significante, havendo ainda uma interação com a taxa de penetração da *Internet*, sobre a criação de políticas na área.

Um fator importante, alinhado a esses autores, para o entendimento do papel do desenvolvimento econômico e humano nos países é o fenômeno dos crimes cibernéticos, que representam uma das maiores preocupações atuais do mundo. Em geral, a expectativa teórica associa aspectos socioeconômicos à explicação da ocorrência de crimes cibernéticos, havendo uma ideia de que o desenvolvimento econômico, assim como o desenvolvimento humano em específico, é uma condição importante para a redução dos crimes cibernéticos nos países (ILIEVSKI; BERNIK, 2016).

Figura 16 - Desenvolvimento Econômico no Brasil: mecanismos causais.



Fonte: Elaboração do autor a partir dos dados da pesquisa.

Como apresentamos na Figura 16, o mecanismo causal esperado em termos de Desenvolvimento Econômico no Brasil ocorre, mas traz em si alguns aspectos específicos, como a manutenção - ou até a expansão - da alta ocorrência de crimes cibernéticos no País. Dessa maneira, cumpre-se os requisitos formais mensurados pelo GCI, o que gera um maior comprometimento com a Segurança Cibernética, mas as relações consequentes esperadas, como a redução dos crimes cibernéticos, não acontecem. Dessa forma, associada à questão da estruturação militarizada do setor cibernético, a emergência dos crimes cibernéticos oferece maiores problemas, como argumentado por Faria (2016):

> Cibercrime pode então ser visto como um fenômeno que não necessariamente precisa ser combatido usando algum tipo de centro de comando cibernético executado pelos militares, mas utilizando as estruturas existentes do Estado de direito. Tal abordagem poderia, portanto, superar os perigos da militarização do ciberespaço e com este, expulsar suas estruturas e métodos existentes e usar os princípios jurídicos. Além disso, poderá opor-se ao emprego de meios militares secretos que vão além do policiamento e métodos intrusivos que permeiam as esferas da vida da sociedade (FARIA, 2016, p. 17).

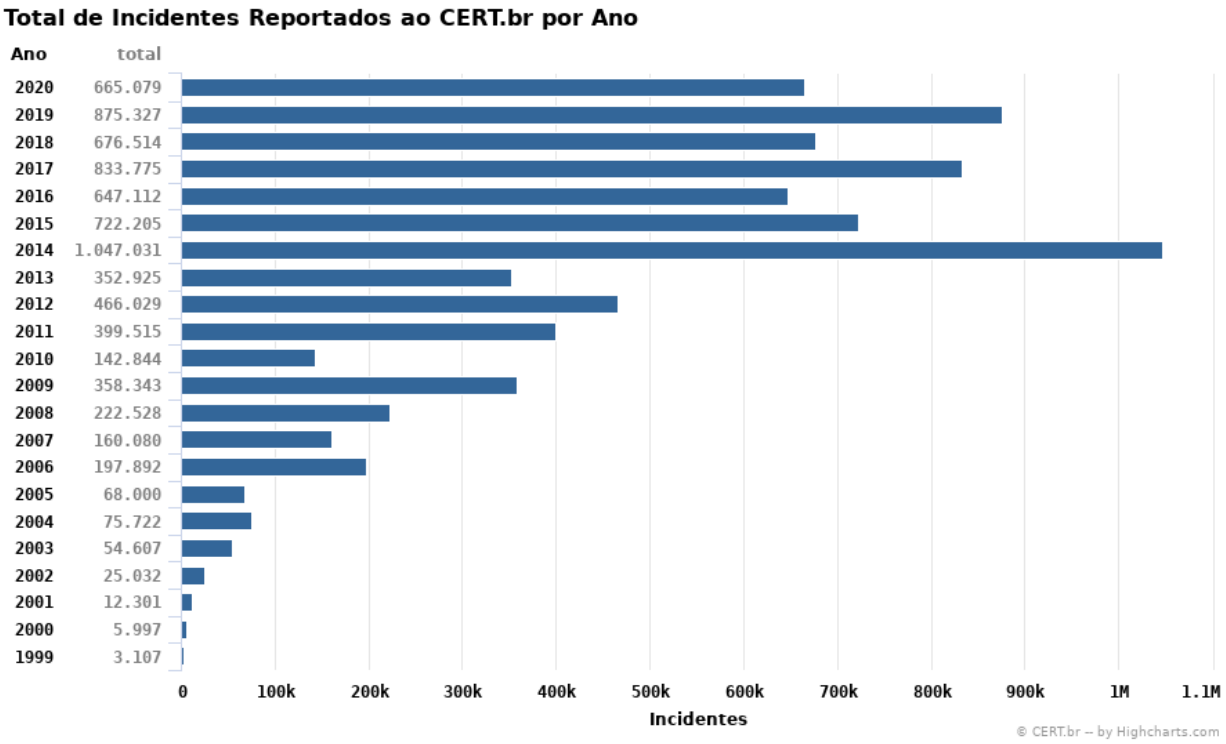
A problemática evidenciada por Faria (2016) prenuncia o eixo dos fatores não abrangidos pelo *Global Cybersecurity Index* que têm grande importância na realidade do Brasil. Embora o construto militarizado do setor cibernético incorra em um maior

comprometimento com a Segurança Cibernética, o aparente desvio da substância civil para a perspectiva militar gera uma perda de capilaridade do setor para o combate aos crimes cibernéticos. Kshetri (2013) também sugere algumas explicações importantes, quando argumenta que:

> Some of the key economic and social characteristics of a developing country include a dual economy, low levels of income and education, which lead to low levels of human development; high unemployment rates, high degrees of income inequality, and weak democratic institutions. Prior e-commerce researchers have linked these characteristics with innovations, intellectual protection rights and diffusion of information technology in developing economies. (...) These characteristics are tightly connected to the natures of cybercrime and cybersecurity. For instance, low levels of income and education lead to relative laggardness in developing world-based consumers' adoption of new technologies. To put things in context, many Internet users in the developing world are inexperienced and not technically savvy as a high proportion of them got their computers and connected to the Internet not long ago. A majority of them also lack English language skills. This later point is crucial due to the fact that most of the information, instructions, and other contents for security products are available in English language only. Many Internet users in economies in the developing world are unable to use IT security products developed in English language. (...) Countries with weak democratic institutions face additional problems. In some authoritarian regimes, cyber-security measures mainly focus on cyber-control activities. For instance, Chinese government agencies allegedly sent viruses to attack websites that were banned. Likewise, the governments of Myanmar and Mauritania have allegedly hired botnet operators to attack their critics' websites with DoS attacks. The government of Myanmar had reportedly built up an advanced cyberwarfare department within the police force, which, in the past, tracked its online critics and sent virus attached e-mails to exiled activists. In 2008, before the anniversary of the Saffron Revolution, at least three websites associated with Burmese exiles experienced DDoS attacks (KSHETRI, 2013, p. 50-52).

Na Figura 17, apresentamos uma relação - provavelmente com subestimação - dos incidentes cibernéticos reportados no País.

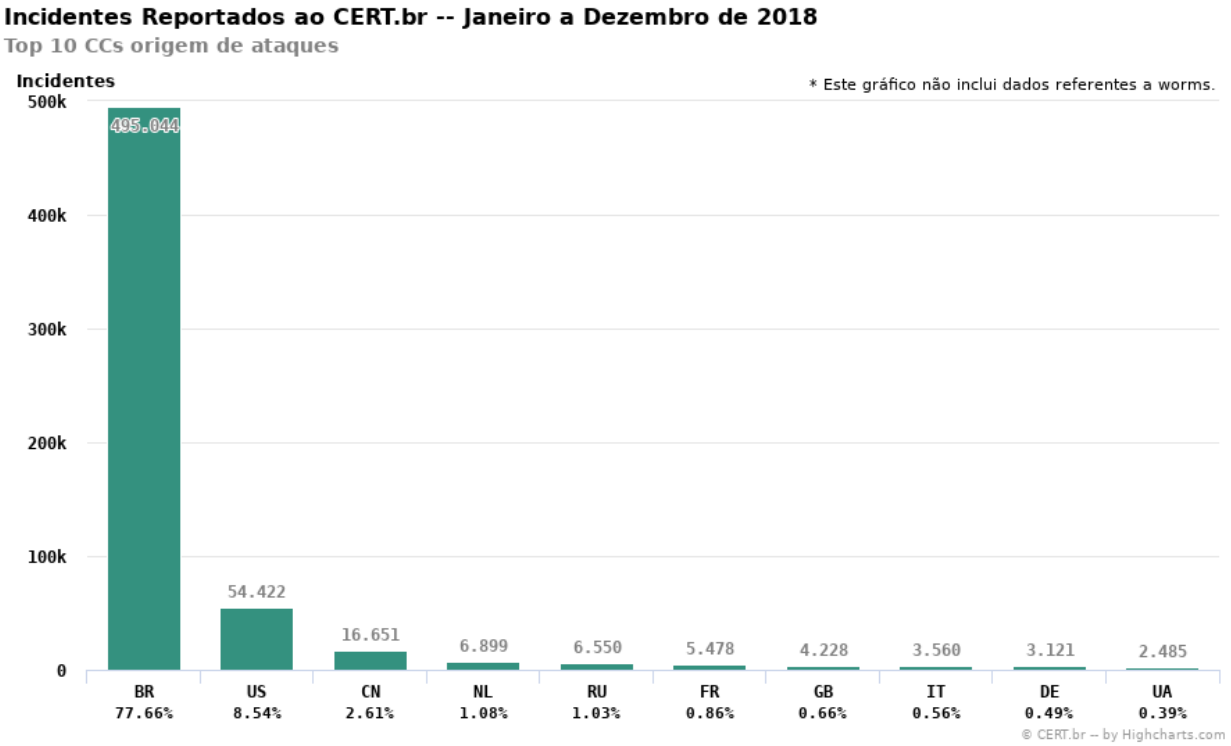
Figura 17 - Incidentes Cibernéticos Reportados por Ano no Brasil.



Fonte: CERT.br (2022).

Como pode ser observado na Figura 17, a partir do ano de 2010, o CERT.br presenciou um crescimento considerável de incidentes cibernéticos reportados, alcançando, no ano-referência de 2018, a marca de quase 680 mil casos registrados. A expectativa teórica aponta também o espaço cibernético como uma zona de transição de algumas das ações que ocorrem nos outros territórios, como o fenômeno do crime organizado (OLIVEIRA, 2006). Ressaltamos a defesa de Lira-Brito (2020) de que os mecanismos identificados por Oliveira (2006) para o crime organizado atualmente possuem desdobramentos no espaço cibernético, principalmente no que se refere às ameaças emergentes identificadas por Muggah, Glenny e Diniz (2014). Além disso, como apresentado na Figura 18, a imensa maioria dos incidentes cibernéticos reportados no Brasil têm como origem o próprio território brasileiro, o que realça os argumentos pela ideia da Segurança Pública Cibernética (LIRA-BRITO, 2020).

Figura 18 - Origem dos incidentes cibernéticos no Brasil.



Fonte: CERT.br (2022).

Ainda em 2010, o CDCiber teve a atribuição de monitorar a rede da Conferência das Nações Unidas sobre Desenvolvimento Sustentável (CNUDS), popularmente conhecida como Rio+20, o que levantou as primeiras dúvidas sobre a atuação dos militares no setor cibernético, e que foi fortemente realçado pelas atuações posteriores em eventos de grande porte no País (SANTOS, 2019).

Dessa maneira, chegamos ao ponto fulcral da análise do nosso estudo de caso. Embora o Brasil tenha atingido um maior comprometimento com a Segurança Cibernética, o caminho causal utilizado, marcado principalmente pela militarização, oferece impactos negativos para o próprio desenvolvimento do setor a longo prazo, como a ausência de capilaridade para a resolução de problemas reais no Estado, com o exemplo da questão do crescimento exponencial dos crimes cibernéticos (GUEDES DE OLIVEIRA, 2017).

Atualmente, existem apenas 17 delegacias civis especializadas no combate e na repressão a crimes cibernéticos no Brasil, número insuficiente para o quantitativo de crimes e incidentes ocorridos no território brasileiro diariamente. Apresentamos, no Quadro 21, essa relação.

Quadro 21 - Delegacias Especializadas em Crimes Cibernéticos no Brasil.

INSTITUIÇÃO	ESTADO	REGIÃO	CONTATO
Grupo Especializado de Repressão aos Crimes por Meio Eletrônicos	Bahia	Nordeste	(71) 3117-6109 (71) 3116-6109
Delegacia de Repressão a Crimes Eletrônicos	Espírito Santo	Sudeste	(27) 3137-2607 (27) 3137-9078
Departamento de Combate aos crimes tecnológicos	Maranhão	Nordeste	(98) 3214-8657
Gerência Especializada de Crime de Alta Tecnologia	Mato Grosso	Centro-Oeste	(65) 3613-5649
Delegacia Especializada de Investigações de Crimes Cibernéticos	Minas Gerais	Sudeste	(31) 3217-9714 (31) 3217-9712 (31) 3217-9714
Divisão de Prevenção e Repressão a Crimes Tecnológicos	Pará	Norte	(91) 3222-7567
Núcleo de Combate aos Cibercrimes	Paraná	Sul	(41) 3321-1900
Delegacia de Polícia de Repressão aos Crimes Cibernéticos	Pernambuco	Nordeste	(81) 3184-3206 (81) 3184-3207
Delegacia Especializada de Repressão aos Crimes de Alta Tecnologia	Piauí	Nordeste	(86) 3216 5212 (86) 3216 5225
Delegacia de Repressão aos Crimes Informáticos	Rio Grande do Sul	Sul	(51) 3288-9815
4ª Delegacia de Delitos Cometidos por Meios Eletrônicos	São Paulo	Sudeste	(11) 2221-0977 (11) 2221-7030 (11) 2221-1761
Departamento de Homicídios e de Proteção à Pessoa / 4ª Delegacia de Polícia de Repressão à Pedofilia	São Paulo	Sudeste	(11) 3311-3536 (11) 3311-3537
Delegacia de Repressão a Crimes Cibernéticos	Sergipe	Nordeste	(79) 3198-1135
Delegacia de Repressão aos	Rio de	Sudeste	(21) 2202-0277

Crimes de Informática	Janeiro		
Divisão de Repressão a Crimes Cibernéticos	Tocantins	Norte	(63) 3218-6986
Delegacia Especial de Repressão ao Crime Cibernético	Distrito Federal	Centro-Oeste	(61) 3207-4892
Delegacia Estadual de Repressão a Crimes Cibernéticos	Goiás	Centro-Oeste	(62) 3201-2650

Fonte: Elaboração do autor com dados da Safer Net[21].

A partir do Quadro 21, pode ser observada a distribuição regional das delegacias especializadas em crimes cibernéticos. Inicialmente, nota-se a disparidade entre regiões, uma vez que as regiões Nordeste e Sudeste são as mais abrangidas por esse tipo de instituição (havendo duas dessas delegacias apenas no Estado de São Paulo), enquanto a região Norte é a mais desprovida desse tipo de serviço.

De fato, ao contrário do esperado para a área, a preocupação do setor acaba sendo voltada principalmente para a Defesa Cibernética, com o exemplo da ênfase dada aos ataques cibernéticos e da possibilidade de vigilância, ao invés do enfoque sobre os crimes cibernéticos e os problemas inerentemente civis na área. Esse desvio chancela a ruptura com a mentalidade liberal acerca da Segurança Cibernética, restando às poucas instituições que abrangem esses aspectos da Segurança Cibernética o trabalho hercúleo de atender às demandas reais da sociedade brasileira.

Portanto, o caminho causal identificado no Brasil, que conduz ao maior comprometimento com a Segurança Cibernética através do desenvolvimento econômico e, principalmente, da militarização do setor, é caracterizado por um histórico de jogos institucionais entre militares e civis em busca de parcelas maiores do orçamento do País. Dessa forma, para legitimar o seu papel e justificar as suas despesas, os militares passam a assumir atribuições inerentemente civis, fagocitam as estruturas e militarizam setores como o da Segurança Cibernética.

Como há uma necessidade contínua de legitimação das suas ações e do seu ordenamento, o cumprimento dos critérios avaliados pelo *Global Cybersecurity Index* surge como uma oportunidade de justificação institucional, já que o reconhecimento de um índice

[21] Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 12 jan. 2022.

mundialmente renomado e organizado por uma agência da ONU aquiesce as ressalvas em relação aos responsáveis pelo feito.

No entanto, o atendimento aos problemas reais da sociedade civil se torna ineficiente por causa do desvio dos objetivos do setor, das medidas consideradas necessárias e das ações tomadas pelos militares, mesmo que em paralelo os critérios mínimos do GCI estejam sendo atendidos.

6 LIMITAÇÕES E AGENDA DE PESQUISA

Durante a realização desta pesquisa, enfrentamos barreiras as mais diversas, a começar pela pandemia da COVID-19, que restringiu as possibilidades do nosso estudo e limitou a própria experiência da pós-graduação ao ensino remoto. Um dos objetivos definidos para o desenvolvimento e aprofundamento deste trabalho era a mobilidade acadêmica proporcionada pela FACEPE, que seria realizada na Escola de Comando e Estado-Maior do Exército (ECEME). Essa modalidade não encontra paralelo em havendo a impossibilidade de atividades presenciais, o que acarretou no cancelamento dos planos nesse sentido.

Como a grande maioria da população brasileira, perdemos familiares durante a pandemia e buscamos conciliar o luto e as consequências da crise sanitária com o desenvolvimento da pesquisa, de forma a não incorrer em atrasos nos prazos estabelecidos pela FACEPE.

Dito isso, o próprio assunto abordado implicou em barreiras específicas, em se considerando a interdisciplinaridade do tema, a escassez de produção empírica e metodologicamente orientada nacional e o ineditismo da utilização da Análise Qualitativa Comparativa em pesquisas da área.

Diante das múltiplas possibilidades de abordagens para o estudo da Segurança Cibernética, envolvendo desde a Ciência da Computação, os Estudos Estratégicos, as Ciências Militares até as Relações Internacionais e a Ciência Política, escolhemos contribuir com a produção científica construindo um modelo explicativo para o comprometimento com a Segurança Cibernética - avaliado pelo GCI - no continente americano, sendo o arcabouço teórico-metodológico majoritariamente da Ciência Política e da linha de pesquisa da Política Comparada.

Seguindo a máxima de que escolher é limitar, avaliamos que as nossas escolhas reduziram as possibilidades de discussão no âmbito das Relações Internacionais, de Segurança Internacional e das outras áreas envolvidas, restando algumas poucas considerações e a utilização de condições explicativas dentro de um modelo orientado principalmente pela Ciência Política.

Além disso, a mensuração dessas condições precisou ocorrer de forma a consistir em proposições mínimas de operacionalização de conceitos. Como exemplo desse caso, ressaltamos as condições Securitização e Militarização do setor cibernético. A primeira originalmente seria avaliada a partir de análise quantitativa de dados qualitativos, mas, devido a fatores exógenos, foi necessário adaptar e buscar simplificações, chegando à consideração

da securitização como medida a partir da existência, do desenvolvimento ou da inexistência de uma Estratégia Nacional de Segurança Cibernética. A Militarização do setor, por sua vez, também seria mensurada em um modelo *text as data*. No entanto, pelos mesmos motivos, realizamos mudanças e passamos a considerá-la a partir do caráter - se civil ou militar - da agência responsável pelo setor. Há limitações, portanto, no que concerne a quanto esses conceitos mínimos e suas operacionalizações perderam em eficiência de explicação da realidade empírica.

A utilização da Análise Qualitativa Comparativa, especificamente o tipo mvQCA, representou outro grande desafio, uma vez que esse é um método menos usual do que os outros - principalmente os quantitativos - e são extremamente escassas as produções introdutórias e didáticas acerca dessa variante e os modos de proceder em *softwares* de análise de dados, restando aos aspirantes da técnica o aprendizado não-linear do autodidatismo.

Nesse sentido, o formato contraintuitivo da mvQCA na maioria das ferramentas de análise nos conduziu a utilização do *Tosmana*, que, mesmo com simplificações e diminuindo a chance de replicação, possibilitou a realização da pesquisa. Os resultados, no entanto, se mostraram satisfatórios e conduziram a uma primeira representação da realidade do continente americano utilizando modelos configuracionais.

Como o desenho de pesquisa implica em metodologia mista, tivemos dificuldade em encontrar paralelos e exemplos de aplicações empíricas na área, com a exceção de alguns poucos trabalhos pioneiros, como o de Vilar-Lopes (2016), o de Kirtilli (2019) e o de Oppermann (2010). Sendo assim, a falta de regularidade desse tipo de produção também limita o horizonte de possibilidades e dificulta a inventividade, pois não há um consenso ou uma tradição reconhecida do que é legítimo teórica e metodologicamente.

A abrangência explicativa do estudo, que se restringe a uma *middle-range theory*, mesmo gerando um aprofundamento dos casos analisados, impossibilita a generalização das inferências, de forma que as discussões apresentadas neste trabalho devem ser testadas e corroboradas por pesquisas posteriores.

Além disso, em consideração à exigência da mvQCA da dicotomização do fenômeno explicado, precisamos transmutar o GCI, que se dividia em três níveis, em uma condição *dummy* entre o maior e o menor comprometimento com a Segurança Cibernética. A partir de alguns testes, optamos por estabelecer 0,450 como o marco divisor, de modo a abranger os três países com alto comprometimento com a Segurança Cibernética e os seis primeiros casos (cerca de metade da categoria) com médio comprometimento com a Segurança Cibernética. O acréscimo de mais países - a partir da redução do marco - geraria maiores contradições lógicas

e a necessidade de soluções mais parcimoniosas, podendo incorrer no esvaziamento do poder explicativo do modelo.

A redução dos países classificados como apresentando um maior comprometimento (por exemplo, com a elevação do limiar para 0,500) afetaria a minimização lógica, gerando uma solução na qual Estados Unidos e Canadá seriam explicados pela ocorrência de múltiplos eventos raros, enquanto Brasil e Colômbia continuariam sendo explicados pela militarização associada ao desenvolvimento elevado e o Uruguai integraria uma nova classe, explicada por desenvolvimento econômico muito elevado, pelo marco jurídico-institucional recente e por um índice de despesas militares médio. Dessa maneira, objetivamos a justa medida entre a noção de parcimônia e a garantia do aprofundamento explicativo, o que não impossibilita a validade de outros trabalhos futuros baseados em limiares mais excludentes ou inclusivos.

Outra limitação em termos metodológicos foi a dificuldade de apresentar na QCA a influência negativa da militarização sobre o setor da Segurança Cibernética, o que foi abordado mais detalhadamente no estudo sobre os mecanismos causais do contexto brasileiro.

Nesse âmbito, há oportunidades as mais diversas, desde a ampliação do número de casos até a comparação de países de outras regiões buscando identificar os percursos e mecanismos causais. Um exemplo de como a produção na área pode avançar a partir dessa contribuição é a pesquisa a ser desenvolvida por Lira-Brito (2022) no Doutorado em Ciência Política no Programa de Pós-Graduação em Ciência Política da Universidade Federal de Pernambuco - PPGCP/UFPE.

O trabalho em questão, intitulado “Driving Cybersecurity: um estudo comparativo do mundo”, e em fase embrionária, também é desenhado a partir de métodos mistos, mas com uma abrangência maior de casos - os 194 países do mundo avaliados pela ITU - e, consequentemente, um poder de generalização maior, que é complementado com o estudo dos casos da Arábia Saudita e do Reino Unido, Estados que pontuam igualmente em todas as esferas no GCI de 2020 e divergem consideravelmente em relação aos mais diversificados aspectos institucionais.

Também indicamos para a agenda de pesquisa outras aplicações da Análise Qualitativa Comparativa e a realização de trabalhos introdutórios com exemplos reais e um manual passo a passo de como utilizar a mvQCA em estudos na Ciência Política e nas Relações Internacionais.

Por último, disponibilizamos os dados e o código utilizados nesta dissertação no repositório do autor no *GitHub*[22], intencionando a replicabilidade e o incentivo à transparência na produção científica nacional nas Ciências Sociais.

[22] Disponível em: https://github.com/lirarenato22/Seguran-a-Cibern-tica-Comparada-o-Brasil-e-as-Am-ricas/tree/main. Acesso em: 22 de jan. de 2022.

7 CONSIDERAÇÕES FINAIS

Mobilizada pela pergunta “Quais fatores explicam o nível de comprometimento com a Segurança Cibernética no continente americano?”, esta dissertação apresentou um modelo explicativo original para os 35 países das Américas com base nos dados do GCI (ITU, 2019), do Banco Mundial (2020), da UNIDIR (2021), da OEA (2021), do PNUD (2019) e do CSIS (2020).

Dessa maneira, realizamos uma Análise Qualitativa Comparativa desses casos no ano de 2018*,* tendo como condições explicativas do modelo: a) Securitização; b) Despesas Militares; c) Ocorrência de Eventos Raros; d) Tempo do Marco Jurídico-Institucional; e) Militarização; e f) Desenvolvimento Econômico.

Como resultados mais significativos da pesquisa, identificamos três caminhos causais para o maior comprometimento com a Segurança Cibernética: 1) Despesas Militares em conjunto ao Desenvolvimento Econômico explicando os Estados Unidos, Canadá, Chile e Uruguai; 2) as Despesas Militares e o Tempo do Marco Jurídico-Institucional explicando Cuba; e 3) a Militarização e o Desenvolvimento Econômico explicando o Brasil e a Colômbia.

Consequentemente, as Despesas Militares, o Desenvolvimento Econômico, o Tempo do Marco Jurídico-Institucional e a Militarização foram confirmadas como condições do tipo INUS, caracterizadas por serem partes insuficientes mas necessárias de um conjunto explicativo que é suficiente mas não é necessário. Sendo assim, as hipóteses secundárias **H1.2**, **H1.4**, **H1.5**, e **H1.6** foram corroboradas pelo modelo. No entanto, por não haver necessidade ou suficiência das condições Ocorrência de Eventos Raros e Securitização, as hipóteses secundárias **H1.1** e **H1.3** não foram corroboradas com base nesta pesquisa. A hipótese central, **H.1**, por fim, foi majoritariamente atendida, uma vez que as condições mobilizadas serviram para explicar cerca de 78% dos países com maior comprometimento com a Segurança Cibernética.

A sistematização e o levantamento dos dados desta dissertação culminaram em um repositório (disponível também nos apêndices deste trabalho) com riqueza de informações sobre o continente americano no que se refere à Segurança Cibernética. Além disso, o código para replicação compartilhado contribui didaticamente apresentando um exemplo prático da utilização da mvQCA em uma pesquisa empírica.

O estudo do contexto brasileiro apontou como mecanismo causal o histórico de militarização de setores no país explicado pelos jogos institucionais de barganha orçamentária

e pela busca de legitimação dos militares frente à sociedade civil. Esses jogos ocorrem em uma situação de assimetria de poder, onde os atores políticos têm menos recompensas e mais custos de oportunidades, uma vez que o embate entre civis e militares pode apresentar riscos para o argumentado equilíbrio institucional da democracia brasileira. Dessa maneira, há previsibilidade no resultado dos jogos institucionais, a militarização de setores civis - com o exemplo da Segurança Cibernética. Essa movimentação ocorre, primordialmente, por uma necessidade de legitimação da atuação dos militares em um contexto de ausência de inimigos externos e grandes conflitos internacionais. Assim, a busca por um maior comprometimento com a Segurança Cibernética representa uma oportunidade de justificação da militarização do setor e da expansão orçamentária dos militares.

Como consequência do caminho percorrido pelo País, elencamos alguns problemas: 1) o desvio da função do setor; 2) a ineficiência na resolução de problemas reais da sociedade, como os crimes cibernéticos. O desvio da função acontece porque o setor, idealmente entendido a partir de uma mentalidade liberal, é estruturado a partir da mentalidade e dos interesses militares. Essa divergência entre o esperado e o que ocorre converge com o não atendimento das demandas da sociedade civil quando deixa de solucionar problemas da realidade empírica, como a ocorrência de crimes cibernéticos, fenômeno não abrangido em sua totalidade pelo *Global Cybersecurity Index*.

Portanto, o estudo do caso brasileiro contribuiu não só para uma confirmação do modelo da Análise Qualitativa Comparativa, como também apresentou ressalvas para o nosso modelo indicando as suas limitações, como a ineficiência para explicar na QCA os pontos onde a militarização da Segurança Cibernética influencia negativamente o desenvolvimento do setor cibernético dos países. Essa questão foi abordada complementarmente no estudo de caso e poderá ser corroborada e testada pela agenda de pesquisa.

REFERÊNCIAS

AUSTIN, G. **Cybersecurity in China: the next wave**. Springer EBooks. 2018. https://doi.org/10.1007/978-3-319-68436-9

BID; OEA. Cibersegurança: Riscos, avanços e o caminho a seguir na América Latina e no Caribe. 2020. Disponível em: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf. Acesso em: 20 de dez. de 2021.

BANCO MUNDIAL. **Indicadores do Desenvolvimento Mundial**. 2020.

BARBAS, J. M. A.; SANCHO HIRANE, C. **Cibersegurança e Políticas Públicas:** análise comparada dos casos chileno e português. Lisboa: Instituto da Defesa Nacional. 2018. Disponível em: https://comum.rcaap.pt/handle/10400.26/23771. Acesso em: 25 de mar. de 2021.

BARBERIA, L. G. **Desenho de Pesquisa em Política Comparada**. Brasília: Enap, 2019. Disponível em: https://repositorio.enap.gov.br/handle/1/4789?mode=full. Acesso em: 20 de jan. de 2021.

_____; DE GODOY, S. R.; BARBOZA, D. P. Novas perspectivas sobre o 'calcanhar metodológico': o ensino de métodos de pesquisa em Ciência Política no Brasil. **Revista Teoria & Sociedade**, 2014.

BAUMARD, P. **Cybersecurity in France**. Springer EBooks. 2017. https://doi.org/10.1007/978-3-319-54308-6

BAWN, K.; KOGER, G. Effort, intensity and position taking: reconsidering obstruction in the pre-cloture Senate. **Journal of Theoretical Politics**, v. 20, n. 1, p. 67-92, 2008.

BERG, D. V. D. **Cybersecurity: Determinants of Cybersecurity Policies**. International Public Management and Policy. Rotterdam. Thesis, International Public Management and Policy, Erasmus University Rotterdam. 2014.

BETARELLI JUNIOR, A.; FERREIRA, S. **Introdução à Análise Qualitativa Comparativa e aos Conjuntos Fuzzy (fsQCA)**. Brasília: Enap, 2018. Disponível em: https://repositorio.enap.gov.br/handle/1/3333. Acesso em: 20 de jan. de 2021.

BRADY, H.; COLLIER, D (eds.). **Rethinking social inquiry: diverse tools, shared standards**. New York: Rowman & Littlefield. 2004.

BRASIL. Ministério da Educação. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. **Relatório Final de atividades do Grupo de Trabalho Impacto e Relevância Econômica e Social**. 2020. Disponível em: https://www.gov.br/capes/pt-br/centrais-de-conteudo/2020-01-03-relatorio-gt-impacto-e-relevancia-economica-e-social-pdf. Acesso em: 25 de jan. de 2021.

_____. Ministério da Defesa. **Glossário das Forças Armadas**. 2015. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf. Acesso em: 26 de jan. de 2021.

_____. Gabinete de Segurança Institucional. **Glossário de Segurança da Informação**. 2019. Disponível em: http://dadosabertos.presidencia.gov.br/dataset/a762e973-ef19-4cdb-8392-2983aee7669a/resource/f4a3bba8-8544-443d-a070-b4762ee8abed/download/glossario-de-seguranca-da-informacao-txt.txt. Acesso em: 25 de out. de 2021.

_____. Ministério da Defesa. **Livro Branco de Defesa Nacional**. 2012a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf. Acesso em: 12 de fev. de 2021.

_____. _____. **Estratégia Nacional de Defesa**. 2012b. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/end.pdf. Acesso em: 12 de fev. de 2021.

_____. _____. **Política Nacional de Defesa**. 2012 c. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf. Acesso em: 13 fev. 2021.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde: segurança cibernética no Brasil / Gabinete de Segurança Institucional**. Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010. 63p.

BUZAN, B.; WAEVER, O.; WILDE, J. **Security:** A new framework for analysis. Boulder: Lynne Rienner. 1998.

CALDERARO, A.; CRAIG, J. S. Transnational Governance of Cybersecurity: policy challenges and global inequalities in cyber capacity building. **Third World Quarterly**, p. 2-22, 2020. https://doi.org/10.1080/01436597.2020.1729729

CAVALCANTI, P. A. **Análise de políticas públicas: o estudo do Estado em ação.** Salvador: Eduneb. 2012.

CAVELTY, M. D. The militarisation of cyberspace: Why less may be better. **4th International Conference on Cyber Conflict**, Tallinn, Estonia, p. 1-13, 2012. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Militarization-Cyberspace.pdf. Acesso em: 15 de fev. de 2021.

_____; EGLOFF, F. J. The Politics of Cybersecurity: balancing different roles of the state. **St Antony's International Review**, v. 15, n. 1, p. 37-57, 2019. https://ssrn.com/abstract=3403971

CERT.br. **Estatísticas dos Incidentes Reportados ao CERT.br**. 2022. Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 20 de jan. de 2022.

CRESWELL, J. W. **Research design: qualitative, quantitative, and mixed methods approaches**. Thousand Oaks, California: Sage, 2009.

CRONQVIST, L. **Tosmana—Tool for cs-, mv-, and fsQCA Version 1.6. 1.0**. Tosmana. University of Trier.

CRÜWELL, S. et al. Seven Easy Steps to Open Science: An Annotated Reading List. **Zeitschrift für Psychologie**, v. 227, n. 4, p. 237-248, 2019. http://dx.doi.org/10.1027/2151-2604/a000387

CSIS, Center for Strategic & International Studies. **Significant Cyber Incidents**. Washington, 2020. Disponível em: www.csis.org/programs/technology-policy-program/significant-cyber-incidents. Acesso em: 25 de out. de 2020.

DAFOE, A. Science Deserves Better: The Imperative to Share Complete Replication Files . **PS: Political Science & Politics**, v. 47, p. 60-66, 2014. https://doi.org/10.1017/S104909651300173X

DOWNS, A. **Uma teoria econômica da democracia**. São Paulo: Editora da USP. 1999.

DUTRA, L. H. A. **Introdução à Epistemologia**. São Paulo: Editora UNESP. 2010.

ELAMIRYAN, R.; BOLGOV, R. Cybersecurity in NATO and CSTO: Comparative Analysis of Legal and Political Frameworks. **GigaNet: Global Internet Governance Academic Network, Annual Symposium**. 2018. http://dx.doi.org/10.2139/ssrn.3490191

FARIA, I. R. **Vigilância ou militarização da segurança cibernética?** Uma análise entre as mentalidades militar e liberal de segurança e a regulação das ameaças do ciberespaço. Brasília, 2016. Trabalho de Conclusão de Curso (Especialização em Relações Internacionais), Instituto de Relações Internacionais, Universidade de Brasília.

FIGUEIREDO FILHO, D. B. et al. Metodologias de pesquisa em ciência política: uma breve introdução. **BIB**, n. 94, p. 1-34, 2021 (publicada em agosto de 2020). http://doi.org/10.17666/bib9402/2021

GERRING, J. Causation: a unified framework for the social sciences. **Journal of Theoretical Politics**, v. 17, p. 163-198, 2005. https://doi.org/10.1177/0951629805050859

_____. The case study: what it is and what It does. In: Boix, C.; Stokes, S. C. **The Oxford Handbook of Comparative Politics**. Oxford: Oxford University Press, 2007.

GOERTZ, G.; MAHONEY, J. **A Tale of Two Cultures:** Contrasting Quantitative and Qualitative Research in the Social Sciences. Princeton: Princeton University Press. 2012.

GUEDES DE OLIVEIRA, M. A.; PORTELA, L. S. As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil. **Rev. Bras. Est. Def.**, v. 4, n. 2, p.77-99. 2017. https://doi.org/10.26792/rbed.v4n2.2017.75014

_____. Ameaças regionais e extrarregionais e as respostas do Brasil. **Centro de Estudos Estratégicos do Exército: Artigos Estratégicos**, v. 3, n. 3, p. 16-27, 2017.

GUSTAFSSON, K.; HAGSTRÖM, L. What is the point? Teaching graduate students how to construct political science research puzzles. **European Political Science**, v. 17, n. 4, p. 634-648. 2017. https://doi.org/10.1057/s41304-017-0130-y

HAGGARD, S.; MCCUBBINS, M. D. Introduction: Political Institutions and the Determinants of Public Policy. In: **Presidents, Parliaments, and Policy**. Cambridge, Cambridge University Press. 2001.

HALL, P. A.; TAYLOR, R. C. R. As Três Versões do Neo-institucionalismo. **Lua Nova**, n. 58, p. 193-223, 2003. https://doi.org/10.1590/S0102-64452003000100010

HANSEN, L., NISSEMBAUM, H. Digital Disaster, Cyber Security, and the Copenhagen School. **International Studies Quarterly**, v. 53, n. 4, p. 1155–1175, 2009. https://www.jstor.org/stable/27735139

HERRMANN, A.; CRONQVIST, L. Contradictions in Qualitative Comparative Analysis (QCA): ways out of the dilemma. **EUI SPS**, n. 6, p. 1-19, 2006.

HOCHTL, J.; PARYCEK, P.; SCHOLLHAMMER, R. Big data in the policy cycle: policy decision making in the digital era. **Journal of Organizational Computing and Electronic Commerce**, v. 26, n. 1-2, p. 147-169, 2015. https://doi.org/10.1080/10919392.2015.1125187

HUDSON, J.; KÜHNER, S. Qualitative Comparative Analysis and Applied Public Policy Analysis: new applications of innovative methods. **Policy and Society**, v. 32, n. 4, p. 279-287, 2013. http://dx.doi.org/10.1016/j.polsoc.2013.10.001

HUNTINGTON, S. P. **A terceira onda: a democratização no final do século XX**. São Paulo: Ática, 1994.

HUREL, L. M. A Securitização e Governança da Segurança Cibernética no Brasil. In: REIS, J.; FRANCISCO, P. A. P.; BARROS, M.; MAGRANI, E. (org.). **Horizonte Presente: Tecnologia e Sociedade em Debate**. Editora Letramento, p. 320-343, 2019.

ILIEVSKI, A.; BERNIK, I. Social-economic aspects of cybercrime. **Peer-reviewed academic journal Innovative Issues and Approaches in Social Sciences**, 2016.

IMMERGUT, Ellen M. **As Regras do Jogo: A Lógica da Política de Saúde na França, na Suíça e na Suécia**. Nova York: Cambridge University Press. 1992.

ITU. **Global Cybersecurity Index (GCI) 2018**. Studies & research. ITU Publications: Geneva, Switzerland. 2019.

_____. **Global Cybersecurity Index (GCI) 2017**. Studies & research. ITU Publications: Geneva, Switzerland. 2017.

_____. **Global Cybersecurity Index (GCI) 2014**. Studies & research. ITU Publications: Geneva, Switzerland. 2016.

_____. **Cybersecurity Index of Indices**. 2015. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Index_of_Indices_GCI.pdf. Acesso em: 20 de maio de 2021.

JIA, X. **Civilization and the Modern Military:** does increased military spending lead to higher levels of innovation in society. Public Policy. Washington, D.C. Thesis, Faculty of the Graduate School of Arts and Sciences, Georgetown University. 2014.

KAHNEMAN, D.; SLOVIC, P.; TVERSKY, A. (Eds.). **Judgment under uncertainty: Heuristics and biases**. New York : Cambridge University Press. 1982.

KELLSTEDT, P.; WHITTEN, G. **The Fundamentals of Political Science Research**. Cambridge: Cambridge University Press, 2013.

KING, G.; KEOHANE, R.; VERBA, S. **Designing social inquiry: scientific inference in qualitative research**. Princeton: Princeton University Press. 1994.

_____.; ZENG, L. Explaining Rare Events in International Relations. **International Organization**, v. 55, p. 693-715, 2001. https://doi.org/10.1162/00208180152507597

KIRTILLI, M. Cybersecurity and Economic Development: comparing developed, developing and emerging economies. **Cyberpolitik Journal**, v. 4, n. 7, p. 43-69, 2019. Disponível em: http://cyberpolitikjournal.org/index.php/main/article/view/28. Acesso em: 20 de jan. de 2021.

KREMER, J. Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace, **Information & Communications Technology Law**, v. 23, n. 3, p. 220-237, 2014. https://doi.org/10.1080/13600834.2014.970432

KSHETRI, N. Cybercrime and cyber-security issues associated with China: some economic and

institutional considerations. **Electronic Commerce Research**, v. 13, n. 1, p. 41-69, 2013.

KUHN, T. S. **The Structure of Scientific Revolutions**. Chicago: University of Chicago Press, 1962.

LAMPEL, J.; SHAMSIE, J.; SHAPIRA, Z. Experiencing the Improbable: Rare Events and Organizational Learning. **Organization Science**, v. 20, n. 5, p. 835-845, 2009. https://doi.org/10.1287/orsc.1090.0479

LANDMAN, T. Why compare countries?. In: **Issues and Methods in Comparative Politics**. Routledge, p. 25-44, 2008.

LAUNAY, M. **A Fascinante História da Matemática: da pré-história aos dias de hoje**. Rio de Janeiro: Bertrand Brasil, 2019.

LÉVY, P. **Cibercultura**. Trad. Carlos I. da Costa. São Paulo: Editora 34. 1999.

LIEBERMAN, E. Nested Analysis as a Mixed-Method Strategy for Comparative Research. **American Political Science Review**, v. 99, n. 3, p. 435-452, 2005. https://doi.org/10.1017/S0003055405051762

LIRA-BRITO, R. V. **Defesa e Segurança Cibernéticas:** crimes cibernéticos e políticas públicas no Brasil. Recife. Trabalho de Conclusão de Curso (Bacharelado em Ciência Política), Departamento de Ciência Política, Universidade Federal de Pernambuco. 2020.

_____. **O Global Cybersecurity Index (GCI) como Medida de Comprometimento com a Segurança Cibernética**. Rede CTIDC, 2021. Disponível em: https://redectidc.com.br/rede-ctidc-o-global-cybersecurity-index-gci-como-medida-de-comprometimento-com-a-seguranca-cibernetica.html. Acesso em: 10 de out. de 2021.

_____. **Driving Cybersecurity:** um estudo comparativo do mundo. Projeto de Tese: versão provisória (Doutorado em Ciência Política), Departamento de Ciência Política, Universidade Federal de Pernambuco. 2022.

MACKIE, J. L. Causes and conditions. **American Philosophical Quarterly**, v. 2, p. 245-264, 1965.

MAHONEY, J. Toward a Unified Theory of Causality. **Comparative Political Studies**, v. 41, n. 4, p. 412-436, 2008.

MAINWARING, S. Presidentialism, Multipartism and Democracy: the difficult combination. **Comparative Political Studies**, v. 26, n. 2, p. 198-228, 1993.

MALAMUD, A.; ALCAÑIZ, I. Managing Security in a Zone of Peace: Brazil´ s Soft Approach to Regional Governance. **Revista Brasileira de Política Internacional**, v. 60, 2017.

MALDONADO, C. E. The rare event: Epistemology and complexity. **Cinta moebio**, n. 56, p. 187-196, 2016. http://dx.doi.org/10.4067/S0717-554X2016000200006

MARQUES, T. C. S. O papel do desenvolvimento econômico no debate teórico sobre transições de regimes políticos. **Política & Sociedade**, v. 17, n. 38, p. 465-480, 2018. https://doi.org/10.5007/2175-7984.2018v17n38p465

MEDEIROS, M. A.; BARNABÉ, I.; ALBUQUERUE, R.; MESQUITA, R. What does the field of International Relations look like in South America?. **Revista Brasileira de Política Internacional**, v. 59, n. 1, e004, 2016.

MIGUEL, E. et al. Promoting Transparency in Social Science Research. **Science**, v. 343, p. 30-31, 2014. https://doi.org/10.1126/science.1245317

MUGGAH, R.; GLENNY, M.; DINIZ, G. Securitização da Cibersegurança no Brasil. **Cadernos Adenauer**, v. 15, n. 4, p. 69-109, 2014. Disponível em: https://www.kas.de/c/document_library/get_file?uuid=e01ed6d1-a531-2d8d-58a3-dae713a1af78&groupId=265553. Acesso em: 10 de mar. de 2021.

MULLER, L. P. **Cyber security capacity building in developing countries:** challenges and opportunities. 2015.

NOBREGA JUNIOR, J. M. P. A militarização da segurança pública: um entrave para a democracia brasileira. **Rev. Sociol. Polit.**, v. 18, n. 35, p. 119-130, 2010. https://doi.org/10.1590/S0104-44782010000100008

NORTH, D. **Institutions, Institutional Change and Economic Performance**. Cambridge: Cambridge University Press. 1990. https://doi.org/10.1017/CBO9780511808678

OLIVEIRA, A. **As Peças e os Mecanismos do Fenômeno Tráfico de Drogas e do Crime Organizado**. Recife. Tese de Doutorado em Ciência Política, Departamento de Ciência Política, Universidade Federal de Pernambuco. 2006.

OLIVEIRA, A. A. **(Des) controle civil sobre os militares no Brasil: um estudo comparado (1945-1964/1985-2009)**. Recife. Tese de Doutorado em Ciência Política), Departamento de Ciência Política, Universidade Federal de Pernambuco. 2010

OLSZEWSKI, B. Militarization of Cyber Space and Multidimensionality of Security. **Journal of Science of The Military Academy of Land Forces**, v. 48, n. 2, p. 104-120, 2016. http://dx.doi.org/10.5604/17318157.1216083

OPPERMANN, D. Virtual attacks and the problem of responsibility: the case of China and Russia. **Carta Internacional**, v. 5, n. 2, p. 11-25, 2010. Disponível em: https://cartainternacional.abri.org.br/Carta/article/view/546/291. Acesso em: 28 de jan. de 2021.

PARANHOS, R. et al. Uma introdução aos métodos mistos. **Sociologias**, v. 18, p. 384-411, 2016.

PASQUARELLI, B. V. L. Política comparada: tradições, métodos e estudos de caso. **Agenda Política**, v. 2, n. 2, p. 10-38, 2014.

PÉREZ-LIÑÁN, A. El método comparativo y el análisis de configuraciones causales. **Revista latinoamericana de política comparada**, v. 3, n. 3, p. 125-148, 2010.

PNUD. **Relatório do Desenvolvimento Humano**. 2019.

POPPER, K. R. **The Logic of Scientific Discovery**. London: Routledge, 1959.

PRZEWORSKI, A. et al. **Democracy and development: Political Institutions and Material Well-Being in the World**. 1950- 1990. Cambridge: Cambridge University Press. 2000.

PUTNAM, R. **Comunidade e democracia: a experiência da Itália moderna**. Rio de Janeiro: Fundação Getúlio Vargas. 1996.

RAGIN, C. C. **The comparative method: moving beyond qualitative and quantitative strategies.** Berkeley: University of California Press. 1987.

_____. **Fuzzy-set Social Science**. Chicago: The University of Chicago Press. 2000.

REZENDE, F. C. Razões emergentes para a validade dos estudos de caso na ciência política comparada. **Rev. Bras. Ciênc. Polít.**, n. 6, p. 297-337, 2011. https://doi.org/10.1590/S0103-33522011000200012

_____. (Desvendando) A Dinâmica do Ajuste Inferencial nas Relações Internacionais (2000-2017). **Conexão Política**, v. 6, n. 1, p. 11-54, 2017.

RIHOUX, B.; LOBE, B. The case for qualitative comparative analysis (QCA): Adding leverage for thick cross-case comparison. **The Sage handbook of case-based methods**, p. 222-242, 2009.

ROHLFING, I. et al. A Reproduction Analysis of 106 Articles Using Qualitative Comparative Analysis, 2016–2018. **PS: Political Science & Politics***,* v. 54, n. 2, p. 292-296, 2021. https://doi.org/10.1017/S1049096520001717

RStudio Team. **RStudio: Integrated Development for R**. RStudio, PBC, Boston, MA. Disponível em: <http://www.rstudio.com/>. 2020.

SANDES FREITAS, V.; BIZARRO NETO, F. Qualitative Comparative Analysis (QCA): usos e aplicações do método. **Revista Política Hoje**, v. 24, n. 2, p. 103-117, 2015.

SANTOS, B. Í. L. O **emprego da capacidade cibernética nas operações militares em grandes eventos no Brasil:** emprego do centro de defesa cibernética nos jogos olímpicos de 2016. 2019. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/5382/1/Artigo%20Cienti%cc%81fico%20Bruno%20%c3%8dgaro%20esao.pdf. Acesso em: 10 de jan. de 2022.

SANTOS, M. L.; BOTELHO, J. C. A. O desafio do método e da política comparada no Brasil: uma experiência com ensino de QCA. **Agenda Política**, v. 6, n. 3, p. 132–162, 2018.

SÁTYRO, N. G. D.; D'ALBUQUERQUE, R. W. O que é um Estudo de Caso e quais as suas potencialidades. **Sociedade e Cultura**, v. 23, 2020.

SCHALLBRUCH, M.; SKIERKA, I. **Cybersecurity in Germany**. Springer EBooks. 2018.

SCHNEIDER, C. Realists and Idealists in QCA. **Political Analysis**, v. 26, n. 2, p. 246-254, 2018. https://doi.org/10.1017/pan.2017.45

SCHWARCZ, L. M. **Sobre o autoritarismo brasileiro**. Editora Companhia das Letras, 2019.

_____; STARLING, H. M. **Brasil: uma biografia: com novo pós-escrito**. Editora Companhia das Letras, 2015.

SKOCPOL, T. **States and social revolutions: A comparative analysis of France, Russia and China**. Cambridge University Press, 1979.

SHUGART, M. S.;CAREY, J. M. **Presidents and Assemblies: Constitutional Design and Electoral Dynamics**. Cambridge, Cambridge University Press, 1992.

SILVA, C. C. V.; PEREIRA, A. E. A Teoria de Securitização e a sua aplicação em artigos publicados em periódicos científicos. **Rev. Sociol. Polit.**, v. 27, n. 69, p. 1-20, 2019. http://dx.doi.org/10.1590/1678987319276907

SMALL, M. L. How to Conduct a Mixed Methods Study: Recent Trends in a Rapidly Growing Literature. **Annual Review of Sociology**, v. 37, p. 57-86, 2011. https://doi.org/10.1146/annurev.soc.012809.102657

SOARES, G. A. D. O calcanhar metodológico da ciência política no Brasil. **Sociologia, Problemas e Práticas**, v. 48, p. 27-52, 2005.

SOLAR, C. Cybersecurity and cyber defence in the emerging democracies. **Journal of Cyber Policy**, v. 5, n. 3, p. 392-412, 2020. https://doi.org/10.1080/23738871.2020.1820546

SOUZA, J. G.; SPINOLA, N. D. Medidas do Desenvolvimento Econômico. **Revista de Desenvolvimento Econômico - RDE**, v. 1, n. 36, p. 78-113, 2017. http://dx.doi.org/10.21452/rde.v1i36.4697

SOUZA JUNIOR, A. F.; STREIT, R. E. Segurança Cibernética: política brasileira e a experiência internacional. **Rev. Serv. Público**, v. 68, n. 1, p. 107-130, 2017. https://doi.org/10.21874/rsp.v68i1.864

STITILIS, D.; PAKUTINSKAS, P.; MALINAUSKAITE, I. EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. **Security Journal**, v. 30, p. 1151–1168, 2017. https://doi.org/10.1057/s41284-016-0083-9

SUMNER, A.; TRIBE, M. **International development studies: Theories and methods in research and practice**. SAGE Publications Ltd. 2008. https://www.doi.org/10.4135/9781446279397

TANNO, G. A Contribuição da Escola de Copenhague aos Estudos de Segurança Internacional. **Contexto Internacional**, v. 25, n. 1, p. 47-80. 2003. https://doi.org/10.1590/S0102-85292003000100002

TATAR, U. et al. **A Comparative Analysis of the National Cyber Security Strategies of Leading Nations**. 2014. Disponível em: https://fuse.franklin.edu/facstaff-pub/38/. Acesso em: 20 de mar. de 2021.

TROEIN, C.; ACAYO, G. **ITU Global Cybersecurity Index Overview**. WTO Cybersecurity Webinar. 2020. Disponível em: https://www.wto.org/english/res_e/reser_e/caroline_troein_and_grace_acoyo.pdf. Acesso em: 15 de maio de 2021.

UNIDIR. Cyber Policy Portal. 2021. Disponível em: <https://unidir.org/cpp/en/>. Acesso em: 13 de dez. de 2021.

VASIU, I.; VASIU, L. Cybersecurity as an Essential Sustainable Economic Development Factor. **European Journal of Sustainable Development**, v. 7, n. 4, p. 171-178, 2018. https://ssrn.com/abstract=3262527

VILAR-LOPES, G. Análise Exploratória da Securitização Militar do Ciberespaço nos EUA, Brasil e Canadá. **Security & Defense Studies Review**. v. 15, p. 116-149. 2014. Disponível em: https://www.williamjperrycenter.org/sites/default/files/publication_associated_files/SDSR%20Vol15.pdf. Acesso em: 20 de fev. de 2021.

VILAR-LOPES, G. **Relações internacionais cibernéticas (CiberRI):** uma defesa acadêmica a partir dos estudos de segurança internacional. Tese de Doutorado em Ciência Política, Departamento de Ciência Política, Universidade Federal de Pernambuco. 2016.

WATANABE, S. Strategic Analysis of Capacity Building for the Cyber Security of the United States in Asia. **Jurnal Asia Pacific Studies**, v. 4, n. 2, p. 100-111. 2020.

ZAVERUCHA, J. De FHC a Lula: A Militarização da Agência Brasileira de Inteligência. **Rev. Sociol. Polít.**, v. 16, n. 31, p. 177-195, 2008. https://doi.org/10.1590/S0104-44782008000200013

_____. A fragilidade do Ministério da Defesa brasileiro. **Revista de Sociologia e Política**, p. 107-121, 2005.

_____. Relações civil-militares no primeiro governo da transição brasileira: uma democracia tutelada. **Revista Brasileira de Ciências Sociais**, v. 9, n. 26, p. 162-178, 1994.

_____; et al. A Literatura sobre Relações civis-militares no Brasil (1964-2002): Uma síntese. **BIB-Revista Brasileira de Informação Bibliográfica em Ciências Sociais.** São Paulo, ANPOCS, 2003.

_____. Polícia, democracia, estado de direito e direitos humanos. **Revista Brasileira de Direito Constitucional**, v. 3, n. 1, p. 37-54, 2004.

_____. **Frágil democracia:** Collor, Itamar, FHC e os militares: (1990-1998). Editora Record, 2000.

APÊNDICE A - Cronograma da Pesquisa.

MÊS 2021/2022 ATIVIDADES	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**	**01**	**02**
Revisão da Literatura	X	X	X	X	X							
Levantamento dos dados					X	X	X	X	X	X		
Primeira versão da pesquisa						X						
Qualificação do projeto							**X**					
Análise dos dados								X	X	X		
Elaboração da dissertação	X	X	X	X	X	X	X	X	X	X	X	
Versão final da pesquisa											X	
Defesa da dissertação												**X**

Fonte: Base de dados da pesquisa. Elaboração do autor.

APÊNDICE B - Cronograma da Coleta de Dados.

ATIVIDADES - 2021	JUL	AGO	SET	OUT	NOV	DEZ
Comprometimento com a Segurança Cibernética	**X**					
Coletar os dados sobre os 35 países	X					
Tabular os dados sobre os 35 países	X					
Desenvolvimento Econômico	**X**					
Coletar os dados sobre os 35 países	X					
Tabular os dados sobre os 35 países	X					
Despesas Militares		**X**				
Coletar os dados sobre os 35 países		X				
Tabular os dados sobre os 35 países		X				
Militarização do Espaço Cibernético			**X**			
Coletar os dados sobre os 35 países			X			
Tabular os dados sobre os 35 países			X			
Tempo do Marco Jurídico-Institucional				**X**		
Coletar os dados sobre os 35 países				X		
Tabular os dados sobre os 35 países				X		
Securitização da Segurança Cibernética					**X**	

Coletar os dados sobre os 35 países					X	
Tabular os dados sobre os 35 países					X	
Eventos Raros						**X**
Coletar os dados sobre os 35 países						X
Tabular os dados sobre os 35 países						X

Fonte: Base de dados da pesquisa. Elaboração do autor.

APÊNDICE C - Despesas Militares como Percentual do PIB nos Países das Américas.

PAÍS	% DO PIB DESTINADO A DESPESAS MILITARES	TIPO[23]
ANTÍGUA E BARBUDA	N/A	0
ARGENTINA	0,745499%	0
BAHAMAS	N/A	0
BARBADOS	N/A	0
BELIZE	1,20473%	1
BOLÍVIA	1,5366%	1
BRASIL	1,50768%	1
CANADÁ	1,32576%	1
CHILE	1,85981%	1
COLÔMBIA	3,0697%	2
COSTA RICA	0%	0
CUBA	2,87621%	2
DOMINICA	N/A	0
EQUADOR	2,35189%	2
EL SALVADOR	1,13622%	1
ESTADOS UNIDOS DA AMÉRICA	3,31624%	2
GRANADA	N/A	0
GUATEMALA	0,348125%	0
GUIANA	1,59694%	1
HAITI	0,000856221%	0
HONDURAS	1,61625%	1
JAMAICA	1,34909%	1
MÉXICO	0,480084%	0

[23] A classificação dos países de acordo com as suas despesas militares ocorre desta forma: 0) N/A e < 1%; 1) 1% < X < 2%; 2) > 2%. Assim, os missing case e os países com despesas militares abaixo de 1% do PIB integram a primeira categoria (0). Em seguida, estão relacionados os países que possuem despesas militares entre 1% e 2% do PIB. Por último (2), estão representados os países com despesas militares acima de 2% do PIB.

NICARÁGUA	0,624072%	0
PANAMÁ	0%	0
PARAGUAI	0,925373%	0
PERU	1,17465%	1
REPÚBLICA DOMINICANA	0,730391%	0
SÃO CRISTÓVÃO E NÉVIS	N/A	0
SANTA LÚCIA	N/A	0
SÃO VICENTE E GRANADINAS	N/A	0
SURINAME	N/A	0
TRINDADE E TOBAGO	0,688%	0
URUGUAI	2,13395%	2
VENEZUELA	N/A	0

Fonte: Elaboração do autor a partir dos dados do Banco Mundial (2020)[24].

[24] Disponível em: https://datacatalog.worldbank.org/dataset/world-development-indicators. Acesso em: 27 set. 2021.

APÊNDICE D - O Índice de Desenvolvimento Humano nos Países das Américas - 2018.

PAÍS	IDH	TIPO[25]	CLASSIFICAÇÃO
ANTÍGUA E BARBUDA	0,776	Elevado (1)	74º Lugar
ARGENTINA	0,830	Muito Elevado (2)	48º Lugar
BAHAMAS	0,805	Muito Elevado (2)	60º Lugar
BARBADOS	0,813	Muito Elevado (2)	56º Lugar
BELIZE	0,720	Elevado (1)	103º Lugar
BOLÍVIA	0,703	Elevado (1)	114º Lugar
BRASIL	0,761	Elevado (1)	79º Lugar
CANADÁ	0,922	Muito Elevado (2)	13º Lugar
CHILE	0,847	Muito Elevado (2)	42º Lugar
COLÔMBIA	0,761	Elevado (1)	79º Lugar
COSTA RICA	0,794	Elevado (1)	68º Lugar
CUBA	0,778	Elevado (1)	72º Lugar
DOMINICA	0,724	Elevado (1)	98º Lugar
EQUADOR	0,758	Elevado (1)	85º Lugar
EL SALVADOR	0,667	Médio (0)	124º Lugar
ESTADOS UNIDOS DA AMÉRICA	0,920	Muito Elevado (2)	15º Lugar
GRANADA	0,763	Elevado (2)	78º Lugar
GUATEMALA	0,651	Médio (0)	126º Lugar
GUIANA	0,670	Médio (0)	123º Lugar
HAITI	0,503	Baixo (0)	169º Lugar
HONDURAS	0,623	Médio (0)	132º Lugar
JAMAICA	0,726	Elevado (1)	96º Lugar
MÉXICO	0,767	Elevado (1)	76º Lugar

[25] De acordo com o PNUD (2019), os valores do IDH são diferenciados a partir dos graus: 1) Muito Elevado (igual ou superior a 0,800); 2) Elevado (Entre 0,700 e 0,799); 3) Médio (Entre 0,550 e 0,699); e 4) Baixo (inferior a 0,550). Para a pesquisa, consideramos as classes “Baixo” e “Médio” como uma só categoria. Assim, chegamos a estes resultados: 0 - baixo ou médio IDH; 1 - IDH elevado; 2 - IDH muito elevado.

NICARÁGUA	0,651	Médio (0)	126º Lugar
PANAMÁ	0,795	Elevado (1)	67º Lugar
PARAGUAI	0,724	Elevado (1)	98º Lugar
PERU	0,759	Elevado (1)	82º Lugar
REPÚBLICA DOMINICANA	0,745	Elevado (1)	89º Lugar
SÃO CRISTÓVÃO E NÉVIS	0,777	Elevado (1)	73º Lugar
SANTA LÚCIA	0,745	Elevado (1)	89º Lugar
SÃO VICENTE E GRANADINAS	0,728	Elevado (1)	94º Lugar
SURINAME	0,724	Elevado (1)	98º Lugar
TRINDADE E TOBAGO	0,799	Elevado (1)	63º Lugar
URUGUAI	0,808	Muito Elevado (2)	57º Lugar
VENEZUELA	0,726	Elevado (1)	96º Lugar

Fonte: Elaboração do autor a partir dos dados do PNUD (2019).

APÊNDICE E - Ocorrência de Eventos Raros nos Países das Américas - 2006/2018.

PAÍS	EVENTOS RAROS	TIPO[26]
ANTÍGUA E BARBUDA	N/A	0
ARGENTINA	N/A	0
BAHAMAS	N/A	0
BARBADOS	N/A	0
BELIZE	N/A	0
BOLÍVIA	N/A	0
BRASIL	1) **October/2016:** Hackers gained control of a major Brazilian bank's Domain Name System addresses and seized the bank's entire online footprint for several hours.	1
CANADÁ	1) **June/2015:** Canada announced that it has experienced DDOS attacks against two government websites. The attacks, which took down the Canadian Security Intelligence Service (CSIS) and the general Canadian government website, Canada.ca also reportedly affected email, Internet access and IT services in the government. Anonymous has claimed responsibility, citing Canada's recently passed Anti-terrorism Act, 2015 as the reason behind the recent attack. 2) **February/2015:** Media reports say that Canada's Communication Security Establishment identified "Babar" and "EvilBunny" as malware developed for espionage purposes by the French government. Babar's primary function is to exfiltrate documents, but it can also log keystrokes, monitor a user's web history, intercept and record communications made via Skype and messenger programs. 3) **July/2014:** Canada's Foreign Minister asks his Chinese counterpart about PLA cyber espionage against the National Research Council, Canada' leading technology research agency.	2

[26] Cada caso é avaliado de acordo com a seguinte classificação: 0 - ausência de eventos raros no país; 1 - Presença de pelo menos um evento de alta significância no país; 2 - Mais de 2 eventos raros de alta significância no Estado. Essas informações foram coletadas no *report* do CSIS sobre eventos altamente significativos em Segurança Cibernética (2020).

	4) **January/2011:** The Canadian government reported a major cyberattack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the internet. Canadian sources attribute the attack to China.	
CHILE	1) **December/2018:** North Korean hackers targeted the Chilean interbank network after tricking an employee into installing malware over the course of a fake job interview.	1
COLÔMBIA	N/A	0
COSTA RICA	N/A	0
CUBA	N/A	0
DOMINICA	N/A	0
EQUADOR	N/A	0
EL SALVADOR	N/A	0
ESTADOS UNIDOS DA AMÉRICA	**More than 70 cases. Examples:** **1) April – October 2008**. A State Department cable made public by WikiLeaks reported that hackers successfully stole "50 megabytes of email messages and attached documents, as well as a complete list of usernames and passwords from an unspecified (U.S. government) agency." The cable said that at least some of the attacks originated from a Shanghai-based hacker group linked to the People's Liberation Army's Third Department. **2) July 2009**. Cyberattacks against websites in the United States and South Korea, including a number of government websites, were launched by unknown hackers. South Korea accused North Korea of being behind the attacks The denial of service attacks did not severely disrupt services but lasted for a number of days and generated a great deal of media attention. **3) December 2011**. U.S. Chamber of Commerce computer networks were completely penetrated for more than a year by hackers who, according to press reports, had ties to the	2

	People's Liberation Army. The Hackers had access to everything in Commerce's computers, including member company communications and industry positions on U.S. trade policy. **4) March 2012**. NASA's Inspector General reported that 13 APT attacks successfully compromised NASA computers in 2011. In one attack, intruders stole 150 user credentials that could be used to gain unauthorized access to NASA systems. Another attack at the Joint Propulsion Laboratory involving China-based IP let the intruders gain full access to key JPL systems and sensitive user accounts.	
GRANADA	N/A	0
GUATEMALA	N/A	0
GUIANA	N/A	0
HAITI	N/A	0
HONDURAS	N/A	0
JAMAICA	N/A	0
MÉXICO	N/A	0
NICARÁGUA	N/A	0
PANAMÁ	N/A	0
PARAGUAI	N/A	0
PERU	N/A	0
REPÚBLICA DOMINICANA	N/A	0
SÃO CRISTÓVÃO E NÉVIS	N/A	0
SANTA LÚCIA	N/A	0
SÃO VICENTE E GRANADINAS	N/A	0
SURINAME	N/A	0
TRINDADE E TOBAGO	N/A	0

URUGUAI	N/A	0
VENEZUELA	N/A	0

Fonte: Elaboração do autor a partir dos dados e relatório do CSIS (2020).

APÊNDICE F - Os Países das Américas e o Tempo do Marco Jurídico-Institucional.

PAÍS	LEI-REFERÊNCIA	ANO	TIPO[27]
ANTÍGUA E BARBUDA	Computer Misuse Act	2006	1
ARGENTINA	Law N. 26.388	2008	1
BAHAMAS	N/A	N/A	0
BARBADOS	Computer Misuse Act 2005-04	2005	1
BELIZE	Telecommunications Act, 2002 (No. 16 of 2002)	2002	2
BOLÍVIA	Criminal Code	2003	1
BRASIL	Law N. 12.965, Marco Civil da Internet	2014	1
CANADÁ	Personal Information Protection and Electronic Documents Act (PIPEDA)	2000	2
CHILE	Law No. 19.223	1993	2
COLÔMBIA	Criminal Code	2009	1
COSTA RICA	Penal Code, Law No. 4573	2001	2
CUBA	Agreement 6058-2007 (Revogada pelo DECRETO-LEY No. 370 de 2019)	2007	1
DOMINICA	N/A	N/A	0
EQUADOR	Law No. 2002-67	2002	2
EL SALVADOR	Special Law against Cybercrime and Related Offenses	2016	1
ESTADOS UNIDOS DA AMÉRICA	Computer Fraud and Abuse Act (18 USC 1030)	1986	2
GRANADA	Electronic Crimes Act	2013	1
GUATEMALA	Penal Code	1973	2
GUIANA	N/A	N/A	0
HAITI	N/A	N/A	0
HONDURAS	Penal Code (Decreto 144-83)	2017	1

[27] Os valores atribuídos aos países, segundo o tempo do marco jurídico-institucional, são: 0) não possui legislação; 1) entre 1 e 15 anos de marco jurídico-institucional; 2) 16 anos ou mais desde o marco jurídico-institucional.

JAMAICA	The Cybercrimes Act	2015	1
MÉXICO	Law on the Protection of Private Personal Data	2010	1
NICARÁGUA	N/A	N/A	0
PANAMÁ	Penal Code	2010	1
PARAGUAI	Penal Code	1997	2
PERU	Law N. 29733	2011	1
REPÚBLICA DOMINICANA	Law N. 53-07	2007	1
SÃO CRISTÓVÃO E NÉVIS	Electronic Crimes Act No. 27	2009	1
SANTA LÚCIA	Criminal Code	2005	1
SÃO VICENTE E GRANADINAS	Cybercrime Bill	2016	1
SURINAME	Telecommunications Facilities Act	2004	1
TRINDADE E TOBAGO	N/A	N/A	0
URUGUAI	Presidential Decree 452/009	2009	1
VENEZUELA	Special Law on Computer Crimes	2001	2

Fonte: Elaboração do autor a partir dos dados da UNIDIR e da OEA (2021).

APÊNDICE G - Os Países das Américas na Convenção de Budapeste.

PAÍS	RATIFICADO	ANO	CONVIDADO	TIPO[28]
ANTÍGUA E BARBUDA	NÃO	N/A	NÃO	0
ARGENTINA	SIM	2018	N/A	2
BAHAMAS	NÃO	N/A	NÃO	0
BARBADOS	NÃO	N/A	NÃO	0
BELIZE	NÃO	N/A	NÃO	0
BOLÍVIA	NÃO	N/A	NÃO	0
BRASIL	NÃO	N/A	SIM	1
CANADÁ	SIM	2015	N/A	2
CHILE	SIM	2017	N/A	2
COLÔMBIA	NÃO	N/A	SIM	1
COSTA RICA	SIM	2017	N/A	2
CUBA	NÃO	N/A	NÃO	0
DOMINICA	NÃO	N/A	NÃO	0
EQUADOR	NÃO	N/A	NÃO	0
EL SALVADOR	NÃO	N/A	NÃO	0
ESTADOS UNIDOS DA AMÉRICA	SIM	2006	N/A	2
GRANADA	NÃO	N/A	NÃO	0
GUATEMALA	NÃO	N/A	SIM	1
GUIANA	NÃO	N/A	NÃO	0
HAITI	NÃO	N/A	NÃO	0
HONDURAS	NÃO	N/A	NÃO	0
JAMAICA	NÃO	N/A	NÃO	0
MÉXICO	NÃO	N/A	SIM	1
NICARÁGUA	NÃO	N/A	NÃO	0

[28] Os valores atribuídos aos países, segundo a sua relação com a Convenção de Budapeste, são: 0 - não ratificou nem foi convidado; 1 - não ratificou mas foi convidado; 2 - ratificou e integra a Convenção.

PANAMÁ	SIM	2014	N/A	2
PARAGUAI	SIM	2018	N/A	2
PERU	NÃO	N/A	SIM	1
REPÚBLICA DOMINICANA	SIM	2013	N/A	2
SÃO CRISTÓVÃO E NÉVIS	NÃO	N/A	NÃO	0
SANTA LÚCIA	NÃO	N/A	NÃO	0
SÃO VICENTE E GRANADINAS	NÃO	N/A	NÃO	0
SURINAME	NÃO	N/A	NÃO	0
TRINDADE E TOBAGO	NÃO	N/A	SIM	1
URUGUAI	NÃO	N/A	NÃO	0
VENEZUELA	NÃO	N/A	NÃO	0

Fonte: Elaboração do autor a partir dos dados do Conselho da Europa (2021).

APÊNDICE H - Os Países das Américas e a Securitização da Segurança Cibernética.

PAÍS	ESTRATÉGIA NACIONAL	ANO	TIPO[29]
ANTÍGUA E BARBUDA	NÃO POSSUI	N/A	0
ARGENTINA	EM DESENVOLVIMENTO	N/A	1
BAHAMAS	EM DESENVOLVIMENTO	N/A	1
BARBADOS	EM DESENVOLVIMENTO	N/A	1
BELIZE	EM DESENVOLVIMENTO	N/A	1
BOLÍVIA	NÃO POSSUI	N/A	0
BRASIL	EM DESENVOLVIMENTO	N/A	1
CANADÁ	POSSUI	2018	2
CHILE	POSSUI	2017	2
COLÔMBIA	POSSUI	2016	2
COSTA RICA	POSSUI	2017	2
CUBA	NÃO POSSUI	N/A	0
DOMINICA	NÃO POSSUI	N/A	0
EQUADOR	EM DESENVOLVIMENTO	N/A	1
EL SALVADOR	NÃO POSSUI	N/A	0
ESTADOS UNIDOS DA AMÉRICA	POSSUI	2018	2
GRANADA	NÃO POSSUI	N/A	0
GUATEMALA	POSSUI	2018	2

[29] Os valores atribuídos aos países, segundo a classificação do Cyber Policy Portal (UNIDIR, 2021) e a análise documental, são: 0 - não possui estratégia nacional sobre Segurança Cibernética; 1 - não possui estratégia nacional sobre Segurança Cibernética, mas está desenvolvendo; 2 - possui estratégia nacional sobre Segurança Cibernética.

GUIANA	EM DESENVOLVIMENTO	N/A	1
HAITI	NÃO POSSUI	N/A	0
HONDURAS	NÃO POSSUI	N/A	0
JAMAICA	POSSUI	2015	2
MÉXICO	POSSUI	2017	2
NICARÁGUA	NÃO POSSUI	N/A	0
PANAMÁ	POSSUI	2013	2
PARAGUAI	POSSUI	2017	2
PERU	EM DESENVOLVIMENTO	N/A	1
REPÚBLICA DOMINICANA	POSSUI	2018	2
SÃO CRISTÓVÃO E NÉVIS	NÃO POSSUI	N/A	0
SANTA LÚCIA	NÃO POSSUI	N/A	0
SÃO VICENTE E GRANADINAS	NÃO POSSUI	N/A	0
SURINAME	EM DESENVOLVIMENTO	N/A	1
TRINDADE E TOBAGO	POSSUI	2013	2
URUGUAI	NÃO POSSUI	N/A	0
VENEZUELA	NÃO POSSUI	N/A	0

Fonte: Elaboração do autor a partir dos dados do Report (2021).

APÊNDICE I - Os Países das Américas e a Militarização da Segurança Cibernética.

PAÍS	SETOR CIBERNÉTICO MILITARIZADO?	RESPONSÁVEL	TIPO[30]
ANTÍGUA E BARBUDA	NÃO	Ministry of Information, Broadcasting, Telecommunications & Information Technology	0
ARGENTINA	NÃO	Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad	0
BAHAMAS	SIM	Ministry of National Security	1
BARBADOS	NÃO	Telecommunications Unit	0
BELIZE	NÃO	Central Information Technology Office	0
BOLÍVIA	NÃO	El Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB)	0
BRASIL	SIM	Comando de Defesa Cibernética, ComDCiber (Cyber Defense Command)	1
CANADÁ	NÃO	Canadian Centre for Cyber Security	0
CHILE	NÃO	Interministerial Committee on Cyber Security	0

[30] Os valores atribuídos aos países, segundo a classificação da UNIDIR e a análise documental, são: 0 - não possui um setor cibernético militarizado, ou seja, a agência responsável pelo setor não é de caráter militar; 1 - o setor cibernético do país é militarizado, estando sob responsabilidade institucional dos militares.

COLÔMBIA	SIM	Commander, Joint Cyber Command	1
COSTA RICA	NÃO	Ministry of Science, Technology and Telecommunications (MICITT)	0
CUBA	NÃO	Centre of Cyberspace Security (Centro de Seguridad del Ciberespacio)	0
DOMINICA	NÃO	Ministry of Information, Science, Telecommunications and Technology	0
EQUADOR	NÃO	Ministry of Telecommunications and the Information Society	0
EL SALVADOR	NÃO	Dirección de Informática y Desarrollo Tecnológico - Ministry of Justice and Public Security	0
ESTADOS UNIDOS DA AMÉRICA	NÃO	Cybersecurity and Infrastructure Security Agency (CISA)	0
GRANADA	NÃO	ICT Unit, Ministry of Communications, Works, Physical Development, Public Utilities, ICT & Community Development	0
GUATEMALA	NÃO	Ministry of the Interior	0
GUIANA	NÃO	CIRT.GY - Ministry of Public Security	0
		Conseil National des	

HAITI	NÃO	Télécommunications (CONATEL)	0
HONDURAS	NÃO	Comisión Nacional de Telecomunicaciones (CONATEL)	0
JAMAICA	NÃO	Information Communication Technology Division	0
MÉXICO	NÃO	Inter-secretarial Commission for the Development of Electronic Government (CIDGE)	0
NICARÁGUA	NÃO	El Consejo Nicarageense de Ciencia y Tecnología	0
PANAMÁ	NÃO	National Authority for Government Innovation	0
PARAGUAI	NÃO	Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICS)	0
PERU	NÃO	National Office of Electronic Government and Information Technology	0
REPÚBLICA DOMINICANA	NÃO	Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología	0
SÃO CRISTÓVÃO E NÉVIS	NÃO	National Telecommunications Regulatory Commission	0

SANTA LÚCIA	NÃO	National Information Communications and Technology Office	0
SÃO VICENTE E GRANADINAS	NÃO	Ministry of Finance, Economic Planning and Information Technology	0
SURINAME	NÃO	Central Intelligence and Security Agency (CIVD)	0
TRINDADE E TOBAGO	NÃO	Trinidad and Tobago Cyber Security Agency	0
URUGUAI	NÃO	La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)	0
VENEZUELA	NÃO	Ministry of Popular Power for University Education, Science and Technology	0

Fonte: Elaboração do autor a partir dos dados do Report (2021).

APÊNDICE J - Código da Pesquisa no RMarkdown[31].

````
---

title: "Base de Dados - Dissertação"

output: html_document

author: Renato Victor Lira Brito

---


```{r setup, include=FALSE}

knitr::opts_chunk$set(echo = TRUE, warning = F)

```


```{r}

library(poliscidata)


library(tidyverse)

```


```{r}

PAÍS <- c("Estados Unidos da América", "Canadá", "Uruguai",

          "México", "Paraguai", "Brasil", "Colômbia", "Cuba",

          "Chile", "República Dominicana", "Jamaica", "Argentina",

          "Peru", "Panamá", "Equador", "Venezuela", "Guatemala",
````

[31] Disponível em: https://rmarkdown.rstudio.com/. Acesso em: 12 de dez. de 2021.
````

"Antígua e Barbuda", "Costa Rica", "Trindade e Tobago", "Barbados", "São Vicente e Granadinas", "Bahamas", "Granada", "Bolívia", "Guiana", "Nicarágua", "Belize", "El Salvador", "Suriname", "Santa Lúcia", "São Cristóvão e Névis", "Haiti", "Honduras", "Dominica")

SIGLA <- c("EUA", "CAN", "URU", "MEX", "PAR", "BRA", "COL", "CUB", "CHI", "DOM", "JAM", "ARG", "PER", "PAN", "ECU", "VEN", "GUA", "ANT", "CRC", "TRI", "BAR", "VIN", "BAH", "GRN", "BOL", "GUY", "NCA", "BIZ", "ESA", "SUR", "LCA", "SKN", "HAI", "HON", "DMA")

RANQUE_REGIONAL <- c(1, 2, 3, 4, 5,

6, 7, 8, 9, 10,

11, 11, 12, 13,

14, 15, 16, 17,

18, 19, 20, 21,

22, 23, 24, 25,

26, 26, 27, 28,

29, 30, 31, 32,

33)

RANQUE_GLOBAL <- c(2, 9, 51, 63, 66, 70, 73, 81, 83, 92, 94, 94, 95, 97, 98, 99, 112, 113, 115, 123, 127, 129, 133, 134, 135, 138, 140, 140, 142, 144, 149, 157, 164, 165, 172)

PONTUAÇÃO_GCI <- c(0.926, 0.892, 0.681, 0.629,

0.603, 0.577, 0.565, 0.481,

0.470, 0.430, 0.407, 0.407,

0.401, 0.369, 0.367, 0.354,

```
0.251, 0.247, 0.221, 0.188,

0.173, 0.169, 0.147, 0.143,

0.139, 0.132, 0.129, 0.129,

0.124, 0.110, 0.096, 0.065,

0.046, 0.044, 0.019)


PONTUAÇÃO_GCI_TRATADO <- c(1, 1, 1, 1, 1,

1, 1, 1, 1, 0,

0, 0, 0, 0, 0,

0, 0, 0, 0, 0,

0, 0, 0, 0, 0,

0, 0, 0, 0, 0,

0, 0, 0, 0, 0)


PONTUAÇÃO_IDH <- c(0.920, 0.922, 0.808, 0.767, 0.724,

0.761, 0.761, 0.778, 0.847, 0.745,


0.726, 0.830, 0.759, 0.795, 0.758,

0.726, 0.651, 0.776, 0.794, 0.799,


0.813, 0.728, 0.805, 0.763, 0.703,

0.670, 0.651, 0.720, 0.667, 0.724,

0.745, 0.777, 0.503, 0.623, 0.724)
```

```
PONTUAÇÃO_IDH_TRATADO <- c(2, 2, 2, 1, 1,
                           1, 1, 1, 2, 1,
                           1, 2, 1, 1, 1,
                           1, 0, 1, 1, 1,
                           2, 1, 2, 2, 1,
                           0, 0, 1, 0, 1,
                           1, 1, 0, 0, 1)

PONTUAÇÃO_MILITARIZAÇÃO_TRATADO <- c("0", "0", "0", "0", "0",
                                     "1", "1", "0", "0", "0",
                                     "0", "0", "0", "0", "0",
                                     "0", "0", "0", "0", "0",
                                     "0", "0", "0", "0", "0",
                                     "0", "0", "0", "0", "0",
                                     "0", "0", "0", "0", "0")

PONTUAÇÃO_EVENTOS_RAROS_TRATADO <- c(2, 2, 0, 0, 0,
                                     1, 0, 0, 1, 0,
                                     0, 0, 0, 0, 0,
                                     0, 0, 0, 0, 0,
                                     0, 0, 0, 0, 0,
                                     0, 0, 0, 0, 0,
                                     0, 0, 0, 0, 0)
```

```
PONTUAÇÃO_TEMPO_DO_MARCO_JURIDICO_INSTITUCIONAL_TRATADO <- c(2, 2, 1, 1,
                                                            2, 1, 1, 1,
                                                            2, 1, 1, 1,
                                                            1, 1, 2, 2,
                                                            2, 1, 2, 0,
                                                            1, 1, 0, 1,
                                                            1, 0, 0, 2,
                                                            1, 1, 1, 1,
                                                            0, 1, 0)


PONTUAÇÃO_DESPESAS_MILITARES_TRATADO <- c(2, 1, 2, 0, 0,
                                          1, 2, 2, 1, 0,
                                          1, 0, 1, 0, 2,
                                          0, 0, 0, 0, 0,
                                          0, 0, 0, 0, 1,
                                          1, 0, 1, 1, 0,
                                          0, 0, 0, 1, 0)


PONTUAÇÃO_SECURITIZAÇÃO_TRATADO <- c(2, 2, 0, 2, 2,
                                     1, 2, 0, 2, 2,
                                     2, 1, 1, 2, 1,
                                     0, 2, 0, 2, 2,
                                     1, 0, 1, 0, 0,
                                     1, 0, 1, 0, 1,
```

0, 0, 0, 0, 0)

BANCO_GCI_2018 <- data.frame(PAÍS, SIGLA, RANQUE_REGIONAL, RANQUE_GLOBAL, PONTUAÇÃO_GCI, PONTUAÇÃO_GCI_TRATADO, PONTUAÇÃO_IDH, PONTUAÇÃO_IDH_TRATADO, PONTUAÇÃO_MILITARIZAÇÃO_TRATADO, PONTUAÇÃO_EVENTOS_RAROS_TRATADO, PONTUAÇÃO_TEMPO_DO_MARCO_JURIDICO_INSTITUCIONAL_TRATADO, PONTUAÇÃO_DESPESAS_MILITARES_TRATADO, PONTUAÇÃO_SECURITIZAÇÃO_TRATADO)

```

```{r}
teste_1 <- lm(PONTUAÇÃO_GCI ~ PONTUAÇÃO_DESPESAS_MILITARES_TRATADO, data = BANCO_GCI_2018)

summary(teste_1)
```

```{r}
teste_2 <- lm(PONTUAÇÃO_GCI ~ PONTUAÇÃO_SECURITIZAÇÃO_TRATADO, data = BANCO_GCI_2018)

summary(teste_2)
```

```{r}

teste_3 <- lm(PONTUAÇÃO_GCI ~
PONTUAÇÃO_TEMPO_DO_MARCO_JURIDICO_INSTITUCIONAL_TRATADO, data =
BANCO_GCI_2018)

summary(teste_3)

```

```{r}

teste_4 <- lm(PONTUAÇÃO_GCI ~ PONTUAÇÃO_EVENTOS_RAROS_TRATADO, data =
BANCO_GCI_2018)

summary(teste_4)

```

```{r}

teste_5 <- lm(PONTUAÇÃO_GCI ~ PONTUAÇÃO_MILITARIZAÇÃO_TRATADO, data =
BANCO_GCI_2018)

summary(teste_5)

```

```{r}

teste_6 <- lm(PONTUAÇÃO_GCI ~ PONTUAÇÃO_IDH, data = BANCO_GCI_2018)

summary(teste_6)

```
```

```{r}
teste_7 <- lm(PONTUAÇÃO_GCI ~ PONTUAÇÃO_IDH_TRATADO, data = BANCO_GCI_2018)

summary(teste_7)
```

```{r}
library(scales)
```

```{r}
ggplot(BANCO_GCI_2018,
aes(PONTUAÇÃO_TEMPO_DO_MARCO_JURIDICO_INSTITUCIONAL_TRATADO,
..count../sum(..count..) )) +
  geom_bar(na.rm = T) +
  scale_y_continuous(labels = percent) + labs(tittle = "Tempo do Marco Jurídico-Institucional - Américas",
       x = "0 = Marco Inexistente; 1 = Marco Recente; 2 = Marco antigo",
       y = "Distribuição dos Casos")
```

```{r}
```

```
ggplot(BANCO_GCI_2018, aes(PONTUAÇÃO_DESPESAS_MILITARES_TRATADO,
..count../sum(..count..) )) +
  geom_bar(na.rm = T) +
  scale_y_continuous(labels = percent) + labs(tittle = "Despesas Militares - Américas",
       x = "0 = N/A ou menos de 1% do PIB; 1 = Entre 1% e 2% do PIB; 2 = Mais de 2% do PIB",
       y = "Distribuição dos Casos")
```

```{r}
ggplot(BANCO_GCI_2018, aes(PONTUAÇÃO_SECURITIZAÇÃO_TRATADO,
..count../sum(..count..) )) +
  geom_bar(na.rm = T) +
  scale_y_continuous(labels = percent) + labs(tittle = "Securitização - Américas",
       x = "0 = Não Securitizado; 1 = Em Securitização; 2 = Securitizado",
       y = "Distribuição dos Casos")
```

```{r}
ggplot(BANCO_GCI_2018, aes(PONTUAÇÃO_IDH_TRATADO, ..count../sum(..count..) )) +
  geom_bar(na.rm = T) +
  scale_y_continuous(labels = percent) + labs(tittle = "Índice de Desenvolvimento Humano -
Américas",
       x = "0 = Baixo ou Médio; 1 = Elevado; 2 = Muito Elevado",
       y = "Distribuição dos Casos")
```

```{r}
ggplot(BANCO_GCI_2018, aes(PONTUAÇÃO_MILITARIZAÇÃO_TRATADO,
..count../sum(..count..) )) +
  geom_bar(na.rm = T) +
  scale_y_continuous(labels = percent) + labs(tittle = "Militarização - Américas",
       x = "0 = Não Militarizado; 1 = Militarizado",
       y = "Distribuição dos Casos")
```

```{r}
ggplot(BANCO_GCI_2018, aes(PONTUAÇÃO_EVENTOS_RAROS_TRATADO,
..count../sum(..count..) )) +
  geom_bar(na.rm = T) +
  scale_y_continuous(labels = percent) + labs(tittle = "Eventos Raros - Américas",
       x = "0 = Ausência de Eventos Raros; 1 = Evento Isolado; 2 = Presença de Eventos Raros",
       y = "Distribuição dos Casos")
```

```{r}
library(QCApro)
help("QCApro")
```

```{r}
```

```
tabela_verdade <- truthTable(BANCO_GCI_2018, outcome = "PONTUAÇÃO_GCI_TRATADO",
neg.out = FALSE, exo.facs = c("PONTUAÇÃO_IDH_TRATADO",
"PONTUAÇÃO_MILITARIZAÇÃO_TRATADO",
"PONTUAÇÃO_EVENTOS_RAROS_TRATADO",
"PONTUAÇÃO_TEMPO_DO_MARCO_JURIDICO_INSTITUCIONAL_TRATADO",
"PONTUAÇÃO_DESPESAS_MILITARES_TRATADO",
"PONTUAÇÃO_SECURITIZAÇÃO_TRATADO"),

        n.cut = 1, incl.cut1 = 1, incl.cut0 = 1, complete = FALSE,

        show.cases = FALSE, decreasing = TRUE,

        inf.test = c("binom"), use.letters = FALSE)


print(tabela_verdade)
```

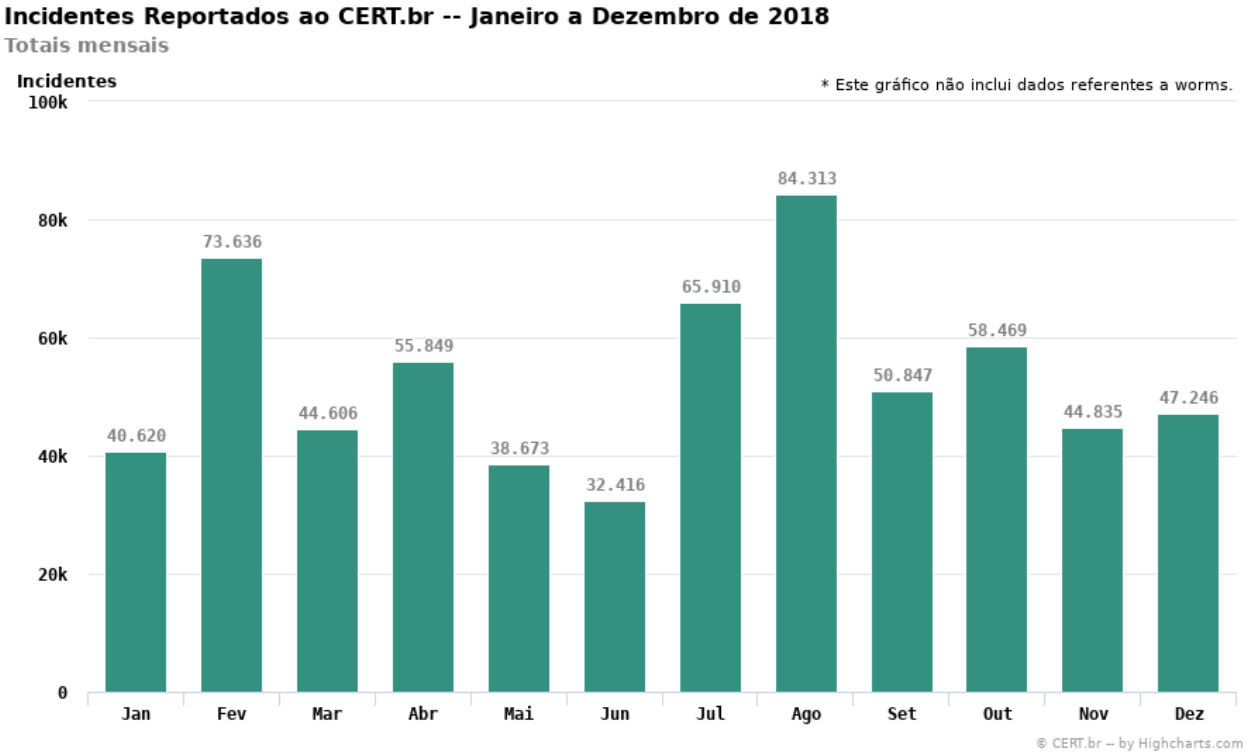
```{r}
ggplot(BANCO_GCI_2018, aes(PONTUAÇÃO_GCI, ..count../sum(..count..) )) +
  geom_bar(na.rm = T) +
  scale_y_continuous(labels = percent)
```

```{r}
cor.test(BANCO_GCI_2018$PONTUAÇÃO_GCI, BANCO_GCI_2018$PONTUAÇÃO_IDH)
```

```{r}
ggplot(BANCO_GCI_2018, aes(PONTUAÇÃO_GCI, PONTUAÇÃO_IDH)) +
```

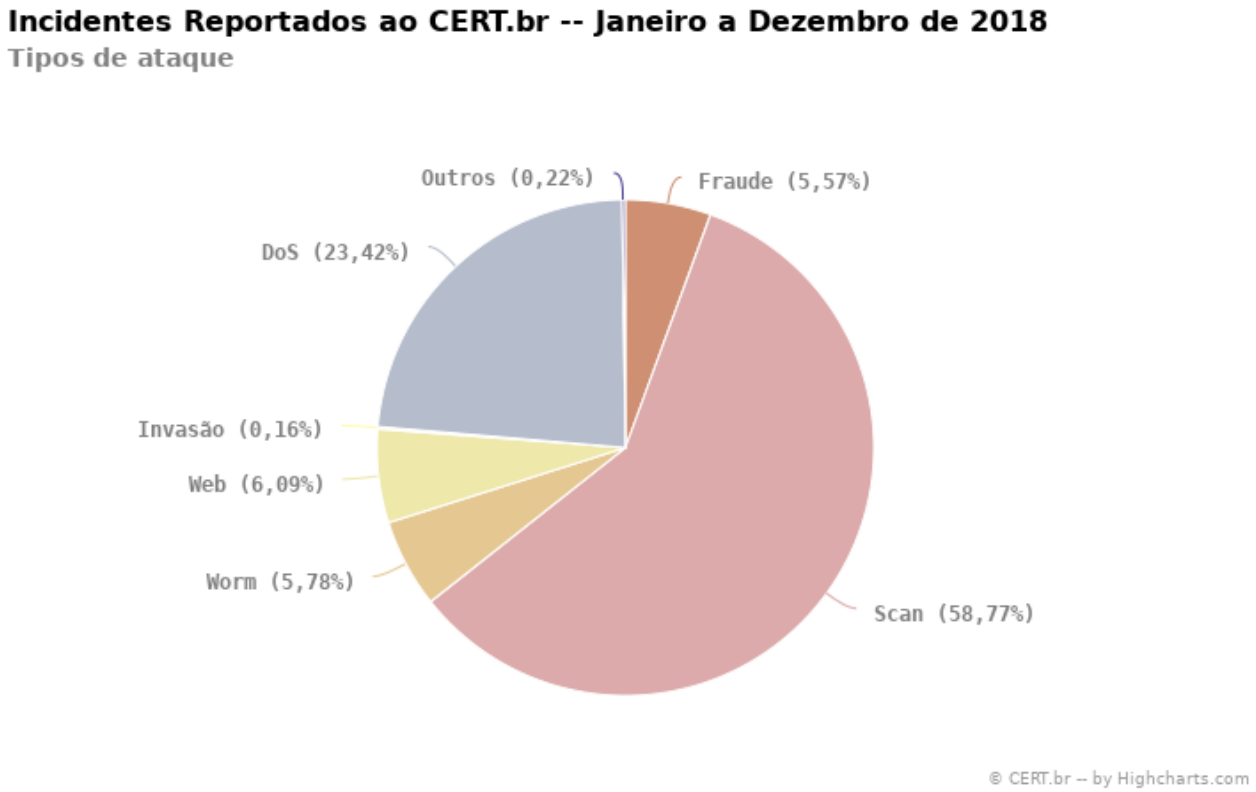
```
geom_jitter() +
  labs(x = "GCI",
y = "IDH")
```

ANEXO A - Incidentes Reportados Mensalmente no Brasil - 2018.



Fonte: CERT.br (2022).

ANEXO B - Tipos de Incidentes Reportados no Brasil - 2018.



Fonte: CERT.br (2022)[32].

[32] Legenda (CERT.br, 2022):
Worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede. *DoS* -- *Denial of Service*: notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede. Invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede. *Web*: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet. *Scan*: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador. Fraude: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem. Outros: notificações de incidentes que não se enquadram nas categorias anteriores.

ANEXO C - Tabela Verdade no Tosmana[33].

Truth Table:

v1: SECURITIZAÇÃO v2: DESPESAS MILITARES
v3: EVENTOS RAROS v4: TEMPO
v5: MILITARIZAÇÃO v6: DESENVOLVIMENTO

O: GCI id: PAÍS

v1	v2	v3	v4	v5	v6	O	id
0	0	0	0	0	0	0	Nicarágua, Haiti
0	0	0	0	0	1	0	Dominica
0	0	0	1	0	1	0	Antígua e Barbuda, São Vicente e Granadinas, Santa Lúcia, São Cristóvão e Névis
0	0	0	1	0	2	0	Granada
0	0	0	2	0	1	0	Venezuela
0	1	0	1	0	0	0	El Salvador, Honduras
0	1	0	1	0	1	0	Bolívia
0	1	0	1	0	2	1	Uruguai
0	2	0	1	0	1	1	Cuba
1	0	0	0	1	2	0	Bahamas
1	0	0	1	0	1	0	Suriname
1	0	0	1	0	2	0	Argentina, Barbados
1	1	0	0	0	0	0	Guiana
1	1	0	1	0	1	0	Peru
1	1	0	2	0	1	0	Belize
1	1	1	1	1	1	1	Brasil
1	2	0	2	0	1	0	Equador
2	0	0	0	0	1	0	Trindade e Tobago
2	0	0	1	0	1	C	México(1), República Dominicana(0), Panamá(0)
2	0	0	2	0	0	0	Guatemala
2	0	0	2	0	1	C	Paraguai(1), Costa Rica(0)
2	1	0	1	0	1	0	Jamaica
2	1	1	2	0	2	1	Chile
2	1	2	2	0	2	1	Canadá
2	2	0	1	1	1	1	Colômbia
2	2	2	2	0	2	1	Estados Unidos

Created with Tosmana Version 1.61

Fonte: Elaboração do autor utilizando o Tosmana.

[33] Disponível em: https://www.tosmana.net/. Acesso em: 14 de dez. de 2021.

ANEXO D - Síntese da Minimização Lógica no Tosmana[34].

Result(s):

EVENTOS RAROS{1,2} + (Estados Unidos+Canadá+Brasil+Chile) SECURITIZAÇÃO{0,2}DESPESAS MILITARES{2} + (Estados Unidos+Colômbia+Cuba) DESPESAS MILITARES{1,2}DESENVOLVIMENTO{2} (Estados Unidos+Canadá+Uruguai+Chile)

EVENTOS RAROS{1,2} + (Estados Unidos+Canadá+Brasil+Chile) DESPESAS MILITARES{1,2}DESENVOLVIMENTO{2} + (Estados Unidos+Canadá+Uruguai+Chile) DESPESAS MILITARES{2}TEMPO{1} (Colômbia+Cuba)

SECURITIZAÇÃO{0,2}DESPESAS MILITARES{2} + (Estados Unidos+Colômbia+Cuba) DESPESAS MILITARES{1,2}MILITARIZAÇÃO{1} + (Brasil+Colômbia) DESPESAS MILITARES{1,2}DESENVOLVIMENTO{2} (Estados Unidos+Canadá+Uruguai+Chile)

SECURITIZAÇÃO{0,2}DESPESAS MILITARES{2} + (Estados Unidos+Colômbia+Cuba) DESPESAS MILITARES{1,2}DESENVOLVIMENTO{2} + (Estados Unidos+Canadá+Uruguai+Chile) TEMPO{1}MILITARIZAÇÃO{1} (Brasil+Colômbia)

SECURITIZAÇÃO{0,2}DESPESAS MILITARES{2} + (Estados Unidos+Colômbia+Cuba) DESPESAS MILITARES{1,2}DESENVOLVIMENTO{2} + (Estados Unidos+Canadá+Uruguai+Chile) MILITARIZAÇÃO{1}DESENVOLVIMENTO{1} (Brasil+Colômbia)

DESPESAS MILITARES{1,2}MILITARIZAÇÃO{1} + (Brasil+Colômbia) DESPESAS MILITARES{1,2}DESENVOLVIMENTO{2} + (Estados Unidos+Canadá+Uruguai+Chile) DESPESAS MILITARES{2}TEMPO{1} (Colômbia+Cuba)

DESPESAS MILITARES{1,2}DESENVOLVIMENTO{2} + (Estados Unidos+Canadá+Uruguai+Chile) DESPESAS MILITARES{2}TEMPO{1} + (Colômbia+Cuba) TEMPO{1}MILITARIZAÇÃO{1} (Brasil+Colômbia)

DESPESAS MILITARES{1,2}DESENVOLVIMENTO{2} + (Estados Unidos+Canadá+Uruguai+Chile) DESPESAS MILITARES{2}TEMPO{1} + (Colômbia+Cuba) MILITARIZAÇÃO{1}DESENVOLVIMENTO{1} (Brasil+Colômbia)

Fonte: Elaboração do autor a partir do Tosmana.

[34] Este é um resumo dos resultados da minimização lógica realizada pelo *software*. A disponibilização de todo o conteúdo aqui faria com que os elementos pós-textuais representassem parcela maior do que a dos elementos textuais. Disponível em: https://www.tosmana.net/. Acesso em: 14 de dez. de 2021.