O Paradoxo da Autossuficiência Digital na Política Externa e Defesa Cibernética Frente à Dependência Tecnológica no Brasil

Laura Neves Diniz

https://doi.org/10.1590/SciELOPreprints.17470

Submetido em: 2026-08-16
Postado em: 2026-08-18 (versão 1)
(AAAA-MM-DD)

O PARADOXO DA AUTOSSUFICIÊNCIA DIGITAL NA POLÍTICA EXTERNA E DEFESA CIBERNÉTICA FRENTE À DEPENDÊNCIA TECNOLÓGICA NO BRASIL

AUTOR/A 1, Laura Neves Diniz.
ORCID: https://orcid.org/0009-0006-5904-7382.
<laurand@id.uff.br>
Universidade Federal Fluminense. Rio de Janeiro, RJ, Brasil

RESUMO: O presente estudo insere-se na grande área de Estudos Estratégicos e Segurança Internacional, com foco na defesa do ciberespaço. Embora a literatura debata amplamente a securitização cibernética, existe uma escassez de análises sobre as fricções institucionais geradas pela imposição de lógicas analógicas de defesa militar a infraestruturas digitais civis, especialmente em países periféricos. A pesquisa preenche essa lacuna ao investigar o caso brasileiro, contrapondo o modelo de governança centralizada de defesa à realidade técnica e de mercado do setor privado. O objetivo é analisar de que maneira o modelo da grande estratégia brasileira, pautado pela busca retórica de "autonomia estratégica" e pela militarização institucional, impacta a proteção prática das infraestruturas críticas operadas pela iniciativa civil. Como metodologia, utiliza-se o rastreamento de processos (process tracing) associado à análise documental sistemática. A coleta de dados baseou-se em fontes primárias de alto nível, incluindo as edições de 2025 da Política e da Estratégia Nacional de Defesa, o Livro Branco de Defesa Nacional (2024), a Doutrina Militar de Defesa Cibernética (2023) e atas do Comitê Nacional de Segurança de Infraestruturas Críticas. Os resultados evidenciam uma falha estrutural de concepção na qual, ao delegar o controle das redes ao estamento militar, o Estado gera um severo descompasso operacional com as corporações que sustentam serviços essenciais, quadro agravado pela crônica dependência tecnológica estrangeira. Conclui-se que a militarização da governança e a estratégia isolada de autossuficiência resultam, paradoxalmente, em maior vulnerabilidade sistêmica, demandando uma transição urgente para um modelo cooperativo civil-militar-privado.

Palavras-chave: estudos estratégicos, defesa cibernética, infraestruturas críticas, militarização, governança da internet.

THE PARADOX OF DIGITAL SELF-SUFFICIENCY IN FOREIGN POLICY AND CYBER DEFENSE AMID TECHNOLOGICAL DEPENDENCE IN BRAZIL

ABSTRACT: This study falls within the broad area of Strategic Studies and International Security, focusing on cyberspace defense. Although the literature widely debates cyber securitization, there is a scarcity of analyses on the institutional frictions generated by imposing analog military defense logics on civilian digital infrastructures, especially in peripheral countries. This research fills this gap by investigating the Brazilian case, contrasting the centralized defense governance model with the technical and market reality of the private sector. The objective is to analyze how the Brazilian grand strategy model, guided by the rhetorical pursuit of "strategic autonomy" and institutional militarization, impacts the practical protection of critical infrastructures operated by the civilian sector. As for methodology, the process tracing method is used in association with systematic documentary analysis. Data collection was based on high-level primary sources, including the 2025 editions of the National Defense Policy and Strategy, the National Defense White Paper (2024), the Military Cyber

Defense Doctrine (2023), and minutes from the National Critical Infrastructure Security Committee. The results show a structural design flaw: by delegating network control to the military establishment, the State generates a severe operational mismatch with the corporations that sustain essential services, a scenario worsened by chronic foreign technological dependence. It is concluded that the militarization of governance and the isolated strategy of self-sufficiency paradoxically result in greater systemic vulnerability, demanding an urgent transition to a cooperative civil-military-private model.

Keywords: strategic studies, cyber defense, critical infrastructures, militarization, internet governance.

INTRODUÇÃO

O advento do ciberespaço transformou radicalmente a matriz de segurança internacional, instaurando um domínio de conflito fluido, assimétrico e transfronteiriço. Diferente dos espaços físicos tradicionais, a arquitetura digital permeia e sustenta as funções vitais das sociedades contemporâneas, convertendo as infraestruturas críticas — redes de telecomunicações, geração de energia, sistemas financeiros e modais de transporte — em alvos estratégicos primordiais. Nesse novo cenário, a capacidade de um Estado proteger suas infraestruturas cibernéticas contra interrupções ou ataques torna-se um pressuposto elementar para a garantia da soberania e da estabilidade nacional.

A despeito do reconhecimento dessa urgência, a abordagem adotada pelo Estado brasileiro revela um profundo descompasso estratégico. A ascensão tecnológica expôs uma tensão entre a retórica governamental, que projeta uma postura de autonomia e inserção internacional vigorosa, e as severas limitações práticas na governança e na proteção das redes nacionais. O Brasil busca gerir a complexidade do ciberespaço valendo-se de concepções de defesa gestadas em paradigmas analógicos e em dinâmicas de segurança territorial, ignorando a natureza descentralizada do ambiente digital e a escassez material do próprio país.

Diante desse cenário, a questão central que orienta este artigo é: de que maneira o modelo adotado pela grande estratégia de defesa cibernética brasileira, pautado por ideais de autossuficiência e pelo controle burocrático-militar, impacta a proteção prática das infraestruturas críticas nacionais operadas pela iniciativa civil?

Para responder a essa indagação, este trabalho defende a tese de que a grande estratégia brasileira para o ciberespaço apresenta uma falha estrutural de concepção. Argumenta-se que a busca do Estado pela "autonomia estratégica" por intermédio da centralização e da militarização institucional da defesa digital é operacionalmente incompatível com a realidade das infraestruturas críticas. Essa

inadequação ocorre porque tais estruturas são majoritariamente de propriedade e operação do setor civil e privado, além de dependerem substancialmente de tecnologias estrangeiras. Consequentemente, o modelo centralizador gera fricções e assimetrias de governança que, de forma paradoxal, enfraquecem a resiliência sistêmica nacional frente às ameaças digitais.

A investigação ampara-se metodologicamente no rastreamento de processos (*process tracing*), essencial para elucidar mecanismos causais por trás de decisões políticas (Tannenwald, 2015; Voltolini, 2017). Para examinar empiricamente esse processo, conduz-se uma análise documental sistemática dos pilares estratégicos brasileiros — edições de 2025 da Política e da Estratégia Nacional de Defesa, Livro Branco de Defesa Nacional (2024), Doutrina Militar de Defesa Cibernética (2023) e atas do Comitê Nacional de Segurança de Infraestruturas Críticas. A combinação desses métodos possibilita mapear os passos intermediários entre as intenções discursivas do Estado e os gargalos institucionais práticos na governança da rede (Vennesson, 2008).

1. A "GRANDE ESTRATÉGIA" BRASILEIRA E A RETÓRICA DA AUTONOMIA ESTRATÉGICA

1.1. A Ontologia Política da Defesa e a Tradição Estratégica Brasileira

No caso brasileiro, o pensamento estratégico e geopolítico foi historicamente monopolizado pelo estamento militar e orientado por imperativos de controle do espaço físico. A matriz clássica estruturou-se a partir do receio histórico da dispersão territorial, buscando integrar um "máximo absoluto de base física com um mínimo absoluto de circulação social e política" (Silva, 1981, p. 7). A necessidade de garantir a unidade continental consolidou uma herança centralizadora em que a segurança nacional é compreendida primariamente pela obstrução de fronteiras e pela centralização decisória no Poder Executivo (Silva, 1981).

Essa concepção geoestratégica analógica arraigou-se profundamente na burocracia de defesa. Consequentemente, ao ser confrontado com novos domínios operacionais, o reflexo imediato do Estado é tentar enquadrar e submeter o ciberespaço — espaço de natureza inerentemente fluida e descentralizada — utilizando a mesma lógica de controle territorial e hierárquico que historicamente orientou sua formação.

Paralelamente à herança centralizadora, a grande estratégia brasileira é caracterizada por uma busca contínua, ainda que por vezes estritamente retórica, por uma autonomia de inserção no sistema

internacional. Durante grande parte da sua história diplomática, o Brasil adotou uma postura marcada pelo pacifismo e pela baixa securitização de ameaças externas, o que resultou em trajetórias institucionais corporativas e isoladas entre o Ministério das Relações Exteriores e as Forças Armadas (Coutinho, 2018). No entanto, a partir da primeira década dos anos 2000, observou-se uma inflexão na política externa e de defesa, promovida por uma convergência ideológica de viés nacional-desenvolvimentista entre diplomatas e grupos militares. Essa aproximação institucional resultou no entendimento político de que o país precisaria se instrumentalizar material e tecnologicamente para respaldar sua projeção diplomática autônoma e reduzir assimetrias frente às potências globais (Coutinho, 2018).

Essa convergência materializou-se politicamente na priorização da defesa e na elaboração de documentos orientadores de alto nível, com destaque para a Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END). Tais documentos alçaram a autonomia tecnológica, o fortalecimento da base industrial e a nacionalização dos meios operacionais ao patamar de pilares inegociáveis para o exercício da soberania (Coutinho, 2018).

Contudo, a articulação prática dessa grande estratégia demonstrou ser sistemicamente frágil. Baseada mais em afinidades políticas conjunturais do que em reformas estruturais duradouras do aparelho estatal, a busca pela autonomia de inserção continuou refém de flutuações e crises internas (Coutinho, 2018). Essa limitação material e estrutural do Estado torna-se o epicentro de um grave descompasso estratégico quando o Brasil tenta impor sua tradição de controle burocrático e sua aspiração declaratória de autossuficiência ao ambiente cibernético, um domínio que exige meios e capacidades que a estrutura estatal, isoladamente, não possui.

1.2. A Securitização do Ciberespaço e as Novas Ameaças

A transição do ciberespaço de um domínio eminentemente tecnológico e civil para uma arena central de defesa estatal exige, antes de sua efetiva militarização, um profundo processo político de securitização. Conforme postula a Teoria da Securitização, desenvolvida pela Escola de Copenhague, as ameaças à segurança não se configuram apenas como dados objetivos, mas sim como construções forjadas por atores políticos que enquadram determinados problemas como ameaças existenciais, justificando, assim, a adoção de medidas excepcionais (Azubuike, 2023, p. 108). No ambiente digital,

os governos passam a utilizar a retórica da segurança cibernética para priorizar políticas e consolidar o controle, enquadrando os ciberataques não apenas como falhas técnicas, mas como riscos diretos à estabilidade e à sobrevivência do Estado (Azubuike, 2023).

Esse movimento discursivo de securitização encontra forte respaldo material na profunda alteração da morfologia dos conflitos contemporâneos. Na chamada Era da Informação, o modelo tradicional de campo de batalha linear e contíguo é substituído por um ambiente difuso, não contíguo e irrestrito (Visacro, 2018). A guerra contemporânea afasta-se da dinâmica clássica de "aproximar e destruir" forças regulares na linha de frente e passa a operar sob a lógica da Guerra Híbrida, caracterizada pela fusão de métodos ortodoxos de combate e táticas irregulares ou subversivas, aplicadas de forma simultânea e encoberta (Cazumba, 2025). Esse novo paradigma frequentemente atua em zonas cinzentas, diluindo as fronteiras jurídicas e temporais tradicionais entre o estado de paz e o estado de guerra (Cazumba, 2025).

Nesse cenário de assimetria, adversários estatais e não estatais evitam o confronto militar simétrico tradicional e transferem o vetor do conflito diretamente para o interior do tecido social do Estado vitimado (Cazumba, 2025). O objetivo das ações estratégicas desloca-se da destruição de tropas no terreno para a paralisação do campo psicossocial e o atingimento da infraestrutura logística e de comando da retaguarda civil (Visacro, 2018). As novas ameaças utilizam a interconexão das redes e a guerra informacional para falsificar acontecimentos, promover a desinformação e degradar a governabilidade de dentro para fora, prescindindo do uso exclusivo da violência militar convencional (Cazumba, 2025, p. 172-173).

É precisamente a constatação dessa vulnerabilidade extrema que serve de alicerce para a securitização do ciberespaço pelo Estado. Sob o impacto dessas transformações, a proteção da integridade estritamente territorial torna-se insuficiente frente ao que se configura como uma ameaça à soberania não territorial do país (Visacro, 2018). Ao reconhecer que os ciberataques possuem a capacidade de paralisar a logística nacional e comprometer infraestruturas críticas sem que haja o disparo de um único projétil cinético (Cazumba, 2025), o Estado eleva o ciberespaço à categoria de ameaça à segurança nacional. Essa formulação política, portanto, cumpre a função de legitimar institucionalmente o passo seguinte do aparelho estatal: a absorção da governança e da proteção das redes civis e privadas pela lógica de controle da burocracia militar.

1.3. A "Soberania por Autossuficiência" nos Documentos Estratégicos (PND, END e Doutrina)

A securitização do ciberespaço consolidou-se normativamente na Política Nacional de Defesa (PND) e na Estratégia Nacional de Defesa (END). Evoluindo de menções incipientes na PND de 2005, o tema ingressou como área estratégica na END de 2008 e, entre 2012 e 2020, passou a novo domínio operacional de defesa. Esse processo culmina nas edições aprovadas em 2025, nas quais o Estado equipara o ciberespaço aos setores nuclear e espacial, atribuindo ao Exército Brasileiro a sua coordenação e desenvolvimento (Brasil, 2025, p. 21). Ao diagnosticar os ciberataques como riscos a "segmentos vitais", a atual PND estabelece a segurança digital como essencial para mitigar a "possibilidade de uma desordem social" (Brasil, 2025, p. 5, 7). Observa-se, portanto, a delegação estritamente militar para a proteção de estruturas civis, com a END exigindo a garantia da "resiliência das infraestruturas críticas nacionais" em áreas prioritárias como comunicações, energia e finanças (Brasil, 2025, p. 12, 23).

Para fazer frente a essa ameaça, a grande estratégia nacional articula sua resposta através do paradigma da "Soberania por Autossuficiência". A PND assevera que "uma base industrial e tecnológica forte constitui fator de autonomia estratégica" e preceitua a autonomia tecnológica nacional como pressuposto de sua concepção política (Brasil, 2025, p. 5). De modo complementar, a END determina que eventuais parcerias internacionais devem ter como premissa "o fortalecimento das capacitações autônomas nacionais", visando à "redução de dependência externa" e à diminuição drástica das aquisições de bens e serviços de defesa no exterior (Brasil, 2025, p. 12, 14). Esse arcabouço documental revela a tentativa do Estado de replicar, no ciberespaço, a mesma concepção geoestratégica de controle soberano integral e de desenvolvimento endógeno que historicamente pautou sua defesa territorial.

Essa visão materializa-se na arquitetura institucional estabelecida pela Doutrina Militar de Defesa Cibernética (Brasil, 2023). O documento oficializa uma separação rígida de competências no espaço cibernético nacional, dividindo-o em níveis de decisão. O "Nível Político" é focado na Segurança Cibernética, sob a coordenação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), cuja atuação abrange a Administração Pública Federal e as infraestruturas críticas. Por sua vez, o "Nível Estratégico" institui a Defesa Cibernética, delegando o protagonismo

operacional ao Ministério da Defesa e às Forças Armadas, que assumem a responsabilidade de impedir ações hostis contra os interesses nacionais.

A referida Doutrina reconhece as dificuldades de imposição de limites neste novo domínio, listando como características inerentes à defesa cibernética a "vulnerabilidade das fronteiras geográficas" — visto que os agentes podem atuar de qualquer local, ignorando os limites físicos do Estado — e a "assimetria", que permite que atores com menores condições econômicas causem danos profundos (Brasil, 2023, p. 22-23). Paradoxalmente, mesmo assumindo formalmente o caráter difuso e assimétrico da ameaça, o modelo estatal adota um viés estratégico de defesa militarizada e hierarquizada para enfrentá-la.

A importação dessa lógica de controle absoluto e de autonomia autárquica para o planejamento cibernético apresenta severas limitações teóricas. Conforme aponta Figueiredo (2004), ao invés de produzirem categorias analíticas que respondam a projetos de nação autônomos e condizentes com suas bases materiais, os países periféricos tendem a desenvolver "estratégias reflexas".[1] Tais nações frequentemente importam doutrinas e lógicas de matriz unipolar e hegemônica que mascaram a sua própria realidade estrutural.

O Brasil projeta nos seus documentos norteadores (PND e END) um modelo de autonomia plena e de controle estatal do ciberespaço que espelha as posturas estratégicas de potências centrais. Na prática, essa pretensão esconde uma subordinação epistemológica: o Estado formula uma estratégia de defesa embasada em uma idealizada independência tecnológica e na securitização centralizada que, como será demonstrado na análise das infraestruturas críticas, não se sustenta frente à dependência industrial crônica do país e à configuração eminentemente civil e privada da rede.

2. A BUROCRACIA DA DEFESA: A MILITARIZAÇÃO DO CIBERESPAÇO

2.1. O Estado, a Tecnologia e a Burocracia como Centro Autônomo de Poder

[1] O conceito de "estratégias reflexas" foi cunhado para explicar como Estados periféricos, inseridos em uma estrutura de poder hegemônico (como a norte-americana), abdicam da formulação de estratégias que partam de sua própria realidade material, passando a importar, de forma subsidiária, as lógicas de defesa das potências centrais (Figueiredo, 2004, p. 259-260).

A securitização do ciberespaço e a formulação de uma grande estratégia voltada à autossuficiência demandam uma estrutura institucional capaz de operacionalizá-las. A decisão do Estado brasileiro de centralizar a defesa cibernética sob a tutela militar não deve ser compreendida como um mero arranjo técnico ou um desdobramento administrativo natural. Sob a ótica da teoria política, o aparelho de Estado e suas Forças Armadas operam como burocracias que desenvolvem dinâmicas e interesses próprios de manutenção e expansão de poder. Conforme aponta Kaplan (1974, p. 24), a burocracia governamental tende a se constituir como um "centro autônomo de decisões", que persegue objetivos próprios e atua para conservar e estender seu âmbito de atividade. Por meio de um crescimento acumulativo e autossustentado, a burocracia se serve do aparato estatal para ascender e ampliar sua autoridade (Kaplan, 1974). Ao absorver a competência cibernética, a burocracia militar legitima a sua própria relevância e assegura sua expansão institucional diante de um novo domínio estratégico.

Além da dinâmica expansionista da burocracia, a própria escolha do modelo institucional e das tecnologias de defesa carrega um peso intrinsecamente político. A partir de uma perspectiva gramsciana sobre o Estado, Carnoy (1988) demonstra que as estruturas administrativas e o desenvolvimento tecnológico não operam em um vácuo de neutralidade. As instituições estatais não são unicamente administrativas, mas encontram-se "imbuídas de um conteúdo político" que reflete a tentativa dos grupos dirigentes de expandir sua capacidade de reproduzir o controle sobre a sociedade (Carnoy, 1988, p. 96). Dessa forma, a alocação da responsabilidade de proteger o ciberespaço nacional nas mãos das Forças Armadas representa uma escolha fundamental de poder hegemônico. O aparato estatal atua como um instrumento de racionalização e controle que, sob a justificativa da segurança e da perícia técnica, acaba por excluir a sociedade civil e os agentes privados do núcleo do processo decisório (Carnoy, 1988).

A intersecção entre a busca por autonomia burocrática e o monopólio do conhecimento técnico consolida o fechamento institucional do setor. O domínio sobre a segurança das redes de informação passa a ser tratado como um "saber burocrático" rigorosamente monopolizado pelas instâncias de defesa (Kaplan, 1974). A burocracia legitima sua atuação ininterrupta por meio da alegação de ser a única detentora do conhecimento especializado (a engenharia militar e os sistemas de comando) necessário para gerir ameaças de alta complexidade.

Esse processo transforma decisões que afetam diretamente o desenvolvimento tecnológico e as infraestruturas de toda a nação em questões estritamente tecnocráticas e subordinadas à autoridade estatal (Carnoy, 1988, p. 147-148). Assim, a militarização do ciberespaço brasileiro revela-se não apenas como uma estratégia de defesa contra ameaças externas, mas como um movimento interno de consolidação de autoridade, no qual a burocracia expande suas prerrogativas ao impor a sua lógica de controle hierárquico sobre uma arena estruturalmente civil.

2.2. O Desenho Institucional: A Estruturação do SMDC e do ComDCiber

O impulso burocrático de centralização e expansão de poder do Estado materializou-se formalmente na arquitetura de defesa brasileira por meio de um arranjo institucional estritamente hierarquizado. Para fazer frente às novas vulnerabilidades, as Forças Armadas estruturaram o Sistema Militar de Defesa Cibernética (SMDC), concebido para operar no nível estratégico e assegurar o controle das ações no ambiente digital (Brasil, 2023).

No epicentro dessa estrutura encontra-se o Comando de Defesa Cibernética (ComDCiber). Definido como um comando operacional conjunto e permanentemente ativado, o ComDCiber atua como o "órgão central do SMDC" (Brasil, 2023, p. 28). A sua consolidação evidencia a transferência da gestão de uma ameaça difusa e em rede para o escopo de uma organização militar tradicional. A doutrina oficial estabelece que a missão deste comando é "planejar; orientar; coordenar; integrar; e executar atividades relacionadas ao desenvolvimento e à aplicação das capacidades cibernéticas" (Brasil, 2023, p. 33). O objetivo declarado dessa centralização é garantir o uso efetivo do espaço cibernético pela Defesa Nacional, de modo a impedir ou dificultar ações hostis contra os interesses do Estado (Brasil, 2023).

O desenho dessa burocracia de defesa revela, ainda, o protagonismo da Força Terrestre na condução da pauta. O Livro Branco de Defesa Nacional atesta que as diretrizes estratégicas do País atribuíram especificamente ao Exército Brasileiro a responsabilidade pela coordenação e pelo desenvolvimento do setor cibernético (Brasil, 2024). Sob a liderança do ComDCiber, a arquitetura institucional ramifica-se em subunidades especializadas, com destaque para o Centro de Ações Cibernéticas (CAC) — função exercida pelo Centro de Defesa Cibernética (CDCiber) —, focado na execução das operações, e a Escola Nacional de Defesa Cibernética (ENaDCiber), incumbida de

formar e qualificar os recursos humanos para o setor (Brasil, 2023; Brasil, 2024). Essa capilaridade estende-se também às demais Forças, que adequam suas estruturas singulares (como os núcleos cibernéticos da Marinha e da Aeronáutica) à coordenação central do SMDC (Brasil, 2023; Brasil, 2024).

A estruturação desse organograma corrobora a tese da militarização do ciberespaço no Brasil. O Estado respondeu à fluidez e à complexidade do ambiente digital enquadrando-o sob uma rígida cadeia de comando e controle. Ao tratar o espaço cibernético mediante a ativação permanente de um comando conjunto, com táticas, técnicas e procedimentos tipicamente voltados ao emprego em operações militares, a burocracia estatal impõe um modelo de segurança analógico a um domínio inerentemente descentralizado.

Essa formatação institucional atende aos interesses de expansão burocrática das Forças Armadas, que consolidam seu poder sobre o novo setor estratégico. Contudo, é exatamente essa arquitetura que fundamenta a base do descompasso estratégico nacional. Ao aplicar uma estrutura hierárquica e militarizada para gerir o ciberespaço, o Estado afasta a dinâmica colaborativa necessária para interagir com a natureza orgânica e privada das redes, pavimentando o caminho para os gargalos institucionais que acometem a proteção das infraestruturas críticas do país.

2.3. A Governança na Prática: O Controle Militar sobre as Infraestruturas Civis

A consolidação teórica e institucional da burocracia de defesa ganha contornos pragmáticos quando se analisa a governança das infraestruturas críticas nacionais. A aplicação do método de process tracing permite observar como o desenho militarizado transcende os limites dos sistemas estritamente operacionais de defesa e passa a tutelar esferas eminentemente civis. O principal locus dessa dinâmica é o Comitê Nacional de Segurança de Infraestruturas Críticas (CNSIC), estrutura governamental responsável por articular e deliberar sobre a proteção de serviços essenciais para a sociedade e a economia do país.

A análise documental primária evidencia a assimetria de poder e a ascendência da burocracia militar e de inteligência sobre esse comitê. A Ata da 1ª Reunião Ordinária do CNSIC, realizada no final de 2024, atesta que a presidência do colegiado é exercida e centralizada pelo Gabinete de Segurança Institucional (GSI) da Presidência da República (Brasil, 2024). Ademais, o documento

revela uma forte concentração de poder decisório nas mãos das instituições de defesa: dos quinze representantes com direito a voto no comitê, figuram de maneira proeminente o Ministério da Defesa e os Comandos da Marinha, do Exército e da Aeronáutica (Brasil, 2024, p. 1).

Esse arranjo institucional comprova que o Estado brasileiro delegou a órgãos de matriz militar e de inteligência a prerrogativa formal de ditar as diretrizes de proteção para infraestruturas operadas, quase em sua totalidade, pelo setor privado (tais como as redes de telecomunicações, as malhas de energia e o sistema financeiro). A efetividade prática desse modelo de controle centralizado é ilustrada pelo próprio governo em eventos estratégicos de grande magnitude. Conforme registrado no mesmo documento oficial, durante os preparativos e a execução da cúpula do G20, o GSI coordenou os Grupos Técnicos de Segurança de Infraestruturas Críticas, atuação considerada de "vital importância para a promoção da continuidade dos serviços de infraestruturas críticas" (Brasil, 2024, p. 2).

O episódio do G20 serve como uma evidência empírica robusta para a tese da militarização. Ele demonstra que o Estado securitizou a ameaça cibernética a tal ponto que transferiu para a coordenação de uma estrutura militarizada a garantia da prestação contínua de serviços civis (Brasil, 2024). Em vez de fomentar uma agência civil, descentralizada e multissetorial para liderar a governança da rede e dos serviços essenciais, a resposta estatal consagra a hierarquia de defesa no topo da cadeia de tomada de decisão.

Configura-se, assim, o fechamento do ciclo de militarização da governança cibernética no Brasil. A burocracia de defesa não apenas justificou sua expansão por meio da criação de comandos próprios, mas também assumiu institucionalmente a condução política da segurança das redes civis e privadas do país. Contudo, a imposição desse paradigma de controle estatal rígido sobre um ecossistema hiperconectado e movido pelas forças de mercado gera um descompasso estrutural severo. É exatamente a inviabilidade material e operacional desse modelo militarizado frente à realidade difusa do ciberespaço que será dissecada a seguir.

3. O DESCOMPASSO: INFRAESTRUTURAS CRÍTICAS, SETOR PRIVADO E FRICÇÃO INSTITUCIONAL

3.1. A Natureza Civil e a Interdependência da Infraestrutura Crítica

O ambiente cibernético difere radicalmente dos domínios operacionais clássicos (terra, mar, ar e espaço) em razão de sua materialidade e propriedade. Embora a retórica militar projete a defesa do ciberespaço como uma prerrogativa soberana, a governança prática da rede revela que o Estado não é o detentor do domínio que visa proteger (DeNardis e Raymond, 2013). A infraestrutura essencial que sustenta as operações digitais globais é construída, operada e mantida majoritariamente por empresas privadas e atores não governamentais. Para desmistificar a percepção ilusória de um campo de batalha etéreo e estritamente virtual, DeNardis e Raymond (2013, p. 5) lembram que, "quer se goste ou não, na verdade existe matéria: edifícios, fontes de alimentação, comutadores, equipamentos de fibra óptica, roteadores e cabos submarinos". Esse cenário evidencia que uma estratégia de defesa estritamente estatal é inerentemente limitada, uma vez que a hierarquia militar não alcança nem possui jurisdição primária sobre as camadas lógicas e físicas geridas diretamente pelo mercado civil.

A complexidade desse ambiente é ampliada quando se analisa a base técnica das infraestruturas críticas nacionais. Setores vitais, como a geração e distribuição de energia, o tratamento de água e os sistemas de transporte, dependem de forma absoluta de Sistemas de Controle Industrial (ICS), com destaque para os sistemas de supervisão e aquisição de dados, conhecidos como SCADA (Alcaraz e Zeadally, 2015). As tecnologias de informação e comunicação formam a verdadeira base dessas infraestruturas, atuando na transmissão de dados sensíveis em tempo real para controlar processos físicos descentralizados (Alcaraz e Zeadally, 2015). Com a modernização e a migração dessas redes de controle para o padrão de protocolos da internet (TCP/IP), buscando maior eficiência e conectividade, os sistemas industriais herdaram as vulnerabilidades inerentes à rede global, expondo serviços essenciais a ciberataques e invasões remotas (Alcaraz e Zeadally, 2015).

A proteção dessas estruturas torna-se ainda mais desafiadora em virtude do alto grau de hiperconexão orgânica entre os diversos setores. A paralisação de um serviço não ocorre de forma isolada, mas propaga-se por meio de relações de interdependência mútua, que podem ser classificadas nas dimensões física, geográfica, cibernética e lógica (Alcaraz e Zeadally, 2015). Devido à densidade dessas conexões, as falhas ultrapassam fronteiras setoriais, de modo que interrupções locais podem gerar um efeito cascata em múltiplas infraestruturas críticas simultaneamente (Alcaraz e Zeadally, 2015). Um erro de software ou um ciberataque direcionado a um simples equipamento de rede de uma operadora de telecomunicações pode, por conseguinte, interromper o funcionamento de hospitais, sistemas financeiros e malhas logísticas.

Essa hiperconexão técnica reflete-se politicamente naquilo que Keohane e Nye (2012) conceituam como "interdependência complexa". No cenário contemporâneo, canais múltiplos e redes transnacionais conectam diretamente as sociedades, diluindo as fronteiras estatais e impedindo que os governos monopolizem as interações internacionais (Keohane e Nye, 2012). Os atores transnacionais operam como correias de transmissão que tornam as políticas domésticas de diferentes países altamente sensíveis umas às outras (Keohane e Nye, 2012). Sob a interdependência complexa, o Estado perde a capacidade de controlar a agenda e manipular estratégias de forma isolada, pois as decisões tomadas por entidades privadas e redes além-fronteiras geram impactos diretos que obrigam os governos a se adaptarem (Keohane e Nye, 2012). Torna-se evidente, portanto, que a tentativa de impor uma governança centralizadora e hierárquica esbarra na natureza inerentemente interdependente e civil das redes que sustentam as infraestruturas críticas.

3.2. O Choque de Governança: "Multistakeholderismo" vs. Militarização Estatal

Historicamente, a governança da internet estruturou-se sob o modelo multistakeholder (multissetorial), caracterizado por delegar as operações técnicas cotidianas da rede ao setor privado e a comunidades civis, operando por meio de uma autoridade horizontal e de processos de consenso (Pohle e Santaniello, 2024). Contudo, na última década, esse arranjo predominantemente civil passou a ser diretamente desafiado pela expansão do discurso de "soberania digital" por parte dos governos. Conforme analisam Pohle e Santaniello (2024), os Estados têm buscado reconfigurar e reforçar o seu controle sobre o ambiente digital, em uma tentativa de reinserir fronteiras territoriais e legislações nacionais na regulação das redes e dos dados. Esse movimento geopolítico global, adotado com nuances por potências centrais e países do BRICS, entra em conflito direto com o paradigma de descentralização que sustenta a arquitetura original da internet.

Essa fricção discursiva traduz-se em uma profunda incompatibilidade institucional entre a morosidade das burocracias estatais e o dinamismo inerente ao setor privado (Hofmann, 2016). Enquanto as empresas de tecnologia e os operadores de infraestrutura exigem flexibilidade para inovar e responder a incidentes em tempo real, os processos governamentais operam tradicionalmente de cima para baixo (top-down) e dependem de longas e rígidas cadeias hierárquicas de decisão (Dutton, 2015). Na tentativa de exercer controle regulatório e de impor a segurança nacional, os governos frequentemente buscam forçar os provedores de serviços privados a atuarem como intermediários de

monitoramento ou pontos de estrangulamento (choke points). Essa abordagem coercitiva desvirtua a arquitetura descentralizada de "ponta a ponta" (end-to-end) da rede, sufoca a inovação e fracassa ao tentar enquadrar um ecossistema multifacetado em modelos regulatórios analógicos e ultrapassados (Dutton, 2015).

No contexto brasileiro, o choque entre a centralização estatal e a governança horizontal manifesta-se de forma aguda na formulação das políticas de proteção de dados e sistemas. Como demonstrado por Pinto e Grassi (2020), as infraestruturas mais sensíveis do país — a exemplo dos setores de energia elétrica, finanças e telecomunicações — são geridas e operadas majoritariamente pelo mercado civil. Todavia, a resposta do Estado para a proteção desses serviços essenciais concentrou os recursos e a autoridade sob a tutela das Forças Armadas, consubstanciada na liderança militarizada do Comando de Defesa Cibernética e no papel do Gabinete de Segurança Institucional (Brasil, 2024). Instala-se, por conseguinte, uma assimetria institucional severa: o agente central incumbido de planejar a defesa atua sob a lógica militar hierárquica, ao passo que o operador cotidiano da infraestrutura a ser protegida responde à racionalidade econômica e civil do mercado privado.

Os efeitos deletérios desse descompasso são evidentes nos próprios diagnósticos governamentais sobre a matéria. Documentos oficiais, como o Livro Verde de Segurança Cibernética, expõem uma expressiva descoordenação entre o planejamento central do Estado e as esferas civis operacionais (Pinto e Grassi, 2020). Dentre os entraves estruturais resultantes dessa governança fragmentada, destacam-se a ausência de integração das políticas setoriais de segurança, a falta de clareza sobre as interdependências críticas e o número insuficiente de equipes civis de resposta a incidentes na sociedade (Pinto e Grassi, 2020). Fica comprovado que o foco eminemente militar dos investimentos cria barreiras para a cooperação intersetorial diária. A grande estratégia nacional falha, portanto, na sua etapa de execução operacional, pois a burocracia militarizada escolhida pelo Estado para prover a segurança é institucionalmente incompatível com a natureza descentralizada e corporativa da infraestrutura que necessita de proteção.

3.3. O Limite da Soberania e a Dependência Tecnológica (A Falha Material)

Além do choque institucional entre as lógicas civil e militar, a estratégia brasileira de "Soberania por Autossuficiência" esbarra em uma limitação material intransponível. Nos arranjos

contemporâneos da economia política internacional, a autoridade e a independência de um Estado são condicionadas pelo seu "poder estrutural", conceituado por Strange (2015) como a capacidade de moldar as estruturas de relacionamento, a produção, a segurança e as finanças globais. No atual cenário, a faceta mais decisiva desse poder reside no controle sobre o conhecimento e a tecnologia (Strange, 2015). Quando um Estado se torna dependente da infraestrutura digital, de componentes físicos, roteadores e softwares desenvolvidos e geridos por empresas transnacionais estrangeiras, a sua autoridade legítima e sua capacidade de atuação são severamente enfraquecidas. A internacionalização das redes e a dependência da tecnologia de terceiros fazem com que o Estado transfira, involuntariamente, o poder de decisão e a gestão dos riscos para essas entidades externas (Strange, 2015).

Essa dependência tecnológica não é uma falha passageira, mas um traço estrutural que acomete grande parte das potências emergentes do Sul Global. Conforme delineado por Stuenkel (2016), países como o Brasil enfrentam um profundo "desafio de capacidade" para sustentar e concretizar suas ambições na ordem internacional. A carência de uma infraestrutura intelectual robusta de ponta, aliada a gargalos históricos na capacidade de inovação endógena, impede a produção nacional e em larga escala de tecnologias cibernéticas sensíveis. Dessa forma, a retórica governamental de defesa, que exalta de forma perene o fortalecimento da base industrial nacional e a autossuficiência estratégica, choca-se frontalmente com a realidade econômica de um país que opera predominantemente como importador e consumidor da arquitetura cibernética produzida no centro do sistema capitalista (Stuenkel, 2016).

O descompasso entre a ambição declaratória da defesa e a escassez material do Estado consolida um quadro que pode ser compreendido com exatidão por meio das diferentes dimensões de soberania propostas por Krasner (1999). O Brasil exerce de forma plena a sua "soberania legal internacional" (Krasner, 1999, p. 7). É valendo-se dessa autoridade jurídica formal que o aparelho estatal formula a Política Nacional de Defesa, cria estruturas como o Comando de Defesa Cibernética e estabelece normas de segurança para o país.

Entretanto, esse arcabouço burocrático mostra-se vazio diante da ausência de "soberania de interdependência", definida como a capacidade empírica de regular e controlar efetivamente os fluxos transfronteiriços de informações, ideias e dados (Krasner, 1999, p. 12). A premissa de Krasner (1999) é contundente: um Estado pode ser amplamente reconhecido no âmbito legal e jurídico, mas ser

completamente incapaz de policiar o que entra e sai de suas redes. A incapacidade de gerenciar autonomamente essa infraestrutura técnica corrói a própria governança doméstica. Assim, o paradoxo se fecha: a burocracia militar brasileira detém a autoridade formal no papel, mas não possui o poder estrutural, civil e tecnológico necessário para assegurar, de fato, a proteção das infraestruturas críticas da nação.

CONSIDERAÇÕES FINAIS

Este artigo buscou demonstrar que a grande estratégia brasileira para o ciberespaço apresenta uma falha estrutural de concepção ao tentar solucionar um problema do século XXI utilizando um arcabouço geopolítico analógico. A análise da Política Nacional de Defesa, da Estratégia Nacional de Defesa e da estruturação do Sistema Militar de Defesa Cibernética revelou que o Estado respondeu à ascensão das ameaças digitais por meio da securitização e de uma consequente militarização institucional. Impulsionada por interesses burocráticos de centralização, a cúpula de defesa buscou enquadrar o ambiente cibernético sob a mesma lógica de controle territorial, autossuficiência e imposição hierárquica que historicamente orientou as Forças Armadas.

Ocorre que a aplicação dessa doutrina tradicional esbarra na complexidade material e na natureza inerentemente privada do domínio cibernético. A tese aqui comprovada é a de que a centralização da governança nas mãos do estamento militar — evidenciada pelo protagonismo do Comando de Defesa Cibernética e do Gabinete de Segurança Institucional — é operacionalmente incompatível com a proteção eficaz das infraestruturas críticas. Essas estruturas vitais, como os setores de energia, telecomunicações e finanças, dependem de redes hiperconectadas operadas pela iniciativa civil, as quais respondem à lógica horizontal do mercado, e não às cadeias de comando típicas de uma estrutura bélica. Somada a esse descompasso de governança, a crônica dependência tecnológica do país frente às potências estrangeiras esvazia a autoridade do Estado, reduzindo a busca por soberania digital a uma declaração estritamente formal.

A inadequação desse modelo de defesa torna-se ainda mais evidente frente às limitações táticas da própria dinâmica cibernética. Como argumenta Van der Meer (2015), o chamado problema da atribuição — a extrema dificuldade técnica e temporal de identificar com absoluta certeza a verdadeira origem de um ciberataque — invalida a aplicação da dissuasão militar clássica no espaço digital. A ameaça de retaliação pelo uso da força perde sua credibilidade em um ambiente marcado pela

assimetria, pelo anonimato e pela atuação de agentes não estatais (Van der Meer, 2015). Consequentemente, o investimento desproporcional na estruturação de um comando militar ofensivo ou dissuasório mostra-se uma resposta ineficaz diante da necessidade premente de construir resiliência defensiva e diplomática.

Nesse sentido, o Estado brasileiro precisa reconhecer que as normas e o comportamento no ciberespaço não são construídos em uma "lousa em branco" (Finnemore e Hollis, 2016). A imposição de diretrizes coercitivas de cima para baixo (top-down) possui eficácia limitada, uma vez que o Estado, diferentemente do controle que exerce sobre seus arsenais cinéticos, não é o proprietário da internet. As ferramentas de tecnologia da informação e as redes que sustentam tanto a economia civil quanto a própria operação burocrática governamental pertencem e são geridas por empresas privadas (Finnemore e Hollis, 2016). Qualquer esforço normativo ou de segurança que aliene esse setor e a comunidade técnica tenderá ao fracasso.

Conclui-se, portanto, a confirmação do paradoxo central desta pesquisa: a busca incessante do Estado brasileiro por "Soberania por Autossuficiência" no ciberespaço, conduzida por meio do isolamento e da militarização da sua governança, resulta em uma maior vulnerabilidade sistêmica. Ao negligenciar o modelo de cooperação multistakeholder, a burocracia de defesa sufoca a coordenação intersetorial e agrava os gargalos operacionais do país. A mitigação desse quadro exige uma profunda revisão doutrinária, na qual a proteção nacional deixe de orbitar a lógica militarizada de controle de domínio para assentar-se em uma arquitetura de governança verdadeiramente civil-militar-privada. Apenas mediante a integração institucional das esferas civis e o fomento incisivo de medidas diplomáticas de construção de confiança internacional, o Brasil poderá resguardar a resiliência de suas infraestruturas críticas na Era da Informação.

REFERÊNCIAS

ALCARAZ, Cristina; ZEADALLY, Sherali. Critical infrastructure protection: Requirements and challenges for the 21st century. **International Journal of Critical Infrastructure Protection**, v. 8, p. 53-66, 2015.

AZUBUIKE, Callistus Francis. Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks. **Nnamdi Azikiwe Journal of Political Science (NAJOPS)**, Awka, v. 8, n. 3, p. 101-114, 2023.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD31-M-07: Doutrina Militar de Defesa Cibernética**. 2. ed. Brasília: Ministério da Defesa, 2023.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa** - END. Anexo II do Decreto nº 12.725, de 18 de novembro de 2025. Diário Oficial da União: seção 1, Brasília, DF, ano 204, ed. 221, p. 2, 19 nov. 2025.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa - PND**. Anexo I do Decreto nº 12.725, de 18 de novembro de 2025. Diário Oficial da União: seção 1, Brasília, DF, ano 204, ed. 221, p. 2, 19 nov. 2025.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Brasília: Ministério da Defesa, 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Ata da 1ª Reunião Ordinária do Comitê Nacional de Segurança de Infraestruturas Críticas (CNSIC)**. Processo nº 00184.000201/2024-81. SEI nº 6324627. Brasília, DF, 5 dez. 2024.

CARNOY, Martin. **Estado e Teoria política**. 2. ed. Campinas: Papirus, 1988.

CAZUMBA, Ricardo Antônio. **A Circulação Internacional do Conceito de Guerra Híbrida e a sua Recepção, Interpretação e Uso no Campo Militar Brasileiro**. 2025. Tese (Doutorado em Estudos Estratégicos de Defesa e Segurança) - Universidade Federal Fluminense.

COUTINHO, Isadora Caminha. Articulação entre política externa e política de defesa do Brasil: obstáculos e avanços. **Agendapolítica** (Revista de Discentes de Ciência Política da UFSCAR), Vol. 6, n. 3, p. 192-213, 2018.

DENARDIS, Laura; RAYMOND, Mark. **Thinking Clearly about Multistakeholder Internet Governance**. In: EIGHTH ANNUAL GIGANET SYMPOSIUM, 2013, Bali. *Anais*... Bali: GigaNet, 2013. Disponível em: https://ssrn.com/abstract=2354377. Acesso em: 14 ago. 2026.

DUTTON, William H. **Multistakeholder Internet Governance?** East Lansing: Quello Center, Michigan State University, 2015. (Quello Center Working Paper). Disponível em: https://ssrn.com/abstract=2615596.

FIGUEIREDO, Eurico de Lima. Globalização, Neoliberalismo e a Estratégia do Poder: os Jogos não Estão Feitos. In: SANTOS, Teothonio dos (coord.). **Os Impasses da Globalização (Hegemonia e Contra-Hegemonia)**. v. 2. Rio de Janeiro: PUC/REGGEN, Edições Loyola, 2004. p. 243-261.

FIGUEIREDO, Eurico de Lima. Estudos Estratégicos como Área de Conhecimento Científico. **Revista Brasileira de Estudos de Defesa**, v. 2, n. 2, p. 107-128, jul./dez. 2015.

FIGUEIREDO, Eurico de Lima. Os Estudos Estratégicos, a Geopolítica e a Guerra. In: Carmona, Ronaldo (org.). **Pensamento Brasileiro sobre a Guerra**, Rio de Janeiro: Editora da ESG, 2023.

FINNEMORE, Martha; HOLLIS, Duncan B. Constructing Norms for Global Cybersecurity. **The American Journal of International Law**, v. 110, n. 3, p. 425-479, 2016.

HOFMANN, Jeanette. Multi-stakeholderism in Internet governance: putting a fiction into practice. **Journal of Cyber Policy**, v. 1, n. 1, p. 29-49, 2016. doi: 10.1080/23738871.2016.1158303.

KAPLAN, Marcos. Estado e Sociedade. In: KAPLAN, Marcos. **Formação do Estado Nacional na América Latina**: crise e mudança social. Tradução de Lygia Maria Baeta Neves. Rio de Janeiro: Eldorado, 1974. cap. 1, p. 9-41. (Coleção América Latina).

KEOHANE, Robert O.; NYE, Joseph S. **Power and Interdependence**: Fourth Edition. Boston: Longman, 2012.

KRASNER, Stephen D. **Sovereignty**: Organized Hypocrisy. Princeton: Princeton University Press, 1999.

PINTO, Danielle Jacon Ayres Pinto; GRASSI, Jéssica Maria. Guerra Cibernética, Ameaças às Infraestruturas Críticas e a Defesa Cibernética do Brasil. **Revista Brasileira de Estudos de Defesa**, v. 7, n. 2, p. 103-131, 2020.

POHLE, Julia; SANTANIELLO, Mauro. From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance?. **Policy & Internet**, v. 16, p. 672–691, 2024. Disponível em: https://doi.org/10.1002/poi3.426.

SILVA, Golbery do Couto. **Conjuntura política nacional**: o Poder Executivo & Geopolítica do Brasil. 3. ed. Rio de Janeiro: J. Olympio, 1981. 266 p. (Coleção Documentos brasileiros, v. 190).

STRANGE, Susan. **States and Markets**. Londres: Bloomsbury, 2015.

STUENKEL, Oliver. **Post-Western World**: How Emerging Powers Are Remaking Global Order. Cambridge: Polity Press, 2016.

TANNENWALD, Nina. Process Tracing and Security Studies. **Security Studies**, v. 24, n. 2, p. 219-227, 2015.

VAN DER MEER, Sico. Enhancing International Cyber Security: A Key Role for Diplomacy. **Security and Human Rights**, v. 26, p. 193-205, 2015.

VENNESSON, Pascal. Case studies and process tracing: theories and practices. In: DELLA PORTA, Donatella; KEATING, Michael (Ed.). Approaches and Methodologies in the Social Sciences: a pluralist perspective. Cambridge: Cambridge University Press, 2008. p. 223-239.

VISACRO, Alessandro. **A Guerra na Era da Informação**. São Paulo: Contexto, 2018.

VOLTOLINI, Benedetta. Framing processes and lobbying in EU foreign policy: case study and process-tracing methods. **European Political Science**, v. 16, p. 354–368, 2017.

DECLARAÇÃO DE DISPONIBILIDADE DE DADOS DA PESQUISA: Todo o conjunto de dados de apoio aos resultados deste estudo foi publicado no próprio artigo.

FINANCIAMENTO: O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES)

CONTRIBUIÇÃO DAS/DOS AUTORES/AS: Laura Neves Diniz: Conceituação, Metodologia, Análise formal, Investigação, Curadoria de dados, Administração do projeto, Redação – rascunho original, Redação – revisão e edição, Obtenção de financiamento.

DECLARAÇÃO DE CONFLITO DE INTERESSE: A autora 1 declara não haver conflitos de interesse.

DECLARAÇÃO DE USO DE INTELIGÊNCIA ARTIFICIAL: A autora declara ter utilizado ferramentas de Inteligência Artificial exclusivamente para fins de revisão de texto e adequação de formatação. A autora leu, revisou e aprovou integralmente o conteúdo gerado, assumindo total responsabilidade pelas ideias, análises originais e pela redação final do manuscrito.

MINIBIOGRAFIAS DOS/DAS AUTORAS DO PAPER

Doutoranda em Estudos Estratégicos de Defesa e Segurança (UFF), Mestre em Economia Política Internacional (UFRJ), Bacharel em Defesa e Gestão Estratégica Internacional (UFRJ).

Este preprint foi submetido sob as seguintes condições:

- Os autores declaram que os necessários Termos de Consentimento Livre e Esclarecido de participantes ou pacientes na pesquisa foram obtidos e estão descritos no manuscrito, quando aplicável.
- Os autores declaram que a elaboração do manuscrito seguiu as normas éticas de comunicação científica.
- Os autores declaram que estão cientes que são os únicos responsáveis pelo conteúdo do preprint e que o depósito no SciELO Preprints não significa nenhum compromisso de parte do SciELO, exceto sua preservação e disseminação.
- Os autores declaram que os dados, aplicativos e outros conteúdos subjacentes ao manuscrito estão referenciados.
- O manuscrito depositado está no formato PDF.
- Os autores declaram que a pesquisa que deu origem ao manuscrito seguiu as boas práticas éticas e que as necessárias aprovações de comitês de ética de pesquisa, quando aplicável, estão descritas no manuscrito.
- Os autores declaram que uma vez que um manuscrito é postado no servidor SciELO Preprints, o mesmo só poderá ser retirado mediante pedido à Secretaria Editorial do SciELO Preprints, que afixará um aviso de retratação no seu lugar.
- Os autores concordam que o manuscrito aprovado será disponibilizado sob licença Creative Commons CC-BY.
- O autor submissor declara que as contribuições de todos os autores e declaração de conflito de interesses estão incluídas de maneira explícita e em seções específicas do manuscrito.
- Os autores declaram que o manuscrito não foi depositado e/ou disponibilizado previamente em outro servidor de preprints ou publicado em um periódico.
- Caso o manuscrito esteja em processo de avaliação ou sendo preparado para publicação mas ainda não publicado por um periódico, os autores declaram que receberam autorização do periódico para realizar este depósito.
- O autor submissor declara que todos os autores do manuscrito concordam com a submissão ao SciELO Preprints.