CIBERTERRORISMO E DEFESA DA AMAZÔNIA: DESAFIOS LEGISLATIVOS E GEOPOLÍTICOS NA FRONTEIRA DIGITAL

Zaryff Said de Lima[1]
http://lattes.cnpq.br/4005011289925192
https://orcid.org/0000-0002-3394-3561
Edson Marcos Leal Soares Ramos[2]
http://lattes.cnpq.br/8324947891255931
https://orcid.org/0000-0001-5425-8531
César Maurício de Abreu Mello[3]
http://lattes.cnpq.br/2079368341132335
https://orcid.org/0000-0003-3086-2624
Erika Natalie Pereira Miralha Duarte[4]
http://lattes.cnpq.br/4935304081624007
https://orcid.org/0009-0004-4904-0182
Adriene da Silva Cursino[5]
http://lattes.cnpq.br/6859657374629858
https://orcid.org/0009-0007-0152-2838

Resumo

Este artigo analisa os desafios legislativos e geopolíticos impostos pelo ciberterrorismo à defesa da Amazônia Brasileira, considerando a vulnerabilidade digital da região e seus riscos geopolíticos. A justificativa para esta pesquisa reside na crescente interdependência da sociedade moderna em relação à tecnologia e na transformação do ciberespaço em um novo domínio de conflitos, onde a Amazônia, com sua riqueza em recursos naturais, se torna um alvo estratégico. A metodologia utilizada é qualitativa e descritiva, baseada em revisão bibliográfica, abordando conceitos como ciberterrorismo e cibersegurança, bem como medidas de prevenção de ciberataques. Os resultados indicam que a Amazônia enfrenta vulnerabilidades estruturais, como dependência tecnológica externa, infraestrutura crítica mal protegida, fragilidade institucional e porosidade das fronteiras física e digital, que facilitam a atuação de redes criminosas e ciberterroristas. Além disso, a pesquisa revela que a falta de coordenação entre agências de segurança e a ausência de legislação específica sobre ciberterrorismo agravaram a situação. A análise conclui que a Amazônia, devido à sua complexidade geopolítica e vulnerabilidades digitais, exige uma abordagem integrada e eficaz

[1] Mestranda no Programa de Pós-Graduação em Segurança Pública (Universidade Federal do Pará). E-mail: zaryff.lima@ifch.ufpa.br
[2] Doutor em Engenharia de Produção, professor Titular da Universidade Federal do Pará.. E-mail: ramosedson@gmail.com
[3] Doutor em Ciências, Professor do Programa de Pós-graduação em Segurança Pública da UFPA e da Universidade do Amazonas. E-mail: mello.cesar@gmail.com
[4] Mestre em Segurança Pública pela Universidade Federal do Pará. E-mail: erikanatalie@hotmail.com
[5] Discente em Direito (Faculdade Santa Teresa-AM). E-mail: adrienecursino@icloud.com

para a proteção de suas infraestruturas críticas e a segurança nacional, destacando a necessidade de cooperação internacional e estratégias de ciberdefesa robustas.

Palavras-chave: Ciberterrorismo; Geopolítica; Amazônia; Fronteira Digital; Cibersegurança.

Abstract

This article analyzes the legislative and geopolitical challenges posed by cyberterrorism to the defense of the Brazilian Amazon, considering the region's digital vulnerability and its geopolitical risks. The justification for this research lies in the growing interdependence of modern society on technology and the transformation of cyberspace into a new domain of conflict, where the Amazon, with its wealth of natural resources, becomes a strategic target. The methodology used is qualitative and descriptive, based on a bibliographic review, addressing concepts such as cyberterrorism and cybersecurity, as well as measures for preventing cyberattacks. The results indicate that the Amazon faces structural vulnerabilities, such as external technological dependence, poorly protected critical infrastructure, institutional fragility, and the porosity of the physical and digital frontiers, which facilitate the operation of criminal and cyberterrorist networks. Furthermore, the research reveals that the lack of coordination among security agencies and the absence of specific legislation on cyberterrorism have aggravated the situation. The analysis concludes that the Amazon, due to its geopolitical complexity and digital vulnerabilities, requires an integrated and effective approach to protect its critical infrastructure and national security, highlighting the need for international cooperation and robust cyber defense strategies.

Keywords: Cyberterrorism; Geopolitics; Amazonia; Digital Frontier; Cybersecurity.

Introdução

A defesa da Amazônia sempre representou desafios para a segurança nacional, devido a diversidade da fauna e flora, além das riquezas de seu subsolo, gerando nessa região interesses externos, com maior ou menor intensidade, desde a época de seu descobrimento (JUNIOR, 2018). Porém, durante a década de 1970, a Amazônia recebeu grandes investimentos em infraestrutura para o desenvolvimento econômico da região, no intuito de garantir a segurança das fronteiras pela ocupação do espaço.

Sob o lema “Integrar para não entregar”, diversos planos do governo federal buscaram o povoamento da fronteira norte do Brasil (JUNIOR, 2018). A globalização, por sua vez, trouxe para a região, principalmente entre os anos 1960 e 1980, uma gama de possibilidades em razão da revolução da tecnologia. (DAS CHAGAS, 2012).

A Internet provocou muitas mudanças rápidas em nossos hábitos, tradições e cultura, pois, ajudaram a promover uma comunicação rápida e instantânea entre as mais longínquas regiões. Entretanto, Costa (2017) cita que apesar dos benefícios que o uso da internet proporcionou, ela apresenta muitas vulnerabilidades, e consequentemente, novos tipos de condutas ilícitas começaram a ser praticadas, tendo algumas, inclusive, danos imensuráveis e podendo trazer caos a um Estado.

A principal ameaça, de acordo com Junior e Trindade (2024), não era mais a invasão do território por outra nação. O espaço cibernético, nos últimos anos, se tornou uma característica essencial da vida moderna, conectando indivíduos e comunidades em todo o mundo, porém tem se tornado também cenário de dinâmicas dos países, pois vem apresentando desafios significativos em termos de segurança e estabilidade (JUNIOR e TRINDADE, 2024).

As vulnerabilidades que a tecnologia carrega tornou possível a existência de diversos tipos de condutas danosas e, por esse motivo, segundo Nunes, Lehfeld e Silva (2020), termos como ciberguerra, ciberataque e ciberterrorismo tomaram espaço no ordenamento jurídico de vários Estados do globo.

Nessa perspectiva, conforme apresenta Grassi e Pinto (2020), as infraestruturas críticas, tanto ligadas ao setor privado quanto ao setor público, passaram a ser alvos principais de uma nova maneira de violência, que apesar de não ser direta, causa danos efetivamente sérios a sociedade e aos Estados. Esses ataques, que visam intimidar ou coagir governos ou sociedades para promover objetivos políticos ou sociais, de acordo com Junior e Trindade (2024), refletem uma nova fronteira de conflito no ciberespaço, a qual, sem limitações geográficas, facilita assim o lançamento de ataques a partir de qualquer local, tornando-se difícil distinguir os atores envolvidos.

Dessa forma, com base nas pesquisas realizadas, surgiram indagações sobre a temática que será discutida, sendo elaborada a seguinte pergunta de pesquisa: como a vulnerabilidade digital da Amazônia Transfronteiriça potencializa riscos geopolíticos, afetando a segurança e o desenvolvimento regional. Para responder a pergunta de pesquisa, o presente estudo possui o objetivo de analisar os desafios legislativos e geopolíticos impostos pelo ciberterrorismo à defesa da Amazônia Brasileira. Quanto a metodologia, trata-se de uma pesquisa qualitativa e descritiva, a partir de uma revisão bibliográfica.

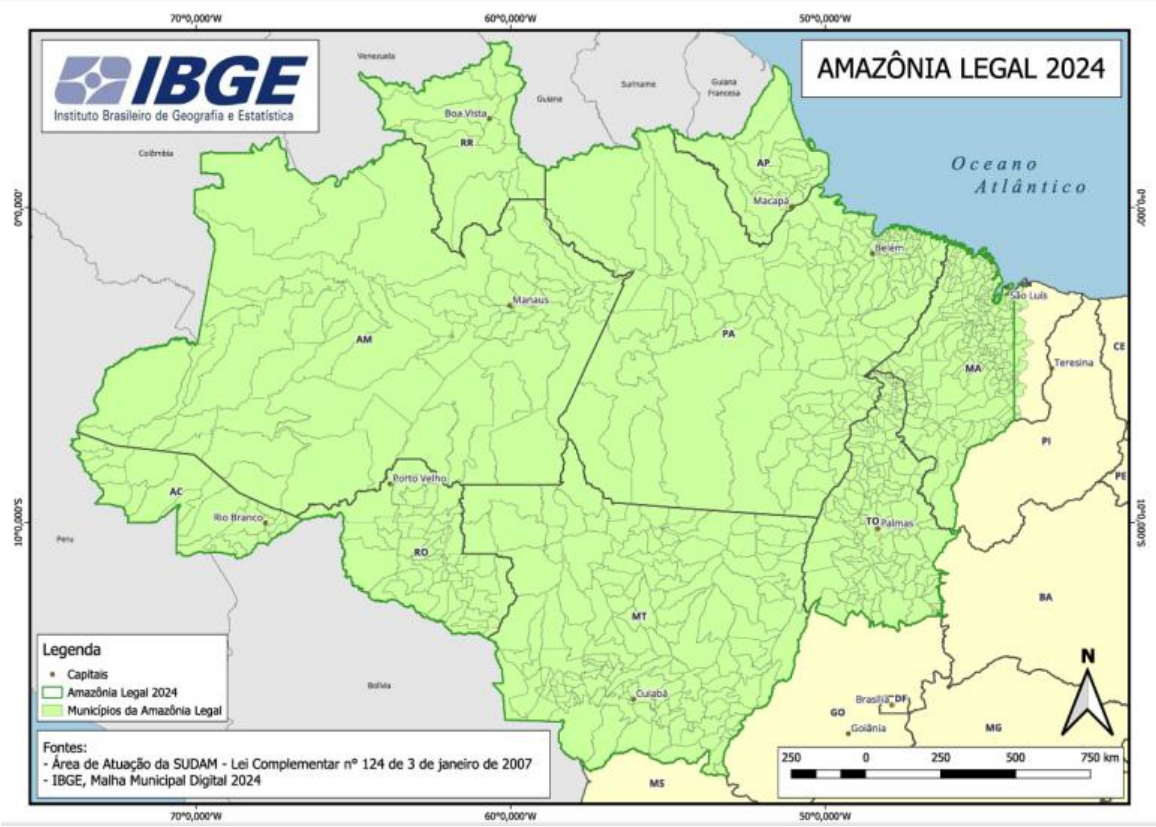
Resultados e discussões:
A complexidade geopolítica da Amazônia e a fronteira digital

A Amazônia Legal é composta por 9 Estados (Acre, Amazonas, Pará, Roraima, Rondônia, Amapá, Maranhão, Tocantins e Mato Grosso) distribuídos em 773 municípios, cobrindo 59% do território brasileiro (5 milhões de metros quadrados), de acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE). Além disso, o Brasil abriga cerca de 64% de toda a floresta amazônica constante na América do Sul (INSTITUTO IGARAPÉ, 2022).

Outras características que podem ser levadas em consideração, são as dinâmicas e peculiaridades geográficas da região. Com uma extensa fronteira de aproximadamente 11 mil km², a Amazônia faz divisa com 7 países sul-americanos, conforme mapa constante na Figura 1. O contexto fronteiriço impõe outros desafios, pois além da Amazônia possuir mais de 100 municípios em áreas de fronteira, a mobilidade se dá, sobretudo, através das redes hidrográficas (INSTITUTO IGARAPÉ, 2022). Apesar da vasta extensão territorial, somente 13% da população brasileira habita a região, e mesmo com crescimento da população do país, a região continua com uma das menores densidades demográficas do mundo (JUNIOR, 2018).

Essa configuração territorial, aliada à baixa densidade populacional, à presença de mais de 25 mil km de rios navegáveis e à vegetação densa que dificulta a vigilância e o controle territorial, configura uma das regiões mais propensas à atuação de redes criminosas transnacionais (DA COSTA e MAIA, 2025).

Figura 1 - Imagem da Amazônia Legal, em 2024.



Fonte: IBGE, 2024

A região tem uma pequena participação na economia nacional, com apenas 8% do Produto Interno Bruto (PIB) do Brasil, porém sua riqueza em recursos naturais e serviços ambientais é inestimável, conforme apresenta Junior (2018). Não é exagero afirmar que a Amazônia brasileira é um dos maiores ativos estratégicos do país, além de ter papel importante na geopolítica mundial no século XXI (INSTITUTO IGARAPÉ, 2022).

A geopolítica, como campo de estudo, investiga as ”relações entre poder e espaço geográfico, buscando compreender as posições políticas e os efeitos das ações ao nível global” (CAVALCANTE, 2024). Nesse contexto, a região Amazônica sempre se destacou como um ponto central na geopolítica mundial, devido aos interesses políticos, econômicos e ambientais em torno de seus recursos naturais.

De acordo com Amusquivar e Passos (2018) *apud* Cavalcante (2024), a geopolítica busca compreender a relação entre a lógica de poder dos Estados, a demarcação dos territórios e as características geográficas disponíveis a esses atores, sendo usada para assegurar a primazia política, econômica e militar por meio da expansão territorial.

A geopolítica, segundo Becker (2005), foi essencial para garantir a soberania sobre o território amazônico, especialmente em momentos de crescente demanda pelo uso dos seus recursos naturais, o que impulsionou a exploração desta vasta área.

Enquanto a Amazônia, em certo período, se encontrava com uma economia de serviços e de base terciária, a geração de riqueza nacional tornou se cada vez mais dependente da internet, passando a estar mais exposta e vulnerável a um leque alargado de novos riscos de segurança, evidenciou Nunes (2022).

A ausência de ações coordenadas pelo país, associada à complexa geografia da região, não sendo prioridade o combate aos crimes ambientais, com legislações deficientes para aplicação de penas, e à proximidade com países produtores de drogas faz com que diferentes redes criminosas se aproveitem do vazio institucional para explorar diferentes economias ilícitas ameaçando a segurança pública. Nesse contexto, ocorreu comprometimento da soberania nacional em função da operação de diferentes redes criminosas que atuam livremente no interior da floresta explorando seus recursos e suas populações (INSTITUTO IGARAPÉ, 2022).

Considerando o espaço de atuação do Estado, que inclui o território físico, o digital estende esse mesmo território, exigindo o exercício de soberania num espaço digital, complementar ao espaço físico.

Um dos aspectos em que esses cuidados se tornam mais sensíveis é precisamente o associado com as suas fronteiras, que delimitam o respectivo território, onde é exercida a soberania, impondo também aqui, a existência de uma soberania do espaço virtual relevante, a designar por soberania digital. Conforme afirma Gouveia (2008), o delimitar da fronteira virtual, que esteja associada com a identidade nacional e com a preservação de informação sensível para um Estado, é crucial para a sua afirmação no século XXI.

A Amazônia desperta interesses hegemônicos devido ao seu vasto potencial como reserva de recursos naturais e território estratégico em contextos econômicos e geopolíticos globais, de acordo com Cavalcante (2024). A crescente mercantilização dos recursos naturais, como ar, biodiversidade e água, complementa a autora, amplifica sua importância estratégica e acirra as disputas internacionais pelo acesso e controle a esses recursos (CAVALCANTE, 2024).

Segundo o Instituto de Energia e Meio Ambiente (2020), constante nos estudos de Cavalcante (2024), os estados da Amazônia Legal abrigam quatro das cinco maiores usinas hidrelétricas no Brasil (Belo Monte, Tucuruí, Jirau e Santo Antônio) que, juntas são responsáveis por mais de 27% da geração de energia elétrica nacional. Esses dados evidenciam que a Amazônia contribui significativamente para o suprimento energético nacional, exportando energia para outras regiões do Brasil (CAVALCANTE, 2024).

Com o avanço da tecnologia, como assevera Junior e Trindade (2024), o terrorismo assumiu novas formas, utilizando-se das tecnologias de informação, internet e comunicação disponíveis para seus propósitos nefastos. Isso, complementa os autores, reflete uma mudança na dinâmica do terrorismo, onde a tecnologia não só facilita a comunicação entre os grupos terroristas, mas também amplifica seu alcance e impacto.

Terrorismo, Ciberterrorismo, Cibersegurança e Ciberdefesa: conceitos e principais diferenças

O nível de inovação e evolução da tecnologia, caracterizando os vários vetores de ataque, fazem crescer o nível da ameaça e os riscos sociais, “colocando em risco as infraestruturas críticas, e os processos de administração do Estado e, de uma forma geral, a própria resiliência nacional” (NUNES, 2022).

Nos anos de 1990, os *hackers* se concentravam na penetração de redes e na produção de software malicioso, porém hoje não configuram a única ameaça. Conforme apresentado por Nunes (2022), ao longo das últimas décadas, algumas áreas como o ativismo social, o crime organizado e o terrorismo, têm utilizado o ciberespaço como vetor de ataque. Estas novas ameaças, complementa o autor, incluem ações desenvolvidas por atores Estatais e não-Estatais, "devido à sua natureza assimétrica e efeitos potencialmente disruptivos e destrutivos, levaram a que este espaço global seja hoje assumido como um novo domínio" (NUNES, 2022).

Diferentemente de ações que envolvem altos riscos e arranjos logísticos complexos, um ataque cibernético pode ser realizado de um local remoto, preservando o anonimato e custos gerando consideravelmente menores, exigindo apenas um computador e acesso à internet. Além disso, como assevera Assis, Dib e Dos Santos (2024), esses ataques possuem o potencial de gerar danos consideráveis as redes e sistemas de computadores de uma nação sem a necessidade da presença física, tornando-os uma alternativa atraente para terroristas.

Sendo assim, um ataque cibernético pode ser classificado como estratégico se suas consequências forem capazes de afetar a habilidade de um Estado no desempenho de suas funções fundamentais, que incluem a segurança e o bem-estar de seus cidadãos (ASSIS, DIB e DOS SANTOS, 2024).

Embora essas atividades possam não significar imediatamente o envolvimento direto de organizações terroristas reconhecidas, surgiram evidências ao longo dos anos, relatadas por Assis, Dib e Dos Santos (2024), que "indicam que certos grupos estavam iniciando explorações nessas novas vias digitais para aumentar sua capacidade de infligir danos".

Devido a isso, atualmente o conceito de terrorismo vem sendo cada vez mais ampliado. Atos de terrorismo não são somente físicos, podendo ser também executados de forma *on-line*. Conforme Villela (2023), os grupos terroristas começaram a usar os computadores e a tecnologia para efetivar seus ataques. Nesse contexto, *hackers* com motivações políticas ou religiosas são recrutados por grupos extremistas.

Nesse viés, de acordo com Novais (2012) *apud* Villela (2023) "o ciberterrorismo resulta em termos simples da convergência do terrorismo e do ciberespaço, e refere-se àquilo que se designa igualmente por terrorismo eletrônico".

Para melhor entendimento de como o ciberterrorismo funciona, é essencial sabermos o que é ciberespaço. A palavra "cyberspace" foi primeiramente designada em 1984, por William Gibson, um escritor de ficção científica (LÉVY, 1998 *apud* DAS CHAGAS, 2012). O ciberespaço, para o autor, constitui "um campo vasto, aberto, ainda parcialmente indeterminado". Pode ser ainda conceituado como um ambiente virtual que se utiliza de aparatos de comunicação para o estabelecimento de relações virtuais ou fenômenos que vão além da comunicação (DAS CHAGAS, 2012).

Essa nova forma de terrorismo, também chamada de terrorismo cibernético, caracteriza-se por uma forma de ciberataque a um governo ou instituição. Isso acontece porque o espaço cibernético simplifica o trabalho dos atos teorristas, pois de acordo com Villela (2023) é possível manter o anonimato, o acesso é facilitado, e o custo é baixo. Gardini (2014) *apud* Villela (2023) define o ciberterrorismo como "ações de objetivos políticos ou religiosos que são realizadas por meio do espaço cibernético para causar graves danos contra a sociedade civil ou governos".

O termo "ciberterrorismo" foi empregado pela primeira vez no ano de 1980, referenciando-se aos ataques conduzidos à longa distância, tornando a população

refém do medo e ameaçando um Estado Democrático de Direito (NUNES, LEHFELD e SILVA, 2020). Ele também é caracterizado como uma "forma de impor terror por meio de ataques contra computadores e suas redes, informações armazenadas, serviços essenciais, sistema bancário entre outros, que causam pânico, acidentes e perdas econômicas" (VILLELA, 2023).

Nunes, Lehfeld e Silva (2020) complementam que os respectivos danos causados por ciberterroristas no tocante à segurança do Estado advém da progressiva interdependência da sociedade moderna para com a tecnologia. Lima (2006) *apud* Das Chagas (2012) reforçam a temática apresentando que o ciberterrorismo é uma extensão natural do terrorismo, e que este se aproveita da dependência que a sociedade tem da tecnologia, em especial da internet.

Segundo os autores Nunes, Lehfeld e Silva (2020), o ciberterrorismo significa o "perigo de ataques conduzidos à longa distância, como consequência da interseção entre mundo físico e virtual, possuindo como alvos infraestruturas críticas de um país". Os autores complementam que os ataques fazem com que a população de um país não consigam "comer, beber, se locomover, ou viver" ALCÂNTARA (2017) apud NUNES; LEHFELD; SILVA (2020).

Ao longo dos últimos anos tem ocorrido a evolução do ciberespaço, a qual não pode ser dissociada das necessidades de ajustes permanentes às suas dinâmicas operacionais e tecnológicas, reforçando que o Estado possui a necessidade de novos processos de cibersegurança e ciberdefesa (NUNES, 2022). Além disso, corrobora o autor que, um mundo mais interligado significa também a existência de um espetro mais alargado de ameaças e riscos (NUNES, 2022).

Fernandes (2012) *apud* Villela (2023) estabelece uma comparação entre cibercrime e ciberterrorismo. Ele acredita que os dois elementos de classificação com as mesmas redes sociais podem ter propósitos semelhantes. De acordo com o autor, o cibercrime possui uma fundamentação técnica, incluindo software e suporte logístico, enquanto o ciberterrorismo oferece uma fundamentação social, como redes pessoais e motivação. Esses elementos resultam em ataques às redes de computadores de adversários ou países (VILLELA, 2023).

Villela (2023) destaca que há duas formas de prevenção contra o ciberterrorismo: a cibersegurança, que envolvea atuação das forças policiais e serviços de informática, e a ciberdefesa, que é realizada exclusivamente pelas forças armadas. Portanto, de de acordo com o autor, a cibersegurança "tem como função a garantia da realização de missões de segurança e defesa nacional, garantindo uma soberania do estado no ciberespaço global", permitindo ações proativas para prevenir ciberataques. Por outro lado, o autor afirma que "a ciberdefesa está interligada com o ciberterrorismo. Pode ser definido como o uso do ciberespaço para a realização de atos terroristas" (VILLELA, 2023).

Ciberterrorismo na Amazônia: atores, motivações e alvos

Após apresentados alguns conceitos, dentre eles o de ciberterrorismo, podemos verificar como ele pode ocorrer na Amazônia, bem como as suas respectivas peculiaridades. Além disso, nesse tópico serão ressaltadas as características dos atores que cometem atos de ciberterrorismo, as suas principais motivações, e quais alvos podem ser atingidos.

Atividades cibernéticas ocorrem no território e envolvem objetos, ou são realizadas por pessoas ou entidades, sobre as quais os Estados podem exercer suas prerrogativas de soberania. Em particular, Nunes (2022) observou que, embora as atividades cibernéticas possam cruzar múltiplas fronteiras ou ocorrer em águas internacionais, no espaço aéreo internacional ou no espaço sideral, todas são conduzidas por indivíduos ou entidades sujeitas à jurisdição de um ou mais Estados.

Mas afinal, quem são os ciberterroristas? Villela (2023) apresentou que um ataque digital pode ser elaborado e executado por qualquer pessoa que "entenda de tecnologia da computação e tenha motivos religiosos ou políticos para causar danos a outros grupos de pessoas". Complementa o autor que podem ser tanto *hackers* amadores como profissionais, e os ataques podem ser realizados somente por um indivíduo ou um grupo terrorista organizado (VILLELA, 2023). Os praticantes desses atos característicos podem ser grupos criados para a prática do ciberterrorismo, ou derivados de grupos terroristas.

Os atores potenciais são heterogêneos, e podem ser: "grupos eco-terroristas radicais que veem o Estado como inimigo da natureza" (VILLELA, 2023); "redes criminosas transnacionais que usam ciberataques como tática de distração durante operações de garimpo ou tráfico" (DA COSTA; MAIA 2025); e Hackers ideológicos recrutados por organizações extremistas (MATUSITZ, 2005).

Nesse sentido, Pinto (2011) *apud* COSTA (2017), defende que os ciberterroristas são normalmente: "jovens do sexo masculino, alguns com habilitações acadêmicas elevadas, que tem a consciência de estar a violar a lei desrespeitando as normas sociais, a ordem e os sistemas de controle social". Além disso, o autor apresenta que eles diferem dos criminosos comuns em pelo menos quatro características fundamentais: "efetuam crimes de forma mais violenta; possuem como meta infligir medo numa população alvo; servem uma agenda social enorme tentando recrutar mais elementos para a causa deles; tentam conseguir exposição máxima".

Por isso, esta forma de terrorismo, segundo Denning (2000) *apud* COSTA (2017), trata-se de ataques feitos para intimidar ou coagir um governo ou seu povo em prol dos objetivos sociais e/ou políticos almejados pelo ciberterrorista. Além disso, os objetivos do ciberterrorismo são simbólicos e mortíferos, e a sua repercussão pelos meios de comunicação social potencializam os efeitos pretendidos por esse ataque, de forma a causar e espalhar pânico e terror na sociedade (COSTA, 2017).

O autor ainda complementa que o ciberterrorismo se utiliza dos meios de comunicação social, e principalmente da internet como meio de garantia de maior alcance aos alvos pretendidos, já que a internet não respeita barreiras e divisões políticas ou geográficas, e ainda permite o anonimato a quem prática atos ciberterroristas.(COSTA, 2017).

No contexto do século XXI, em meio à inclusão digital, é possível evidenciar vários setores que estão conectados à rede e que realizaram esse sistema para operar. Serviços essenciais para a vida humana, como energia, transporte, saúde e telecomunicações, estão sujeitos ao âmbito virtual (ALMEIDA CUNHA, 2017 *apud* NUNES; LEHFELD; SILVA, 2020).

Diante dessa perspectiva, torna-se fácil compreender o terror e o medo que predomina quanto a uma ameaça ciberterrorista. (NUNES; LEHFELD; SILVA, 2020). Além disso, no ciberespaço não existem barreiras físicas, tais como postos de controle para navegar e não existem fronteiras para cruzar. A variedade e o número de alvos são enormes. Os ciberterroristas poderiam ter como alvo os computadores e redes de computadores de governos, indivíduos, serviços públicos, companhias

aéreas privadas, e assim por diante. O grande número e a complexidade de alvos potenciais permitem que os terroristas encontrem fraquezas e vulnerabilidades para explorar (DAS CHAGAS, 2012).

Sobre as Infraestruturas Críticas Nacionais, Grassi e Pinto (2020) apresentam o Artigo 2º da Portaria nº 2, de 8 de fevereiro de 2008, do Gabinete de Segurança Institucional da Presidência da República do Brasil, a qual define Infraestruturas Críticas (IEC) como “as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional”. Na referida portaria, em seu Artigo 3º, expõe-se que são consideradas áreas prioritárias de IEC: “I - Energia; II - Transporte; III - Água; IV - Telecomunicações; e V — Finanças.” (Brasil, 2008).

De acordo com os estudos de Reis (2025), o Sistema de Informação de Geração da Agência Nacional de Energia Elétrica (SIGA, 2025), são 1.330 aproveitamentos hidrelétricos em operação no Brasil, sendo 214 Usinas Hidrelétricas, 427 Pequenas Centrais Hidrelétricas e 689 Centrais Geradoras Elétricas distribuídas pelo país**.** Além disso a autora complementa que as Usinas Hidrelétricas distribuem-se de forma mais ampla, priorizando áreas com potencial hídrico excepcional, como a Bacia Amazônica, mesmo que esteja distante de centros consumidores. Essa lógica é de que grandes projetos se adaptam a estratégias nacionais ou globais, enquanto pequenas usinas atendem demandas locais (RODRIGUES, 2020 *apud* REIS, 2025)

As infraestruturas críticas, como redes de energia elétrica e serviços de emergência, conforme apresentado por Das Chagas (2012), são vulneráveis a um ataque ciberterrorista porque “as infraestruturas e os sistemas de computadores que os executam são altamente complexos, tornando-se efetivamente impossível eliminar todas as fraquezas”. Dessa forma, segundo Batista, Ribeiro e Amaral (2004) *apud* Costa (2017), os “programas de gestão e controle dos serviços essenciais de um Estado, provocam a sua paralisação ou até a sua destruição”. Algumas estruturas estão incluídas neste programa de gestão: redes de distribuição elétrica, de água potável e de gás; redes de controle de tráfego aéreo; redes hospitalares; redes bancárias e financeiras; redes governamentais (BATISTA; RIBEIRO; AMARAL, 2004 *apud* COSTA, 2017)

Desse modo, os alvos são as estruturas vitais dos estados e das empresas multinacionais conectadas a rede através de computadores. Logo, devido a necessidade das nações se modernizarem, estes estão aumentando em grande quantidade a possibilidade de alvos para os ciberterroristas, pois caso sofressem um ataque, seriam capazes de instituir uma situação catastrófica, disseminando o medo e o pânico na sociedade (COSTA, 2017)

Por outro lado, importante levar em consideração também a possibilidade de ataques aos sistemas de comunicação, de controle e os de apoio à decisão, o que diminuiria a capacidade operacional e logística das Forças Armadas do país. Já a ciberguerra teria como objetivo os sistemas de controle e a comunicação operacional, uma vez que, afetando ou destruindo estes, levaria ao comprometimento da capacidade de coordenação e manobra de um grupo das Forças Armadas (Silva, 2014 apud GRASSI e PINTO, 2020).

Especificamente na Amazônia, os alvos preferenciais estariam direcionados aos sistemas de energia (usinas hidrelétricas); redes de água e saneamento; infraestrutura de telecomunicações; sistemas de monitoramento ambiental como o Instituto Nacional de Pesquisas Espaciais (INPE), e Instituto Brasileiro do Meio

Ambiente e dos Recursos Naturais Renováveis (IBAMA); comunicações militares como o Sistema Integrado de Monitoramento de Fronteira (SISFRON) e Projeto Calha Norte (PCN), dentre outros.

Além desses alvos, bem como diante das pesquisas realizadas, foram detectadas algumas vulnerabilidades na fronteira amazônica: 1. Dependência tecnológica externa: satélites, softwares e equipamentos de telecomunicação são frequentemente fornecidos por empresas estrangeiras, criando riscos de backdoors ou interrupção de serviço (GRASSI e PINTO, 2020); 2. Infraestrutura crítica mal protegida: usinas hidrelétricas utilizam sistemas desatualizados, sem segmentação de rede (GALVÃO, 2025); 3. Fragilidade institucional local: escassez de profissionais de cibersegurança nas regiões remotas limita a resposta a incidentes (INSTITUTO IGARAPÉ, 2022); e 4. Porosidade física e digital: mais de 25 mil km de rios navegáveis e 11 mil km de fronteiras terrestres facilitam a infiltração de atores ilegais que, por sua vez, exploram o ciberespaço para coordenar operações (DA COSTA E MAIA, 2025)

Na opinião do Comitê Internacional da Cruz Vermelha (CICV), nos estudos apresentados por Nunes (2022) isso inclui danos devido aos previsíveis efeitos diretos e indiretos (ou ditos “reverberantes”) de um ataque; por exemplo, “a morte de pacientes em unidades de terapia intensiva causada por uma operação cibernética em uma rede de eletricidade que resulta no corte de um fornecimento de eletricidade ao hospital”. Além disso, os ataques que interrompem significativamente os serviços essenciais sem necessariamente causar danos físicos constituem um dos riscos mais importantes para os civis.

Essas vulnerabilidades são agravadas pela falta de interoperabilidade entre agências de inteligência e segurança, além da cultura de sigilo excessivo que impede o compartilhamento de dados (DA COSTA e MAIA, 2025).

Desafios legislativos e lacunas de soberania no enfrentamento ao ciberterrorismo

Atualmente, a maior parte das ameaças na arena internacional envolvem uma gama de fatores complexos que fazem tanto sua origem, quanto suas consequências serem marcadas pela incerteza (BUZAN, 2007 apud JUNIOR, 2018. Cada vez mais se observa Estados lutando contra atores não-estatais.

A vigilância digital e a liberdade no contexto do direito cibernético formam um campo de interesse e preocupação em expansão. Com o avanço da sociedade em direção às tecnologias digitais, as entidades públicas e privadas ampliaram exponencialmente sua capacidade de coleta, armazenamento e análise de dados. Essa expansão acarreta diversos desafios jurídicos e éticos, especialmente no que tange à proteção da privacidade, à liberdade de expressão e ao exercício da cidadania na era digital (JUNIOR e TRINDADE, 2024). Os os autores acrescentam que a questão se torna ainda mais complexa ao levar em conta o caráter transnacional da internet, que desafia as jurisdições e as capacidades de aplicação das leis tradicionais (JUNIOR e TRINDADE, 2024).

Portanto, o principal desafio da a cibersegurança está relacionada ao valor da informação, que é essencial e confidencial, considerando o interesse nacional (LEITE, 2016 apud VILLELA, 2023). A tecnologia permitiu o acesso a novas realidades sem limites, o que teve um impacto na segurança, uma vez que qualquer indivíduo ou

programa de computador pode interagir com interesse ilícito. Nesse contexto, a atuação da Defesa Nacional é crucial para a proteção do Estado (VILLELA, 2023).

A interconexão dos sistemas e a falta de regulamentação no ciberespaço "facilitam ataques que podem causar rupturas políticas e militares, especialmente por causa do potencial desse cenário de controle de objetos físicos e da dificuldade de rastreamento do agressor" (GRASSI e PINTO, 2020).

Considerando esses pontos, Olson (2012) apud Grassi e Pinto (2020) sugere que as vulnerabilidades severas e os riscos de um ataque contínuo e coordenado tornam inviável a defesa completa de uma rede extensa, como as redes de fornecimento de petróleo, que dependem de sistemas computacionais. Assim, o autor alerta que "o potencial prejuízo econômico de uma campanha cibernética coordenada por uma grande potência contra gargalos nos sistemas mundiais (ou nacionais) seria incalculável" (OLSON, 2012 apud GRASSI e PINTO, 2020).

Apesar de ser um tema que entrou na pauta de Segurança Internacional muito recentemente, Oliveira e Teixeira (2022) apresentam que o potencial de destruição das atuais ameaças cibernéticas já foi percebido em alguns casos concretos, a exemplo do ataque cibernético sofrido pela Estônia, em 2007; a Operação Orchard realizada por Israel, ainda em 2007; a guerra Russo-Georgiana, em 2008; o vírus Stuxnet, que infectou uma usina nuclear iraniana, em 2010; o ataque de hacker à *Sony Pictures*, em 2014; a denúncia de violação de e-mails da Presidente Dilma Rousseff em 2015, pela Agência de Segurança Nacional (NSA), dos EUA; e os ciberataques sofridos pelos Estados Unidos da América (EUA), em 2015 e 2016, que teve forte influência nas eleições presidenciais de 2017.

Nesse contexto, com o surgimento dessas novas dinâmicas, Grassi e Pinto (2020) afirmam que, ao analisar o Brasil, constata-se que o país está entre os mais atacados pelos cibercriminosos no mundo. Os os autores acrescentam que essa situação evidencia a relevância de investigar como o país tem incorporadoo tema em sua política de defesa, além de como gerenciar as oportunidades criadas nesse novo espaço de atuação e as vulnerabilidades crescentes diante do avanço tecnológico .

Isso é especialmente importante para estabelecer métodos eficazes de proteção de suas infraestruturas críticas (GRASSI e PINTO, 2020).do avanço . Isso é especialmente importante para estabelecer métodos eficazes de proteção de suas infraestruturas críticas (GRASSI e PINTO, 2020).

O Brasil, sendo também o país que mais sofre com ataques cibernéticos na América Latina, conforme Netscout (2024) apud Galvão (2025), enfrenta uma realidade na qual a crescente digitalização de serviços e a dependência de tecnologias conectadas tornam as Infraestruturas Críticas alvos estratégicos para ciberataques. Essas ameaças, complementa o autor, têm o potencial de causar impactos significativos na economia, na segurança nacional e no bem-estar da população, destacando a necessidade de estratégias de defesa cibernética eficientes. Nesse contexto, torna-se fundamental avaliar as medidas que o Brasil tem adotado para aprimorar sua capacidade de resposta a essas ameaças, elevando sua segurança frente a esses desafios contemporâneos.

Não há como negar que a tecnologia transformou o mundo e a sociedade, possibilitando a criação de uma sociedade virtual no ciberespaço. Os Estados começaram a necessitar de políticas públicas para garantir sua Segurança Nacional no ciberespaço (LEITE, 2016 apud VILLELA , 2023).

A Lei Antiterrorismo n.º 13.260 de 2016, regulamenta o ciberterrorismo no Brasil. Assim, a dificuldade em filtrar esse fluxo de informações que circula pelo espaço cibernético aumenta a vulnerabilidade do sistema. O artigo 2º, inciso IV, da supracitada Lei estabelece que "sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou ocorrer-se de mecanismos cibernéticos, do controle totalou parcial, ainda que de modo temporário […]" (BRASIL, 2016). Além disso, verifica-se que o país possui uma regulamentação aplicável a essa prática criminosa, entretanto, não dispõe de uma legislação específica para o caso (VILLELA, 2023).

Em termos tecnológicos, a interoperabilidade entre sistemas de inteligência e segurança pública ainda é incipiente. A inexistência de plataformas tecnológicas integradas e seguras para compartilhamento de dados impede a circulação oportuna de informações sensíveis, prejudicando a construção de diagnósticos estratégicos e a coordenação interagências. De acordo com Da Costa e Maia (2025), a ausência de protocolos comuns e a cultura de sigilo excessivo entre instituições acentuam esse problema, reforçando a fragmentação institucional.

A atividade prejudicial de Tecnologia da Informação e Comunicação (TIC) contra infraestruturas críticas que fornecem serviços no mercado interno, regional ou global, conforme apresentado nos estudos de Nunes (2022), está se tornando cada vez mais séria. Uma preocupação específica é a atividade maliciosa de TIC que afeta a infraestrutura de informação, a infraestrutura que fornece serviços essenciais ao público, a infraestrutura técnica essencial para integridade da Internet e entidades do setor de saúde.

Com o crescimento exponencial da capacidade de vigilância digital e das ameaças à segurança cibernética, "as autoridades se deparam com o desafio de criar regulamentações e práticas que salvaguardem os direitos individuais sem prejudicar a eficácia das medidas de segurança" (JUNIOR e TRINDADE, 2024). A crescente dependência da infraestrutura digital para diversas atividades públicas e privadas tornou a regulação do ciberespaço ainda mais importante, afirmam os autores (JUNIOR e TRINDADE, 2024).

O Brasil também participa ativamente de organizações e fóruns internacionais relevantes, com a participação de representantes do Ministério das Relações Exteriores, do Gabinete de Segurança Institucional e do Comando de Defesa Cibernética (ComDCiber), dentre outras agências (AXON e STOLZ, 2023). As Equipes Brasileiras de Resposta a Incidentes de Segurança Cibernética (CSIRT) em nível nacional são membros do Fórum de Equipes de Resposta a Incidentes e Segurança (FIRST) em nível global, e especialistas brasileiros dão contribuição de destaque para as atividades e desenvolvimento do FIRST e outros fóruns internacionais, como o Fórum de Governança da Internet das Nações Unidas (IGF) (AXON; STOLZ, 2023).

No nível regional, Axon e Stolz (2023) asseveram que o Brasil é membro da Organização dos Estados Americanos (OEA) e participa de seu programa de segurança cibernética. Os participantes, complementa os autores, relataram que o Brasil e a OEA estão considerando organizar conjuntamente eventos de segurança cibernética para a região. O Brasil também participa do Comitê Cibernético do projeto Agenda Digital do Mercado Comum do Sul (Mercosul), do qual o Brasil ocupou a presidência em 2023, e estaria negociando um acordo sobre segurança cibernética

e discutindo a possibilidade de desenvolver uma taxonomia comum de segurança cibernética para a região.

Apesar da existência da Organização do Tratado de Cooperação Amazônica (OTCA), não há mecanismos regionais de cooperação em cibersegurança. Enquanto a União Europeia e os EUA avançam em centros de resposta a incidentes conjuntos, os países das regiões amazônicas permanecem fragmentados (AXON e STOLZ, 2023). No Brasil, embora existam avanços como o Comando de Defesa Cibernética (ComDCiber), a Escola Nacional de Defesa Cibernética (ENaDCiber) e o exercício Guardião Cibernético, Galvão (2025) apresenta que a governança é descentralizada e setorializada, com o GSI coordenando a segurança cibernética e o Ministério da Defesa a defesa cibernética. Essa divisão impede uma resposta integrada em zonas de fronteira, onde ameaças não respeitam hierarquias institucionais. Ademais, a Lei Antiterrorismo (nº 13.260/2016) menciona "mecanismos cibernéticos" como forma de sabotagem, mas não tipifica o ciberterrorismo de forma autônoma, gerando lacunas na persecução penal (ALBUQUERQUE, 2019 *apud* VILLELA, 2023).

Sendo assim, o Estado é obrigado a proteger os direitos humanos *on line* e *off line*, protegendo os indivíduos de possíveis violações desses direitosincluindo, mas não se limitando à liberdade de opinião e expressão, o direito de acesso à informação e o direito à privacidade (NUNES, 2022).

Através do ciberespaço e a partir dele, atores mal-intencionados podem lançar ataques tanto nos domínios sociais, políticos, econômicos e militares por meio do ciberespaço e a partir dele. Nesse cenário, fica evidente que a dimensão "ciberespaço" ingressou de forma definitiva em sua etapa de uso instrumental como "vetor de projeção de poder à escala global, ao serviço de consecução dos objetivos estratégicosde atores Estado e não-Estado" (NUNES, 2022). O autor acrescenta que os novos modelos de interação fornecidos pelo ciberespaço terão, progressivamente, um impacto significativo e inegável tanto na sociedade civil quanto no âmbito militar. Isso se deve especialmente ao fato de que o ciberespaço, como um espaço global, comum e não restrito às esferas públicas ou privadas, internas ou externas, civis ou militares (NUNES, 2022).

Cooperação e estratégias de ciberdefesa

A partir dos anos 1980,o governo brasileiro implementou diversas estratégias de defesa, tanto para o país como um todo, quanto para a região amazônica. Em 1985, o governo lançou o Programa Calha Norte, com o objetivo de aumentar a presença do Estado e das Forças Armadas na Amazônia. O Programa envolvia a criação de pequenas unidades militares, conhecidas como Pelotões Especiais de Fronteira (PEF), ao longo da fronteira norte e noroeste do país, funcionando como ponto de apoio para revitalizar a faixa de fronteira (MARQUES, 2007 apud JUNIOR, 2018).

Na década de 1990, foi implementado o Sistema de Proteção da Amazônia (SIPAM), que visava, além da proteção e garantia da soberania brasileira sobre a região, a organização e a maximização das ações governamentais na Amazônia (JUNIOR, 2018).

O surgimento de novas ameaças em meio às instabilidades no sistema internacional motivou o Brasil a buscar uma defesa mais sólida por meio do planejamento estratégico de Estado. Isso levou à consolidação, em 2005, da Política Nacional de Defesa (PND) e, em 2008, da Estratégia Nacional de Defesa (END) (GALVÃO, 2025). A Defesa Nacional do Brasil obteve uma orientação mais precisa em relação à

proteção do país graças a esses dois documentos. De forma inovadora, esses documentos deram início à discussão sobre a criação de estruturas de defesa cibernética, além da necessidade de incluir a proteção das infraestruturas críticas e garantir a preparação contra potenciais ameaças cibernéticas. Ainda no âmbito da END, ressalta-se a relevância de fortalecer a "Capacidade de Proteção". Nesse sentido, a Estratégia reitera a importância de aprimorar a defesa no domínio cibernético (GALVÃO, 2025).

Outro progresso, segundo Grassi e Pinto (2020), foi a fundação do Centro de Defesa Cibernética (CDCiber) em 2010, no âmbito do Exército Brasileiro. Atualmente, essa instituição faz parte do Comando de Defesa Cibernética das Forças Armadas (ComDCiber).

A Política de Defesa Cibernética foi publicada em 2012, e a primeira Doutrina de Defesa Cibernética foi aprovada em 2014. No final de 2020, de acordo com Axon e Stolz (2023), foram estabelecidas novas leis diretrizes e organizacionais para a defesa cibernética. Importantes decretos e instrumentos jurídicos desde 2020 levaram a uma implementação mais consistente da doutrina e a uma melhor capacidade de participação internacional.

Com essas ações, a defesa brasileira buscou aprimorar a segurança da informação, protegendo as infraestruturas críticas do país e tornando essencial o fortalecimento do setor cibernético. Isso foi reforçado com a aprovação da Doutrina Militar de Defesa Cibernética Brasileira, que visa definir diretrizes e procedimentos focados na Defesa Cibernética. Em particular, a estabilização do Sistema Militar de Defesa Cibernática (SMDC) durante sua primeira edição em 2014, resultou na criação do Comando de Defesa Cibernética das Forças Armadas (ComDCiber) (GALVÃO, 2025).

Nesse contexto, a aprovação da Doutrina visa estabelecer um entendimento compartilhado sobre o meio cibernético no Ministério da Defesa, com o objetivo de promover a colaboração entre as três Forças Armadas para proteger o Brasil no espaço cibernético. O modelo adotado pela doutrina em questão, conforme afirma Galvão (2025), adota uma estratégia majoritariamente defensiva, reafirmando os princípios de uma nação não beligerante, em consonância com a política do país, priorizando soluções diplomáticas e colaboração internacional. Em contrapartida, o mesmo documento destaca a relevância de medidas proativas, reiterando a necessidade do país estar preparado para qualquer eventualidade.

A Política Nacional de Segurança da Informação (PNSI), que trata de questões principalmente externas à defesa cibernética, foi publicada em 2018). Além disso, a Escola Nacional de Defesa Cibernética (ENaDCiber) foi criada e inaugurada em fevereiro de 2019. A escola possui um sistema de ensino dual, civil e militar, e sua missão é "promover e disseminar as habilidades permitidas para a Defesa Cibernética [...] além de contribuir para as áreas de pesquisa, desenvolvimento, operação e gestão do assunto, bem como para a melhoria da qualificação da mão de obra nacional no setor" (Ministério da Defesa, 2019 apud GRASSI e PINTO, 2020).

Em 2020, foi inaugurada a Estratégia Nacional de Segurança Cibernética (E-Ciber), com o objetivo de promover o Brasil no âmbito digital e fortalecer a defesa contra possíveis ameaças cibernéticas. Isso fortalece a posição do país no cenário internacional, apesar de ambos os documentos não se aplicarem às operações militares.

O Plano Nacional de Segurança de Infraestruturas Críticas (PlanSIC) foi aprovado pelo Decreto 11.200 em setembro de 2022. Através do PlanSIC, ocorreram progressos na identificação de infraestruturas críticas, na coordenação e atribuição de responsabilidades pela sua proteção e no desenvolvimento de padrões de segurança cibernética recomendados para todos os setores de. Muitos elementos do PlanSIC ainda não estão totalmente implementados e, como tal, a segurança cibernética ainda não está regulamentada em todos os setores (AXON e STOLZ, 2023)

Galvão (2025) apresentou em seus estudos as simulações dos cenários de ataques cibernéticos em larga escala, as quais proporcionaram uma plataforma prática para testar e aprimorar as estratégias e procedimentos estabelecidos pela doutrina cibernética. Ademais, o exercício apresentado pelo autor, envolve a coordenação entre diferentes órgãos do governo e da iniciativa privada, fortalecendo a capacidade de resposta a incidentes e a resiliência das infraestruturas críticas do país (GALVÃO, 2025).

No mais, os estudos supracitados apresentados por Galvão (2025) também contribui para o alinhamento contínuo das políticas de segurança cibernética com a realidade do ciberespaço, de modo a garantir a melhor aplicação das estratégias de defesa cibernética na mitigação de riscos e vulnerabilidades, conforme previsto na Política Nacional de Cibersegurança.

Assim, entende-se que, apesar do Brasil estar, atualmente, em posições relevantes no que diz respeito às preparações da defesa cibernética contra possíveis ameaças, ainda existem aspectos a serem melhorados. Conforme Galvão (2025), o país sofre com a baixa atenção dada para a academia, setor importante para a discussão e a pesquisa de políticas que visam a melhoria do setor de defesa. Outro ponto relatado pelo autor, devido esses estudos focarem estritamente em questões relacionadas aos setores das infraestruturas críticas, acaba deixando de lado outras áreas também importantes para o funcionamento de um país, como questões relacionadas à saúde e educação (GALVÃO, 2025).

Por fim, quando olhamos para os documentos brasileiros que versam sobre sua defesa, em especial dos que tratam da área cibernética, Grassi e Pinto, 2020 mostram que é possível perceber que há um valioso esforço em construir elementos sólidos para o desenvolvimento das atividades das forças armadas nessa seara. Porém, os documentos não trazem efetivamente um entendimento específico e direto sobre guerra cibernética, dando ao Estado brasileiro maior flexibilidade de ação quando entenda necessário no mundo virtual.

Sendo assim, identificar uma violação de soberania com base na utilização de limites territoriais físicos é bem mais fácil do que fazê-lo quando a violação ocorre por meio de uma operação cibernética maliciosa (OLIVEIRA e TEIXEIRA, 2022). Ao contrário do que ocorre com as fronteiras físicas, os autores complementam que a dimensão cibernética de um Estado não possui fronteiras, tal fato afeta os antigos critérios estabelecidos para a evidência da soberania e jurisdição do Estado. Desta forma, a compreensão do conceito clássico de soberania territorial do Estado se torna importante para que se possa enxergar a complexidade relacionada à adaptação deste conceito às nuances que acompanham as operações realizadas no ciberespaço (OLIVEIRA e TEIXEIRA, 2022).

Mesmo diante deste cenário, os esforços para sedimentar conceitos jurídicos e técnicos, que possam fazer frente a estas novas ameaças, ainda caminham de forma bem vagarosa. Isto porque as operações realizadas no ciberespaço extrapolam as fronteiras geográficas convencionais, apesar de suas estruturas físicas, lógicas, bem como os operadores "estarem abrigados em jurisdições diversas, interagindo numa relação de interdependência de estruturas cuja dinâmica não segue uma relação entre o espaço físico e o espaço virtual ou cibernético" (SALDAN, 2012 apud OLIVEIRA e TEIXEIRA, 2022)

O ciberespaço não pertence e não é administrado por governos, mas por diversos utilizadores de uma sociedade de informação globalizada (VILLELA, 2023). Em função do rápido crescimento das Tecnologias da Informação e Comunicação, o espaço cibernético permanece em constante mutação. Dessa forma, os elementos tradicionais de regulamentação e soberania praticados pelos Estados com o objetivo de diminuir os perigos decorrentes do ciberespaço são complexos de serem implementados.

Entretanto, para Nunes (2012) apud Villela (2023): "garantir a segurança do ciberespaço (cibersegurança) constitui hoje um imperativo nacional, essencial para garantir a soberania e a sobrevivência do país". É importante analisar as vulnerabilidades estratégicas e as possíveis ameaças presentes no espaço cibernético, sendo necessária a elaboração de uma Estratégia Nacional de Cibersegurança. VILLELA, 2023

"A Segurança Nacional começa em casa" (CALDAS e FREIRE, 2013 apud VILLELA (2023). Não basta somente nos sentirmos seguros dentro das nossas fronteiras físicas, devemos também estar seguros no ciberespaço. Para manter o ciberespaço seguro, Villela (2023) mostra que é necessário ter o conhecimento de quais informações devem ser protegidas e desenvolver uma estratégia de defesa da informação. Além disso, o autor complementa que deve haver um plano de proteção de infraestruturas críticas, no qual devem ser abordadas as seguintes questões: a caracterização de uma infraestrutura crítica; se possui conexão com a internet; se depende de tecnologias de informação; saber se caso seja perdida, se pode ameaçar a Segurança Nacional; se houver uma falha, existe a possibilidade de ser recuperado (VILLELA, 2023).

A postura conciliatória e pacifista do Brasil, que convive em paz com seus vizinhos há mais de um século, tendo realizado, em acordo com os demais países, a delimitação de suas fronteiras, o que contribuiu historicamente para a estabilização da região (JUNIOR, 2018). A posição de liderança do Brasil, que possui o maior poder militar e econômico da região, somado à sua postura diplomática de cooperação contribuem para a estabilidade e a prosperidade do entorno brasileiro, reforçando a segurança do País com efeitos positivos sobre todos os países da América do Sul (BRASIL, 2012 *apud* JUNIOR, 2018).

Em suma, o ciberespaço representa um campo complexo e dinâmico, onde questões legais, éticas e sociais estão constantemente interligadas e em evolução (JUNIOR e TRINDADE, 2024).

Conclusão

O ciberespaço surge como um novo cenário para fenômenos como o ciberterrorismo, desafiando os paradigmas de poder e governança e demandando estratégias diversas para sua compreensão e controle (Moniz, 2020). Entretanto, é

fundamental entender que a luta contra o terrorismo digital é um processo contínuo e dinâmico, que exige constante adaptação às novas ameaças e desafios que surgem.

Como uma evolução do terrorismo tradicional, o ciberterrorismo utiliza o ciberespaço para atingir metas políticas, religiosas ou ideológicas, alterando o cenário de batalha. Esse fenômeno não só amplia as fronteiras do terrorismo, como também agrava os problemas de segurança que Estados e organizações internacionais enfrentam (ASSIS, DIB e DOS SANTOS, 2024).

O combate ao terrorismo digital traz desafios complexos para a sociedade atual, demandando abordagens multidisciplinares e estratégias flexíveis. Com o aumento do terrorismo digital, que utiliza as tecnologias da informação e comunicação para espalhar propaganda extremista e organizar ações terroristas, é fundamental a adoção de medidas eficazes de combate (Gomes, 2018).

A implementação de políticas preventivas deve incluir não apenas o aprimoramento das capacidades tecnológicas, mas também a criação de estruturas regulatórias que definam responsabilidades, padrões de segurança e mecanismos de supervisão. Em contrapartida, as estratégias de combate devem incluir uma ampla gama de ações, desde a criação de equipes especializadas para enfrentar ataques cibernéticos até a elaboração de planos de contingência que possibilitem a rápida recuperação dos sistemas prejudicados (ASSIS, DIB e DOS SANTOS, 2024).

Portanto, é fundamental entender que nenhum sistema está completamente protegido contra ameaças digitais. Contudo, é importante considerar as opiniões de outros setores da sociedade, incluindo o setor acadêmico, responsável por conduzir pesquisas relevantes para abordar as lacunas nos temas relacionados. Assim, a cooperação entre governo, academia e setor privado é fundamental para reforçar as habilidades cibernéticas do país, incentivando uma estratégia mais unificada e eficaz para lidar com as ameaças digitais.

Nesse contexto, a pesquisa e o desenvolvimento de tecnologias de segurança cibernética, além da análise de tendências e padrões de comportamento online, são fundamentais para garantir a eficácia das estratégias de combate. É essencial assegurar que os direitos fundamentais dos cidadãos sejam protegidos e respeitados enquanto se trabalha para neutralizar as ameaças terroristas no ambiente digital.

A implementação de um "princípio da soberania" no ciberespaço é, de fato, desafiadora, devido à variedade de ações dos Estados nas áreas cinzentas do direito internacional cibernético em desenvolvimento. OLIVEIRA; TEIXEIRA, 2022. No entanto, uma questão fundamental é a necessidade de identificar o agressor com precisão para fazer inferências confiáveis e, assim, retaliar o ator transgressor. Contudo, é bastante desafiador identificar as origens dos ataques cibernéticos devido à estrutura do ciberespaço (GRASSI e PINTO, 2020).

Em suma, o ciberterrorismo no cenário geopolítico atual demanda uma ação conjunta entre os países e organizações internacionais. A natureza global e descentralizada da guerra informacional exige que os governos colaborem para criar estratégias de ciberdefesa eficientes (ASSIS; DIB; DOS SANTOS, 2024).

Referências

ASSIS, Herbert Bruno Magalhies; DIB, Rebeca Dantas; DOS SANTOS, Jorge Lucas Mota. Ciberterrorismo: a nova guerra moderna e a teoria das ondas do terrorismo. **Revista Delos**, v. 17, n. 62, p. 01-20, 2024.

AXON, Louise; STOLZ, Marcel. **Revisão das capacidades de segurança cibernética do Brasil**. Centro Global de Capacidade de Segurança Cibernética, 2023.

BECKER, Bertha Koiffmann. Geopolítica da Amazônia. **Estudos Avançados,** v. 19, n. 53, 2005.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. Lei nº. 13.260/2016 de 17 de março de 2016. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Publicado no D.O.U. de 17/03/2016. Brasília-DF, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13260.htm Acesso em: 18 out. 2025.

BRASIL. Norma Federal. Portaria GSIPR nº 2 de 08/02/2008. Publicado no Diário Oficial em 11 fev 2008. Institui Grupos Técnicos de Segurança de Infra-estruturas Críticas (GTSIC) e dá outras providências, 2008.

CAVALCANTE, Maria Madalena de Aguiar. A Amazônia no centro da Geopolítica Global. **Terra Livre**, v.2, n.63, p. 221-241, 2024.

COSTA, Matheus Souza. **O Ciberterrorismo diante do atual ordenamento jurídico brasileiro.** 2017. 62f. Monografia (Bacharelado em Direito). Universidade Federal de Lavras, Lavras, Minas Gerais, Brasil, 2017.

DA COSTA, Maurício Kenyatta Barros; MAIA, Nathan Ramires. Cooperação Interagências e Inteligência de Estado na Amazônia: estratégias integradas para o enfrentamento ao crime organizado transnacional. **Revista da Escola da Magistratura do Estado de Rondônia**, v. 1, n. 35, p. 287-314, 2025.

DAS CHAGAS, Morgana Santos. **Ciberterrorismo: as Possibilidades da Expansão do Terror nas Relações Internacionais**. 2012. 53f. Monografia **(**Bacharelado em Relações Internacionais**).** Universidade Estadual da Paraíba, João Pessoa, Paraíba, Brasil, 2012.

GALVÃO, Maria Luiza Alves Rocha. **Uma análise da defesa cibernética no Brasil: o papel do Guardião Cibernético**. 2025. 48f. Monografia (Bacharelado em Relações Internacionais). Universidade Federal da Paraíba, João Pessoa, Paraíba, Brasil, 2025.

GOUVEIA. Luís Borges. O Digital e a sua relação com as fronteiras físicas dos Estados. Trabalho de investigação individual. Curso de Defesa Nacional 2007/2008, **Instituto de Defesa Nacional**, Brasil, 2008

GRASSI, Jéssica Maria; PINTO, Danielle Jacon Ayres. 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

INSTITUTO IGARAPÉ; FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Governar para não entregar: uma agenda de segurança multidimensional para a Amazônia brasileira**. 2022. Disponível em: https://igarape.org.br/wp-content/uploads/2022/09/Agenda-de-Seguranca-Multidimensional-para-a-Amazonia.pdf. Acesso em: 14 out 2025.

JUNIOR, Julio Cesar Noschang. **As ameaças à soberania e à segurança do Estado no contexto das vulnerabilidades da Amazônia**. 2018. 73f. Dissertação (Mestrado em Ciências Aeroespaciais). Programa de Pós-Graduação em Ciências Aeroespaciais. Universidade da Força Aérea, Rio de Janeiro, Rio de Janeiro, Brasil, 2018.

JUNIOR, José Elias Seibert Santana; TRINDADE, Bruno Silva. Terrorismo Cibernético e Direitos Civis: explorando os limites do Direito Cibernético. **Revista Foco**, v. 17, n. 5, p. 01-29, 2024.

MATUSITZ, Jonathan. (2005). Cyberterrorism: How can American foreign policy be strengthened in the Information Age? **American Foreign policy Interests**, n. 27, v. 2, p. 137–147, 2025

NUNES, Danilo Henrique; LEHFELD, Lucas Souza; SILVA, Jonatas Santos. Ciberterrorismo: a internet como meio de propagação do terror. **Revista Húmus**. (UFMA Online), v. 10, n. 29, p. 209-234, 2020.

NUNES, Paulo Fernando Viegas. Cibersegurança, Tecnologias Disruptivas e Ciberdefesa Nacional: uma visão estratégica para a resiliência digital. **Cibersegurança, inteligência artificial e novas tecnologias na área de defesa**. XXIII Conferência de Direitos dos Colégios de Defesa Ibero Americanos. Escola Superior de Guerra, Rio de Janeiro, p. 324-349, 2022.

OLIVEIRA, Liziane Paixão Silva; TEIXEIRA, Alexandre Peres. O Direito Internacional e a Defesa Cibernética da soberania na Amazônia Azul: uma abordagem sob a luz do Manual de Tallinn 2.0. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 28, n. 2, p. 355-404, 2022.

REIS, Rafaela Pereira da Silva. Gestão Territorial na Amazônia: desafios da expansão hidrelétrica**. Terra Livre**, v.1, n. 64, p 418-443, 2025.

VILLELA, Stephanie Casanova. O Ciberterrorismo no século XXI: os desafios da Cibersegurança. **Revista do Ministério Público do Rio Grande do Sul**, v. 1, n. 93, p. 143-160, 2023.

Recebido em: 10/10/2025
Aprovado em: 28/10/2025
Publicado em: 31/10/2025