REVISTA ESMAT

Artigo

CONEXÃO ENTRE ELEMENTOS DE DEFESA CIBERNÉTICA E SEGURANÇA PÚBLICA NAS ATIVIDADES DAS POLÍCIAS MILITARES

Connection between cyber defense and public security elements in military police activities

Conexión entre elementos de defensa cibernética y seguridad pública en las actividades de las policías militares

Jorge Fabricio dos Santos[1]
Universidade Federal do Pará, Programa de Pós-Graduação em Desenvolvimento Sustentável do Trópico Úmido, Belém, PA, Brasil.
https://orcid.org/0000-0003-0349-183X
E-mail: fabrcio06@yahoo.com.br

Carlos Stilianidi Garcia[2]
Universidade Federal do Pará, Programa de Pós-Graduação em Desenvolvimento Sustentável do Trópico Úmido, Belém, PA, Brasil.
https://orcid.org/0000-0001-7765-326X
E-mail: carlosstilianidi@gmail.com

Durbens Martins Nascimento[3]
Universidade Federal do Pará, Programa de Pós-Graduação em Desenvolvimento Sustentável do Trópico Úmido, Belém, PA, Brasil.
https://orcid.org/0000-0002-8118-5152
E-mail: durbens@ufpa.br

Histórico do artigo:
Recebido em: 09 de julho de 2026
Aceito em: 21 de agosto de 2026
Revisado em: 14 de setembro de 2026
Publicado em: 18 de setembro de 2026

Editor responsável: Dr. Tarsis Barreto Oliveira
Assistente editorial: Me. Francielly Oliveira Rodrigues da Silva
Revisado por: Maria Ângela Barbosa Lopes

[1] Doutorando em Ciências do Desenvolvimento Socioambiental e mestre em Segurança Pública. CEL PMPA RR. Advogado inscrito na OAB/PA.
[2] Doutorando em Ciências do Desenvolvimento Socioambiental e mestre em Segurança Pública. Promotor de Justiça do Ministério Público do Pará (MPPA).
[3] Doutor em Ciências do Desenvolvimento Socioambiental e mestre em Segurança Pública. Professor da UFPA.

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

RESUMO

Este artigo investiga a integração da Defesa Cibernética às atividades de segurança pública desenvolvidas pelas polícias militares brasileiras, considerando o ordenamento jurídico vigente e o crescimento das ameaças no ambiente digital. O objetivo é analisar as possibilidades de integração entre a Defesa Cibernética e as competências institucionais dessas corporações. Trata-se de uma pesquisa aplicada, qualitativa e exploratória, realizada por meio de revisão narrativa da literatura, procedimentos bibliográficos e documentais. Os resultados demonstram que as polícias militares possuem respaldo jurídico para desenvolver ações preventivas contra crimes cibernéticos, produzir inteligência, proteger ativos institucionais, cooperar na segurança de infraestruturas críticas, resguardar grupos vulneráveis e fortalecer a cultura de segurança da informação, em articulação com os sistemas de segurança pública e defesa nacional. Conclui-se que a integração entre Defesa Cibernética e segurança pública é compatível com as competências constitucionais das polícias militares, desde que devidamente regulamentada, o que contribui para a preservação da ordem pública, da soberania nacional e dos direitos fundamentais. Destaca-se, ainda, a necessidade de capacitação permanente e de aperfeiçoamento institucional para enfrentamento das ameaças cibernéticas contemporâneas.

Palavras-Chave: Proteção de Ativos. Crimes Cibernéticos. Ações Preventivas. Infraestruturas Críticas. Grupos Vulneráveis.

ABSTRACT

This article investigates the integration of Cyber Defense into public security activities carried out by Brazilian Military Police forces, considering the current legal framework and the growing threats in the digital environment. The objective is to analyze the possibilities for integrating Cyber Defense with the institutional competencies of these organizations. The research is applied, with a qualitative approach and exploratory objectives, conducted through a narrative literature review and bibliographic and documentary procedures. The results demonstrate that Military Police forces have legal support to develop preventive actions against cybercrime, produce intelligence, protect institutional assets, cooperate in the security of critical infrastructures, protect vulnerable groups, and strengthen the information security culture, in coordination with public security and national defense systems. It is concluded that the integration of Cyber Defense and public security is compatible with the constitutional competencies of Military Police forces, provided that it is properly regulated, contributing to the preservation of public order, national sovereignty, and fundamental rights. The study also highlights the need for ongoing training and institutional improvement to address contemporary cyber threats.

Keywords: Asset Protection. Cybercrime. Preventive Actions. Critical Infrastructure. Vulnerable Groups.

RESUMEN

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

Este artículo investiga la integración de la Defensa Cibernética en las actividades de seguridad pública desarrolladas por las policías militares brasileñas, considerando el ordenamiento jurídico vigente y el crecimiento de las amenazas en el entorno digital. El objetivo es analizar las posibilidades de integración entre la Defensa Cibernética y las competencias institucionales de estas corporaciones. La investigación es aplicada, de enfoque cualitativo y objetivos exploratorios, realizada mediante una revisión narrativa de la literatura y procedimientos bibliográficos y documentales. Los resultados demuestran que las policías militares cuentan con respaldo jurídico para desarrollar acciones preventivas contra los delitos cibernéticos, producir inteligencia, proteger activos institucionales, cooperar en la seguridad de infraestructuras críticas, proteger a grupos vulnerables y fortalecer la cultura de seguridad de la información, en articulación con los sistemas de seguridad pública y defensa nacional. Se concluye que la integración entre la Defensa Cibernética y la seguridad pública es compatible con las competencias constitucionales de las policías militares, siempre que esté debidamente regulada, contribuyendo a la preservación del orden público, la soberanía nacional y los derechos fundamentales. Asimismo, se destaca la necesidad de capacitación permanente y perfeccionamiento institucional para enfrentar las amenazas cibernéticas contemporáneas.

Palabras Clave: Protección de Activos. Delitos Cibernéticos. Acciones Preventivas. Infraestructuras Críticas. Grupos Vulnerables.

1 INTRODUÇÃO

A Defesa Cibernética é um tema recente que vem ganhando mais espaço nas discussões acadêmicas e políticas, tendo em vista a intensa conexão informacional nas últimas décadas e a utilização de meios de tecnologia da informação em todas as atividades humanas, até mesmo em sistemas que fornecem serviços essenciais aos países, como segurança e defesa. Esses sistemas têm sido alvo de organizações e agentes maliciosos que desejam obter resultados ilegítimos (Pinto; Grassi, 2020; Hurel, 2021).

Nesse sentido, as organizações que atuam na Defesa Nacional não são as únicas que devem realizar atividades em prol da sociedade no campo cibernético; as corporações de segurança pública também precisam atuar nessa área (Souza; Almeida, 2016; Pena *et al*., 2024). Afinal, muitos agentes adversos pertencem a grupos criminosos que, por suas ações, afetam a soberania nacional e a segurança das pessoas – atribuições inerentes às polícias militares.

Este artigo, após verificar a conjuntura no Brasil, estabelece como problema de pesquisa: de que modo a Defesa Cibernética pode integrar-se às atividades de segurança pública desenvolvidas pelas polícias militares conforme os parâmetros jurídicos vigentes, por

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

meio da cibersegurança, da segurança da informação e da inteligência cibernética? E a partir deste questionamento científico, definiu-se como objetivo geral analisar, de acordo com as normas jurídicas brasileiras, como a Defesa Cibernética pode integrar-se às atividades de segurança pública desenvolvidas pelas polícias militares, sob as premissas da segurança da informação, da cibersegurança e do ramo cibernético da atividade de inteligência.

A partir da finalidade geral deste estudo, elencam-se como objetivos específicos: a) apresentar os fundamentos jurídicos da Defesa Cibernética no Brasil, atrelados ao temas da cibersegurança, da segurança da informação e da inteligência cibernética; b) demonstrar a concepção da segurança pública no contexto da Defesa Cibernética e seus elementos ao anteriormente citados, conforme as pesquisas publicadas acerca do tema; e c) descrever as atribuições das polícias militares em relação aos parâmetros da defesa cibernética.

O estudo apresenta relevância institucional tendo em vista a necessidade de modernização da segurança pública ante as ameaças cibernéticas que afetam tanto a Defesa Nacional quanto os direitos fundamentais dos cidadãos. No que concerne à Defesa Nacional, compreender essa problemática possibilita que as polícias militares possam colaborar com as Forças Armadas em ações estratégicas e operacionais. Dessa forma, a compreensão da Defesa Cibernética poderá auxiliar na criação de mecanismos normativos, doutrinários e tecnológicos para essas corporações.

No âmbito social, a pertinência é observada pela importante atribuição constitucional das polícias militares na prevenção de quaisquer tipos de ilícitos, incluindo os de natureza cibernética – como fraudes e divulgação ilegal de dados pessoais. Tais crimes registram crescimento anual, vitimando diversos segmentos da sociedade e potencializando os casos envolvendo grupos de alta vulnerabilidade social, como crianças, adolescentes, pessoas idosas e os neurodivergentes.

A relevância acadêmica é notória, visto que é evidente a limitada produção científica nacional direcionada a discutir a relação entre Defesa Cibernética e a atuação das polícias militares. Dessa maneira, a pesquisa pode contribuir para o avanço das discussões interdisciplinares envolvendo segurança pública, inteligência, gestão da informação, defesa e tecnologia, bem como alargar o debate científico acerca da adaptação das instituições policiais às ameaças digitais contemporâneas, o que servirá como referencial para futuras pesquisas relacionadas ao tema.

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

Este artigo está estruturado da seguinte forma: o Capítulo 1 introduz o tema com sua pergunta-problema, objetivos e justificativa; o Capítulo 2 (Desenvolvimento) estabelece os fundamentos jurídicos e teóricos sobre o temática; em seguida, o Capítulo 3 (Metodologia) descreve a natureza do estudo, com seu lócus de pesquisa, fontes, procedimentos de coleta de dados e técnicas de análise; o Capítulo 4 (Resultados e Discussão) demonstra a conexão entre as competências das polícias militares e a Defesa Cibernética; por fim, o artigo encerra-se com as Considerações Finais, apresentando os principais resultados, conclusões, limitações e sugestões sobre o tema.

2 REFERENCIAL TEÓRICO

2.1 Defesa cibernética: elementos normativos brasileiros

Inicialmente, a Defesa Cibernética foi prevista normativamente na Estratégia Nacional de Cibersegurança (E-Ciber), instituída pelo Decreto nº 12.573, de 2025, a qual define elementos relacionados ao setor cibernético, considerado como estratégico para o Brasil e estabelece diretrizes para sua organização (Brasil, 2025a). O texto normativo define, até mesmo cibersegurança, ciberdefesa e cibercrime, sendo este último conceituado como "crime praticado contra ou por meio de ciberativos"[4] (Brasil, 2025a).

Essa norma estabelece que a ciberdefesa é competência do Ministério da Defesa (Nonato; Pinho, 2021), tendo em vista que um dos objetivos é prover a segurança dos ciberativos que impactam a defesa nacional – aspecto já mencionado no Livro Branco de Defesa Nacional (LBDN) –, versão de 2024 (Brasil, 2025c). Por sua vez, a E-Ciber conceitua a cibersegurança como o complexo de processos, diretrizes, ferramentas e tecnologias destinado a proteger o espaço cibernético e os ciberativos (Vianna; Camelo, 2020; Brasil, 2025a), distinguindo-a da ciberdefesa por apresentar maior alinhamento com as funções da segurança pública (Pinto; Grassi, 2020; Gomes, 2024).

Nesse sentido, a Estratégia Nacional de Cibersegurança prevê, conforme o art. 4º (Brasil, 2025a), ações direcionadas à proteção e à conscientização do cidadão e da sociedade, como a prevenção e o enfrentamento de cibercrimes e outros delitos virtuais (Barbosa,

[4] "Art.2º "I - ciberativos - *hardwares*, *softwares*, redes, dispositivos, aplicações, serviços, sistemas e dados utilizados para processar, armazenar ou transmitir informações por meio eletrônico ou digital [...]" (Brasil, 2025).

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

2024), o aprimoramento de normas e estruturas voltadas ao combate a tais crimes (Graça, 2015), além da capacitação e do aperfeiçoamento dos órgãos de persecução penal (Brasil, 2025; Silva; Maletta, 2021). No ambiente acadêmico, a norma fomenta a produção de conhecimento acerca da cibersegurança (Brasil, 2025a).

A E-Ciber propõe a integração entre vários atores institucionais, privados e públicos, para a consecução das suas diretrizes e para a proteção da Defesa Nacional no campo virtual (Graça, 2015; Araújo, 2020), tendo o Plano Nacional de Cibersegurança como um dos seus principais instrumentos (Brasil, 2025a).

Ressalta-se que a atual E-Ciber (de 2025) representa uma evolução de normas anteriores. Entre elas, destaca-se a versão instituída pelo **Decreto nº 10.222, de 2020**, concebida como o primeiro módulo da Estratégia Nacional de Segurança da Informação, que previu a prevenção e a mitigação de ameaças cibernéticas e a adoção de parcerias estratégicas. Mencionam-se, ainda, o ***Livro Verde*: segurança cibernética no Brasil,** publicado em 2010, que contribuiu para a consolidação do debate estatal sobre a proteção do espaço cibernético e das infraestruturas críticas, e a **Portaria Normativa nº 3.389/MD/2012,** que aprovou a primeira edição da **Política Cibernética de Defesa (MD31-P-02),** cujo foco restringia-se à Defesa Nacional, além de outros regramentos nacionais sobre a temática.

Nesse sentido a Defesa Cibernética, conforme a Doutrina Militar de Defesa Cibernética -MD31-M008, é:

> [...] conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (Brasil, 2014, p.18).

A Defesa Cibernética configura-se como instrumento de proteção da soberania nacional no âmbito do espaço cibernético, sob a gestão do Ministério da Defesa, que emprega os processos da atividade de inteligência – a qual é "caracterizada pelo exercício permanente de ações especializadas no cumprimento de duas funções: informar e executar" (Brasil, 2023c, p. 90). Estas ações, quando empregam meios cibernéticos, recebem a nomenclatura de Inteligência Cibernética[5].

[5] "**Inteligência cibernética**: área de atuação da inteligência voltada a temas relativos ao espaço cibernético, cuja produção busca apoiar a atuação do Brasil ante vulnerabilidades e ameaças cibernéticas, informando políticas

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

A Política Nacional de Cibersegurança (PNCiber), instituída pelo Decreto nº 11.856, de 2023, reforça as diretrizes e os objetivos da E-Ciber. Nesse momento destacam-se como relevantes o fomento às atividades de pesquisa científica, previsto no inciso VIII do art. 3º, e os princípios relativos à proteção virtual de grupos vulneráveis, à cooperação entre entidades públicas dos entes federativos e à garantia de proteção de direitos fundamentais (Brasil, 2023a) – sendo estes últimos diretamente relacionados à segurança da informação (Galdoni; Rodrigues; Medeiros, 2024).

Para tanto, o desenvolvimento do artigo fundamenta-se em uma análise crítica da literatura especializada, articulando doutrina, legislação, jurisprudência, documentos normativos e produção científica relacionada ao objeto investigado.

2.2 A Segurança Pública enquanto serviço estatal

Nessa esteira, o arcabouço normativo complementa-se, no âmbito da segurança pública, pela Política Nacional de Segurança da Informação (Decreto nº 12.572/2025b). Esta norma, que além de incluir a Defesa Nacional entre os seus princípios, elenca ainda no art. 3º, inciso III, "a garantia dos direitos fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a privacidade e o acesso à informação, ressalvadas as hipóteses de sigilo previstas em lei [...]" (Brasil, 2025b).

Essa realidade é verificável quando da eclosão de crimes cibernéticos, situação em que a prevenção e a repressão por meio da investigação criminal requerem níveis atualizados de conhecimentos teóricos e práticos atualizados (Jesus; Silva, 2023).

No Brasil, em 2018, foram instituídos o Sistema Único de Segurança Pública (SUSP) e a Política Nacional de Segurança Pública e Defesa Social (PNSPDS), por meio da Lei nº 13.675, de 2018. Essa legislação estabeleceu a integração de todos os entes federativos na prestação da segurança pública – incluindo os municípios – e elencou diversos parâmetros doutrinários e instrumentais para a efetividade desse serviço público (Brasil, 2018). Nessa norma jurídica, destacam-se, no art. 4º, incisos I, III, IV e V, os princípios da PNSPDS relativos à obrigatoriedade de os órgãos do SUSP promoverem o respeito aos direitos

públicas e planos estatais nesse domínio, bem como acompanhar e avaliar capacidades, intenções e atividades de atores externos no espaço cibernético" (Brasil, 2023c, p. 159).

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

fundamentais mediante ações preventivas e repressivas contra ilícitos penais, sem vedar a execução de medidas no meio cibernético (Reis Netto; Santos; Chagas, 2021).

Outro elemento que se correlaciona com a Política Nacional de Segurança da Informação no âmbito das polícias militares é a atividade de inteligência de segurança pública – mais especificadamente aquela que emprega meios cibernéticos. Esse cenário resulta de ações operacionais com foco na prevenção de ilícitos que necessitam de instrumentos tecnológicos robustos à coleta e à análise de dados, a fim de produzir conhecimento para os gestores dessas organizações.

Dessa forma, a partir da apresentação de elementos normativos e conceituais relevantes para este estudo, evidencia-se a articulação entre os termos norteadores desta pesquisa.

Figura 1 – Quadro analítico dos elementos de estudo do artigo

Elemento de Análise	Definição	Previsão Legal
Ciberdefesa	Capacidade de proteção dos interesses da Defesa Nacional no espaço cibernético contra ameaças e ações adversas	Decreto nº 12.573, de 2025 – Estratégia Nacional de Cibersegurança (E-Ciber), Política Cibernética de Defesa- MD31-P-02 e Doutrina Militar de Defesa Cibernética - MD31-M-07
Cibersegurança	Conjunto de ações destinadas à prevenção, à proteção, à detecção, à resposta e à recuperação diante de incidentes e ameaças no espaço cibernético	Decreto nº 11.856, de 2023 –Política Nacional de Cibersegurança (PNCiber)
Segurança da Informação	Proteção das informações e dos ativos informacionais, buscando preservar atributos como confidencialidade, integridade, disponibilidade e autenticidade	Decreto nº 9.637, de 2018 – Política Nacional de Segurança da Informação (PNSI)
Inteligência Cibernética	Produção de conhecimento a partir de dados e informações do ambiente	Doutrina Nacional de Inteligência / Doutrina Nacional de Inteligência de

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

	cibernético	Segurança Pública

Fonte: Elaborado pelos autores (2026).

2.3 Polícias Militares

As polícias militares, enquanto órgãos previstos na Constituição Federal, em seu art.144, § 5º, são responsáveis por realizar serviços em prol da segurança pública, especificamente na preservação da ordem pública, prevenindo ilícitos penais por meio do chamado policiamento ostensivo fardado (Brasil, 1988). Ademais, são expressamente definidas como forças auxiliares e reserva do Exército Brasileiro, com foco na defesa interna e na preservação das instituições democráticas (Moraes; Augusto Júnior, 2021).

Com o advento da Lei Orgânica Nacional das Polícias Militares e Corpos de Bombeiros Militares, tais órgãos estatais passaram a integrar formalmente o Sistema de Defesa Nacional, conforme preconiza a alínea "b" do inciso V do art. 2º da Lei nº 14.751, de 2023 (Brasil, 2023b), em consonância com a previsão constitucional de subordinação às forças armadas terrestres (Maccari, 2024).

As normas jurídicas evidenciam que a atuação das Polícias Militares deve anteceder o crime. Assim não se limita ao policiamento ostensivo, mas engloba igualmente metodologias vinculadas à prevenção primária, isto é, práticas orientativas destinadas a evitar que grupos sociais cometam infrações penais.

2.4 Metodologia

No que tange à sua finalidade, este artigo optou por uma pesquisa de natureza aplicada, visto que objetivou averiguar como os pressupostos normativos da Estratégia de Defesa Cibernética Brasileira podem ser aplicados pelas polícias militares (Prodanov; Freitas, 2013). Quanto aos procedimentos técnicos utilizados, propôs-se uma pesquisa bibliográfica e documental, conduzida mediante revisão bibliográfica e narrativa; de modo que a primeira fundamentou-se em dados de artigos científicos e pesquisas afins, e a segunda, derivada de apurações das legislações em vigência referentes ao tema, integrando tais informações, a fim de responder à pergunta-problema do artigo (Gil, 2019).

No que concerne aos objetivos, empregou-se uma pesquisa exploratória, pois o escopo deste artigo foi demonstrar, de forma mais geral, as maneiras de atuação das polícias militares

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

conforme as premissas da Defesa Cibernética no Brasil (Brasileiro, 2024). Por fim, quanto à abordagem, definiu-se a realização de uma pesquisa qualitativa, baseada em dados normativos e teóricos, os quais dispensam o uso de métodos matemáticos e/ou estatísticos (Prodanov; Freitas, 2013).

Tendo em vista a avaliação da estratégica nacional aplicável a organizações públicas, o Brasil foi definido como o lócus da pesquisa – mais precisamente, todas as unidades da Federação nas quais as polícias militares atuam como órgãos de segurança pública. Tais instituições são encarregadas de prover a manutenção da ordem pública e a garantia dos direitos fundamentais, por meio de ações de prevenção a ilícitos e vulnerabilidades sociais e, indiretamente, de garantia da Defesa Nacional, até mesmo no meio cibernético.

Nesse sentido, a bibliografia adotada foi coletada virtualmente mediante buscas nos acervos acadêmicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes) e *Scientific Eletronic Library Online* (*SciELO*), com recorte temporal de 2015 a 2026, visto que as atuais ameaças à segurança cibernética se intensificaram nos últimos anos. Os dados de natureza documental (jurídica) foram obtidos diretamente nos sítios eletrônicos institucionais que disponibilizam legislações e normas técnicas correlacionados ao tema pesquisado, como o Portal do Planalto, entre outros.

Ainda sobre a pesquisa bibliográfica, a busca por trabalhos publicados foi realizada com a utilização de descritores “Defesa Cibernética”, “Segurança Pública”, “Polícia Militar”, “Segurança da Informação” e “Inteligência Cibernética”, em textos produzidos em língua portuguesa. Adotaram-se como critérios de inclusão os trabalhos de conclusão de curso, teses, dissertações e artigos acadêmicos, sendo encontradas, inicialmente, 30 pesquisas; entretanto, após avaliação da pertinência temática, chegou-se a 20 estudos, os quais foram utilizados neste trabalho.

2.5 Resultados e discussão

As polícias militares, enquanto órgãos de segurança pública, seguem os ditames constitucionais e infraconstitucionais. Sendo integrantes do Sistema de Defesa Nacional, como disposto na Lei nº 14.751, de 2023, e do Sistema Único de Segurança Pública, de acordo com a Lei nº 13.675, de 2018, elas podem atuar em várias vertentes, integrando ambos os sistemas e suas finalidades à luz da Defesa Cibernética no Brasil.

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

Observa-se, ante as normas jurídicas vigentes no país, que as polícias militares devem atuar de modo cooperativo com as instituições de defesa nacional, subordinadas à coordenação dessas organizações e seguindo rigidamente as legislações quando se tratar de atividades da Ciberdefesa; entretanto, quanto à Cibersegurança, as referidas organizações estaduais devem realizar atividades de maneira direta. O mesmo se aplica à chamada Inteligência Cibernética (na produção de conhecimento para o processo decisório) e às diretrizes e procedimentos de Segurança da Informação, uma vez que esta se destina à proteção dos ativos informacionais das polícias militares.

2.5.1 Prevenção de crimes cibernéticos no âmbito da ordem pública

Como instituições que possuem em sua essência o caráter preventivo de quaisquer ações que violem a ordem pública e os direitos fundamentais, como descrito no art. 144, § 5º, da Constituição Federal (Brasil, 1988), as polícias militares abrangem, além do ambiente físico, o virtual, em que práticas ilícitas também ocorrem, como os crimes virtuais, já que este tipo de crime é elemento conjuntural muito presente no Brasil.

Essas atividades devem atender ao Eixo 1 – Proteção e conscientização do cidadão e da sociedade do E-Ciber (Brasil, 2025a), os princípios e objetivos da PNCiber (Brasil, 2023a) e aos princípios e objetivos da PNSI (Brasil, 2025b), de modo que as polícias militares possam:

1. Desenvolver programas de conscientização sobre golpes eletrônicos, fraudes bancárias, crimes contra crianças e adolescentes e idosos na internet e desinformação digital;
2. Realizar campanhas educativas em escolas, universidades e comunidades;
3. Produzir alertas de segurança para a população por meio das redes sociais institucionais;
4. Atuar na prevenção de ataques que gerem perturbação da ordem pública, como a disseminação coordenada de notícias falsas capazes de provocar pânico social.

Tais ações atendem diretamente aos incisos X, XI, XII, XIII e XIV do art. 4º do Decreto nº 12.573, de 2025, no que tange aos cibercrimes, desde a atividade orientativa preventiva para as potenciais vítimas até as ações e as operações no ambiente virtual (Brasil, 2025a), além do cumprimento dos incisos II e V do art. 2º e incisos III, IV e VII do art.3º do

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

Decreto nº 11.856, de 2023 (Brasil, 2023a) e incisos II, III, IV e V do art.3º e incisos I, VI e VII do art. 4º do Decreto nº 12.572, de 2025 (Brasil, 2025b).

Dentro desse campo, ainda deve ter um olhar específico para o denominado crime organizado digital, uma vez que inúmeras Organizações Criminosas (Orcrim) utilizam tecnologias de informação para a consecução de lavagem de dinheiro, extorsões digitais, fraudes eletrônicas, comércio ilícito em ambientes virtuais e coordenação de atividades criminosas. Dessa forma, as polícias militares podem colaborar por meio de ações de inteligência policial militar. identificando padrões de atuação criminosa no ambiente digital, compartilhando informações e prestando apoio operacional a forças-tarefa integradas com outros órgãos de segurança pública e de defesa nacional (Souza; Almeida, 2016; Jesus; Silva, 2023; Pena *et al*., 2024), considerando que as Orcrim atuam em conjunto com grupos criminosos transnacionais.

Outro item relevante para a segurança cibernética quanto ao combate a ilícitos diz respeito à proteção de pessoas que fazem parte de grupos vulneráveis, como crianças, adolescentes e idosos que, por sua hipossuficiência de conhecimento do mundo virtual (Pena *et al*., 2024), podem ser vitimizadas com mais frequência do que outras pessoas.

2.5.2 Produção de inteligência de segurança pública no ambiente cibernético e proteção de ativos

Considerando que as polícias militares realizam a atividade de inteligência de segurança pública seguindo os parâmetros da Doutrina Nacional de Inteligência de Segurança Pública (DNISP) (Brasil, 2014), essas organizações coletam dados em várias fontes para a produção de conhecimento, com o fito de identificar as ameaças à ordem pública e de subsidiar a tomada de decisão de seus gestores (Corrêa, 2024). Muitas vezes, essa atuação ocorre em ambientes e sistemas virtuais, visando proteger seus ativos – principalmente pessoas, organizações e suas informações estratégicas (Vianna; Camelo, 2020) –, podendo abranger as seguintes ações:

1. Monitorar fontes abertas (*Open Source Intelligence (OSINT)*) para identificação de riscos à segurança pública;
2. Detectar movimentações de organizações criminosas em ambientes digitais;

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

3. Identificar campanhas de radicalização, recrutamento criminoso e planejamento de ações violentas;
4. Compartilhar informações estratégicas com órgãos do Sistema Brasileiro de Inteligência e demais instituições de segurança;
5. Implantar centros de segurança da informação;
6. Desenvolver equipes de resposta a incidentes cibernéticos (CSIRT/CERT);
7. Proteger bancos de dados operacionais e estratégicos;
8. Implementar políticas de gestão de riscos cibernéticos;
9. Realizar auditorias de segurança e testes de vulnerabilidade.

É importante ressaltar que a atividade de inteligência das polícias militares, tanto em ambientes físicos quanto virtuais, não se confunde com a investigação criminal, uma vez que esta última é atribuída legalmente às polícias judiciárias (Polícia Federal e polícias civis), durante a persecução penal em apoio ao Sistema de Justiça – embora possa ser realizada pelas polícias militares no caso dos crimes de natureza militar (Santos; Garcia, 2026), conforme normas específicas. A DNISP prevê a Atividade de Inteligência Policial Judiciária como instrumento auxiliar da investigação (Brasil, 2014).

A atividade de inteligência cibernética praticada pelas polícias militares atende ao previsto nos incisos XII e XIV do art. 4º do Decreto nº 12.573, de 2025, mediante o aumento do volume de conhecimentos elaborados para o enfrentamento dos crimes cibernéticos, atendendo aos pressupostos da E-Ciber (Brasil, 2025a), seja no cumprimento dos princípios dos incisos VI e VII do art. 2º do Decreto nº 11.856, de 2023 (Brasil, 2023a) relativos à PNCiber, seja quanto à cooperação entre as diversas instituições no compartilhamento de dados, informações e conhecimentos acerca de ameaças no ambiente cibernético (Silva e Maletta, 2021; Veronese, 2025), além dos objetivos descritos nos incisos II, V e IX do art. 3º da mesma norma (Brasil, 2023a), que correspondem ao provimento dos atributos essenciais das informações armazenadas, processadas ou em transmissão, a saber: confidencialidade, integridade, autenticidade e disponibilidade (Ayres Pinto; Grassi, 2020; Galdoni; Rodrigues; Medeiros, 2024).

Esses requisitos da informação seguem ainda os parâmetros da PNSI (Brasil, 2025b) segundo os quais as polícias militares devem envidar esforços quanto aos princípios expressos nos incisos I, II, V e VI do ar. 3º do Decreto nº 12.572 de 2025, quais sejam: trabalhar para

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

viabilizar a soberania nacional, estabelecendo diretrizes relacionadas à segurança da informação sob o poder da instituição militar, atuar de forma colaborativa com outras entidades e órgãos da administração pública de todos os entes federativos (Graça, 2015; Araújo, 2024; Gomes, 2024) e atuar no escopo da gestão de riscos internos de segurança da informação e dos cidadãos-usuários de seus serviços (Nonato; Pinho, 2021; Veronese, 2025).

2.5.3 Cooperação na proteção de infraestruturas críticas

A segurança interna e a proteção das instituições democráticas também se configuram como competência das polícias militares. Para isso, tais organizações devem integrar-se às instituições de defesa nacional, porque, sendo a soberania nacional um instituto jurídico que abrange a função de proteção das infraestruturas críticas (Lima *et al*., 2025; Vianna; Camelo, 2020), essas organizações militares estaduais devem desenvolver processos finalísticos e administrativos (Araújo, 2024), como, por exemplo, em:

- Sistemas de energia;
- Abastecimento de água;
- Telecomunicações;
- Transporte público;
- Sistema bancário;
- Sistema judiciário e policial;
- Sistemas governamentais essenciais.

Essas estruturas funcionam hoje com base em sistemas de tecnologia da informação que podem ser violados e, se forem afetados por agentes maliciosos, prejudicar tanto a soberania nacional quanto os direitos fundamentais das pessoas, as quais poderão ter suas necessidades basilares comprometidas. Para tanto, faz-se necessária, conforme preconizam o art. 5º da E-Ciber – que trata da segurança e da resiliência dos serviços essenciais e das infraestruturas críticas – e o seu art. 9º, referente à soberania nacional e governança (Brasil, 2025a), além do inciso II do art. 2º da PNCiber, relativo ao princípio de prevenção de incidentes e de ataques cibernéticos não somente às estruturas críticas nacionais, mas também aos serviços considerados essenciais à sociedade (Nonato; Pinho, 2021) e do objetivo IX do seu art. 3º (Brasil, 2025a), a atuação coordenada em questões de segurança cibernética entre órgãos estaduais (aqui incluídas às polícias militares) e órgãos de demais entes federativos

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

(Araújo, 2024).

Nesses casos, a atuação das polícias militares pode ocorrer por meio da articulação com órgãos de defesa civil, uma vez que, de acordo com a Lei Orgânica Nacional das Polícias Militares e dos Corpos de Bombeiros Militares, tais organizações são integrantes do Sistema de Defesa Civil (Maccari, 2024), além das Forças Armadas, agências reguladoras e empresas responsáveis pelos serviços essenciais, atendendo aos presupostos da E-Ciber e também aos dispositivos dos incisos I, V e VI do art. 2º do Decreto nº 12.572, de 2025 referentes à PNSI (Brasil, 2025b).

2.5.4 Proteção de grupos vulneráveis no ambiente digital

Em atendimento à premissa do art. 3º da E-Ciber, que estabelece a necessidade de proteção e de conscientização do cidadão e da sociedade – especialmente de pessoas em situação de vulnerabilidade (Brasil, 2025a) –, a literatura destaca que a governança da cibersegurança deve integrar ações de educação, de coordenação institucional e de fortalecimento de políticas públicas (Galdoni; Rodrigues; Medeiros, 2024; Pena *et al*., 2024).

Nesse contexto, crianças, adolescentes, idosos e pessoas com características neurodivergentes demandam atenção específica. Além disso, a Política Nacional de Cibersegurança reitera essa diretriz no art. 3º, III, do Decreto nº 11.856, de 2023 (Brasil, 2023a), em consonância com a necessidade de mecanismos regulatórios e de proteção de dados que fortaleçam a segurança e a defesa cibernéticas (Barbosa, 2024).

Assim, as polícias militares podem atuar por meio de:

- programas de prevenção ao *cyberbullying*;
- orientação a idosos sobre golpes eletrônicos;
- ações de proteção a crianças e adolescentes contra a exploração sexual *online*;
- apoio a vítimas de violência digital e perseguição virtual.

Verifica-se que a atuação das polícias militares, conforme a PSI, também deve direcionar-se à formação e à capacitação de agentes públicos para a promoção da segurança da informação, atendendo a critérios de diversidade (Brasil, 2025b). Tal direcionamento é relevante, uma vez que pessoas em situação de vulnerabilidade social – como crianças, adolescentes, idosos e indivíduos neurodivergentes – muitas vezes não possuem

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

conhecimento suficiente acerca dos riscos presentes no ambiente virtual, o que as torna mais suscetíveis a agentes maliciosos (Pena *et al*., 2024).

Nesse contexto, a capacitação dos agentes públicos constitui elemento essencial para a implementação de políticas de conscientização e de proteção da sociedade, fortalecendo a governança da cibersegurança (Galdoni; Rodrigues; Medeiros, 2024). Além disso, a articulação entre capacitação, regulação e proteção de dados contribui para o fortalecimento da segurança da informação e da defesa cibernética no âmbito da administração pública (Barbosa, 2024).

Para o cumprimento dessas atribuições, conforme destacado neste artigo, a capacitação dos policiais militares quanto aos fundamentos jurídicos e aos procedimentos à Defesa Cibernética no tocante à segurança cibernética é um elemento essencial para a efetividade dessas atividades. Como tais competências decorrem de ações formativas e de especializações técnicas, sugere-se que as polícias militares realizem: a) a criação de cursos de cibersegurança para policiais militares e colaboradores internos das organizações; b) a inclusão de disciplinas relacionadas ao ciberespaço nos cursos de formação de Oficiais e Praças; c) o desenvolvimento de especializações em inteligência cibernética; e d) a capacitação de gestores para proteção de ativos digitais institucionais.

3 CONSIDERAÇÕES FINAIS

O presente artigo teve como objetivo geral analisar, à luz das normas jurídicas brasileiras, de que forma a Defesa Cibernética pode integrar as atividades de segurança pública desenvolvidas pelas polícias militares. A investigação caracterizou-se como uma pesquisa de natureza aplicada, com abordagem qualitativa, objetivos exploratórios e procedimentos bibliográficos – configurando-se como uma revisão narrativa da literatura – e documentais, pautada na interpretação das normas que disciplinam a cibersegurança, a defesa cibernética e a segurança pública no ordenamento jurídico brasileiro.

Os resultados obtidos permitiram responder de forma satisfatória à pergunta-problema inicialmente proposta. Verificou-se que o ordenamento jurídico brasileiro, especialmente após a instituição da Política Nacional de Cibersegurança, da Estratégia Nacional de Cibersegurança e da Política Nacional de Segurança da Informação, oferece fundamentos normativos suficientes para que as polícias militares atuem de maneira integrada às políticas

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

nacionais de Defesa Cibernética. Contudo, para a efetivação dessa atuação pelas corporações, ainda é necessária a adoção de normas jurídicas mais assertivas.

Embora a ciberdefesa permaneça como atribuição estratégica do Ministério da Defesa, constatou-se que as competências legais das polícias militares – estabelecidas, principalmente, pela Lei Orgânica Nacional das Polícias Militares e dos Corpos de Bombeiros Militares – permitem sua atuação preventiva, colaborativa e complementar na proteção do espaço cibernético, especialmente nas atividades relacionadas à segurança pública, à preservação da ordem pública, à proteção de direitos fundamentais e à cooperação interinstitucional.

No desenvolvimento da pesquisa, foi possível identificar que as atividades das polícias militares extrapolam o policiamento ostensivo tradicional, atendendo a novas demandas decorrentes da transformação digital da sociedade. Nesse contexto, verificou-se que a prevenção dos crimes cibernéticos constitui uma das principais formas de integração entre a segurança pública e a Defesa Cibernética, mediante campanhas educativas, orientação da população, enfrentamento à desinformação, prevenção de fraudes eletrônicas, proteção de crianças, de adolescentes, de idosos e demais grupos em situação de vulnerabilidade, além da produção de conhecimento voltado ao fortalecimento da cultura de segurança digital.

Também se constatou que a atividade de inteligência de segurança pública representa um importante mecanismo de integração com a Defesa Cibernética, possibilitando às polícias militares o desenvolvimento de ações de monitoramento de fontes abertas, identificação de ameaças digitais, compartilhamento de informações estratégicas, proteção de ativos institucionais, gestão de riscos cibernéticos e cooperação com os órgãos integrantes do Sistema Brasileiro de Inteligência, do Sistema Único de Segurança Pública e do Sistema de Defesa Nacional. Da mesma forma, verificou-se que a atuação dessas corporações pode contribuir para a proteção das infraestruturas críticas nacionais e dos serviços essenciais, reforçando a resiliência institucional diante das ameaças cibernéticas contemporâneas.

Conclui-se, portanto, que a Defesa Cibernética e a segurança pública não constituem áreas isoladas, mas complementares no âmbito da proteção do Estado e da sociedade brasileira. A evolução normativa demonstra uma tendência de fortalecimento da governança da segurança cibernética mediante atuação coordenada entre órgãos civis e militares, permitindo que as polícias militares exerçam um relevante papel preventivo, educativo, estratégico e de inteligência, respeitando os limites constitucionais de suas competências.

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

Assim, a incorporação de práticas relacionadas à cibersegurança representa uma medida compatível com a missão legal dessas instituições, contribuindo simultaneamente para a preservação da ordem pública, da soberania nacional e da proteção dos direitos fundamentais.

Nota-se, por fim, que a segurança jurídica da atuação das polícias militares requer a instituição de regulamentação específica, por meio de normas jurídicas efetivas, as quais possibilitarão, sem margens para dúvidas, a realização dessas atividades, além de favorecerem a cooperação institucional, capacitação técnica e a criação de salvaguardas adicionais.

Como propostas decorrentes deste estudo, sugere-se que as polícias militares promovam a institucionalização de políticas permanentes de segurança cibernética, mediante a criação de núcleos especializados, a implantação de Centros de Resposta a Incidentes Cibernéticos (CSIRTs), o fortalecimento das atividades de inteligência cibernética, a ampliação da cooperação técnica com as Forças Armadas, a Polícia Federal, as polícias civis e demais órgãos integrantes do Sistema Único de Segurança Pública (SUSP), bem como a inclusão de conteúdos relacionados à Defesa Cibernética, à Segurança da Informação, à Proteção de Dados, à Inteligência Digital e à Gestão de Riscos nos cursos de formação, aperfeiçoamento e especialização de Oficiais e Praças.

Recomenda-se, ainda, a elaboração de protocolos operacionais voltados à atuação preventiva em crimes cibernéticos, à proteção de infraestruturas críticas e ao atendimento de grupos vulneráveis no ambiente digital, fortalecendo a capacidade institucional das corporações ante as ameaças emergentes. Como limitações desta investigação, destaca-se que a pesquisa concentrou-se na análise normativa e bibliográfica, não contemplando estudos empíricos nas polícias militares brasileiras nem avaliações quantitativas acerca da implementação das políticas de Defesa Cibernética nas corporações estaduais.

Além disso, por tratar-se de um campo em constante evolução tecnológica e normativa, novas legislações, doutrinas e estruturas institucionais poderão alterar o cenário atualmente analisado. Dessa forma, recomenda-se que pesquisas futuras desenvolvam estudos de caso em diferentes unidades da Federação, realizem análises comparativas entre modelos nacionais e internacionais de atuação policial no ambiente cibernético e investiguem o grau de maturidade das polícias militares brasileiras na implementação de Políticas de Cibersegurança e Defesa Cibernética.

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

REFERÊNCIAS

ARAUJO, José Euclides Oliveira de. **A atuação da Defesa Cibernética na proteção de infraestruturas críticas do Brasil**. 2020. Trabalho de Conclusão de Curso (Especialização em Altos Estudos em Defesa) – Escola Superior de Guerra, Brasília, 2020.

BARBOSA, Jeferson Dias. **A influência da regulação e fiscalização da Lei Geral de Proteção de Dados (LGPD) na segurança e defesa cibernética no Brasil**. 2024. Trabalho de Conclusão de Curso (Curso Superior de Segurança e Defesa Cibernética) – Escola Superior de Guerra, Rio de Janeiro, 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 jun. 2026.

BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11856.htm. Acesso em: 4 jun. 2026.

BRASIL. **Decreto nº 12.572, de 4 de agosto de 2025**. Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12572.htm. Acesso em: 4 jun. 2026.

BRASIL. **Decreto nº 12.573, de 4 de agosto de 2025**. Institui a Estratégia Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12573.htm. Acesso em: 4 jun. 2026.

BRASIL. **Decreto nº 12.725, de 18 de novembro de 2025**. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro-branco-de-defesa-nacional-lbdn-1/arquivos/livro-branco-de-defesa-nacional/decreto-no-12-725-de-18-de-novembro-de-2025-dou_lbdn.pdf. Acesso em: 4 jun. 2026.

BRASIL. **Lei nº 13.675, de 11 de junho de 2018**. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar nº 79, de 7 de janeiro de 1994, a Lei nº 10.201, de 14 de fevereiro de 2001, e a Lei nº 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei nº 12.681, de 4 de julho de 2012. Brasília, DF: Presidência da República, 2018. Disponível em:

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13675.htm. Acesso em: 22 jun. 2026.

BRASIL. **Lei nº 14.751, de 12 de dezembro de 2023**. Institui a Lei Orgânica Nacional das Polícias Militares e dos Corpos de Bombeiros Militares dos Estados, do Distrito Federal e dos Territórios, nos termos do inciso XXI do caput do art. 22 da Constituição Federal, altera a Lei nº 13.675, de 11 de junho de 2018, e revoga dispositivos do Decreto-Lei nº 667, de 2 de julho de 1969. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14751.htm. Acesso em: 19 jun. 2026.

BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. **Doutrina Nacional de Inteligência de Segurança Pública – DNISP**. 4. ed. Brasília: SENASP, 2014.

BRASIL. **Portaria GAB/DG/ABIN/CC/PR nº 1.205, de 27 de novembro de 2023**. Aprova a Doutrina da Atividade de Inteligência. Brasília: Abin, 2023.

BRASIL. **Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014**. Aprova a Doutrina Militar de Defesa Cibernética – MD31-M-08. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_ciberneticaa_1a_2014.pdf. Acesso em: 22 ago. 2026.

BRASILEIRO, Ada Magaly Matias. **Como produzir textos acadêmicos e científicos**. 1. ed. São Paulo: Contexto, 2024.

CORRÊA, Gabriel. **Integração de estruturas de cibersegurança na Polícia Militar de Santa Catarina**: um estudo sobre a sinergia entre defesa e investigação cibernética. 2024. Ensaio Acadêmico (Curso Superior de Segurança e Defesa Cibernética) – Escola Superior de Guerra, Rio de Janeiro, 2024.

GALDONI, Luiz Rogério Franco; RODRIGUES, Karina Furtado; MEDEIROS, Breno Pauli. Qual é o futuro da governança de cibersegurança no Brasil? **Cadernos Gestão Pública e Cidadania**, São Paulo, v. 29, e90972, p. 1-14, 2024. DOI: 10.12660/cgpc.v29.90972.85588.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2019.

GOMES, Nilton Lopes da Silva. **A segurança e a defesa cibernética no Brasil**: análise dos discursos das Forças Armadas brasileiras (2016-2021). 2024. Dissertação (Mestrado em Segurança Internacional e Defesa) – Escola Superior de Guerra, Rio de Janeiro, 2024.

GRAÇA, Ronaldo Bach da. Enfoque jurídico da defesa cibernética aplicada às sociedades empresárias. **Revista Brasileira de Direito Empresarial**, Minas Gerais, v. 2, n. 1, p. 231-254, jul./dez. 2015. DOI: 10.26668/IndexLawJournals/2526-0235/2015.v1i1.615.

HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. **Instituto Igarapé**, Rio de Janeiro, p. 1-39, abr. 2021. Disponível em:

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

https://igarape.org.br/ciberseguranca-no-brasil-uma-analise-da-estrategia-nacional/. Acesso em: 30 maio 2026.

JESUS, Brenda Cordeiro de; SILVA, Devanildo Braz da Silva. Crimes cibernéticos: desafios da segurança pública e seu enfrentamento. In: NOGUEIRA, F. L.; SILVA, D. B.; FÉLIZ, Y. S. (org.). **Gestão em segurança pública**: relevância e desafios na perspectiva dos direitos humanos. Campo Grande: Editora UFMS, 2023.

LIMA, Zaryff Said de; RAMOS, Edson Marcos Leal Soares; MELLO, César Maurício de Abreu; DUARTE, Erika Natalie Pereira Miralha; CURSINO, Adriene da Silva. Ciberterrorismo e defesa da Amazônia: desafios legislativos e geopolíticos na fronteira digital. **Revista Geopolítica Transfronteiriça**, Manaus, v. 9, n. 4, p. 1-19, 2025. Disponível em: https://periodicos.uea.edu.br/index.php/revistageotransfronteirica/article/view/4927. Acesso em: 21 ago. 2026.

MACCARI, Ana Luiza. **A (in)constitucionalidade do dispositivo que estabelece regras de estabilidade e os reflexos da Lei Orgânica Nacional das Polícias Militares, Lei Federal nº 14.751/2023, para os policiais militares estaduais de Santa Catarina**. 2024. Trabalho de Conclusão de Curso (Curso de Altos Estudos de Política e Estratégia) – Escola Superior de Guerra, Rio de Janeiro, 2024.

MORAES, Jucimar Inácio de; AUGUSTO JÚNIOR, Paulo de Tarso. As atribuições das polícias militares no sistema de segurança pública conforme a Constituição de 1988. **RIBSP – Revista Interdisciplinar de Segurança Pública**, São José do Rio Preto, v. 4, n. 9, p. 112-126, maio/ago. 2021. DOI: 10.36776/ribsp.v4i9.144.

NONATO, Marcos Paulo Cardoso; PINHO, Harley de. **A integração do Sistema Militar de Defesa Cibernética (SMDC) com a proteção cibernética das infraestruturas críticas de interesse para Defesa Nacional**. 2021. Trabalho de Conclusão de Curso (Especialização em Altos Estudos em Defesa) – Escola Superior de Defesa, Brasília, 2021.

PENA, Stanley Araújo; GONCALVES FILHO, Cid; GALIZA, João Pedro Lima de Medeiros; MARQUES, Júnior Souto. Estratégias de políticas públicas no combate aos crimes cibernéticos: uma análise crítica. **Revista do Instituto Brasileiro de Segurança Pública – RIBSP**, v. 7, n. 18, p. 27-42, maio/ago. 2024. DOI: 10.36776/ribsp.v7i18.244.

PINTO, Danielle Jacon Ayres; GRASSI, Jéssica Maria. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. **Revista Brasileira de Estudos de Defesa**, Brasília, v. 7, n. 2, p. 103-131, jul./dez. 2020. DOI: 10.26792/rbed.v7n2.2020.75178.

PRODANOV, Cesar C.; FREITAS, Ernane C. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013. Recurso eletrônico.

REIS NETTO, Roberto Magno; SANTOS, Jorge Fabricio dos; CHAGAS, Clay Anderson Nunes. Segurança pública na era digital: ensino da legislação correlata à segurança da informação na polícia militar frente aos crimes informáticos durante a pandemia de covid-19

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360

no estado do Pará. **Revista Jurídica da Defensoria Pública do Estado do Tocantins – ADSUMUS**, Palmas, v. 6, n. 1, p. 191-211, 2021. Disponível em: https://editorial.defensoria.to.def.br/adsumus/edicao/5/seguranca-publica-na-era-digital-ensino-da-legislacao-correlata-a-seguranca-da-informacao-na-policia-militar-frente-aos-crimes-informaticos-durante-a-pandemia-de-covid-19-no-estado-do-para. Acesso em: 21 ago. 2026.

SANTOS, Jorge Fabricio dos; GARCIA, Carlos Stilianidi. A utilização do perfilamento criminal na investigação de crimes militares cometidos por milícia privada nas polícias militares. **Revista do Ministério Público Militar**, Brasília, ano 53, n. 50, p. 205-220, 1º sem. 2026. DOI: 10.5281/zenodo.19734485.

SILVA, Ana Luísa Diniz; MALETTA, Giselle Villela. Cibersegurança e ciberdefesa: uma nova abordagem da segurança nacional brasileira. **Revista Brasileira de Inteligência Artificial e Direito – RBIAD**, Brasília, v. 2, n. 1, p. 1-3, 2021. Disponível em: https://rbiad.com.br/index.php/rbiad/article/view/32. Acesso em: 4 jun. 2026.

SOUZA, Eduardo André Araújo; ALMEIDA, Nival Nunes de. A questão da segurança e defesa do espaço cibernético brasileiro, e o esforço político-administrativo do Estado. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 22, n. 2, p. 381-410, maio/ago. 2016. DOI: 10.21544/1809-3191/regn.v22n2p381-410.

VERONESE, Luís Guilherme de Lima. **Inteligência em segurança cibernética**: proposta de modelo de avaliação de maturidade na atividade de inteligência da PMSC. 2025. Ensaio Acadêmico (Curso Superior de Segurança e Defesa Cibernética) – Escola Superior de Guerra, Rio de Janeiro, 2025.

VIANNA, Eduardo Wallier; CAMELO, José Ricardo Souza. Defesa cibernética no Brasil: primícias de uma história de sucesso. **Revista da Escola Superior de Guerra**, Rio de Janeiro, v. 35, n. 75, p. 127-154, set./dez. 2020. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/view/1144/941. Acesso em: 21 ago. 2026.

DOI: 10.29327/270098.19.2-13 | ISSN eletrônico: 2447-9896 | ISSN impresso: 2177-0360