ABORDAGENS EM SEGURANÇA, DESENVOLVIMENTO E DEFESA:

a pesquisa no Lab-SDD

volume 2

Viviane Machado Caminha
Érika Rigotti Furtado
Organizadoras

ESCOLA SUPERIOR DE DEFESA
ESD
DEFENDENDO PER SCIENTIAM

Viviane Machado Caminha (org.)
Érika Rigotti Furtado (org.)

ABORDAGENS EM SEGURANÇA, DESENVOLVIMENTO E DEFESA: a pesquisa no Lab-SDD

volume 2



Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Abordagens em segurança, desenvolvimento e defesa : a pesquisa no LAB-SDD : volume 2 / Érika Rigotti Furtado, Viviane Machado Caminha (org.). -- Brasília, DF : Escola Superior de Defesa, 2026.

Vários autores.
Bibliografia.
ISBN 978-65-989042-1-0

1. Administração pública 2. Defesa (Ciência militar) 3. Governança 4. Segurança pública - Brasil I. Furtado, Érika Rigotti. II. Caminha, Viviane Machado.

26-372259.0 CDD-363.109

Índices para catálogo sistemático:

1. Segurança pública : Problemas sociais 363.109

Eliane de Freitas Leite - Bibliotecária - CRB 8/8415

DISTRIBUIÇÃO GRATUITA
Todos os direitos reservados à
Escola Superior de Defesa - ESD
Setor de Habitações Individuais Sul - Rodovia Df-001-Km 27,4 SN
71686-900 – Jardim Botânico – Brasília/DF
https://www.gov.br/esd/pt-br

As informações e os posicionamentos expressos nesta obra são de responsabilidade dos autores, não refletindo a opinião institucional da Escola Superior de Defesa, do Ministério da Defesa, das Forças Armadas ou do Governo Federal

Em consonância com as boas práticas de integridade acadêmica e com a Política de Integridade na Atividade Científica do CNPq, instituída pela Portaria nº 2.664, de 6 de março de 2026, os autores foram instados a declarar eventual utilização de ferramentas de inteligência artificial generativa na produção dos capítulos desta obra. A responsabilidade pelo conteúdo, pelas interpretações, pelos dados apresentados e pela observância dos padrões éticos e científicos permanece integralmente atribuída aos respectivos autores.

ESCOLA SUPERIOR DE DEFESA (ESD)

COMANDANTE E REITOR
Major-Brigadeiro Médico Laerte Lobato de Moraes

SUBCOMANDANTE E PRÓ-REITOR DE PESQUISA E PÓS-GRADUAÇÃO
Contra-Almirante Leonardo Braga Martins

COORDENADOR-GERAL ACADÊMICO
Contra-Almirante (RM1) Jeferson Denis Cruz de Medeiros

CONSELHO EDITORIAL
Prof. Dr. Augusto Wagner Menezes Teixeira Junior
Prof. Dr. Fábio Albergaria de Queiroz
Prof. Dr. Gills Lopes Macêdo Souza
Cel R/1 (EB) Thadeu Luiz Crespo Alves Negrão

ORGANIZADORAS
Profa. Dra.Viviane Machado Caminha
Profa. Dra. Érika Rigotti Furtado

REVISÃO, DIAGRAMAÇÃO E CAPA
Major QCO Ana Rita de Avila Belbute Peres
Capa elaborada com auxílio de ferramentas de inteligência artificial.

©2026 Escola Superior de Defesa

Sumário

Apresentação _____ 9

Parte 1

Desafios Contemporâneos em Segurança, Tecnologia e Defesa

Do Caribe ao Atlântico Sul: securitização crescente nas Américas _____ 13

Wellington Dantas de Amorim
Marcelo Marcel Félix

O Brasil no combate ao crime organizado transnacional no âmbito da OTCA: ações no contexto das cúpulas internacionais na Amazônia (2023-2025) _____ 37

Bruno Cezar Pereira Soares
Michele Eduarda Brasil de Sá
Leonardo Ulian Dall Evedove

Proteção de infraestruturas de computação de alto desempenho como pilar da soberania digital: desafios e implicações para o Estado Brasileiro _____ 59

Jaime de Melo Gama da Silva
Rômulo Ferreira dos Santos
Matheus Henrique de Souza

O problema da Ética na Guerra Cognitiva _____ 85

Érika Rigotti Furtado
Ivan Fernandes Faria

Parte II

Segurança e Defesa na Era Digital: desafios cognitivos, educacionais e operacionais

Plataformas digitais, (des)informação e a mobilização do 8 de janeiro: um Estado do Conhecimento _____ 105

Gabriel Carlos dos Reis Costa Dias
Nádia Xavier Moreira
Viviane Machado Caminha

Competências em inteligência artificial e ensino profissional em segurança e defesa: articulações conceituais e experiências na Escola Superior de Defesa _____ 129

Aline Barbosa Xavier Muniz
Patrícia Pontes Bezerra
Lorena Hermenegildo de Oliveira

Guerra Remota: emergência, fundamentos teóricos e dificuldades conceituais à luz do Estado do Conhecimento _____ 151

André Barros de Oliveira
Viviane Machado Caminha
Nádia Xavier Moreira

Parte III

Estado, Governança e Defesa: perspectivas atuais

Mídias sintéticas em conflitos armados: tensões ao comando e controle e ao Direito Internacional Humanitário _____ 179

Matheus Henrique de Souza
Rômulo Ferreira dos Santos
Jaime de Melo Gama da Silva

Centralização das compras públicas de defesa: governança, eficiência e o caso do Exército Brasileiro _____ 205

Marcelo Batista Soares Barroso
Peterson Ferreira Silva

Resiliência do segmento de armas e munições leves da base industrial de defesa brasileira _____ 229

José Irismar Cabral Junior
Julio Eduardo da Silva Menezes

Planejamento logístico estratégico e análise custo-efetividade: o caso da Operação de Combate ao Crime Organizado na crise de segurança pública do Rio Grande do Norte _____ 253

Camila Araújo Machado
José Sérgio Marques dos Santos
Luiz Gustavo Celuppi
Carlos Eduardo Gomes
Clayton Mendes da Silva

Mudanças climáticas, segurança nacional e resiliência: o exemplo da Operação "Taquari II" (2024) _____ 279

Thiago Abreu de Figueiredo
Cintiene Sandes Monfredo Mendes
José Roberto Pinho de Andrade Lima

Sobre os autores e autoras _____ 295

Apresentação

A diversidade temática assentada no tripé segurança, desenvolvimento e defesa constitui relevante espaço de reflexão na contemporaneidade. Em um cenário marcado por transformações aceleradas, disputas geopolíticas, reconfigurações tecnológicas, desafios ambientais e humanos, novas modalidades de conflito e crescente interdependência entre atores estatais e não estatais, impõe-se, cada vez mais, a adoção de abordagens analíticas capazes de superar as tradicionais compartimentalizações disciplinares e conceituais, o que se constitui em requisito indispensável da produção científica.

Essa produção ganha especial relevância quando observada à luz das transformações ocorridas, nas últimas décadas, no campo dos estudos de segurança e defesa, em um movimento de ampliação significativa do escopo da pesquisa. Nesse contexto, o diálogo permanente com diferentes áreas do saber enriqueceu o debate científico ao afirmar, sob um enfoque interdisciplinar, o caráter multifacetado dos objetos de estudo, abarcando dimensões variadas, como a política, a estratégica, a institucional, a tecnológica e a sociocultural, no enfrentamento de questões concretas.

O volume 2 da obra *Abordagens em Segurança, Desenvolvimento e Defesa: a pesquisa no Lab-SDD*[1] se insere precisamente nesse espaço de convergência, buscando oferecer instrumentos de análise e reflexão de modo a fortalecer a produção científica em um ambiente caracterizado pela complexidade e interdisciplinaridade. Assim, reconhece que a investigação científica exige não apenas domínio conceitual, mas também pluralidade metodológica e abertura ao diálogo entre diferentes tradições de pesquisa.

Além de reunir estudos sobre áreas distintas, este livro propõe uma reflexão integrada sobre os desafios enfrentados pela sociedade contemporânea, que raramente se enquadram em categorias rígidas ou isoladas. As ameaças e vulnerabilidades atuais atravessam fronteiras disciplinares, institucionais e territoriais, exigindo enfoques diversificados para a compreensão de fenômenos

[1]O volume 1 está diponível no seguinte endereço eletônico: https://www.gov.br/esd/pt-br/central-de-conteudo/publicacoes/producao-academica-da-esd/livros-capitulos-de-livros/livros.

complexos e interdependentes. Desse modo, os capítulos aqui reunidos oferecem ao leitor não apenas análises específicas, mas também contribuições para a consolidação de uma agenda de pesquisa comprometida com o aprofundamento científico dos estudos de segurança e defesa. Mais do que fornecer respostas definitivas, a obra busca estimular novas perguntas, ampliar horizontes analíticos e fortalecer uma comunidade científica comprometida com a construção de conhecimento sobre temas que se encontram no centro das preocupações do Estado, da sociedade e da comunidade internacional.

É nesse espírito que o Laboratório de Pesquisa em Segurança, Desenvolvimento e Defesa (Lab-SDD)[2], da Escola Superior de Defesa (ESD), a partir de pesquisas originárias dos grupos de pesquisa Segurança Internacional, Geopolítica e Diplomacia de Defesa (GP 1); Dimensão Humana dos Estudos de Defesa (GP 2); e Políticas Públicas de Segurança e Defesa (GP 3), oferece ao público a presente obra, como contribuição ao permanente esforço de compreender temáticas e relações complexas em um mundo progressivamente dinâmico, interdependente e desafiador.

Profa. Dra. Viviane Machado Caminha
Profa. Dra. Érika Rigotti Furtado
(Organizadoras)

[2] Para mais informações, acessar: https://www.gov.br/esd/pt-br/a-esd/pesquisa-e-pos-graduacao/laboratorio-de-pesquisa-em-seguranca-desenvolvimento-e-defesa-lab-sdd.

Parte I

Desafios Contemporâneos em Segurança, Tecnologia e Defesa

Do Caribe ao Atlântico Sul:
securitização crescente nas Américas

Wellington Dantas de Amorim
Marcelo Marcel Félix

Introdução

No dia 3 de janeiro de 2026, os Estados Unidos da América (EUA) conduziram uma operação militar especial de sucesso que culminou com a captura do líder político venezuelano Nicolás Maduro. A denominada Operação Determinação Absoluta alcançou seu objetivo político por meio de uma combinação de planejamento minucioso e sincronização precisa.[1] Entretanto, a ação militar norte-americana representou apenas a ponta do *iceberg* de todo um processo político-estratégico construído. O que observamos ao longo dos meses que antecederam o acontecimento foi o desenvolvimento, por parte do Governo norte-americano, de argumentos e arcabouço normativo necessários para a atuação em território venezuelano.

A associação direta do narcotráfico com o terrorismo por meio da Ordem Executiva 14.157, possibilitou a Washington maior liberdade de ação sem necessidade de aprovação direta do Congresso americano.[2] Adicionalmente, a incorporação do combate ao narcotráfico no discurso de segurança dos EUA pode ser compreendida como um processo típico de securitização, no qual a prática do crime tornou-se questão de segurança nacional para os EUA.[3] Esse

[1]How Maduro's capture went down – a military strategist explains what goes into a successful special op. Disponível em: https://theconversation.com/how-maduros-capture-went-down-a-military-strategist-explains-what-goes-into-a-successful-special-op-272671. Acesso em: 10 jan.2026.

[2]Assinada em 20 de janeiro de 2025 e intitulada *Designating Cartels and Other Organizations as Foreign Organization and Specially Designated Global Terrorists* criou o processo pelo qual cartéis internacionais e outras organizações crimainais transnacionais podem ser designadas como *Foreign Terrorist Organization* (FTOs). Disponível em: https://www.whitehouse.gov/presidential-actions/2025/01/designating-cartels-and-other-organizations-as-foreign-terrorist-organizations-and-specially-designated-global-terrorists/. Acesso em: 1 fev. 2026.

[3]Peter Andreas destaca que esse processo de securitização das drogas não é algo recente. A denominada "guerra às drogas" foi declarada em 1971, durante a administração de Richard Nixon e reforçada nos anos 1980, principalmente durante a administração Reagan. (Andreas, 2009, p.43-55).

processo ganhou contornos mais contundentes com a recém-publicação da *National Security Strategy* (NSS) e da *National Defense Strategy* (NDS) que apresentam de maneira clara a postura estratégica combativa norte-americana em relação aos crimes transnacionais (Estados Unidos, 2025a; 2026).

No plano operacional, o arranjo político-estratégico desenhado pelo Governo Trump traduziu-se no aumento da presença naval norte-americana no Caribe, com emprego de meios da United States Navy (*US Navy*), incluindo o Grupo de Batalha do Porta-aviões *USS Gerald R. Ford.*[4] As ações culminaram, em um primeiro momento, no afundamento de embarcações de narcotraficantes e, posteriormente, no apresamento de navios petroleiros que transportavam petróleo venezuelano. Além disso, foi do mar que partiu o ataque final a Caracas para a captura de Maduro, o que revelou o principal interesse norte-americano na presença constante dos navios da *US Navy* no Mar do Caribe.

Nesse contexto, este capítulo sustenta que a atuação norte-americana recente configura um processo de securitização dos espaços marítimo e litorâneos, no qual o discurso antidrogas e antiterror funciona como justificativa para projeção de poder norte-americano nas áreas de interesse. Em perspectiva, argumenta-se que tal modelo de intervenção poderá ser replicado no Atlântico Sul, sob o argumento da "segurança" norte-americana frente às ameaças do crime organizado transnacional. O estudo busca, assim, proporcionar o entendimento, mesmo que limitado, dos riscos da militarização do Atlântico Sul, associados à nova agenda político-estratégica e discutir alternativas disponíveis aos países sul-americanos para mitigar esses riscos. Para tal, o trabalho foi dividido em três partes: a primeira é a presente Introdução; a segunda, abrangendo o Desenvolvimento, trata da apresentação do conceito de securitização e sua utilização pelos EUA. Depois, traz-se à baila a operacionalização da teoria na prática com o argumento do combate ao narcotráfico por parte dos EUA. Adicionalmente, analisam-se a ampliação do conceito de securitização embutido na ESN e na EDN e seus eventuais desdobramentos, inclusive relativos ao Brasil. Posteriormente, analisam-se os impactos na estratégia brasileira voltada

[4]Na *US Navy* um Grupo de Batalha (também denominado *Carrier Strike Group* – CSG) é a principal unidade operacional de projeção de poder naval. Ele reúne, sob um único comando, diferentes tipos de navios e meios aéreos para operar de forma integrada, tendo um Porta-aviões como núcleo do Grupo. Disponível em: https://www.navalanalyses.com/2016/12/infographics-23-us-navy-carrier-strike.html?utm_source=chatgpt.com#google_vignette Acesso em: 13 jan. 2026.

para o Atlântico Sul, além de sugerir posturas que poderiam ser adotadas pelo Brasil, juntamente com os países da região, diante do ambiente externo que se apresenta. A terceira parte apresenta as Considerações Finais, consolidando o que foi analisado.

Desenvolvimento

Antes de refletirmos sobre as ações securitizantes dos norte-americanos para o hemisfério ocidental, faz-se necessário ancorarmos os conceitos relativos à securitização, pormenorizando detalhes importantes que nos ajudarão na melhor compreensão da realidade.

Entendendo o fenômeno da securitização

A teoria da securitização foi escolhida por possuir um arcabouço conceitual eficaz para o entendimento das alterações das questões da política ordinária para o campo da exceção, legitimando ações extraordinárias que alteram profundamente o uso dos instrumentos estatais de poder. Nesse sentido, Barry Buzan, Ole Wæver e Jaap de Wilde definem securitização como: "processo que leva a política para além das regras estabelecidas e enquadra a questão como um tipo especial de política ou como algo acima da política." (Buzan *et al.*, 1998, p. 23. Tradução livre). De forma mais objetiva, a securitização pode ser compreendida como o processo pelo qual um ator transforma uma questão ordinária de qualquer ordem em uma questão de segurança, transformando em ameaça existencial, exigindo ações urgentes e excepcionais. Importante ressaltar que essa alteração não é somente semântica ou discurso. No campo institucional, ela condiciona a estrutura lógica do processo decisório, amplia as possibilidades de atuação do Governo e reduz os freios normativos que caracterizam a política ordinária. Logo, estabelece-se a segurança como o resultado de um processo social e político, e não como um fato em si, objetivo e inquestionável.[5]

[5]Esta visão "objetiva" foi majoritária durante o período da Guerra Fria, por exemplo. Para uma análise geral da evolução dos estudos de Segurança Internacional, ver Buzan; Hansen (2012) e, no caso específico da securitização, p. 321-328.

No caso dos EUA, especialmente no contexto recente de tensões com a Venezuela, a securitização tem funcionado como um instrumento ativo da política de segurança nacional. Ao acusarem e condenarem Nicolas Maduro por ajudar a administrar o Cartel de Soles[6] e oferecerem 50 milhões de dólares por recompensa,[7] a administração Trump articulou um discurso no qual o narcotráfico é apresentado como ameaça direta à segurança dos EUA, vinculando essa prática à noção de "narcoterrorismo". Essa reconfiguração da percepção de segurança nacional norte-americana possibilitou a adoção de medidas que, em outras circunstâncias, estariam restritas a instrumentos civis ou de cooperação internacional. Na prática, foi possível observar uma série de medidas extraordinárias respaldadas pelo processo de securitização: bloqueio naval no Mar do Caribe, interdição e apreensão de navios que transportavam petróleo venezuelano; expansão da presença militar norte-americana na Região do Caribe; uso da força em ações ofensivas diretas contra embarcações de narcotraficantes.[8] Em todos os exemplos, a maneira como as ações foram conduzidas por Washington, gerou forte repudio da Comunidade Internacional, o que não foi suficiente para deter o ímpeto norte-americano.

O processo de securitização, tendo o narcotráfico como ator principal, não é algo novo ou criado pela administração Trump. Pelo contrário, trata-se de um processo que ao longo do tempo foi ganhando contornos que estimularam a definição da militarização como o principal antídoto à questão das drogas.

O narcotráfico como ameaça existencial

O combate ao narcotráfico é ponto de convergência entre os países das Américas. A pauta é prioridade dentro da Secretaria de Segurança Multidimensional (SSM) da Organização dos Estados Americanos (OEA) que articula esforços focados em cidadãos, segurança pública e fortalecimento das

[6]Cartel de los Soles é uma suposta organização criminosa venezuelana chefiada por membros de alto escalão das Forças Armadas da Venezuela. Disponível em: https://pt.wikipedia.org/wiki/Cártel_de_los_Soles Acesso em: 10 jan. 2026.

[7]Disponível em: https://www.state.gov/nicolas-maduro-moros Acesso em: 10 jan 2026.

[8]Enhanced Counter-Narcotics Operations in the Caribbean Sea and Eastern Pacific. Disponível em:https://www.southcom.mil/Media/Special-Coverage/Enhanced-Counter-Narcotics-Operations. Acesso em: 16 jan. 2026.

capacidades institucionais dos Estados. A atuação da SSM está voltada para ampliar a cooperação na luta contra as drogas, tendo muitos projetos focados na redução de oferta e procura, além de desenvolver um forte movimento antidrogas em cada Estado membro.[9] Sendo assim, a Organização reconhece que a abordagem para o combate às drogas passa pela busca por soluções cooperativas que respeitem o Direito Internacional e os Direitos Humanos. Vale ressaltar que tal posição não encontra convergência com o processo de securitização do narcotráfico que podemos observar na Política Externa norte-americana.

Ao longo das últimas décadas, observou-se a intensificação do processo de securitização do tráfico de drogas associando-o a outras ameaças transnacionais. Segundo Peter Andreas (2009), o problema do narcotráfico foi incorporado de maneira progressiva como ameaça à segurança nacional dos Estados Unidos, servindo como pivô no reforço às políticas de controle de fronteiras e imigração. Além de fortalecer a retórica da "integridade territorial" e proteção da sociedade.[10] Entretanto, o que se observa na prática é uma escalada da militarização, com o uso de tecnologia militar e aumento do efetivo para sinalizar controle, mesmo que o fluxo de drogas continue alto (Andreas, 2009).

Bruce Bagley (2012), apresenta o narcotráfico transnacional como elemento que exacerba a violência, compromete as instituições estatais e mina a qualidade democrática, limitando o Estado de Direito. Nesse contexto, esse enquadramento torna-se um passo fundamental no processo de securitização, ao elevar o problema das drogas de uma questão de saúde pública ou crime comum para uma ameaça à sobrevivência das instituições democráticas. Dessa forma, os Estados legitimam o uso da força militar e políticas de exceção, manifestando claramente o processo de securitização na adoção de modelos militares para lidar com o problema.[11] Nesse contexto, a militarização do combate ao narcotráfico

[9]Disponível em: https://www.oas.org/pt/topicos/drogas.asp. Acesso em: 24 jan. 2026.

[10]Durante os mandatos do Presidente Ronald Reagan (1981-1989) o narcotráfico foi elevado formalmente ao campo da segurança nacional, por meio da *National Security Decision Directiv*e 221 (NDSS-221), militarizando o combate as drogas e possibilitando a reclassificação de Estados produtores de drogas em Estados hostis, conforme a conveniência dos EUA.

[11]Dois modelos históricos podem ser citados como exemplo de "vitórias parciais" sem continuidade no tempo. **Plan Colômbia**: o governo de Uribe implementou uma política de segurança democrática, apoiada por quase US$ 8 bilhões em ajuda dos EUA que focou em uma estratégia de contrainsurgência e no aumento de tropas de combate; **Iniciativa Mérida**: no México, o presidente Felipe Calderón promoveu a militarização da "guerra às drogas",

encontra-se incorporada e aceita nas políticas dos Estados, mesmo com a falta de resultados expressivos dessa estratégia de combate, em detrimento da perda ou diminuição da soberania do Estado envolvido diretamente no combate.

Jonathan Rosen (2014), argumenta que embora o narcotráfico represente um risco relevante à estabilidade política dos Estados e, por consequência, à segurança regional. No longo prazo, a securitização excessiva provoca ciclos de violência e adaptações das organizações criminosas, como alteração geográfica das rotas ilícitas.[12] O que se percebe é que o enquadramento do narcotráfico como ameaça existencial do Estado não elimina o problema, mas frequentemente o reconfigura, produzindo novos desafios estratégicos.

Nesse contexto, o Professor Thiago Rodrigues adiciona valor à nossa reflexão. O autor brasileiro argumenta que a política antidrogas nas Américas, progressivamente, abandonou o campo da saúde pública sendo incorporada à pauta de segurança do estado, o que gerou processos de militarização e normalização de medidas excepcionais que exploram o combate ao narcotráfico, *per se*, reconfigurando as relações de poder e soberania no plano regional (Rodrigues, 2012). Nessa perspectiva, a securitização das drogas não apenas legitima o uso ampliado da força, mas contribui para a consolidação de um estado de exceção permanente no enfrentamento de um fenômeno estruturalmente complexo.

A securitização do narcotráfico exemplifica de forma clara como ameaças não tradicionais podem ser incorporadas ao núcleo duro da política de segurança nacional. Ao combinar discurso, arcabouço normativo e instrumentos de força, os EUA transformam um fenômeno criminal complexo em justificativa para a ampliação de sua atuação estratégica regional.

A literatura especializada sobre o assunto aponta que o processo de securitização segue em direção oposta ao entendimento de cooperação multilateral defendido pela OEA. Apesar disso, a securitização acompanhada da militarização no combate ao narcotráfico encontra-se plenamente incorporada às agendas de segurança nacional dos principais Estados membros daquela Organização Internacional. Nesse contexto, mesmo diante do uso da força extrema, como podemos observar no Caribe, não se verifica de forma

utilizando o Exército para enfrentar os cartéis (Bagley, 2012).

[12] Rosen (2014) utiliza o **Plan Colômbia** como "case" para confirmar seu argumento.

contundente o repúdio a tais ações norte-americanas, o que nos leva a crer que Washington seguirá com liberdade para agir na América, quando e onde seus interesses estiverem em jogo, sendo o caso venezuelano somente mais um episódio desse processo contínuo de intervenção norte-americana.

A Estratégia de Segurança Nacional e a Estratégia de Defesa Nacional dos EUA como discursos securitizadores em relação à América Latina e Caribe

Os EUA publicaram a National Security Strategy 2025 (NSS) (Estados Unidos, 2025a), em novembro do mesmo ano, e a National Defense Strategy 2026 (NDS[13]) (Estados Unidos, 2026), em janeiro de 2026. Nelas, diversos elementos de securitização do narcotráfico no Hemisfério Ocidental ficam patentes. De fato, o Hemisfério Ocidental pode ser visualizado como prioritário para a Segurança e Defesa dos EUA, em ambas as publicações.[14]

Por exemplo, na ESN (p.5) fica explícito que "queremos um Hemisfério cujos governos cooperem conosco contra narcoterroristas, cartéis e outras organizações criminosas" (tradução livre). Mais ainda, na EDN (p. 3), a ênfase chega a ser maior. Ao elencar a primeira das prioridades do Departamento de Guerra[15] em relação ao solo pátrio (Homeland), automaticamente inclui o Hemisfério no item, como se fosse uma extensão natural:

[13]A partir deste ponto do texto, a NSS e NDS serão mencionadas como ESN (Estratégia de Segurança Nacional) e EDN (Estratégia de Defesa Nacional), respevtivamente.

[14]Alguns analistas já apontaram a possibilidade de que a prioridade dada ao Hemisfério Ocidental seria precursora de uma divisão do poder mundial em regiões, com a China e (também para alguns) a Rússia. Embora não esteja no escopo do presente capítulo, entendemos que a prioridade seja muito mais o fortalecimento de uma posição em um arranjo tático que possibilite mais sucesso no embate com a China (aliada ou não à Rússia) no futuro de mais longo prazo. Logo, a relativa estabilidade no curto e médio prazos seria apenas a preparação para algo muito mais amplo, analogamente às várias negociações entre os países na década de 1930.

[15]Conforme orientação do Presidente Trump, em seu segundo mandato, o Departamento de Defesa passou a se chamar Departamento de Guerra. O Departamento de Guerra foi criado em 1789; com a criação do Departamento da Marinha, em 1794, passou a se dedicar às operações não-navais. Posteriormente, em 1947, criou-se também o Departamento da Força Aérea. Em 1949, as três forças ficaram subordinadas ao Departamento de Defesa. Embora não seja escopo deste capítulo, tal mudança evidencia ainda mais o processo de securitização, pois enquanto a Defesa também abrange elementos de diplomacia e possibilidade de cooperação, a Guerra pressupõe conflito a ser resolvido primariamente via esforço bélico e/ou coercitivo e instila na população uma sensação maior de insegurança e consequente necessidade de eliminar a fonte responsável por tal sentimento, sejam quais forem os sacrifícios.

> Proveremos o Presidente Trump com opções militares dignas de confiança para serem utilizadas contra narcoterroristas onde quer que estejam.[16] Trabalharemos em boa-fé com nossos vizinhos, do Canadá aos nossos parceiros na América Central e do Sul, mas nos asseguraremos que eles respeitem que façam sua parte para defender nossos interesses mútuos. E onde eles não o cumpram, estaremos prontos, estaremos preparados para tomar ações focadas e decisivas que concretamente vão ao encontro de interesses dos EUA. Este é o Corolário Trump à Doutrina Monroe, e os militares da América estão prontos a aplicá-lo com velocidade, poder e precisão, como o mundo viu na Operação DETERMINAÇÂO ABSOLUTA.(Estados Unidos, 2026, p. 3, tradução livre).

Curiosamente, entre os princípios apresentados para a ESN (p. 9), consta o da Predisposição ao Não-Intervencionismo. No entanto, ressalta-se que "para um país cujos interesses são tão numerosos e diversos como o nosso, aderência rígida ao não-intervencionismo não é possível. No entanto essa predisposição deveria estabelecer um alto patamar para o que constitui uma intervenção justificada."(tradução livre). Logo, deduz-se a importância do processo de securitização em procurar legitimar qualquer intervenção.[17]

Outro princípio citado na EDN (p. 10) é o Equilíbrio do Poder:

> Os Estados Unidos não podem permitir que outra nação se torne tão dominante que poderia ameaçar nossos interesses. Trabalharemos com aliados e parceiros para manter equilíbrios de poder globais e regionais que previnam a emergência de adversários dominantes. Como os Estados Unidos rejeitam o malfadado conceito de dominação global em si mesmo, temos que prevenir a dominação global, e em alguns casos regional, de outros. (Estados Unidos, 2026, p. 10, tradução livre).

O texto mencionado ecoa os dizeres de John Mearsheimer, em sua célebre obra "The Tragedy of Great Power Politics". Mearsheimer, ao afirmar

[16] Já houve diversas declarações oficiais e artigos acadêmicos, nos EUA, que sustentam que a China facilitaria a exportação de fentanyl para incrementar o vício por substâncias opioides naquela sociedade. Ironicamente, caso essas versões sejam verídicas, teríamos a China revertendo o processo por que passou, em meados do século XIX, por conta das iniciativas do Reino Unido, e que culminou na Guerra do Ópio. Essa analogia é bem explorada por Danahay (2025). Para as iniciativas do Governo dos EUA em relação ao fentanyl, ver EUA (2025b).

[17] Registre-se que o então candidato Trump se elegeu, em 2020, condenando a presença militar dos EUA em conflitos no exterior.

que haveria apenas uma potência hegemônica no mundo (os EUA, e mesmo assim apenas regional, não global), acrescenta:

> Estados que alcançam hegemonia regional procuram prevenir que grandes potências em outras regiões alcancem o mesmo feito. Hegêmonas regionais, em outras palavras, não querem pares.(…) Hegêmonas regionais tentam conter hegêmonas aspirantes em outras regiões porque temem que uma grande potência rival que domina sua própria região será um adversário especialmente poderosos que terá Liberdade de causar problemas no temível quintal da própria potência (Mearsheimer, 2001, p. 43, tradução livre).

A ESN (p. 15) explicita a *rationale* exposta por Mearsheimer, ao afirmar decididamente: "Nós negaremos aos competidores não-hemisféricos a possibilidade de posicionar forças ou outras formas de ameaça militar, ou controlar estrategicamente ativos vitais, em nosso Hemisfério". Mais adiante, na página seguinte, ressalta-se que, entre os elementos "óbvios" (sic) para reconsiderar a presença militar no Hemisfério Ocidental, está a preocupação com a redução do tráfico humano e de drogas e com o combate aos cartéis.

Já a EDN (p. 16), ao analisar a chamada Linha de Esforço 1 (Proteção do Solo Pátrio), destaca entre seus objetivos prioritários:

> Conter Narco-Terroristas no Hemisfério. Mesmo enquanto o Departamento trabalha para assegurar as fronteiras da América, nós reconhecemos que ameaças a tais fronteiras também têm que ser levadas em conta no hemisfério. Portanto nós ajudaremos a capacidade de parceiros em degradar organizações narcoterroristas ao longo das Américas e apoiá-los enquanto assim o fazem, enquanto também mantendo nossa capacidade de tomar decisivamente ações unilaterais. Mas se nossos parceiros não puderem ou fizerem sua parte, então estaremos preparados para agir decisivamente por nós mesmos, como na Força Conjunta demonstrada na Operação DETERMINAÇÃO ABSOLUTA (Estados Unidos, 2026, p. 10, tradução livre).

Portanto, pode-se afirmar que os dois documentos enfatizam a importância do combate às drogas pelos EUA, securitizando-o, ao considerá-lo um dos aspectos vitais dos documentos principais de Segurança e Defesa dos EUA.

Domínio marítimo no Caribe e projeção estratégica na América do Sul

A influência sobre o Caribe e, posteriormente, sobre a América do Sul, foi elemento importante para a estruturação de todo o processo de expansão dos EUA, ao longo da história. Partindo de 13 colônias na Costa Atlântica, a incorporação da Flórida, da Louisiana Francesa e de parte do território mexicano foram elementos cumulativos essenciais para a sua *rationale* geopolítica. Afinal, o porto de Nova Orleans sempre representou (e representa) parcela significativa do comércio marítimo dos EUA, tanto para importação (especialmente de produtos provindos da América Central e América do Sul quanto exportação dos excedentes agrícolas originalmente transportados por meio da bacia do Mississippi-Missouri. Por extensão, o Golfo do México também se destaca.

Além do aspecto econômico, a importância da América Central e de seu *chokepoint* emblemático (o istmo do Panamá, posteriormente Canal do Panamá) conferiu à região papel de protagonismo na expansão e consolidação do poder dos EUA, tornando o Caribe, na prática, no chamado "Mediterrâneo" dos EUA, segundo ênfase dada originalmente pelos geopolíticos Alfred T. Mahan e Nicholas J. Spykman e ressaltada por Santa Bárbara (2025, p. 110), ou seja, "Spykman, portanto, descreveu a inserção do "mediterrâneo americano" no Hemisfério Ocidental a partir do olhar geopolítico centrado na seletividade territorial dos interesses nacionais dos EUA."[18]

De fato, a chamada Doutrina Monroe, exposta em 1823, tinha um cunho eminentemente defensivo, perante eventuais iniciativas europeias em "recolonizar" países das Américas recém-independentes. No entanto, principalmente após a iniciativa francesa de ocupar o México, durante a Guerra Civil Americana, acelerou a transformação da Doutrina em um mecanismo orientador intervencionista (Santa Bárbara, p. 61). As diversas ocasiões subsequentes em que os EUA intervieram militarmente nas Américas, em variados países, de maneira direta ou indireta, atestaram essa transição. Como resultado,

[18]Consideramos a obra de Marcelo de Jesus Santa Bárbara como muito significativa, aprofundando os termos de comparação entre a formulação teórica e motivações geopolíticas dos EUA em relação ao Caribe e América do Sul (como Mahan, Spykman e outros) e a lógica de pensadores brasileiros (Golbery do Couto e Silva, Carlos de Meira Mattos e especialmente Mario Travassos).

> [...] formou-se um perímetro de segurança territorial não institucionalizado a partir de Porto Rico, Cuba e Panamá, Colômbia e Venezuela. Tais países se tornaram à época pontos vitais, formando uma espécie de "colar de pérolas" norte-americano, funcionando também como um primeira linha de defesa territorial para proteger o Golfo do México, a foz do Mississippi e a Costa Leste estadunidense (Santa Bárbara, 2025, p. 96)

Em relação aos países da América do Sul que estivessem mais distantes da América do Norte, como Brasil, Argentina e Chile, o maior temor dos EUA é o que eles efetivassem uma política de "equilíbrio de poder" e na prática prejudicassem os interesses estadunidenses. Conforme Santa Bárbara (2025, p. 120), "nesse caso, a Argentina, o Brasil e o Chile (...) poderiam buscar sua segurança comum, se protegendo contra ameaças externas à América do Sul, caso fosse necessário."

No entanto, no caso dos países citados, as diversas tentativas de convergência e minimização das discordâncias somente veio a se realizar a partir dos anos 1980, e mesmo assim circunscritos a Brasil e Argentina. Com o final da Guerra Fria, embora o Mercosul se estabelecesse em 1991 e pouco a pouco se expandisse, as iniciativas de uma integração mais substantiva (inclusive em termos militares) não se solidificou, pelo dissenso relativo à carga ideológica de algumas sugestões (e, no caso da Venezuela, sempre enfatizando os EUA como uma grande ameaça).

A reação dos EUA a esses movimentos foi enfatizar a necessidade da gendarmerização[19] das Forças Armadas dos países sul-americanos, apontando que os conflitos interestatais não deveriam ser preocupação dos mesmos. Tal discurso de securitização obteve boa acolhida em diversos países, afligidos por crises de segurança pública; em termos econômicos, os EUA propuseram uma Área de Livre-Comércio englobando as três Américas, mas a reação foi negativa. Ao mesmo tempo, os laços da região com a China, tanto em termos comerciais ou de investimentos, ampliaram-se de forma muito significativa.

O resultado de tais eventos foi a existência de um país claramente revisionista (Venezuela), com presença estratégica de potenciais adversários (especialmente Rússia e Irã), conjugado com uma presença econômica de outro

[19]Gendarmerização seria o processo de alocar as Forças Armadas de um país basicamente para combater a segurança pública, num papel constabular. Sobre a gendarmerização, especialmente no caso brasileiro, ver Alsina Júnior (2018).

adversário (China) por todo o continente. Sentindo-se pressionados, a partir de 2025 os EUA optaram por recorrer a medidas drásticas de intervenção militar, já citadas.

Logo, a evolução histórica da importância do Caribe e América do Sul para os propósitos geopolíticos dos EUA aponta que o caso da securitização das drogas é apenas um fator a ser considerado numa estratégia muito mais ampla.

Em relação ao Atlântico Sul, tanto a ESN quanto a EDN não o mencionam.[20] No entanto, ao deixar tão claro o conceito de Hemisfério Ocidental (e que seria a principal prioridade dos EUA), implicitamente a área é abrangida como de importância para o país.

Desdobramentos na estratégia brasileira voltada para o Atlântico Sul

O Brasil é o maior país da América do Sul e, devido a sua posição geográfica, exerce forte influência nas duas margens do Atlântico Sul.[21] Ademais, essa região marítima figura como importante espaço de reserva, fonte de recursos[22] e meio de projeção internacional para o Brasil. Nesse sentido, o Brasil tem interesse em mater a região sul-atlântica como uma região de paz e afastada das disputas geopolíticas da atualidade.

O interesse no Atlântico Sul pode ser verificado na Política Nacional de Defesa (PND), documento de mais alto nível de defesa do País:

> A PND estabelece como área de interesse prioritário o entorno estratégico brasileiro, que inclui a América do Sul, o espaço aéreo sobrejacente ao território nacional, **o Atlântico Sul**, e os países africanos lindeiros ao Atlântico Sul e à Antártica (Brasil, 2025, grifo nosso).

[20]Nos dois documentos, a única menção ao Oceano Atlântico refere-se ao fluxo transatlântico envolvendo Europa e Estados Unidos.

[21]Para efeito deste trabalho, entendemos como Atlântico Sul o que preconiza a Política Nacional de Defesa (2025): O Atlântico Sul é a região delimitada geoestrategicamente ao Norte pelo paralelo 16º N; ao Sul pelo Continente Antártico; a Leste pelo litoral africano e a Oeste pela América do Sul.

[22]Recursos econômicos – biológicos, minerais e energéticos – e ambientais que compõem a Economia Azul. Disponível em: https://www.marinha.mil.br/economia-azul/sobre. Acesso em: 30 jan. 2026.

Assim, o Brasil reconhece a importância estratégica desse espaço marítimo, entendendo a necessidade de protegê-lo de ameaças e tensões de naturezas diversas.[23]

A PND também deixa claro que as questões relacionadas com a segurança marítima devem ser uma preocupação do Setor de Defesa do País:

> A segurança marítima do Atlântico Sul, em face da natural vocação marítima brasileira, respaldada pelo seu extenso litoral, pela magnitude do seu comércio marítimo e pelas atividades econômicas associadas ao uso direto ou indireto do mar, deve ser uma preocupação constante do Setor de Defesa para apoiar o desenvolvimento sustentável do Brasil (Brasil, 2025).

Assim, o Estado brasileiro entende que a segurança marítima é uma das pautas prioritárias, uma vez que, sem águas seguras o seu comércio pode ser brutalmente afetado.[24] Nesse sentido, o aparato estatal deve desenvolver estratégias para atingir o objetivo de manter o Atlântico Sul como uma região segura, livre de intervenções externas e próspera para os países lindeiros

Nesse contexto, ameaças como os crimes transnacionais que ocorrem no Atlântico Sul, principalmente o narcotráfico internacional que se utiliza de rotas oriundas do Brasil, depõem negativamente sobre a imagem e a credibilidade das instituições brasileiras.

Em estudo publicado na Revista Brasileira de Inteligência, Dantas (2025) aponta um crescimento significativo no uso de narcossubmarinos nas rotas atlânticas e na utilização de portos em cidades brasileiras como ponto de apoio logístico. O estudo analisou as apreensões de narcossubmarinos no período de 2010 a 2025, buscando relação qualitativa entre elas, ou seja, não foi dado um tratamento isolado a cada caso, buscando-se conexão entre eles que indicassem uma padronização logística na atuação dos narcotraficantes.[25] A conclusão do estudo apontou a existência de um "narcoeixo" submerso

---

[23] As ameaças poderiam ser categorizadas em três tipos: as clássicas, as implementadas pelo processo de globalização e as neotradicionais ou as "novas ameaças". (Almeida Silva; Marcondes, 2019).

[24] O Atlântico Sul é o sítio das rotas marítimas brasileiras, cujo comércio marítimo corresponde a 95% do seu comércio exterior.

[25] Para detalhes do estudo ver: "Narcossubmarinos no Oceano Atlântico: crime transnacional emergente, desafios para o Brasil". Disponível em: https://share.google/f8dAw2YHB05leCVBx. Acesso em: 31 jan. 2026.

que utiliza cidades brasileiras ao norte do País como ponto de apoio para a partida desses veículos submersos em direção, principalmente, dos Continentes europeu e africano.

O caso dos narcossubmarinos é somente um exemplo de ameaça existente na região marítima brasileira que constitui objeto potencial de securitização pelos EUA. Sob argumento semelhante ao utilizado contra a Venezuela, Washington pode, em um futuro breve, criar o discurso securitizante para respaldar uma intervenção. Diante disso, como tornar o Atlântico Sul mais seguro mitigando o risco de securitização? A própria PND nos propõe uma resposta:

> A promoção da estabilidade no Atlântico Sul atende a interesses estratégicos brasileiros. Portanto, a revitalização da Zona de Paz e Cooperação do Atlântico Sul - ZOPACAS constitui prioridade para a **política externa brasileira.** Além de importante foro de concertação e cooperação para enfrentar a situação securitária no Atlântico Sul, a ZOPACAS oferece espaço para a cooperação entre seus integrantes em diversas áreas, como mapeamento do fundo marinho, pesquisa oceanográfica, meio ambiente, transporte aéreo e marítimo, defesa, educação, entre outros. (Brasil, 2025, grifo nosso).

A Diplomacia brasileira tem plena consciência da importância da ZOPACAS no contexto da segurança do Atlântico Sul. Na XVIII Reunião Ministerial do Fórum, ocorrida em abril de 2023 em Cabo Verde, o Ministro Mauro Vieira (Chanceler brasileiro) deixou claro em seu discurso o potencial inexplorado da ZOPACAS e que o estreitamento das relações entre os países do foro, por meio de iniciativas concretas de cooperação e de constante diálogo sobre problemas comuns, podem evitar que o Atlântico Sul seja percebido como um vazio de poder.[26]

A revitalização da ZOPACAS nos parece um caminho plausível do ponto de vista do objetivo da manutenção da segurança marítima no Atlântico Sul e da redução das condições de um ambiente securitizante atualmente desenvolvido pelos EUA. Nesse contexto, a Marinha do Brasil (MB) cresce em importância

[26]Discurso do Ministro Mauro Vieira na XVIII Reunião Ministerial da ZOPACAS, Cabo Verde em 18 de abril de 2023, disponível em: https://www.gov.br/mre/pt-br/zopacas/documentos/discursos/participacao-do-ministro-mauro-vieira-na-viii-reuniao-ministerial-da-zopacas-2013-18-de-abril. Acesso em: 31 jan. 2026.

estratégica, sendo um dos entes estatais possuidores dos meios capazes de contribuir com a cooperação e o diálogo. Além de possuir os instrumentos de coerção e uso da força que poderiam ser aplicados quando necessários.

A Estratégia de Defesa Marítima (EDM), publicada em 13 de dezembro de 2023, apresenta diversas prioridades estratégicas no campo da Segurança Marítima, voltadas para proteção das águas sul-atlânticas e da Diplomacia Naval, voltadas para o apoio ao Ministério das Relações Exteriores no fortalecimento da ZOPACAS (Brasil, 2023).

O referido documento, em seu Conceito Estratégico, prevê que a MB deverá atuar de forma integrada com outros órgãos federais (Polícia Federal, Receita Federal etc.) na prevenção e repressão a delitos transnacionais, incluindo o tráfico de drogas, adotando uma postura coercitiva. Quanto ao apoio ao MRE na ZOPACAS, o documento prevê que a MB priorizará uma postura cooperativa nos relacionamentos com as Marinhas Amigas, em especial os países membros da ZOPACAS (Brasil, 2023).

Na análise dos documentos citados, podemos observar que o Estado brasileiro possui orientações claras no nível político-estratégico que, se implementadas, teriam o potencial de mitigar os riscos da evolução de um processo de securitização no Atlântico Sul. Essas orientações trazem um misto de atuação diplomática com base na cooperação e aumento de poder naval crível como meios de coerção. O caminho nos parece coerente, tendo em vista o acumulado histórico da diplomacia brasileira,[27] diante dos desafios de segurança atinentes ao Atlântico Sul e de uma possível intervenção norte-americana nesse importante espaço marítimo.

[27] Segundo Amado Cervo, a política exterior do Brasil, em sua evolução, vem agregando princípios e valores à diplomacia, de modo a tornar tais elementos inerentes à sua conduta. Amado Cervo cita alguns padrões que podem ser identificados: autodeterminação, não-intervenção; ação externa cooperativa e não-confrontacionista; multilateralismo normativo; realismo e pragmatismos; e outros. Ver: Cervo (2008), p. 26-31.

Sugestões de posturas a serem adotadas pelo Brasil, juntamente com os países da região, diante do ambiente externo com a ESN e a EDN dos EUA.

A partir do que foi exposto anteriormente, a questão da securitização das drogas, estimulada pelos EUA, não é um fenômeno ocasional, haja vista o papel significativo tanto na ESN quanto na EDN. Além disso, consideramos que o movimento estratégico em que a securitização está inserida (ou seja, o protagonismo do Hemisfério Ocidental para a geopolítica dos EUA, reforçando elementos já presentes em termos históricos, desde a Doutrina Monroe) não é algo fortuito ou que irá se desvanecer sensivelmente após o Governo Trump.

Afinal, os movimentos dos EUA provocaram grande abalo nas relações com os países aliados ou quase-aliados, ensejando neles uma mudança estratégica significativa. Já que os EUA tomaram a iniciativa de propor uma abordagem mais autárquica, em termos relativos, relevando a segundo plano a rede de alianças costurada desde a II Guerra Mundial, a busca por alternativas estratégicas, especialmente no caso da Europa, tornou-se prioritária, e mesmo uma reviravolta (que consideramos pouco provável em governos subsequentes, com no máximo alguns aspectos sendo atenuados) daquele país sempre será visto com ressalvas.

Portanto, elencaremos algumas sugestões que, ao nosso ver, facilitariam o relacionamento com os EUA, sem que estes incorressem em intervenções traumáticas e que prejudicariam iniciativas, objetivos e projetos brasileiros e, por extensão, nosso relacionamento com os demais países da região.

Em termos estratégicos, já foi observado que os EUA buscam basicamente insular (na medida do possível) o Hemisfério Ocidental de maiores influências (políticas, econômicas, militares) de países extrarregionais, especialmente China, Rússia, Irã e Coreia do Norte, mencionados nominalmente na EDN. Por exemplo, no caso da China, embora o documento afirme categoricamente que não é intenção dos EUA um conflito bélico, a postura de demonstrar poder perante os orientais é a de "...Simplesmente assegurar que nem a China ou qualquer outro país possa nos dominar ou aos nossos aliados" (Estados Unidos, 2025a, p. 10, tradução livre).

Por exemplo, ao mencionar um certo degelo no nível de tensão entre os dois países, no momento em que este capítulo está sendo escrito, Fedirka

(2026) enfatiza esse aspecto, ao elencar os interesses dos EUA em garantir supremacia tecnológica, logística e financeira na região:

> Ao final, qualquer acomodação entre EUA e China (em relação à América Latina) será transacional. Mesmo na melhor das circunstâncias, parcerias geopol´tiicas são mutáveis e evoluem baseadas em necessidades individuais. Washington e Beijing não estão próximos de se tornarem parceiros vigorosos; eles simplesmente entendem que uma compreensão mútua é propícia, e que terá alguns muros de proteção colocados.

Logo, qualquer movimento de aproximação mais estreita (político-militar) com China, Rússia ou Irã, por exemplo, por parte do Brasil ou outro país da região, será interpretado como ameaça aos interesses dos EUA. Nesse sentido, estreitar o relacionamento com países como Japão, Índia, Alemanha, França ou Reino Unido, pode trazer diversificação estratégica necessária para o Brasil, sem necessariamente causar reações negativas pelos EUA. Tal tipo de relacionamento pode nos proporcionar dividendos econômicos (em termos de intercâmbio comercial e financeiro), tecnológico (absorção de tecnologias não-sensíveis, num primeiro momento) e políticos (apoio nos fóruns internacionais em relação a pontos de interesses comuns a Potências Médias).

Outro ponto fundamental é a busca por maior integração na América do Sul e junto aos demais países da ZOPACAS, especialmente africanos. Tal postura, caso concretizada, poderia constituir uma liderança legitimada e funcional para os EUA, tendo em vista que se supõe que os maiores pontos de fricção entre as Grandes Potências devem continuar na Eurásia, em primeiro lugar, com África em segundo lugar.[28] Logo, o Brasil seria visto como "confiável" a exercer uma liderança regional e que prescindisse da presença ostensiva dos EUA, ao reduzir preventivamente focos de tensão. Além disso, uma maior presença efetiva do Brasil no continente africano (especialmente se em ação conjunta com a Índia) contribuiria para contrabalançar a crescente presença chinesa (e, secundariamente, russa), naquele continente.

Em relação aos próprios EUA, a postura brasileira deveria ser a de ressaltar que há muito mais interesses compatíveis do que antagônicos, ressaltando uma "transparência estratégica" ao enfatizar nichos de cooperação. Entre eles, destacam-se diversos setores em que o Brasil poderia se valer do

[28]No caso da EDN (Estados Unidos, 2026, p. 20), a menção à África se resume apenas ao perigo de terroristas islâmicos adentrarem o Hemisfério Ocidental.

processo de “near-shoring” e “friend-shoring” em que diversas empresas transnacionais se deslocam para regiões mais próximas/” confiáveis” dos países consumidores (geralmente, saindo da China...)

Outro aspecto que é interessante para ambos os países é a questão da Segurança Marítima, ameaçada pelo crescimento das organizações criminosas transnacionais, conforme já mencionado. Logo, um melhor aparelhamento da Marinha Brasileira, e mesmo a participação conjunta de nações europeias no Atlântico Sul, em termos de vigilância, seria bem-vinda pelos EUA.[29]

Considerações Finais

O presente capítulo buscou analisar o processo de securitização no Mar do Caribe desenvolvido pelos EUA nos últimos meses. Pôde-se perceber que – após a análise histórica na bibliografia especializada e documentos oficiais do Governo norte-americano – a nova postura de Washington tem o potencial de se expandir para outras regiões marítimas do Continente americano, inclusive no Atlântico Sul. O enquadramento do narcotráfico internacional como ação terrorista ampliou ainda mais a capacidade de atuação do Governo norte-americano dentro de uma agenda de segurança nacional, cuja pauta do combate às drogas com o uso de força militar já foi incorporada ao imaginário popular dos países do Hemisfério ao longo das últimas décadas do Século XX e início de XXI.

A análise histórica da questão das drogas permitiu-nos verificar que a percepção do narcotráfico como uma ameaça não ocorreu de forma abrupta, mas foi resultado de um processo cumulativo de associação entre crime, instabilidade regional e percepção de ameaça à soberania. Na literatura especializada foi possível verificar que o narcotráfico foi aos poucos sendo incorporado à agenda de segurança dos EUA, sobretudo no contexto do controle das fronteiras e da internacionalização das políticas antidrogas. Dessa forma, o Caribe passou a ser percebido não somente como um espaço permissivo ao ato ilícito, mas como área estratégica para a integridade norte-americana.

[29]A propósito, o Atlântico Sul não é mencionado em nenhum dos dois documentos analisados.

A leitura dos documentos condicionantes de segurança e defesa dos EUA – notadamente a *National Security Strategy* e a *National Defense Strategy* – revelou que o discurso securitizante foi institucionalizado como política de Estado. Nesse sentido, o crime transnacional, principalmente o narcotráfico, é categorizado como ameaça direta à estabilidade interna e à soberania nacional. Para se contrapor a isso, a EDN deixa claro que os EUA terão opções militares dignas de confiança para atuar no Hemisfério com velocidade, poder e precisão, como na Operação Determinação Absoluta. O que se pôde depreender da leitura de ambos os documentos é que o Corolário Trump à Doutrina Monroe tem como alvo principal a garantia da integridade do *Homeland* que, na percepção norte- americana atual, abrange todo o Hemisfério.

No âmbito militar-naval, os efeitos dessa postura incorporada à política de Estado puderam ser verificados no Caribe, onde foram executadas operações de interdições marítimas com afundamento de embarcações de narcotraficantes, abordagens e apresamento de navios mercantes que transportavam petróleo venezuelano. Nesse contexto, a articulação entre o discurso e a ação militar confirma o argumento central desse capítulo de que a securitização do narcotráfico, na administração Trump, não se limita à retórica, mas é elemento chave na gestão de espaços marítimos considerados sensíveis e/ou estratégicos para os EUA.

Nesse ponto surge um alerta para os demais países do Continente, principalmente os sul-americanos, de que as ações norte-americanas não se restringem ao entorno imediato dos EUA. A consolidação de mecanismos de interdição extrarregional provocam reflexões acerca de possíveis ações em outros espaços marítimos considerados de relevância estratégica como o Atlântico Sul. Em que pese não haver evidências claras de uma replicação imediata do modelo do Caribe no Atlântico Sul, a amplificação do repertório securitizante associado ao poder militar norte-americano amplia a margem de atuação extrarregional e reforça a importância do mar como vetor de competição e controle no contexto geopolítico atual.

Nesse contexto, o Brasil assume uma importância fundamental como ator capaz de gerar um balanço de poder no Hemisfério. Em que pese sua baixa capacidade militar-naval para se contrapor aos EUA, o Brasil exerce forte influência político-diplomática nas duas margens do Atlântico Sul e é percebido por seus vizinhos como uma liderança regional. Adicionalmente, a Estratégia de

Defesa Marítima reafirma o Atlântico Sul como entorno estratégico prioritário do Brasil, do ponto de vista da soberania, desenvolvimento e estabilidade regional. Diferente da lógica norte-americana de securitização, o documento privilegia a cooperação, a governança marítima e a convergência entre defesa e diplomacia como instrumentos centrais de proteção dos interesses nacionais.

Diante da possibilidade de securitização no Atlântico Sul, o Estado brasileiro necessita tomar medidas claras que demonstrem a sua capacidade de articulação e influência regional. Nesse sentido, a valorização de fóruns multilaterais como a Zona de Paz e Cooperação do Atlântico Sul torna-se fundamental e um eixo estratégico primordial para o atingimento do objetivo da manutenção desse importante espaço marítimo como uma região livre das disputas geopolíticas extrarregionais. No nível operacional, a Marinha do Brasil – alinhada com o interesse do Estado brasileiro – tem capacidade de promover exercícios navais de grande envergadura com os países regionais do Atlântico Sul. Tal medida tem o potencial de demonstrar a capacidade de organização operacional da MB em ambientes multinacionais. Além disso, medidas como essa reforçam o multilateralismo e a diplomacia militar, elementos importantes no combate a ações unilaterais securitizantes.

O capítulo revelou que a securitização do narcotráfico pelos Estados Unidos da América constitui, *per se*, uma possível ameaça aos interesses brasileiros no espaço marítimo do Atlântico Sul, tendo em vista que a utilização do modelo de ampliação da securitização tem o potencial de se estender onde e quando os interesses norte-americano estiveram em jogo. Adicionalmente, as escolhas políticas para a solução dos problemas advindos dos crimes transnacionais seguem caminhos diferentes nas tradições estratégicas dos dois países, o que pode tornar-se ponto atrito entre eles e uma justificativa para uma ação mais contundente da parte dos EUA.

O Atlântico Sul, historicamente percebido como um espaço de cooperação, vive atualmente sobre a sombra da ameaça da securitização. Nesse sentido, a resposta brasileira a essa ameaça dependerá menos do confronto e mais da capacidade de articulação estratégica e de influência regional do Brasil. Nesse contexto, o debate sobre a segurança no Atlântico Sul, na atualidade, deveria ser um tema central na sociedade e na elite política e intelectual brasileira. Tal debate não pode ser mais dissociado das dinâmicas e mecanismos mais amplos de securitização e projeção de poder observadas no Caribe. Compreender o

processo em curso é fundamental para avaliar risco, oportunidades e limites da atuação brasileira dentro de um ambiente internacional marcado por crescentes disputas geopolíticas.

O evento relativo à iniciativa "Shield of the Americas", realizado em Miami em 07/03/2026, congregando diversos representantes das Américas (mas não tendo a presença de Brasil, Colômbia ou México, entre outros)[30], além da divulgação quase simultânea de um ataque conjunto de forças equatorianas e dos EUA contra narcotraficantes (Buschschlüter; Graham, 2026), ressaltam que a tendência analisada ao longo do capítulo mostra-se cada vez mais presente, com impactos significativos e que demandarão uma atuação com mínima margem de erro, por parte dos grandes decisores nos diversos países, em especial o Brasil.

Referências

ALMEIDA SILVA, Antonio Ruy de; MARCONDES, Danilo. Globalização, Segurança e Defesa no Atlântico Sul. *Nação e Defesa* nº 154 pp. 69-88. Lisboa, 2019.

ALSINA JR., João Paulo. *Ensaios de grande estratégia brasileira*. Rio de Janeiro: FGV Editora, 2018.

ANDREAS, Peter. *Border games: policing the U.S.–Mexico divide*. 2. ed. Ithaca: Cornell University Press, 2009.

BAGLEY, Bruce M. *Drug trafficking and organized crime in the Americas*. Washington, DC: Woodrow Wilson International Center for Scholars, 2012.

BRASIL. Ministério da Defesa. *Política Nacional de Defesa*. Brasília, 2025.

BRASIL. Ministério da Defesa. Marinha do Brasil. *Estratégia de Defesa Marítima*. Brasília, 2023.

[30]The Guardian (2026); para uma análise do impacto do "Shield of the Americas" no Sistema multilateral e arquitetura de segurança nas Américas, especialmente na OEA e JID, ver Foro de Seguridad Multinivel (2026).

BUZAN, Barry; HANSEN, Lena. *A evolução dos estudos de segurança internacional*. São Paulo: UNESP, 2012.

BUZAN, Barry; WÆVER, Ole; DE WILDE, Jaap. *Security: a new framework for analysis*. Boulder: Lynne Rienner Publishers, 1998.

CERVO, Amado Luiz. *Inserção internacional: formação dos conceitos brasileiros*. São Paulo: Saraiva, 2008.

DANAHAY, Martin. What the Opium Wars can tell us about China, the U.S. and fentanyl. *The Conversation*, 20 jan. 2025. Disponível em: https://theconversation.com/what-the-opium-wars-can-tell-us-about-china-the-u-s-and-fentanyl-247170. Acesso em: 28 jan. 2026.

DANTAS, Alberto. Narcossubmarinos no Oceano Atlântico: crime transnacional emergente, desafios para o Brasil. *Revista Brasileira de Inteligência*, Brasília, Brasil. https://doi.org/10.58960/rbi.2025.20.255.

ESTADOS UNIDOS. Department of War. *National Defense Strategy*. 23 jan. 2026.

ESTADOS UNIDOS. The White House. *National Security Strategy*. 2025a.

ESTADOS UNIDOS. The White House. President Donald J. Trump designates fentanyl as a weapon of mass destruction. 2025b. Disponível em: https://www.whitehouse.gov/videos/president-donald-j-trump-designates-fentanyl-as-a-weapon-of-mass-destruction/. Acesso em: 28 jan. 2026.

ESTADOS UNIDOS. Department of Defense. United States Southern Command. *Enhanced counter-narcotics operations in the Caribbean Sea and Eastern Pacific*. Miami: U.S. Southern Command, 2020.

FEDIRKA, Allison. Washington's red lines in Latin America. *Geopolitical Futures*, 4 feb. 2026.

MEARSHEIMER, John J. *The tragedy of great power politics*. New York: W. W. Norton, 2001.

RODRIGUES, Thiago. *Política e drogas nas Américas*. São Paulo: Editora Desatino, 2012.

ROSEN, Jonathan D. *The lost war: plan Colombia and the fight against coca*. Albany: State University of New York Press, 2014.

SANTA BÁRBARA, Marcelo de Jesus. *A talassocracia dos Estados Unidos da América e a projeção continental do Brasil: contrapontos geopolíticos*. Curitiba: Appris, 2025

TRUMP convenes 'Shield of Americas' summit with 12 Latin American leaders. *The Guardian*, 07/03/2026. Disponível em: https://www.theguardian.com/us-news/2026/mar/07/trump-shield-of-americas-summit. Acesso em: 10 anr. 2026.

O Brasil no combate ao crime organizado transnacional no âmbito da OTCA:
ações no contexto das cúpulas internacionais na Amazônia (2023-2025)[1]

Bruno Cezar Pereira Soares
Michele Eduarda Brasil de Sá
Leonardo Ulian Dall Evedove

Introdução

Para iniciarmos a abordagem do tema específico deste artigo, é necessário que se façam algumas definições básicas. Concordamos com a definição teórica de Cepik e Borba (2011) de crime organizado como uma violação da lei escrita, executada por grupos estáveis, economicamente motivada e com danos difusos à sociedade e ao Estado. Consideramos importante acrescentar, a partir da leitura mencionada, que o crime organizado tem uma relação conservadora e parasitária com a ordem estatal, o que o distancia de situações de grupos insurgentes que pretendam estabelecer outra ordem distinta da vigente.

A perspectiva teórica acima apresentada parece não divergir muito da concepção da Convenção de Palermo sobre grupo criminoso organizado, que seria um grupo estruturado de três ou mais pessoas, situado no tempo, agindo em concerto em crimes graves ou infrações estabelecidas em convenção para fins econômicos e materiais (Brasil, 2004).

O uso do adjetivo transnacional nas definições apresentadas acima não é fortuito. Também de acordo com a Convenção de Palermo, a transnacionalidade se estabelece quando o crime for cometido em mais de um Estado; em um único Estado, mas com parte substancial de suas cadeias de planejamento e execução em outro Estado; quando envolver grupo criminoso organizado atuante em

[1] Neste artigo, foram utilizadas as ferramentas Lex Page, para revisão gramatical do texto, e ChatGPT (GPT-4o), como apoio à revisão gramatical, à pesquisa de informações e à estruturação textual. O conteúdo intelectual, as interpretações, as conclusões e a redação final foram integralmente elaborados, revisados e validados pelo autor, que assume total responsabilidade pelo trabalho apresentado.

mais de um Estado; ou quando for cometido em um único Estado, mas com efeitos substanciais em outro Estado (Brasil, 2004, adaptado). Succi Junior e Castro (2019) asseveram que o conceito de crime transnacional não organizado também se apresenta como um fenômeno mais amplo, estudado por autoras como Marmo e Chazal (2016).

Este trabalho está dividido em quatro seções, contando com esta introdução. Na segunda, será apresentado o perfil brasileiro de combate ao crime transnacional na Amazônia. Na terceira, serão apresentadas algumas questões preliminares sobre o combate ao crime transnacional no âmbito da OTCA. Na quarta, será abordada a atuação brasileira nas cúpulas internacionais na Amazônia e, por fim, estabeleceremos interlocuções possíveis como palavras finais.

A posição internacional do Brasil quanto ao crime organizado: uma revisão

Nesta seção, procuramos realizar uma revisão bibliográfica da produção brasileira sobre o COT, a área de Relações Internacionais e a posição internacional do Brasil sobre o tema, se possível, com foco na Amazônia internacional. Para tanto, recorremos à busca simples pelos termos crime, crime transnacional e COT nas ferramentas de busca das próprias revistas científicas dos extratos A1-A4, da área-mãe ciência política/relações internacionais do país. Além disso, associamos livremente artigos e livros não localizados pela busca sistemática, mas com relevância no tema para a comunidade especializada.

Em prefácio a um dossiê especial sobre crime e relações internacionais, Viana et al. (2020) afirmam que a academia brasileira acumulou trabalhos em diversas áreas sobre o crime entre as décadas de 1980 e 1990. A área de relações internacionais (RI), no entanto, veria seu primeiro trabalho publicado em periódico de relevo em 1997, com o artigo de Procópio Filho e Vaz sobre o narcotráfico, que abordaremos com mais detalhe abaixo. Recorrendo a outras revisões bibliográficas anteriores a 2020, não encontramos referências que afirmem o contrário (Oliveira; Zaverucha, 2009).

Uma vez inaugurado o estudo do crime transnacional com o artigo referido acima, estudiosos da área permaneceram pouco numerosos até o presente momento. Em levantamento realizado em 2019 sobre trabalhos apresentados

em congressos da Associação Brasileira de Relações Internacionais (ABRI), os mesmos estudiosos citados no início do parágrafo acima identificaram 34 trabalhos com temas relacionados ao crime na área de RI entre 2007 e 2019. Além de serem poucos os trabalhos, quase todos estavam relacionados a poucos estudiosos mais experientes que articulam e orientam na área (Viana *et al*., 2020). Parte do quadro pode ter a ver com a construção teórica da disciplina de relações internacionais e a subárea de segurança internacional, que tem uma visão binária entre o nacional e o internacional, em choque com um fenômeno "interméstico" (Succi Junior; Castro, 2019).

Ainda que pouco volumoso, o estudo do crime transnacional pela área de relações internacionais foi impulsionado por alguns fenômenos, alguns de ordem política e outros de ordem conceitual. No campo político, temos o fim da Guerra Fria, o aprofundamento dos fenômenos da globalização e da regionalização, nas áreas econômica, política, cultural e territorial desde o fim da década de 1980. Além disso, houve o fenômeno da guerra às drogas nos EUA, atrelado à execução extraterritorial do ordenamento jurídico estadunidense e à associação de crime transnacional, narcotráfico e insurgência política em países da América do Sul (Viana *et al.,* 2020; Vitelli *et al.,* 2020).

No campo conceitual, temos a emergência dos Estudos de Segurança Internacional (ESI) e do fenômeno da securitização como um de seus pilares (Buzan *et al.,* 1998; Buzan *et al.,* 2003). Além disso, temos a proposição, pelos Estados Unidos e pela OEA, do conceito de segurança multidimensional, atrelando o crime transnacional à segurança internacional e à segurança dos Estados latino-americanos, carregando em seu interior a proposição de uma militarização das polícias e uma policialização das Forças Armadas (Vitelli *et al.,* 2020). Estudos também foram realizados sobre a construção da noção de COT como parte de uma construção sociopolítica interna aos EUA, de cristalização de ameaça imigrante estrangeira, de redes criminosas, atrelamento do tema à globalização e à expansão do terrorismo (Pereira, 2015). Um exemplo disso é a própria Convenção de Palermo.

O artigo pioneiro de Procópio Filho e Vaz (1997), já mencionado, traz uma cronologia sobre a cooperação internacional global contra o narcotráfico transnacional. Os autores situam os primórdios da cooperação internacional em acordos relativos à repressão do comércio do ópio, no início do século XX. Em seguida, citam acordos nas décadas de 1920, 1930 e 1960 no esteio da Liga

das Nações e da ONU. Na década de 1980, os autores chamam a atenção para a Convenção das Nações Unidas contra o Tráfico Ilícito de Estupefacientes e Substâncias Psicotrópicas. A UNODP, criada em 1990, é citada como uma importante organização facilitadora do diálogo sobre o tema, uma vez que tem baixo perfil de capacidade de implementar políticas. Todos esses acordos e processos contaram com a adesão do Brasil (Procópio Filho; Vaz, 1997).

De acordo com os mesmos autores, quanto ao tratamento do tema no entorno hemisférico brasileiro, a história traz a forte influência que a política estadunidense exerceu sobre os demais países americanos, estabelecendo um pólo repressivo sobre a oferta, bilateral e militarizante da parte dos EUA, e uma postura heterogênea, multilateral e relativista dos países latinos. Alguns dos terrenos em que isso se verificou foram diversas cúpulas governamentais (Cartagena, San Antonio e Miami) e a Comissão Interamericana para o Controle do Abuso de Drogas (CICAD) da Organização dos Estados Americanos (OEA), no seio da qual, após debates ocorridos ao longo de anos, geraram-se alguns acordos de cooperação, como a Estratégia Antidrogas do Hemisfério, de 1996 (Procópio Filho; Vaz, 1997). Outras referências importantes foram as conferências hemisféricas de ministros da defesa de Williamsburg (1995) e Bariloche (1996), e as cúpulas do Grupo do Rio, nas quais as linhas gerais do perfil estadunidense e latino-americano se mantiveram. O tema do narcotráfico, no entanto, constitui apenas parte do assunto mais amplo abordado neste artigo.

No Cone Sul, nos anos 1990, no esteio das aproximações de parte dos seus países em torno do Mercosul, algumas primeiras iniciativas bilaterais foram firmadas, como a de Brasil e Argentina em 1995 (Procópio Filho; Vaz, 1997).

O trabalho de Rodrigues (2012) é bastante citado em diversos trabalhos posteriores a sua publicação, trazendo reflexões específicas sobre a guerra às drogas promovida pelos EUA na América Latina e o processo de militarização da segurança interna dos países, já mencionado acima. Essas questões, no entanto, são apenas parte do foco deste artigo.

Villa (2014), ao escrever sobre macrossecuritização e a presença dos EUA na América do Sul, discute o posicionamento daquele país frente ao crime transnacional na região, cujos focos são o narcotráfico, tendo por centro nevrálgico a Colômbia e suas imediações e a tríplice fronteira entre Argentina,

Brasil e Paraguai, vista como zona de articulação de redes criminais, lavagem de dinheiro, financiamento do terrorismo e contrabando.

No campo bilateral, chamamos a atenção para a cooperação entre Brasil e Colômbia na repressão ao narcotráfico, a reboque da cooperação em defesa, no contexto da discussão das novas ameaças à segurança típicas do início do século XXI (Closs, 2020).

No entanto, as principais ações do governo brasileiro em escala regional no combate ao narcotráfico concentraram-se no âmbito da UNASUL, a partir de 2008. Procurando uma via alternativa à OEA, com a abordagem hemisférica e a participação dos EUA, buscou imprimir uma perspectiva regional sul-americana. Na Cúpula de 2009, Lula articulou consenso em torno da Declaração de São Carlos de Bariloche, que previu cooperação regional contra o terrorismo e o narcotráfico e rejeitou a presença de potências extrarregionais. A diplomacia brasileira foi central na criação do Conselho de Defesa Sul-Americano (CDS) e do Conselho Sul-Americano sobre o Problema Mundial de Drogas (CSPMD), separando as agendas de defesa e de drogas. No CSPMD, o Brasil defendeu a responsabilidade compartilhada e uma abordagem que incluísse redução da oferta e da demanda, saúde pública, educação, lavagem de dinheiro, controle e desenvolvimento sustentável. Apesar dessas iniciativas diplomáticas, os arranjos institucionais internos mantiveram-se baseados na lógica proibicionista (Closs, 2020). Como se pode observar, a noção de COT não foi utilizada como plataforma articuladora da atuação brasileira ou regional.

No levantamento que nos foi permitido pelas técnicas apontadas no início dessa seção, não encontramos maiores informações sobre a atuação brasileira no COT nos governos Rousseff, Temer ou Bolsonaro, o que aponta para um caminho importante de pesquisa. A questão amazônica, a OTCA ou as cúpulas de presidentes da Amazônia internacional também não foram encontradas. Dessa forma, as discussões abaixo adotaram uma abordagem exploratória e estabeleceram um primeiro olhar articulado sobre esses temas.

O combate ao crime organizado transnacional no âmbito da OTCA

Crimes ambientais, incluindo a biopirataria, tráfico de drogas, tráfico de pessoas, contrabando de pessoas, tráfico de armas, medicamentos fraudulentos e o cibercrime representam desafios urgentes que demandam

esforços conjuntos de governança multilateral na Amazônia. O aproveitamento inadequado dos recursos genéticos e os demais ilícitos descritos comprometem o desenvolvimento regional e evidenciam a necessidade de integrar a pauta ambiental à segurança e à cooperação internacionais. No chamado Arco de Instabilidade Andino-Amazônico, a OTCA apresenta-se como ferramenta plausível e eficaz para combater atividades ilícitas transnacionais na região, especialmente se considerarmos o enfraquecimento da UNASUL, o *locus* que deveria abrigar os debates relacionados à defesa e à segurança (Teixeira; Cunha; Queiroz, 2024).

Inicialmente, pode-se dizer que a OTCA era guiada por uma atmosfera intergovernamental e soberanista da parte de cada país em particular, dada a desconfiança entre os signatários do tratado. Embora os artigos VIII, IX, X e XII do Anteprojeto do Tratado de Cooperação Amazônica (TCA) previssem assuntos como integração física, complementação econômica e o estabelecimento de um "foro para discutir a defesa da integridade da Amazônia", estes assuntos acabaram perdendo força por conta desta atmosfera de desconfiança (Nunes, 2016, p. 240). No entanto, a necessidade impunha a abertura gradativa, o que se foi observando ao longo do tempo. Na Reunião de Ministros das Relações Exteriores realizada em 25 de novembro de 2005, em Iquitos, Peru, o assunto foi trazido a debate e a incorporação da questão como um dos vetores da cooperação amazônica deu um passo para tornar-se algo mais concreto. Em 13 de julho de 2006, por iniciativa da Colômbia, realizou-se, em Bogotá, a Primeira Reunião Ministerial sobre Defesa e Segurança Integral da Amazônia.

Rodrigues e Paiva (2025, p. 32), tratando de projetos de desenvolvimento sustentável cooperativos, chamam a atenção para a necessidade de se retomar e intensificar o espírito político-institucional inicial da celebração do TCA, uma vez que não se pode prescindir da atuação conjunta para enfrentar os complexos desafios comuns. A mesma necessidade existe no tocante à segurança e à defesa. Embora discutir defesa ainda seja uma tarefa espinhosa, é fato que tratar de segurança tornou-se um imperativo. A segurança hoje é um dos dez eixos temáticos da OTCA e a luta contra o COT é, desde a própria apresentação deste eixo, "uma prioridade compartilhada pelos oito países amazônicos" (OTCA, 2025d).

Um avanço concreto da última década foi a criação, no âmbito da OTCA, de uma Comissão Especial de Segurança Pública e Ilícitos Transfronteiriços

e Transnacionais na Região Amazônica, cuja primeira reunião ocorreu em Letícia, em 09 de junho de 2025 (Brasil, 2025a). O encontro marcou o início das atividades da Comissão, com vistas à estruturação de subcomissões temáticas para tratar, entre outros temas, da coordenação operacional entre as forças de segurança e do combate a delitos ambientais. Na prática, a participação do Brasil se materializa na presença de delegações interministeriais (relações exteriores, justiça/segurança pública, defesa e meio ambiente) nas reuniões da Comissão, que negociam protocolos de cooperação e fluxos de informação. A ênfase brasileira em delitos ambientais – como desmatamento ilegal, garimpo e tráfico de espécies – aparece como prioridade, articulando segurança pública com agenda climática e de biodiversidade.

O eixo de segurança da OTCA também se articula com a proteção de direitos humanos na Amazônia, a partir do compromisso de proteção de defensores ambientais e sociais. Comunidades indígenas e outros grupos locais também são alvo de violência relacionada ao COT. Estudos realizados por *think tanks,* como o Instituto Igarapé, denunciam ameaças e ataques de organizações criminosas contra líderes locais (Risso *et al.,* 2024), o que motivou debates na Cúpula Presidencial da OTCA em 2025 sobre medidas regionais de proteção.

Uma das respostas da OTCA à proliferação de crimes ambientais na bacia amazônica foi o diálogo "Fortalecimento da cooperação regional para enfrentar os crimes ambientais na Bacia Amazônica", organizado durante a COP 16 da Convenção sobre Diversidade Biológica (CDB), em que representantes da OTCA e de institutos de pesquisa enfatizaram a necessidade de respostas regionais coordenadas à exploração ilegal de recursos naturais, ao desmatamento e mineração ilegal, muitas vezes articulados em redes transnacionais de crime organizado.

Outra resposta (desta vez uma decisão política tomada no marco da OTCA) foi a intensificação de arranjos de cooperação bilateral e trilateral em áreas de fronteira, sobretudo entre Brasil, Colômbia e Peru, materializada no Protocolo de intercâmbio de informações de inteligência entre a Marinha da Colômbia e a Polícia Federal do Brasil, assinado em Bogotá em janeiro de 2026 no âmbito do Programa Global de Combate ao Crime Marítimo (GMCP) do Escritório das Nações Unidas sobre Drogas e Crime no Brasil (em inglês, UNODC). O objetivo deste documento é fortalecer a cooperação operacional e o intercâmbio de informações no combate ao COT ligado ao tráfico de drogas

em espaços marítimos e fluviais na região amazônica compartilhada, em consonância com a Convenção da ONU contra o COT.

Esse protocolo se soma a outro acordo semelhante firmado entre a Marinha da Colômbia e a Polícia Nacional do Peru em 2025, consolidando uma arquitetura de segurança que conecta os três países que compartilham importantes corredores fluviais transfronteiriços na Amazônia. Trata-se de um espaço crítico, uma vez que tais corredores são frequentemente utilizados no tráfico de drogas e de outros ilícitos. A coordenação operacional – incluindo a troca de inteligência, reuniões trimestrais e ações combinadas – reforça a capacidade brasileira de enfrentar o crime transnacional, a partir de decisões e agendas discutidas também na OTCA. Embora sejam acordos sob a égide da ONU, sua justificação política remete à necessidade de fortalecer a governança multinível da Amazônia, na qual a OTCA é referência.

Diante do exposto, percebemos que há iniciativas importantes envolvendo a OTCA e seus membros quanto à questão mais abrangente do COT; no entanto, há tendência a setorizar as discussões. A investigação que aqui se apresenta continuará buscando uma visão articulada e generalista que alinhe os esforços acima elencados.

A atuação brasileira nas cúpulas internacionais da Amazônia

O crescimento da produção de cocaína nos países andinos, somado à instabilidade e aos conflitos na região, amplia as rotas do narcotráfico que cruzam o continente para abastecer o mercado externo, fortalecendo grupos criminosos que atuam para além das fronteiras nacionais. Aproveitando-se da imensa cobertura florestal e da baixa capacidade de controle dos Estados, dificultada pelas próprias características geográficas da Amazônia, essas organizações praticam delitos como o tráfico de drogas e armas, bem como a extração e venda ilegais de madeira e ouro. Esse cenário intensifica a violência, a corrupção e a destruição do meio ambiente. A atuação dessas redes criminosas coloca em risco direto a segurança das populações tradicionais, a soberania territorial dos países amazônicos e as iniciativas de conservação ambiental (Brasil; Colômbia, 2025).

Somente na Amazônia Legal brasileira, os dados apontam que dos "772 municípios amazônicos, 344 (44,6%) apresentam alguma evidência da presença

de facções, demonstrando um processo de capilarização que transcende os grandes centros urbanos" (Fórum Brasileiro de Segurança Pública - FBSP, 2025, p.54). Essa presença tem implicações para a segurança pública e também potencializa a prática de crimes ambientais, já que esses grupos também praticam a grilagem de terras e a mineração ilegal, esta última também utilizada para esquemas de lavagem de dinheiro (Conselho Nacional de Justiça - CNJ, 2024).

Dado o desafio que essas organizações representam para os países da região, é necessário intensificar a colaboração entre os integrantes da OTCA, incluindo temas de segurança nas pautas de discussão e na atuação da entidade. Portanto, abordaremos a seguir as iniciativas brasileiras nesse sentido ocorridas na IV e na V Reunião de Presidentes da OTCA, bem como na COP 30.

IV Reunião de Presidentes da OTCA

A OTCA vem experimentando um "reativamento" de suas atividades, impulsionado, em parte, pela realização da COP 30 em Belém, em 2025. Esse movimento gera otimismo quanto ao avanço de sua agenda e à implementação de novos projetos. Um marco importante desse processo foi a IV Reunião de Presidentes dos Países Membros, realizada em 9 de agosto de 2023, também em Belém. O encontro resultou na Declaração de Belém, um documento que fortalece a cooperação internacional entre os países signatários ao definir novas orientações estratégicas para a atuação da OTCA.

Nela há um conjunto de normas destinadas a "reforçar e ampliar a cooperação policial, judicial e de inteligência no combate a atividades ilícitas, incluindo crimes ambientais" (OTCA, 2023a, p. 27). Suas decisões de números 61 até a 67 tratam, respectivamente: da expansão da colaboração policial e de inteligência para investigação de crimes; do apoio entre os países para o combate ao tráfico de espécies, mineração ilegal e atividades conexas; da assistência mútua entre órgãos de fiscalização e de julgamento de delitos ambientais e relacionados, com vistas à harmonização da legislação; do trabalho conjunto para erradicação da mineração ilegal, contrabando de mercúrio e infrações relacionadas, como a lavagem de dinheiro; do estabelecimento do Centro de Cooperação Policial Internacional da Amazônia (CCPI Amazônia), com sede em Manaus, para o intercâmbio de informações e o desenvolvimento de

investigações conjuntas; do início do processo de diálogo para a criação do Sistema de Controle de Tráfego Aéreo Integrado entre os Estados Partes da OTCA, com vistas à colaboração no monitoramento do tráfego aéreo ilícito e no combate ao narcotráfico; e da proposta da realização de uma Reunião de Ministros e autoridades dos setores de Segurança Pública dos Estados Partes para avaliar a situação do COT na Amazônia.

O CCPI Amazônia iniciou suas atividades no dia 9 de setembro de 2025, congregando órgãos de segurança pública do Brasil, Bolívia, Colômbia, Equador, Guiana, Peru, Suriname, Venezuela e França (Guiana Francesa), além dos nove estados brasileiros da Amazônia Legal (UNODC, 2025b). O centro também articula a cooperação com redes internacionais, como a Interpol, a Ameripol e a Europol, ampliando o intercâmbio estratégico no combate de crimes ambientais, ao tráfico de entorpecentes, de armas e de pessoas. O novo centro integra o Plano Amas - Amazônia: Segurança e Soberania (Brasil, 2023), que recebeu R$318,5 milhões em recursos do Fundo Amazônia (Brasil, 2024).

Atualmente, não há, no seio da OTCA, qualquer indicativo acerca do andamento do diálogo sobre a criação de um sistema de controle de tráfego aéreo (OTCA, 2025d). Em novembro de 2023 ocorreu a XIV Reunião de Ministros de Relações Exteriores da OTCA em Brasília, Brasil. Nela foi aprovada a Declaração de Brasília, que avança nas pautas estabelecidas pela Declaração de Belém. A Resolução nº 9 do documento estabeleceu a Comissão Especial de Segurança Pública e Ilícitos Transnacionais na Região Amazônica, além de ter instruído a Secretaria Permanente da organização a elaborar um módulo para monitoramento de crimes transnacionais no âmbito do Observatório Regional Amazônico (ORA), buscando consolidar informações no combate ao crime (OTCA, 2023b). A Comissão Especial realizou em junho de 2025, em Letícia, Colômbia, a sua primeira reunião, na esteira da Reunião de Ministros e Altas Autoridades em matéria de Segurança Pública dos Estados Partes. Nesse evento foi aprovado o plano de trabalho da comissão, porém não foi possível encontrar mais informações sobre como essa instância atuará (OTCA, 2025c).

V Reunião de Presidentes da OTCA

Em 22 de agosto de 2025 aconteceu a V Reunião de Presidentes dos Estados Partes do Tratado de Cooperação Amazônica, em Bogotá, Colômbia.

Ela serviu como um último grande alinhamento político antes da COP 30. Nela foi aprovada a Declaração de Bogotá, que reafirmou e buscou aprofundar os compromissos assumidos na Declaração de Belém e na Declaração de Brasília (OTCA, 2025a). O documento reconhece a necessidade de abordar de maneira integral "a expansão de economias ilegais [...], o crime organizado transnacional", bem como a "contaminação de mercúrio resultante de atividades ilegais" (OTCA, 2025a, p. 1).

Dentre as trinta e cinco decisões tomadas na reunião, cabe destacar o apoio à Comissão Especial de Segurança Pública e Atividades Ilegais Transfronteiriças e Transnacionais na Região Amazônica na implementação da "cooperação policial, judicial e de inteligência na luta contra as atividades ilegais transfronteiriças" (OTCA, 2025a, p. 6) e na troca de experiências "na rastreabilidade do ouro, reconhecendo as ligações entre a mineração ilegal [...] e outras ameaças ambientais" (OTCA, 2025a, p. 6).

Como parte desse esforço colaborativo, a Agência Brasileira de Inteligência (ABIN) e a *Dirección Nacional de Inteligencia* (DNI), da Colômbia, publicaram o relatório "Desafios da Amazônia Compartilhada". No documento, é traçado um diagnóstico sobre os impactos e as tendências de ameaças comuns como o narcotráfico, a mineração ilegal de ouro e o contrabando de migrantes (Brasil; Colômbia, 2025).

O encontro presidencial também decidiu apoiar o processo de negociação das propostas para um ou mais protocolos para a Convenção das Nações Unidas contra o Crime Organizado Transnacional (UNTOC), dada a preocupação com o aumento e alcance dos crimes ambientais (OTCA, 2025a).

Ainda na esteira da preparação para a COP 30, a OTCA debateu a harmonização das legislações florestais na Pan-Amazônia entre os dias 27 e 28 de janeiro de 2025 em Brasília (Brasil, 2025c). Em conjunto com o Superior Tribunal de Justiça (STJ), o Banco Interamericano de Desenvolvimento (BID), gestores, juízes e especialistas, discutiu-se a "Iniciativa Global da Lei Florestal Modelo" (MoFAI - *Model Forest Act Initiative*). A medida busca compatibilizar as legislações florestais e penais entre os membros da OTCA, facilitando o combate a pessoas e organizações criminosas que atuam em múltiplas jurisdições (OTCA, 2025b).

O Brasil também realizou junto à Colômbia e ao Peru a Quinta Reunião Tripartite sobre Aplicação da Lei nos Rios da Bacia Amazônica, em Brasília, entre os dias 12 e 14 de agosto de 2025. A reunião promoveu a cooperação policial, marítima e fluvial contra o narcotráfico e os delitos conexos na tríplice fronteira entre os países. Sob a facilitação do Programa Global de Crimes Marítimos (GMCP) do Escritório das Nações Unidas sobre Drogas e Crime (UNODC), essa iniciativa estabeleceu redes de contato direto entre oficiais de ligação e discutiu estratégias para aprimorar a troca de informações em tempo real entre agências, avançando, assim, na cooperação para operações e investigações coordenadas (UNODC, 2025a).

COP 30

A Convenção-Quadro das Nações Unidas sobre Mudança do Clima (UNFCCC, em inglês) realizou a 30ª Conferência das Nações Unidas sobre a Mudança do Clima (Conferência das Partes - COP 30) dos dias 10 a 21 de novembro de 2025 na cidade de Belém, no estado do Pará, Brasil. Trata-se de um encontro global onde líderes mundiais, cientistas, organizações não governamentais e representantes da sociedade civil se reuniram para discutir ações de combate às mudanças climáticas (COP 30, 2025d).

A Conferência não deu destaque para as pautas de segurança ou combate ao COT, havendo, portanto, pouco a ser discutido sobre as iniciativas governamentais brasileiras quanto a esses temas junto a seus parceiros da OTCA, no âmbito dessa cúpula. De fato, dentro do conjunto de 29 decisões do chamado "Pacote de Belém" (COP 30, 2025b), nenhuma aborda esses assuntos (UNFCCC, 2025).

As únicas afirmações relacionadas encontram-se em dois documentos oficiais da Cúpula do Clima de Belém, mas que não integram o "pacote da COP30". O primeiro é a Declaração de Belém sobre Fome, Pobreza e Ação Climática Centrada nas Pessoas, que propõe "Proteger os direitos de propriedade sobre florestas e outros direitos dos Povos Indígenas e comunidades locais como estratégia eficaz para fortalecer a resiliência, combater atividades ilegais nas florestas e promover a gestão responsável" (Brasil, 2025b, p. 4). O segundo é o Chamado à Ação sobre Manejo Integrado do Fogo e Resiliência a Incêndios Florestais, que busca:

Reforçar, quando apropriado, as capacidades institucionais, a transparência e a cooperação entre as autoridades de aplicação da lei, a fim de enfrentar de forma eficaz as atividades ilegais que contribuem para ou se beneficiam de incêndios florestais. (Nações Unidas, 2025, p. 4)

Embora esses trechos não estejam focados em organizações criminosas, eles reconhecem a necessidade de se combater as atividades ilegais nas florestas, uma vez que há relação entre as ações de grupos criminosos e a degradação ambiental (Brasil; Colômbia, 2025; CNJ, 2024).

Também cabe pontuar que, dos 144 painéis realizados pelo Brasil na Zona Azul do evento, exclusiva para delegações oficiais, chefes de Estado, observadores e imprensa credenciada, apenas o promovido pelo Ministério da Justiça e da Segurança Pública (MJSP), "Plano AMAS - Amazônia: Segurança e Soberania" abordou a temática da segurança (COP 30, 2025a). O MJSP atuou de maneira semelhante na Zona Verde, espaço destinado ao diálogo entre a sociedade civil, instituições públicas, privadas e líderes globais. Dos 142 painéis previstos, o intitulado "Segurança na Amazônia", também foi singular quanto ao objeto (COP 30, 2025c).

A partir do exposto, percebemos uma atividade importante do Brasil na proposição e articulação de iniciativas. O foco na Amazônia parece estar atrelado fortemente à temática ambiental, influenciado fortemente pelo fato de o país ser a sede da COP 30 no período abordado. Como observado na seção 3, não houve uma abordagem única e generalista sobre o COT, sendo mantida aquela baseada em áreas diversas.

Quadro 1 - Cronologia das iniciativas de segurança 2023-2025 (continua)

Data	Evento / Marco	Medida Principal	Resultado Concreto de Segurança
Ago 2023	IV Cúpula (Belém)	Declaração de Belém (Arts. 61-67)	Mandato para criar a Comissão Especial de Segurança da OTCA.
Dez 2023	Lançamento Plano AMAS	Destinação de Fundo Amazônia para Segurança	R$ 318,5 milhões garantidos para logística e inteligência.

Data	Evento / Marco	Medida Principal	Resultado Concreto de Segurança
Jan 2025	Evento STJ/OTCA	Iniciativa MoFAI	Início da harmonização de leis penais ambientais.
Ago 2025	V Cúpula (Bogotá)	Declaração de Bogotá	Consenso sobre rastreabilidade de ouro e protocolos UNTOC.
Set 2025	Inauguração CCPI	Abertura do Centro em Manaus	Integração física de polícias de 9 países + 9 estados.

Fonte: Elaborado pelos autores (2026).

Considerações finais

Empreendemos um estudo exploratório sobre a posição brasileira em conjunto com os demais países amazônicos e associados à OTCA sobre o COT. Percebemos que, embora haja iniciativas e contextos importantes a serem abordados, tanto o debate acadêmico quanto a realidade da política internacional, vinculados a uma resposta articulada do país ao COT, ainda têm muito a se desenvolver.

Na primeira seção do trabalho, percebemos que as principais produções da área de Relações Internacionais no Brasil se dedicam mais ao tema do narcotráfico e dos desafios geopolíticos que a política antidrogas e repressiva dos EUA trouxe para a América do Sul e as políticas regional e global brasileiras. Os estudos mais adensados do COT como fenômeno abrangente circunscrevem-se majoritariamente à criminologia ou a debates sobre segurança pública e justiça internamente ao país.

Na segunda, observamos que a abordagem da OTCA sobre o crime transnacional é historicamente setorizada, privilegiando questões relacionadas ao crime ambiental e à política de fronteiras, fortemente atrelada à cooperação intergovernamental em matéria de segurança e justiça. Também relatamos a necessidade de a organização superar seu passado de distanciamento entre seus membros por conta de desconfianças relacionadas ao dilema de segurança.

Na última seção, vimos uma intensificação das iniciativas brasileiras em matéria de cooperação policial, judicial e de inteligência contra atividades ilícitas e crimes ambientais, inclusive com a criação de um centro de cooperação policial internacional. Obteve-se ainda cooperação e financiamento internacional para a implantação do Plano Amazônia Segurança e Soberania. No âmbito da OTCA, houve a criação da Comissão Especial de Segurança Pública e Ilícitos Internacionais na Região Amazônica, com monitoramento via ORA.

O que se pode afirmar preliminarmente, ainda que não de forma categórica, é que o Brasil promoveu uma abordagem mais significativa sobre o COT no âmbito da Amazônia, num sentido incremental às estruturas previamente existentes em suas parcerias e arcabouço institucional via OTCA. Intensificaram-se ações de órgãos subnacionais, nacionais e intergovernamentais entre países na região. Rotas de cooperação com fundos internacionais indicam a intenção de atrair observadores extrarregionais para a adesão dos países da região ao enquadramento do COT a uma perspectiva mais aberta e multilateral de abordagem do tema. Todas as percepções aqui apresentadas são, no entanto, parciais, e constituem-se em material de trabalho para aprofundamento e futuros trabalhos a serem desenvolvidos.

Referências

ARRAES, Virgílio. Narcotráfico e segurança humana. *Revista Brasileira de Política Internacional,* n. 44, v.1, 2001. Disponível em: https://www.scielo.br/j/rbpi/a/BRLLRVzvSqJyTBNB3FhgLSd/. Acesso em: 23 fev. 2026.

BRASIL. Decreto nº 5.015, de 12 de março de 2004. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional. *Diário Oficial da União*, Brasília, DF, 15 mar. 2004. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm. Acesso em: 10 mar. 2026.

BRASIL. Banco Nacional de Desenvolvimento Econômico e Social - BNDES; União Federal, por meio do Ministério da Justiça e Segurança Pública - MJSP. *Contrato de Aplicação de Recursos Não Reembolsáveis nº 24.2.0134.1.* Rio de Janeiro, 17 jun. 2024. 31 p. Disponível em: https://www.

fundoamazonia.gov.br/export/sites/default/pt/.galleries/documentos/contratos-aditivos/MJSP-contrato.pdf. Acesso em: 22 fev. 2026

BRASIL. Decreto nº 11.614, de 21 de julho de 2023. Institui o Plano Amazônia: Segurança e Soberania - Plano Amas. *Diário Oficial da União:* seção 1, Brasília, DF, ano 160, n. 138, p. 1, 24 jul. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11614.htm. Acesso em: 22 fev. 2026.

BRASIL. Ministério das Relações Exteriores. *Primeira reunião da Comissão Especial de Segurança Pública e Ilícitos Transfronteiriços e Transnacionais na Região Amazônica da OTCA.* Brasília, DF: MRE, 10 jun. 2025a. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/primeira-reuniao-da-comissao-especial-de-seguranca-publica-e-ilicitos-transfronteiricos-e-transnacionais-na-regiao-amazonica-da-otca. Acesso em: 3 fev. 2026.

BRASIL. Presidência da República. *Declaração de Belém sobre Fome, Pobreza e Ação Climática Centrada nas Pessoas.* Belém, Brasil: Presidência da República, 7 nov. 2025b. Disponível em: https://cop30.br/pt-br/noticias-da-cop30/documentos/. Acesso em: 23 fev. 2026.

BRASIL. Superior Tribunal de Justiça. *Relatório do Presidente*: 22 de agosto de 2024 a 19 de dezembro de 2025. Brasília, DF: STJ, 2025c. 88 p. Disponível em: https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/Relatorio%20Presidente%202024-2025.pdf. Acesso em: 23 fev. 2026.

BRASIL; COLÔMBIA. *Desafios da Amazônia Compartilhada***.** Brasília: Agência Brasileira de Inteligência, 2025. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/desafios-da-amazonia-compartilhada/desafios-da-amazonia-compartilhada. Acesso em: 19 dez. 2025.

BUZAN, Barry; WÆVER, Ole. *Regions and powers:* the structure of international security. Cambridge: Cambridge University Press, 2003.

BUZAN, Barry; WÆVER, Ole; WILDE, Jaap de. *Security:* a new framework for analysis. Boulder: Lynne Rienner Publishers, 1998.

CEPIK, Marco; BORBA, Pedro. Crime Organizado, Estado e Segurança Internacional. *Contexto Internacional,* Rio de Janeiro, v. 33, n. 2., 2011.

CLOSS, Marília B. Política externa como política pública: o combate ao narcotráfico no governo de Lula da Silva. *Brazilian Journal of International Relations*, Marília, SP, v. 9, n. 1, p. 125–146, 2020. DOI: 10.36311/2237-7743.2020.v9n1.08.p125. Disponível em: https://revistas.marilia.unesp.br/index.php/bjir/article/view/10152. Acesso em: 24 fev. 2026.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Relatório sobre crimes ambientais na Amazônia Legal.* Brasília, DF: CNJ, 2024. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2024/04/relatorio-crimes-ambientais-na-amazonia-legal-final.pdf. Acesso em: 13 jan. 2025.

COP 30. *Blue Zone.* [S. l.], 2025a. Disponível em: https://cop30.br/pt-br/sobre-a-cop30/blue-zone?activeAccordion=cb3bda20-cf83-498b-957c-30d72c491a87. Acesso em: 23 fev. 2026.

COP 30. *COP 30 aprova o Pacote Belém.* [S. l.], 2025b. Disponível em: https://cop30.br/pt-br/noticias-da-cop30/cop30-aprova-o-pacote-belem. Acesso em: 24 fev. 2026.

COP 30. *Green Zone.* [S. l.], 2025c. Disponível em: https://cop30.br/pt-br/sobre-a-cop30/green-zone?activeAccordion=8ef743be-732f-4e0e-b17d-7bedbc14b609. Acesso em: 23 fev. 2026.

COP 30. *Perguntas mais frequentes.* [S. l.], 2025d. Disponível em: https://cop30.br/pt-br/sobre-a-cop30/perguntas-mais-frequentes?activeAccordion=9d79ffa8-e4b4-4701-8ea3-52cb07ca93bd%2Ce63054b1-48d9-4d44-9161-11c2ee1065ef. Acesso em: 24 fev. 2026.

FEITOSA, Gustavo Raposo Pereira; PINHEIRO, José Augusto de Oliveira. Lei do Abate, guerra às drogas e defesa nacional. *Revista Brasileira de Política Internacional,* Brasília, v. 55, n.1, 2012. Disponível em: https://www.scielo.br/j/rbpi/a/dH4VBBcpfXmTySmgrJ3MPjk/. Acesso em: 23 fev. 2026.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. *Cartografias da violência na Amazônia.* 4. ed. São Paulo, SP: Fórum Brasileiro de Segurança Pública, 2025.

MARMO, Marinella; CHAZAL, Nérida. *Transnational crime and criminal justice.* Londres: SAGE Publications, 2016.

NAÇÕES UNIDAS. Organização das Nações Unidas para a Alimentação e a Agricultura. *Chamado à Ação sobre Manejo Integrado do Fogo e Resiliência a Incêndios Florestais.* Belém, Brasil: FAO/UNFCCC, 2025. Disponível em: https://cop30.br/pt-br/noticias-da-cop30/documentos/. Acesso em: 23 fev. 2026.

NUNES, Paulo Henrique Faria. A Organização do Tratado de Cooperação Amazônica: uma análise crítica das razões por trás da sua criação e evolução. *Revista de Direito Internacional,* v. 13, n. 2, p. 221-245, 2016.

OLIVEIRA, Adriano; ZAVERUCHA, Jorge. Conceito e origens do crime organizado: uma revisão bibliográfica. *BIB - Revista Brasileira de Informação Bibliográfica em Ciências Sociais,* n. 68, p. 5–16, 2009. Disponível em: https://bibanpocs.emnuvens.com.br/revista/article/view/331. Acesso em: 10 mar. 2026.

ORGANIZAÇÃO DO TRATADO DE COOPERAÇÃO AMAZÔNICA (OTCA). *Declaração de Belém 2023.* [S. l.], 2023a. Disponível em: https://otca.org/pt/wp-content/uploads/2023/10/Declaracao-de-Belem.pdf. Acesso em: 21 dez. 2024.

ORGANIZAÇÃO DO TRATADO DE COOPERAÇÃO AMAZÔNICA (OTCA). Declaración de Brasilia. In: XIV REUNIÓN DE MINISTROS DE RELACIONES EXTERIORES DE LA ORGANIZACIÓN DEL TRATADO DE COOPERACIÓN AMAZÓNICA. *Anais.[...]* Brasília, Brasil, 23 nov. 2023b. Disponível em: https://otca.org/wp-content/uploads/2021/09/0_DECL__RES_XIV-MRE-OTCA_01-29_ESP.pdf. Acesso em: 9 fev. 2026.

ORGANIZAÇÃO DO TRATADO DE COOPERAÇÃO AMAZÔNICA (OTCA). Declaração de Bogotá. In: V REUNIÃO DE PRESIDENTES DOS ESTADOS PARTES DO TRATADO DE COOPERAÇÃO AMAZÔNICA. *Anais[...]* Bogotá, Colômbia: OTCA, 22 ago. 2025a. Disponível em: https://otca.org/wp-content/uploads/2025/08/DECLARACAO-DE-BOGOTA_Cupula-Presidentes.pdf. Acesso em: 6 fev. 2026.

ORGANIZAÇÃO DO TRATADO DE COOPERAÇÃO AMAZÔNICA (OTCA). *Mesa discute harmonização jurídica para proteger as florestas amazônicas em evento no STJ.* Brasília, DF, 2025b. Disponível em: https://otca.org/pt/mesa-discute-harmonizacao-juridica-para-proteger-as-florestas-

amazonicas-em-evento-no-stj/. Acesso em: 23 fev. 2026.

ORGANIZAÇÃO DO TRATADO DE COOPERAÇÃO AMAZÔNICA (OTCA). *Ministros da segurança pública dos países amazônicos se reúnem em Leticia para fortalecer a cooperação no enfrentamento aos ilícitos transnacionais.* Brasília, DF, 2025c. Disponível em: https://otca.org/pt/ministros-da-seguranca-publica-dos-paises-amazonicos-se-reunem-em-leticia-para-fortalecer-a-cooperacao-no-enfrentamento-aos-ilicitos-transnacionais/. Acesso em: 22 fev. 2026.

ORGANIZAÇÃO DO TRATADO DE COOPERAÇÃO AMAZÔNICA (OTCA). *Segurança.* Brasília, DF, 2025d. Disponível em: https://otca.org/pt/eixo/seguranca/. Acesso em: 22 fev. 2026.

PEREIRA, Paulo. Os Estados Unidos e a ameaça do crime organizado transnacional nos anos 1990. *Revista Brasileira de Política Internacional,* v. 58, n. 1, 2015. Disponível em: https://doi.org/10.1590/0034-7329201500105. Acesso em: 2 mar. 2026.

PIMENTA, Marília Carolina Barbosa de Souza; ROSERO, Luis Fernando Trejos. Crime organizado transnacional na América do Sul: uma análise da presença e governança de atores armados não estatais na fronteira entre a Colômbia e a Venezuela. *Monções:* Revista de Relações Internacionais da UFGD, v. 9, n. 17, p. 364–393, 2020. DOI: 10.30612/rmufgd.v9i17.10952. Disponível em: https://ojs.ufgd.edu.br/moncoes/article/view/10952. Acesso em: 25 fev. 2026.

PROCÓPIO FILHO, Argemiro; VAZ, Alcides Costa. O Brasil no contexto do narcotráfico internacional. *Revista Brasileira de Política Internacional,* Brasília, v. 40, n. 1, 1997. Disponível em: https://www.scielo.br/j/rbpi/a/mhDdvn6Mgkrqtyyy9bLrdmg/. Acesso em: 23 fev. 2026.

RISSO, Melina et al. *Dinâmicas do ecossistema dos crimes ambientais na Amazônia Legal.* Artigo Estratégico 64. Rio de Janeiro: Instituto Igarapé, 2024. Disponível em: https://igarape.org.br/wp-content/uploads/2024/08/SC_PT_AE-64-Dinamicas-ecossistema-crimes-ambientais-Amazonia-legal.pdf. Acesso em: 14 jan. 2026.

RODRIGUES, Bernardo Salgado; PAIVA, Paulo Vinícius dos Santos. O ressurgimento da Organização do Tratado de Cooperação Amazônica (OTCA): o avanço institucional na promoção de políticas de desenvolvimento sustentável. *Revista de Segurança, Desenvolvimento e Defesa,* v. 2, n. 2, p. 26-42, 2025.

RODRIGUES, Thiago. Narcotráfico e militarização nas Américas: vício de guerra. *Contexto Internacional.* Rio de Janeiro, v. 34, n. 1, p. 9-41, 2012.

SANTANA, Adalberto. A globalização do narcotráfico. *Revista Brasileira de Política Internacional,* Brasília, v. 42, n. 1, p. 75-122, 1997. Disponível em: https://www.scielo.br/j/rbpi/a/NKWcy3jTMdydYHs4TKKFVmv/. Acesso em: 23 fev. 2026.

SILVA, Luiza L. *A questão das drogas nas relações internacionais:* uma perspectiva brasileira. Brasília: FUNAG, 2013.

SUCCI JUNIOR, David Paulo. Missões militares, técnica e política: o emprego das forças armadas em segurança pública. *Brazilian Journal of International Relations,* Marília, SP, v. 6, n. 2, p. 413–436, 2017. DOI: 10.36311/2237-7743.2017.v6n2.10.p413. Disponível em: https://revistas.marilia.unesp.br/index.php/bjir/article/view/6701. Acesso em: 11 mar. 2026.

SUCCI JUNIOR, David Paulo; CASTRO, Helena S. Crime organizado transnacional e missões militares. *Conjuntura Austral.* Porto Alegre, RS, v.10, n. 52, p. 38-58, 2019. DOI: https://doi.org/10.22456/2178-8839.95051

TEIXEIRA, Carlos Alfredo Lazary; DA CUNHA, Guilherme Lopes; DE QUEIROZ, Fábio Albergaria. A Polycentric Governance Model Through the Amazon Cooperation Treaty Organization: Capabilities for Tackling Transnational Threats. *In:* RICCIO, Vicente; DA CUNHA, Guilherme Lopes. (ed.). *Policing the Amazon.* Routledge, 2024. p. 109-121.

UNITED NATIONS FRAMEWORK CONVENTION ON CLIMATE CHANGE (UNFCCC). *Belém Political Package.* [S. l.], 2025. Disponível em: https://unfccc.int/cop30/belem-political-package. Acesso em: 24 fev. 2026.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). *Brasil, Colômbia e Peru fortalecem cooperação contra crimes transnacionais em 5ª reunião tripartite de países amazônicos promovida pelo UNODC.* [S. l.], ago.

2025a. Disponível em: https://www.unodc.org/cofrb/pt/noticias/2025/8/brasil--colmbia-e-peru-fortalecem-cooperacao-contra-crimes-transnacionais-em-5-reuniao-tripartite-de-paises-amazonicos-promovida-pelo-unodc.html. Acesso em: 23 fev. 2026.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). *UNODC Brasil reforça parceria estratégica na inauguração do Centro de Cooperação Policial Internacional da Amazônia.* [S. l.], set. 2025b. Disponível em: https://www.unodc.org/cofrb/pt/noticias/2025/9/unodc-brasil-reforca-parceria-estrategica-na-inauguracao-do-centro-de-cooperacao-policial-internacional-da-amazonia.html. Acesso em: 22 fev. 2026.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). 2026. *Organized crime.* Disponível em: https://www.unodc.org/toc/en/crimes/organized-crime.html. Acesso em: 13 mar. 2026.

VIANA, Manuela Trindade; CAMPOS, Marcelo da Silveira; PEREIRA, Paulo José dos Reis; RODRIGUES, Thiago. Criminalidade transnacional: olhares para além da disciplina de Relações Internacionais. *Monções: Revista De Relações Internacionaisda UFGD,* [S. l.], v. 9, n. 17, p. 15-21, 2020.

VILLA, Rafael Duarte. O paradoxo da macrossecuritização: quando a guerra ao terror não securitiza outras guerras na América do Sul. *Contexto Internacional,* Rio de Janeiro, v. 36, n. 2, p. 349-383, jul./dez., 2014.

VITELLI, Marina Gisela; MATHIAS, Suzeley Kalil; CASTRO, Helena Salim de. Crime organizado: confrontando a perspectiva securitizadora com as contribuições sobre state-crime collusion. Implicações disciplinares. *Monções:* Revista de Relações Internacionais da UFGD, [S. l.], v. 9, n. 17, p. 105–138, 2020. DOI: 10.30612/rmufgd.v9i17.10866. Disponível em: https://ojs.ufgd.edu.br/moncoes/article/view/10866. Acesso em: 14 jan. 2026.

Proteção de infraestruturas de computação de alto desempenho como pilar da soberania digital: desafios e implicações para o Estado Brasileiro

Jaime de Melo Gama da Silva
Rômulo Ferreira dos Santos
Matheus Henrique de Souza

Introdução

A transformação digital das estruturas estatais redefiniu a natureza dos ativos estratégicos que sustentam a soberania nacional. A centralidade da infraestrutura digital, da capacidade de processamento de dados e da conectividade global deslocou parte significativa do exercício do poder estatal para o domínio tecnológico. No contexto contemporâneo, a autonomia não depende apenas de recursos naturais, capacidade industrial ou poder militar convencional, mas também da habilidade de produzir, processar e proteger informações estratégicas.

A Computação de Alto Desempenho (HPC) consolidou-se como elemento estruturante dessa nova configuração do poder. Supercomputadores viabilizam simulações científicas complexas, modelagens energéticas e climáticas, análise de grandes volumes de dados e desenvolvimento de aplicações avançadas de inteligência artificial, sustentando decisões governamentais de elevado impacto estratégico (Deelman *et al.,* 2025, p. 829–830).A HPC, nesse sentido, integra o núcleo das capacidades analíticas do Estado e influencia diretamente políticas públicas, planejamento de infraestrutura e estratégias de desenvolvimento tecnológico.

A literatura sobre soberania digital enfatiza que a autonomia contemporânea está vinculada à capacidade de assegurar acesso contínuo a tecnologias críticas e de reduzir dependências estruturais em cadeias globais concentradas geograficamente (Fang *et al.,* 2026, p. 2-3).A interdependência tecnológica global, especialmente no setor de semicondutores, infraestrutura de dados e serviços computacionais, introduz vulnerabilidades sistêmicas que

podem comprometer a autonomia decisória de Estados que não detêm controle sobre suas próprias capacidades estratégicas.

Nesse ambiente de competição tecnológica e disputas geopolíticas, a infraestrutura de supercomputação passa a integrar o campo da diplomacia tecnológica. O domínio de capacidades avançadas de processamento influencia a inserção internacional do Estado, sua posição em negociações científicas e sua capacidade de participar de cadeias de inovação de alto valor agregado. A proteção desses ativos, portanto, transcende o campo técnico e assume dimensão estratégica.

A crescente classificação de infraestruturas digitais como infraestruturas críticas reforça essa visão, uma vez que sua interrupção pode comprometer serviços essenciais e a estabilidade estatal (Silva *et al.,* 2025, p. 2–3). Ambientes de supercomputação utilizados para pesquisa estratégica e processamento de dados governamentais vêm sendo progressivamente reconhecidos como ativos críticos, dada sua importância para simulações de segurança nacional, análise de dados sensíveis e desenvolvimento de capacidades tecnológicas avançadas (Guo *et al.,* 2024, p. 1–2).

Do ponto de vista técnico, ambientes HPC apresentam vulnerabilidades específicas decorrentes de sua arquitetura distribuída, da execução paralela de tarefas e do compartilhamento intensivo de recursos entre múltiplos usuários (Koleini; Pahlevanzadeh, 2024, p. 12–13). O comprometimento de um único ponto pode permitir movimentação lateral e escalonamento indevido de privilégios, afetando a integridade dos dados e a confiabilidade das análises produzidas.

Diante da sofisticação crescente das ameaças digitais e da erosão das fronteiras tradicionais das redes, modelos baseados exclusivamente na defesa perimetral mostram-se insuficientes, sobretudo porque pressupõem confiança implícita no "interior" do ambiente e ampliam o impacto de credenciais comprometidas (Rose *et al*., 2020, p. 1-2). Nesse contexto, paradigmas como Zero Trust e mecanismos apoiados por Infraestruturas de Chaves Públicas (ICP/PKI) emergem como alternativas para reforçar o controle de identidade, autenticação e autorização, reduzindo a exposição prolongada de credenciais e limitando a movimentação lateral em ambientes compartilhados (Rose *et al.,* 2020, p. 7-9; Guo *et al.,* 2024, p. 10-12). No caso brasileiro, a ampliação do uso de supercomputadores por universidades, centros de pesquisa e instituições

estatais reforça a necessidade de compreender a proteção desses ambientes como componente da soberania digital e da estratégia nacional de segurança, uma vez que a integridade das análises produzidas por sistemas de HPC influencia decisões relacionadas à segurança energética, gestão ambiental, planejamento de infraestrutura e desenvolvimento científico (Deelman *et al.,* 2025, p. 829-830).

Problema de Pesquisa e Lacuna

A consolidação da Computação de Alto Desempenho (HPC) como infraestrutura estratégica ampliou a centralidade da segurança desses ambientes no contexto da soberania digital (Deelman *et al.,* 2025, p. 829-830). No Brasil, o Plano Brasileiro de Inteligência Artificial (PBIA 2024-2028) prevê investimentos de R$ 23 bilhões para fortalecer a autonomia tecnológica nacional, incluindo a expansão de supercomputadores como o Santos Dumont (LNCC), que passou de 1,7 para 18,85 petaflops (Brasil, 2025). Paralelamente, a nova Estratégia Nacional de Cibersegurança (E-Ciber) estabelece como eixo estruturante a "soberania nacional e governança", reconhecendo infraestruturas críticas como ativos sensíveis à autonomia decisória estatal (Brasil, 2025a, art. 1º, IV).

A literatura especializada identifica vulnerabilidades em ambientes HPC decorrentes de sua arquitetura distribuída, compartilhamento de recursos e risco de movimentação lateral após comprometimento inicial (Guo *et al*., 2024, p. 10-12). Embora modelos como Zero Trust sejam reconhecidos para superar limitações de abordagens centradas no perímetro (Rose *et al*., 2020, p. 1-2), permanece limitada a sistematização de como estruturar tais mecanismos em HPC estatal brasileiro, articulando segurança técnica e soberania digital.

Evidencia-se lacuna na integração entre: (I) vulnerabilidades técnicas de ambientes HPC; (II) mecanismos avançados de autenticação; e (III) implicações para a soberania digital brasileira.

Problema de pesquisa:

Como estruturar mecanismos avançados de autenticação em ambientes de Computação de Alto Desempenho utilizados por instituições estatais

brasileiras, de modo a fortalecer a soberania digital e mitigar vulnerabilidades estratégicas no contexto de competição tecnológica internacional?

Objetivos

Objetivo Geral

Analisar a proteção cibernética de infraestruturas de Computação de Alto Desempenho utilizadas por instituições estatais, com ênfase na adoção de mecanismos avançados de autenticação baseados em Infraestruturas de Chaves Públicas e princípios de verificação contínua, sob a perspectiva da soberania digital e da diplomacia tecnológica.

Objetivos Específicos

a) Examinar o papel estratégico da Computação de Alto Desempenho na consolidação da soberania digital e na capacidade estatal de formulação de políticas públicas sensíveis;

b) Identificar vulnerabilidades estruturais típicas de ambientes HPC de grande escala, considerando arquitetura distribuída e compartilhamento intensivo de recursos;

c) Avaliar a aplicabilidade de mecanismos de autenticação baseados em certificados digitais e PKI em contextos de supercomputação classificados como infraestrutura crítica;

d) Analisar a compatibilidade do paradigma *Zero Trust* com arquiteturas de HPC utilizadas por instituições públicas;

e) Propor diretrizes conceituais para a estruturação de arquitetura de autenticação segura voltada a supercomputadores estratégicos no contexto brasileiro.

Fundamentação Teórica

Soberania Digital, Autonomia Tecnológica e Poder Estatal

A soberania digital pode ser compreendida como um desdobramento contemporâneo da soberania clássica no domínio tecnológico, decorrente da integração profunda de economias e sociedades ao ciberespaço e da centralidade estratégica das infraestruturas digitais para o exercício do poder estatal (Baldoni; Di Luna, 2025, p. 91-92). Nesse quadro, a autonomia política e estratégica não depende apenas de controle territorial ou capacidade coercitiva, mas também da capacidade de manter acesso contínuo a capacidades tecnológicas críticas confiáveis (critical technological capabilities – CTCs) para armazenar, transferir e processar dados produzidos domesticamente, condição que sustenta a segurança e a autonomia decisória do Estado em períodos de turbulência geopolítica e cadeias globais de suprimento complexas (Baldoni; Di Luna, 2025, p. 92-94).

Baldoni e Di Luna (2025) destacam que a dependência de um número reduzido de provedores e de cadeias produtivas transnacionais para CTCs (como semicondutores, nuvem, sistemas operacionais e serviços avançados de IA) cria assimetrias estruturais e vulnerabilidades de soberania. A confiabilidade dessas capacidades pode ser comprometida por ataques cibernéticos e adulterações na cadeia de suprimentos, enquanto o acesso contínuo pode ser restringido por decisões políticas, controles de exportação, aquisições predatórias e até por decisões corporativas de atores privados dominantes (Baldoni; Di Luna, 2025, p. 93-96). Nesse sentido, a autonomia tecnológica deixa de ser apenas uma variável econômica e passa a constituir elemento estruturante da segurança nacional, na medida em que a interrupção ou a perda de confiabilidade dessas capacidades reduz a autonomia estratégica do Estado e limita sua capacidade de proteger infraestruturas críticas e dados sensíveis (Baldoni; Di Luna, 2025, p. 92-93).

A digitalização das economias e das organizações elevou a cibersegurança – e, por consequência, a infraestrutura tecnológica que sustenta processos digitais — a um tema estratégico associado à continuidade operacional, à proteção de ativos críticos e à preservação de valor econômico e reputacional em ambientes cada vez mais hostis (Balzano; Marzi, 2025, p. 181-

182). Nesse contexto, a capacidade de coletar, processar e interpretar grandes volumes de dados passa a depender de decisões gerenciais e institucionais que integrem segurança ao planejamento, uma vez que a ampliação do uso de tecnologias digitais expande a superfície de ataque e expõe organizações (inclusive públicas) a riscos com impactos econômicos, legais e políticos (Balzano; Marzi, 2025, p. 181-183). Assim, a infraestrutura digital deixa de ser um suporte meramente técnico e se consolida como componente estruturante da estratégia e da governança no Estado contemporâneo, na medida em que a resiliência frente a ameaças digitais requer abordagem contínua, proativa e multidimensional (Balzano; Marzi, 2025, p. 182-183).

A Computação de Alto Desempenho insere-se nesse contexto como instrumento capaz de ampliar a capacidade analítica nacional. Ao viabilizar modelagens energéticas, simulações climáticas, análise de riscos sistêmicos e desenvolvimento tecnológico avançado, a HPC contribui diretamente para a consolidação da autonomia estratégica. Dessa forma, deixa de representar mero instrumento científico e passa a integrar o núcleo da soberania digital, na medida em que sustenta decisões que afetam o posicionamento internacional do Estado.

Infraestruturas Críticas Digitais e Segurança Nacional

A proteção de infraestruturas críticas digitais transcende a defesa técnica e se estende ao domínio da produção política de conhecimento sobre segurança nacional (Egloff; Smeets, 2023, p. 502-504). A atribuição de ataques cibernéticos opera como mecanismo de redução de incerteza que estabelece conexões entre incidentes técnicos e suas implicações estratégicas, mas permanece inerentemente contestável e sujeita a limitações epistêmicas (Rid; Buchanan, 2015, P. 4-6; Brandão *et al.,* 2020, p. 2–4). Conforme argumentam Egloff e Dunn Cavelty (2021), esse processo não é neutro: baseia-se em suposições analíticas que podem produzir "verdades" temporárias e influenciar a configuração da estrutura de segurança no ciberespaço, refletindo tanto capacidades técnicas quanto escolhas políticas sobre como interpretar evidências ambíguas (Egloff; Smeets, 2023, p. 520–525).

A sustentabilidade operacional dessas infraestruturas exige que sistemas de defesa e processamento de dados mantenham alta eficiência energética para

garantir continuidade em cenários de operação contínua. Em aplicações de segurança baseadas em aprendizado de máquina, o desempenho energético do hardware constitui fator crítico tanto para a escalabilidade quanto para a viabilidade econômica de sistemas de monitoramento em tempo real (Schwartz *et al.*, 2020, p. 54–56). Nesse contexto, Seok *et al.* (2021) desenvolveram o somador COREA, que utiliza técnicas de especulação de transporte (carry speculation) para reduzir o atraso do caminho crítico e o consumo energético. Esta abordagem permite que o hardware alcance eficiência energética até 3,84 vezes superior aos modelos tradicionais, mantendo precisão adequada para aplicações de monitoramento de infraestruturas críticas (Seok *et al.*, 2021, p. 1–3). Tal otimização revela-se especialmente relevante diante das crescentes demandas computacionais de algoritmos de segurança baseados em inteligência artificial, onde a eficiência energética determina a viabilidade de operação em larga escala (Patterson *et al*., 2021, p. 2–4).

No caso de ambientes HPC, Macaulay e Bhasker (2024) argumentam que a supercomputação se tornou infraestrutura essencial para aplicações estratégicas, incluindo inteligência artificial, pesquisa científica sensível e processamento de dados governamentais. A crescente designação de centros de supercomputação como ativos críticos decorre de sua centralidade na sustentação de atividades estatais estratégicas.

A classificação de supercomputadores como infraestrutura crítica implica que sua proteção deve atender a padrões elevados de resiliência, continuidade operacional e capacidade de resposta a incidentes. Nesse contexto, a segurança técnica de ambientes HPC torna-se dimensão indissociável da segurança nacional, consolidando a interdependência entre proteção cibernética e estabilidade institucional.

Arquitetura Distribuída e Vulnerabilidades Estruturais em HPC

Ambientes de Computação de Alto Desempenho distinguem-se por sua arquitetura distribuída, elevada interconectividade e processamento paralelo intensivo. Essa configuração permite desempenho superior, mas simultaneamente amplia a superfície de ataque e demonstram que clusters de supercomputação apresentam vulnerabilidades associadas à multiplicidade de

nós, à heterogeneidade de componentes e ao compartilhamento intensivo de recursos.

A movimentação lateral constitui risco significativo nesses ambientes. O comprometimento inicial de um único nó pode permitir acesso progressivo a outras camadas do sistema, especialmente quando mecanismos de segmentação interna e verificação contínua são insuficientes. A persistência de credenciais estáticas e a ausência de monitoramento granular ampliam a possibilidade de escalonamento indevido de privilégios.

Macaulay e Bhasker (2024) destacam que a necessidade de alta disponibilidade e desempenho contínuo em infraestruturas de computação de alto desempenho (HPCI) impõe restrições à aplicação de medidas de segurança intrusivas, uma vez que controles que introduzem latência ou consomem recursos podem comprometer cargas críticas de pesquisa, simulações industriais e IA (Macaulay; Bhasker, 2024, p. 2–4). Como HPCI frequentemente constitui infraestrutura crítica, indisponibilidades prolongadas geram impactos institucionais relevantes e afetam funções sensíveis (Macaulay; Bhasker, 2024, p. 1–3). Nesse contexto, os autores indicam que um nível de maturidade "Traditional" (nível 2 de 4 no ZTMM) representa o alvo mais adequado para HPCI, pois níveis superiores tornam-se problemáticos devido a custos, complexidade e impactos de performance, especialmente em dispositivos e redes de workload (Macaulay; Bhasker, 2024, p. 16–20). Assim, a proteção de ambientes HPC exige soluções que conciliem eficiência operacional, escalabilidade e robustez criptográfica sem comprometer a continuidade dos processos computacionais (Macaulay; Bhasker, 2024, p. 19).

A integração de múltiplas camadas tecnológicas e a utilização de software de código aberto também introduzem desafios relacionados à cadeia de suprimentos digital. A complexidade sistêmica desses ambientes reforça a necessidade de modelos de autenticação capazes de operar de forma distribuída e adaptativa, reduzindo riscos estruturais sem comprometer desempenho.

Infraestruturas de Chaves Públicas e Gestão Estratégica de Identidades

Infraestruturas de Chaves Públicas oferecem modelo de autenticação baseado em certificados digitais emitidos por Autoridades Certificadoras confiáveis. Em ambientes distribuídos, como os de HPC, esse mecanismo

permite validação criptográfica robusta de identidades humanas e não humanas, garantindo integridade da comunicação entre nós do sistema (Luo *et al*., 2019). A emissão de certificados de curta duração reduz a exposição associada a credenciais persistentes, limitando a janela temporal para exploração de chaves comprometidas. A possibilidade de revogação imediata fortalece a capacidade de resposta a incidentes, elemento essencial em ambientes classificados como estratégicos.

A implementação de cadeias de certificação controladas internamente reforça autonomia tecnológica e reduz dependência de provedores externos. O controle nacional da autoridade certificadora contribui para preservar a integridade da cadeia de confiança e fortalecer a capacidade estatal de governança digital. A aplicação de PKI em ambientes HPC permite autenticação descentralizada e controle granular de identidades, mitigando vulnerabilidades associadas à confiança implícita em redes internas e reduzindo risco de movimentação lateral.

Paradigma *Zero Trust* e Segurança em Infraestruturas Críticas

O modelo Zero Trust fundamenta-se na premissa de que nenhum usuário, dispositivo ou processo deve ser considerado confiável sem verificação contínua. Esse paradigma emerge como resposta à erosão do modelo tradicional baseado em perímetro de rede, cuja eficácia diminui diante da mobilidade de usuários e da complexidade de ambientes distribuídos (Balzano; Marzi, 2025).

Macaulay e Bhasker (2024) argumentam que a aplicação de princípios de Zero Trust em infraestruturas críticas fortalece a mitigação de riscos associados à movimentação lateral e ao uso indevido de credenciais válidas. A segmentação interna, a autenticação contínua e o princípio do privilégio mínimo constituem pilares desse modelo (Macaulay; Bhasker, 2024).

Em ambientes HPC, a adaptação do paradigma Zero Trust exige compatibilização entre rigor de verificação e manutenção de desempenho. A verificação frequente de identidades deve ocorrer sem comprometer a eficiência operacional do cluster. Ainda assim, a adoção de mecanismos de validação contínua reduz significativamente a probabilidade de permanência prolongada de agentes mal-intencionados (Macaulay; Bhasker, 2024).

A integração entre PKI e Zero Trust amplia o controle sobre identidades e fluxos de comunicação, estabelecendo arquitetura de proteção compatível com ambientes distribuídos de grande escala (Macaulay; Bhasker, 2024; Balzano; Marzi, 2025).

Geopolítica da Supercomputação e Diplomacia Tecnológica

A capacidade de supercomputação tornou-se variável estratégica no sistema internacional contemporâneo. Países que detêm infraestrutura avançada de HPC conseguem acelerar desenvolvimento científico, aprimorar inteligência estratégica e fortalecer cadeias produtivas de alto valor agregado.

A competição internacional por liderança tecnológica envolve políticas industriais estratégicas, restrições de exportação e disputas por domínio de semicondutores e arquiteturas computacionais avançadas. Nesse ambiente, a autonomia computacional influencia não apenas segurança interna, mas também posicionamento diplomático e capacidade de negociação internacional.

A proteção de supercomputadores utilizados por instituições públicas integra o conjunto de medidas que sustentam a diplomacia tecnológica. Demonstrar controle seguro de infraestruturas críticas reforça credibilidade internacional, amplia confiança em cooperações científicas e reduz vulnerabilidades associadas à dependência externa.

Assim, a segurança em ambientes HPC não deve ser analisada exclusivamente versando sobre a técnica. Ela integra a arquitetura de poder estatal contemporânea, articulando segurança cibernética, autonomia tecnológica e inserção geopolítica em um cenário internacional marcado por disputas tecnológicas crescentes.

Metodologia de Pesquisa e Desenho do Estudo

Tipo de Pesquisa e Delineamento Metodológico

A presente pesquisa caracteriza-se como aplicada, pois busca produzir conhecimento orientado à formulação de diretrizes conceituais destinadas ao fortalecimento da proteção de infraestruturas estratégicas de Computação de

Alto Desempenho. A natureza aplicada justifica-se pelo fato de que o estudo não se limita à descrição de fenômenos técnicos, mas procura oferecer subsídios analíticos voltados ao aprimoramento de práticas de autenticação em ambientes classificados como críticos para o Estado.

Quanto aos objetivos, a pesquisa assume caráter exploratório e descritivo. É exploratória porque investiga lacuna específica na literatura relativa à articulação entre segurança técnica em ambientes HPC, soberania digital e implicações geopolíticas. A literatura especializada frequentemente aborda esses temas de forma segmentada, sem integrá-los em um mesmo quadro analítico. É descritiva na medida em que sistematiza vulnerabilidades estruturais de clusters de grande escala e examina modelos contemporâneos de autenticação aplicáveis a esses ambientes.

Em relação à abordagem, adota-se método qualitativo, fundamentado em análise interpretativa da literatura especializada. A opção pelo enfoque qualitativo decorre da natureza complexa do objeto investigado, que envolve dimensões técnicas, institucionais, estratégicas e geopolíticas. A proteção de ambientes HPC não pode ser reduzida a métricas puramente técnicas, pois envolve também implicações para soberania digital, diplomacia tecnológica e autonomia estatal.

O delineamento metodológico baseia-se em revisão bibliográfica analítica e integrativa. A revisão é classificada como integrativa por reunir contribuições provenientes de diferentes campos do conhecimento, incluindo segurança cibernética, governança de infraestruturas críticas, soberania digital e geopolítica tecnológica. O objetivo consiste em construir arcabouço teórico capaz de sustentar proposições conceituais coerentes com as exigências de proteção de supercomputadores estratégicos.

Cenário Internacional

A pesquisa insere-se em um cenário internacional caracterizado pela intensificação da competição tecnológica e pela crescente centralidade da soberania digital nas agendas de segurança nacional. A análise considera um ambiente geopolítico no qual cadeias globais de suprimento tecnológico, semicondutores, infraestrutura de dados e capacidades de supercomputação tornaram-se variáveis estratégicas relevantes (Baldoni; Di Luna, 2025).

Adicionalmente, reconhece-se que a ampliação das ameaças cibernéticas e a evolução de técnicas de exploração impõem desafios crescentes à proteção de infraestruturas críticas digitais (Balzano; Marzi, 2025). A classificação progressiva de ambientes HPC como ativos estratégicos reforça a necessidade de modelos de segurança compatíveis com exigências de resiliência e continuidade operacional (Macaulay; Bhasker, 2024).

A consideração do cenário internacional possui caráter contextual e analítico, não se tratando de uma comparação empírica entre países. Busca-se compreender como disputas tecnológicas globais, restrições de exportação e dependências estruturais influenciam a necessidade de fortalecimento da proteção de supercomputadores utilizados por instituições estatais.

Participantes e Contexto

Por tratar-se de estudo teórico e documental, não há participação de sujeitos humanos nem aplicação de instrumentos empíricos diretos. O contexto de análise envolve infraestruturas de Computação de Alto Desempenho utilizadas por instituições públicas, centros de pesquisa e organizações estatais responsáveis por processamento de dados estratégicos.

O foco recai sobre ambientes HPC classificados como estratégicos em razão de sua utilização em setores sensíveis, tais como energia, modelagem ambiental, pesquisa científica avançada e suporte à formulação de políticas públicas. A delimitação do contexto decorre do problema de pesquisa, que busca compreender mecanismos de autenticação aplicáveis a sistemas cuja integridade influencia diretamente a soberania digital e a autonomia tecnológica do Estado.

Procedimentos e Instrumentos de Coleta

A coleta de dados realizou-se por meio de levantamento bibliográfico sistematizado das referências previamente selecionadas e disponibilizadas. Foram considerados artigos científicos, relatórios técnicos e publicações acadêmicas que abordam:

a) Segurança em ambientes HPC.

b) Classificação de infraestruturas digitais como críticas.

c) Soberania digital e autonomia tecnológica.

d) Modelos de autenticação baseados em Infraestruturas de Chaves Públicas.

e) Aplicação do paradigma *Zero Trust* em infraestruturas estratégicas.

A seleção priorizou estudos que articulam dimensões técnicas e estratégicas, permitindo integração entre vulnerabilidades operacionais e implicações geopolíticas. A análise concentrou-se nos argumentos centrais dos autores, nas soluções propostas e nos riscos identificados.

O procedimento analítico desenvolveu-se em três etapas complementares:

Na primeira etapa, realizou-se identificação e categorização temática dos conteúdos, organizando-os em eixos conceituais relacionados a soberania digital, infraestruturas críticas, vulnerabilidades estruturais em HPC e modelos de autenticação.

Na segunda etapa, procedeu-se à análise crítica das convergências e divergências entre os autores, com ênfase na identificação de lacunas referentes à integração entre segurança técnica e dimensão estratégica estatal.

Na terceira etapa, realizou-se síntese interpretativa, na qual os elementos extraídos da literatura foram articulados para fundamentar proposição conceitual de arquitetura de autenticação segura aplicável a ambientes HPC estratégicos.

Métricas e Critérios de Avaliação

Embora a pesquisa não envolva experimentação empírica ou testes operacionais, foram estabelecidos critérios analíticos para avaliar a adequação dos modelos de autenticação examinados. Tais critérios derivam das exigências impostas por ambientes HPC classificados como estratégicos e por sua relevância para a soberania digital.

Foram considerados os seguintes parâmetros:

a) Capacidade de reduzir a exposição prolongada de credenciais, avaliando se o modelo limita temporalmente a validade de chaves e certificados;

b) Compatibilidade com arquiteturas distribuídas de grande escala, considerando impacto sobre desempenho, escalabilidade e paralelismo computacional;

c) Capacidade de mitigar movimentação lateral, analisando mecanismos de segmentação interna e verificação contínua de identidade;

d) Contribuição para autonomia tecnológica estatal, avaliando o grau de dependência de provedores externos na cadeia de confiança e na governança da autenticação;

e) Adequação a contextos classificados como infraestrutura crítica, considerando requisitos de resiliência, continuidade operacional e resposta a incidentes.

Esses critérios orientaram a análise comparativa entre métodos tradicionais de autenticação e abordagens fundamentadas em Infraestruturas de Chaves Públicas e princípios de *Zero Trust*, permitindo avaliar sua pertinência não apenas sob perspectiva técnica, mas também estratégica.

Resultados e Avaliação

A análise integrativa da literatura permitiu identificar quatro eixos centrais de resultado: a presença de vulnerabilidades estruturais inerentes à arquitetura de ambientes HPC, as limitações dos modelos tradicionais de autenticação, o potencial estratégico da adoção de Infraestruturas de Chaves Públicas com certificados de curta duração e as implicações da aplicação do paradigma *Zero Trust* em infraestruturas classificadas como críticas. A interpretação desses eixos não se restringe ao plano técnico, mas incorpora dimensão estratégica vinculada à soberania digital e à autonomia tecnológica estatal.

Vulnerabilidades Estruturais e Exposição Sistêmica

Os estudos examinados convergem ao apontar que ambientes de Computação de Alto Desempenho apresentam superfície de ataque ampliada em razão de sua arquitetura distribuída, elevada interconectividade e processamento paralelo intensivo (Luo *et al*., 2019). A multiplicidade de nós computacionais,

aliada ao compartilhamento intensivo de recursos, cria um ambiente propício para exploração progressiva após um comprometimento inicial.

Luo *et al.* (2019) demonstram que falhas em mecanismos de autenticação e a persistência prolongada de credenciais constituem vetores críticos de exploração. Em clusters de grande escala, o acesso indevido a um único nó pode permitir escalonamento progressivo de privilégios e acesso transversal a diferentes camadas do sistema. Tal característica evidencia que o risco não se limita à perda de um ponto isolado, mas pode comprometer a integridade sistêmica do ambiente.

Macaulay e Bhasker (2024) acrescentam que a exigência de alta disponibilidade e desempenho contínuo restringe a aplicação de medidas corretivas invasivas, o que reforça a necessidade de mecanismos preventivos robustos. Em ambientes utilizados por instituições estatais, a interrupção de serviços pode impactar diretamente processos decisórios estratégicos, ampliando as consequências institucionais de incidentes de segurança.

Assim, os resultados indicam que as vulnerabilidades estruturais de ambientes HPC transcendem riscos corporativos convencionais, pois estão associadas à confiabilidade de análises que fundamentam decisões governamentais sensíveis.

Limitações dos Modelos Tradicionais de Autenticação

A literatura evidencia que modelos baseados em credenciais persistentes, como chaves estáticas e autenticação centralizada tradicional, mostram-se inadequados frente à complexidade de ambientes distribuídos de grande escala (Luo *et al.,* 2019). A permanência prolongada de credenciais válidas amplia a janela temporal de exploração em caso de comprometimento.

Em contextos estratégicos, essa limitação assume dimensão crítica. Sistemas que processam dados energéticos, ambientais ou científicos de interesse nacional não podem depender de mecanismos que permitam uso prolongado de credenciais potencialmente comprometidas. A ausência de controle granular e de verificação contínua fragiliza a capacidade de resposta a incidentes.

Balzano e Marzi (2025) argumentam que a erosão do modelo baseado exclusivamente em perímetro de rede exige reconfiguração das políticas de

segurança organizacional. A mobilidade de usuários, a integração de sistemas e a complexidade de ambientes digitais tornam insuficiente a distinção rígida entre ambientes internos e externos. Nesse sentido, a dependência de modelos tradicionais compromete não apenas a segurança técnica, mas também a governança estratégica da infraestrutura.

Avaliação de PKI e Certificados de Curta Duração

A adoção de Infraestruturas de Chaves Públicas revelou-se, à luz dos critérios definidos na metodologia, alternativa superior aos modelos tradicionais de autenticação. Certificados digitais de curta duração reduzem significativamente a exposição prolongada de credenciais, limitando a janela de exploração em caso de comprometimento (Luo *et al*., 2019).

Sob o critério de redução de exposição temporal, o modelo baseado em certificados temporários apresentou desempenho conceitualmente mais adequado para ambientes HPC estratégicos. A possibilidade de revogação imediata e renovação automatizada fortalece a capacidade de contenção de incidentes sem necessidade de interrupções prolongadas.

No que se refere à compatibilidade com arquiteturas distribuídas, a autenticação baseada em PKI permite validação descentralizada entre nós do cluster, preservando escalabilidade e eficiência operacional. Macaulay e Bhasker (2024) destacam que soluções alinhadas à lógica distribuída de HPC são mais compatíveis com ambientes classificados como infraestrutura crítica.

No que tange à soberania digital, a implementação de cadeia de certificação controlada internamente reduz dependência de provedores externos e fortalece autonomia estratégica (Baldoni; Di Luna, 2025). O controle nacional sobre a cadeia de confiança não apenas mitiga riscos técnicos, mas também reduz vulnerabilidades geopolíticas associadas à dependência tecnológica.

Aplicação do Paradigma *Zero Trust*

A análise indica que o paradigma Zero Trust apresenta elevada compatibilidade conceitual com ambientes HPC estratégicos. A verificação contínua de identidade, combinada com segmentação interna e aplicação do

princípio do privilégio mínimo, reduz substancialmente a probabilidade de movimentação lateral (Macaulay; Bhasker, 2024).

Sob o critério de mitigação de movimentação lateral, o modelo demonstrou superioridade teórica em relação a frameworks baseados em confiança implícita. A segmentação granular limita a propagação de acessos indevidos entre nós do cluster e restringe o alcance de credenciais comprometidas.

Balzano e Marzi (2025) ressaltam que a sofisticação crescente das ameaças digitais exige abordagem integrada e estratégica da segurança. Zero Trust alinha-se a essa necessidade ao deslocar o foco da defesa perimetral para o controle contínuo de identidade e comportamento.

Entretanto, a implementação do paradigma em ambientes HPC exige calibragem cuidadosa para preservar desempenho. A verificação contínua deve ser implementada de modo compatível com exigências de paralelismo e processamento intensivo, sob pena de comprometer a eficiência operacional.

Implicações Estratégicas para o Estado Brasileiro

A integração entre Infraestruturas de Chaves Públicas e princípios de *Zero Trust* revelou-se, à luz dos critérios estabelecidos, a alternativa mais compatível com ambientes HPC classificados como estratégicos. Essa combinação permite redução significativa da exposição prolongada de credenciais, mitigação de movimentação lateral, maior controle sobre a cadeia de confiança, compatibilidade com arquiteturas distribuídas e reforço da autonomia tecnológica.

Sob perspectiva geopolítica, a capacidade de proteger supercomputadores utilizados por instituições estatais fortalece a posição do país em negociações. A governança segura da infraestrutura computacional contribui para a credibilidade institucional e ampliação da margem de autonomia estratégica.

A análise evidencia que a segurança de ambientes HPC transcende dimensão técnica e integra o campo da política de defesa e da diplomacia tecnológica. A proteção dessas infraestruturas fortalece a resiliência institucional, preserva a soberania digital e consolida a capacidade do Estado de atuar em cenário internacional marcado por competição tecnológica crescente.

Discussões

A análise desenvolvida ao longo do capítulo permite aprofundar a compreensão da proteção de ambientes de Computação de Alto Desempenho como fenômeno situado na intersecção entre segurança cibernética, soberania digital e geopolítica tecnológica. Os resultados indicam que a segurança de supercomputadores utilizados por instituições estatais não pode ser compreendida exclusivamente sob ótica técnica, pois envolve implicações institucionais e estratégicas diretamente relacionadas à autonomia decisória do Estado.

A literatura examinada demonstra que a arquitetura distribuída de ambientes HPC amplia a superfície de ataque e favorece a movimentação lateral em caso de comprometimento inicial (Luo *et al.,* 2019). Quando tais ambientes sustentam modelagens energéticas, análises ambientais ou processamento de dados estratégicos, eventuais falhas de proteção podem comprometer a integridade de decisões governamentais. Nesse sentido, a vulnerabilidade técnica converte-se em risco institucional.

A dependência tecnológica e a concentração global de cadeias produtivas críticas introduzem vulnerabilidades estruturais que transcendem a dimensão operacional (Baldoni; Di Luna, 2025). A proteção de ambientes HPC, portanto, integra o conjunto de medidas voltadas à redução de assimetrias e ao fortalecimento da autonomia tecnológica. A governança da infraestrutura de autenticação, especialmente quando baseada em cadeias de certificação controladas internamente, assume relevância estratégica.

A integração entre Infraestruturas de Chaves Públicas e princípios do paradigma Zero Trust demonstrou compatibilidade conceitual com as exigências de ambientes HPC classificados como críticos (Macaulay; Bhasker, 2024). A redução da exposição prolongada de credenciais e a verificação contínua de identidade contribuem para mitigar a movimentação lateral e limitar a permanência de agentes mal-intencionados. Entretanto, a adoção desses modelos exige equilíbrio entre rigor de segurança e manutenção de desempenho computacional, especialmente em contextos de processamento intensivo.

A discussão evidencia ainda que a segurança de supercomputadores deve ser inserida no campo mais amplo da diplomacia tecnológica. A

capacidade de operar infraestruturas críticas de forma segura fortalece credibilidade internacional, amplia confiança em cooperações científicas e reduz vulnerabilidades associadas à dependência externa. Nesse sentido, a proteção de HPC integra a arquitetura contemporânea do poder estatal.

Limitações dos Estudos

Embora o capítulo avance na articulação entre segurança técnica, soberania digital e implicações geopolíticas, algumas limitações devem ser explicitadas.

Primeiramente, a análise baseia-se predominantemente em revisão bibliográfica qualitativa, o que restringe a possibilidade de validação empírica direta das proposições apresentadas. A ausência de estudos de caso aplicados a centros específicos de supercomputação limita a mensuração quantitativa do impacto comparativo entre modelos de autenticação.

Em segundo lugar, parte significativa da literatura sobre HPC concentra-se em aspectos técnicos operacionais, enquanto estudos sobre soberania digital privilegiam infraestrutura de dados e governança de plataformas, havendo relativa escassez de pesquisas que integrem explicitamente supercomputação estratégica à discussão geopolítica. Essa lacuna teórica impõe desafios à consolidação de modelos analíticos integrados.

Adicionalmente, o foco do estudo concentrou-se na dimensão de autenticação e gestão de identidades. Outras camadas de segurança relevantes para ambientes HPC estratégicos, como segurança física, proteção da cadeia de suprimentos de hardware, governança regulatória e controle de exportações tecnológicas, não foram exploradas em profundidade. Tais dimensões podem influenciar significativamente a resiliência sistêmica.

Por fim, a aplicação do paradigma *Zero Trust* em ambientes de alto desempenho ainda carece de maior maturidade empírica. Embora haja consenso teórico sobre sua adequação a infraestruturas críticas, estudos quantitativos que mensurem impacto em desempenho e latência em clusters de grande escala permanecem limitados.

Implicações Teóricas e Estratégicas

Apesar dessas limitações, o estudo contribui ao propor quadro analítico que integra vulnerabilidades estruturais de HPC, modelos avançados de autenticação e soberania digital. A discussão reforça a necessidade de compreender a segurança de supercomputadores como variável estratégica no contexto da competição tecnológica internacional.

Ao demonstrar que mecanismos de autenticação não são apenas instrumentos técnicos, mas componentes da governança da autonomia tecnológica, o capítulo amplia o debate sobre diplomacia digital e segurança nacional. A capacidade de controlar a própria cadeia de confiança emerge como elemento estruturante da soberania contemporânea.

A discussão aponta ainda que políticas públicas voltadas ao fortalecimento da infraestrutura nacional de certificação digital e à modernização da segurança de ambientes HPC podem contribuir para redução de vulnerabilidades geopolíticas. Assim, a proteção de supercomputadores estratégicos deve ser integrada a agendas de política industrial, defesa e cooperação internacional.

Considerações Finais

O presente estudo teve como propósito analisar a proteção cibernética de infraestruturas de Computação de Alto Desempenho utilizadas por instituições estatais, com ênfase na adoção de mecanismos avançados de autenticação fundamentados em Infraestruturas de Chaves Públicas e em princípios de verificação contínua. A investigação partiu da premissa de que a supercomputação deixou de representar mero suporte técnico à atividade científica para consolidar-se como componente estruturante da capacidade estratégica do Estado contemporâneo.

A análise desenvolvida ao longo do capítulo evidenciou que a crescente dependência de supercomputadores para modelagens energéticas, simulações ambientais, processamento de dados estratégicos e desenvolvimento tecnológico amplia a centralidade dessas infraestruturas no contexto da soberania digital. Em um cenário internacional marcado por competição tecnológica, disputas por cadeias produtivas críticas e assimetrias estruturais no domínio da infraestrutura

digital, a autonomia tecnológica tornou-se variável decisiva para a preservação da segurança nacional.

Os resultados demonstraram que ambientes HPC apresentam vulnerabilidades estruturais decorrentes de arquitetura distribuída, elevada interconectividade e multiplicidade de usuários, fatores que ampliam a superfície de ataque e favorecem a movimentação lateral após um comprometimento inicial. Quando esses ambientes sustentam atividades estratégicas do Estado, tais vulnerabilidades transcendem a dimensão técnica e assumem implicações institucionais relevantes.

Verificou-se que modelos tradicionais de autenticação, baseados em credenciais persistentes e em controle perimetral, mostram-se insuficientes diante da complexidade e da criticidade de clusters de grande escala. A permanência prolongada de chaves estáticas e a ausência de verificação contínua ampliam a janela de exposição e reduzem a capacidade de resposta rápida a incidentes em ambientes classificados como infraestrutura crítica.

A avaliação comparativa indicou que a adoção de Infraestruturas de Chaves Públicas, associadas a certificados digitais de curta duração, contribui significativamente para a redução da exposição temporal de credenciais e para o fortalecimento de mecanismos de revogação imediata. A integração com princípios do paradigma Zero Trust amplia a capacidade de mitigar a movimentação lateral, reduzir a confiança implícita em redes internas e estabelecer controle granular de identidades humanas e não humanas.

Sob a ótica estratégica, a implementação de cadeias de certificação controladas internamente reforça a autonomia tecnológica estatal e reduz dependências externas na governança da infraestrutura de confiança. Esse elemento é particularmente relevante em um contexto geopolítico no qual a infraestrutura digital constitui variável de poder e instrumento de influência internacional.

O estudo contribui para a literatura ao integrar três dimensões frequentemente tratadas de forma isolada: vulnerabilidades técnicas de ambientes HPC, soberania digital e implicações geopolíticas da autonomia tecnológica. Ao articular esses eixos, evidencia-se que a proteção de supercomputadores utilizados por instituições públicas deve ser compreendida como parte integrante

da estratégia nacional de segurança e da diplomacia tecnológica, e não apenas como uma questão operacional de tecnologia da informação.

Entre as contribuições teóricas, destaca-se a proposição de critérios analíticos que permitem avaliar modelos de autenticação em ambientes HPC, considerando a redução da exposição de credenciais, a compatibilidade com arquiteturas distribuídas, a mitigação de movimentação lateral, a resiliência operacional e a contribuição para a autonomia tecnológica. Esses critérios permitem transcender análises puramente técnicas e incorporar a dimensão institucional e geopolítica à avaliação de mecanismos de segurança.

No que se refere às limitações, reconhece-se que a pesquisa adotou uma abordagem qualitativa fundamentada em revisão bibliográfica integrativa, não envolvendo análise empírica direta de centros específicos de supercomputação. A ausência de um estudo de caso aplicado restringe a mensuração quantitativa do impacto operacional comparativo entre diferentes modelos de autenticação. Ademais, o foco concentrou-se na dimensão de autenticação e gestão de identidades, não abrangendo de forma aprofundada outras camadas de proteção, como segurança física, cadeia de suprimentos ou governança regulatória.

Para pesquisas futuras, recomenda-se a realização de estudos empíricos aplicados a centros nacionais de supercomputação, com avaliação quantitativa do impacto de certificados de curta duração e de arquiteturas baseadas em Zero Trust sobre desempenho e resiliência. Sugere-se também o aprofundamento da análise sobre a governança nacional de cadeias de certificação, a dependência de componentes críticos e as implicações diplomáticas da cooperação internacional em infraestrutura de supercomputação. A ampliação da investigação para políticas industriais voltadas ao fortalecimento da autonomia computacional e à redução de vulnerabilidades na cadeia de suprimentos digital mostra-se igualmente relevante.

Conclui-se que a proteção de ambientes HPC estratégicos deve ser tratada como componente estruturante da soberania digital, da resiliência institucional e da política de defesa. Em um sistema internacional marcado por crescente disputa tecnológica, a capacidade de operar supercomputadores de forma segura, autônoma e resiliente constitui não apenas um requisito técnico, mas um elemento central da diplomacia tecnológica e da autonomia estratégica brasileira.

Referências

BRASIL. Ministério da Ciência, Tecnologia e Inovação. *Plano Brasileiro de Inteligência Artificial (PBIA) 2024-2028*. Brasília, DF: MCTI, 2024. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial

BRASIL. *Decreto nº 12.573,* de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança. *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 5 ago. 2025a. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Decreto/D12573.htm

BALDONI, Roberto; DI LUNA, Giuseppe. *Sovereignty in the digital era: the quest for continuous access to dependable technological capabilities*. IEEE Security & Privacy, [S. l.], v. 23, n. 1, p. 91–96, 2025. DOI: 10.1109/MSEC.2024.3500192

BALZANO, Marco; MARZI, Giacomo. At the cybersecurity frontier: key strategies and persistent challenges for business leaders. *Strategic Change*, [S. l.], v. 34, p. 181–192, 2025. DOI: 10.1002/jsc.2622.

BRANDÃO, Ana; MÜHLENHAUS, Katharina; PAWLAK, Patryk. Cyber attribution: a systematic literature review. Journal of Cybersecurity, Oxford, v. 6, n. 1, p. 1–18, 2020. DOI: 10.1093/cybsec/tyaa013.

DEELMAN, Ewa; DONGARRA, Jack; HENDRICKSON, Bruce; RANDLES, Amanda; REED, Daniel; SEIDEL, Edward; YELICK, Katherine. High-performance computing at a crossroads. *Science*, Washington, D.C., v. 387, n. 6736, p. 829–831, 21 fev. 2025. DOI: 10.1126/science.adu0801. Disponível em: https://www.science.org/doi/10.1126/science.adu0801. Acesso em 25 fev. 2026.

EGLOFF, Florian J.; DUNN CAVELTY, Myriam. Attribution and knowledge creation assemblages in cybersecurity politics. Journal of Cybersecurity, Oxford, v. 7, n. 1, p. 1–16, 2021. DOI: 10.1093/cybsec/tyab002.

EGLOFF, Florian J.; SMEETS, Max. Publicly attributing cyber attacks: a framework. Journal of Strategic Studies, [S. l.], v. 46, n. 3, p. 502–533, 2023. Disponível em: https://www.ingentaconnect.com/content/routledg/jss/2023/00000046/00000003/art00002

FANG, Xuexian; YU, Yuanyuan; CAI, Jingwen; YIN, Yifen; WANG, Chunning; HO, Wai In: HU, Haoqian. Managing technological sovereignty: a systematic review of semiconductor industry policy and regional ecosystem governance. *Frontiers in Research Metrics and Analytics*, Lausanne, v. 11, n. 1762083, p. 1–18, 6 mar. 2026. DOI: 10.3389/frma.2026.1762083. Disponível em: https://www.frontiersin.org/journals/research-metrics-and-analytics/articles/10.3389/frma.2026.1762083/full. Acesso em 6 abr. 2026.

GUO, Yang; CHANDRAMOULI, Ramaswamy; WOFFORD, Lowell; GREGG, Rickey; KEY, Gary; CLARK, Antwan; HINTON, Catherine; PROUT, Andrew; REUTHER, Albert; ADAMSON, Ryan; WARREN, Aron; BANGALORE, Purushotham; DEUMENS, Erik; FARKAS, Csilla. *High-Performance Computing Security*: architecture, threat analysis, and security posture. Gaithersburg, MD: National Institute of Standards and Technology, 2024. (NIST Special Publication, 800-223). DOI: 10.6028/NIST.SP.800-223. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-223.pdf. Acesso em 6 abr. 2026.

KOLEINI, Sara; PAHLEVANZADEH, Bahareh. Enhancing High-Performance Computing (HPC) Security: a comprehensive review of detection and protection strategies. *Journal of Distributed Computing and Systems*, v. 6, n. 12, p. 12–24, 20 mar. 2024. Disponível em: https://www.jdcs.ir/article_201350_20c38df200b8831e375afa1bc41f2674.pdf. Acesso em: 6 abr. 2026.

LUO, Zhengping; QU, Zhe; NGUYEN, Tung Thanh; ZENG, Hui; LU, Zhuo. Security of HPC systems: from a log-analyzing perspective. *EAI Endorsed Transactions on Security and Safety*, v. 6, n. 21, e5, 2019. DOI: https://doi.org/10.4108/eai.19-8-2019.163134

MACAULAY, Tyson; BHASKER, Daksha. *High Performance Computing Infrastructure and Zero Trust Architecture.* Ottawa: National Centre for Critical Infrastructure Protection, Security and Resilience, Carleton University, 2024. Disponível em: https://ojs.library.carleton.ca/index.php/PPJ-CIPSER/article/download/4990/3642/15736. Acesso em 7 abr. 2026.

PATTERSON, David; GONZALEZ, Joseph; LE, Quoc; LIANG, Chen; LAI, Lluis-Miquel; MOORE, Travis; PESTER, David; RUDD, Eric; SCHALAMON, Mark; SINGER, Jeff. *Carbon emissions and large neural network training.* arXiv, Ithaca, 2021. Disponível em: https://arxiv.org/abs/2104.10350

RID, Thomas; BUCHANAN, Ben. Attributing cyber attacks. *Journal of Strategic Studies*, [S. l.], v. 38, n. 1-2, p. 4–37, 2015. DOI: 10.1080/01402390.2014.977382

ROSE, Scott; BORCHERT, Oliver; MITCHELL, Stu; CONNELLY, Sean. *Zero Trust Architecture*. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2020. (NIST Special Publication, 800-207). DOI: 10.6028/NIST.SP.800-207. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

SCHWARTZ, Roy; DODGE, Jesse; SMITH, Noah A.; ETZIONI, Oren. Green AI. *Communications of the ACM*, New York, v. 63, n. 12, p. 54–63, 2020. DOI: 10.1145/3381831. Disponível em: https://doi.org/10.1145/3381831.

SEOK, Hyelin; SEO, Hyoju; LEE, Jungwon; KIM, Yongtae. COREA: delay- and energy-efficient approximate adder using effective carry speculation. *Electronics, Basel,* v. 10, n. 18, art. 2234, 2021. DOI: 10.3390/electronics10182234

SILVA, Edvan Gomes da; GEORG, Marcus Aurélio Carvalho; RIBEIRO JÚNIOR, Luiz Antonio; FERREIRA, Leonardo Rodrigo; MELO, Laerte Peotta de; NUNES, Rafael Rabelo. International perspectives on critical infrastructure: evaluation criteria and definitions. *Revista PPEE*, Brasília, DF, v. 13, n. 2, p. 1–25, jul. 2025. Disponível em: https://ppee.unb.br/wp-content/uploads/2025/09/International-perspectives-on-critical-infrastructure-Evaluation-criteria.pdf. Acesso em: 25 fev. 2026.

O problema da Ética na Guerra Cognitiva

Érika Rigotti Furtado
Ivan Fernandes Faria

Introdução

Partindo da reflexão sobre a maneira como a ética imiscui-se no ambiente da guerra cognitiva e transitando entre referenciais que abordam a Política e a Guerra, emerge a constatação de que o fenômeno apresenta características que destoam da concepção clássica de Guerra, consolidada por Clausewitz e internalizada nas doutrinas, conceitos teóricos e legislação contemporâneos. Neste cenário, objetiva-se investigar como, e em que medida, os fundamentos da ética atuam na esfera da guerra cognitiva. Tal incerteza decorre de que essa tipologia de conflito não depende, necessariamente, de meios bélicos, tampouco produz efeitos cinéticos invariáveis, o que desafia os referenciais normativos aplicados às Guerras em sentido estrito.

A problemática exige uma reavaliação conceitual, visto que a expressão "guerra" foi progressivamente expandida para abarcar disputas jurídicas, informacionais, econômicas e políticas, afastando-se do conceito clássico. Essa inflação semântica, embora funcional, compromete a precisão analítica, sobretudo no momento de identificar qual ética é mobilizada, em que condições ela se aplica e com quais limites. Se tudo se converte em "guerra", os critérios que diferenciam violência, coerção, manipulação, persuasão ou influência tornar-se-ão indistintos. Portanto, compreender sua natureza implica necessariamente reafirmar o conceito de Guerra, sob pena de dissolver as categorias que sustentam qualquer juízo consistente.

A análise ética exige, portanto, o exame estrutural do ato avaliado: o que se faz, como se faz, por que se faz e quando se faz. No caso da guerra cognitiva, esses elementos se complexificam porque o objeto do ato é a manipulação da cognição humana, seja de líderes ou de populações inteiras; os meios empregados são informacionais, psicológicos e tecnológicos; as motivações oscilam entre objetivos táticos e disputas políticas; e o contexto pode situar-se abaixo do limiar do conflito armado até a integração de um esforço de Guerra.

Dessa elasticidade decorrem os seguintes objetivos específicos: verificar se, e em que medida, a guerra cognitiva se vincula à estrutura da guerra convencional, ou fora dela; e analisar os fundamentos da ética diante das práticas cognitivas em ambientes de competição estratégica e de conflito armado. Neste contexto, o presente estudo adota uma abordagem teórico-analítica de natureza interdisciplinar, articulando contribuições da filosofia, da teoria da guerra e do Direito Internacional Humanitário. O objetivo consiste em examinar de que maneira os pressupostos epistemológicos e éticos influenciam a compreensão e a utilização da guerra cognitiva, distinguindo-se, para fins analíticos, entre o nível estratégico das campanhas cognitivas e o nível operacional das ações cognitivas.

A Ética, a Política, a Guerra e a Guerra Cognitiva

O conceito clássico de guerra

A teoria clausewitziana constitui o principal referencial para a definição da Guerra,[1] ao caracterizá-la como instrumento da política e como ato de força destinado a compelir o inimigo a cumprir a vontade do oponente, configurando sua continuação por meios inexoravelmente violentos (Clausewitz, 2010). Sua definição articula três elementos indissociáveis: a política como finalidade orientadora, a violência organizada como meio distintivo das demais práticas e a célebre trindade composta pelo povo, pelas forças armadas e pelo governo. Ademais, em sentido estrito, a Guerra envolve o emprego da violência extrema e o derramamento de sangue, expresso no termo original alemão "*Blutvergießen"* (Clausewitz, 2010), ainda que sua intensidade, duração, forma e recursos variem conforme o contexto histórico e estratégico.

A Doutrina Militar de Defesa brasileira acolhe esse entendimento ao enquadrar a Guerra e o "conflito armado" como sinônimos e ao reafirmar o choque violento, armado e organizado como instrumento da política, destinado a sujeitar o oponente à vontade do vencedor. Nesse sentido, caracteriza o

[1]Neste texto, utilizaremos o termo Guerra com letra maiúscula para referir-nos à guerra que adira ao conceito clausewitziano, obrigatoriamente envolvendo a tríade de Clausewitz, as ações cinéticas e a violência extrema.

emprego da Expressão Militar do Poder Nacional como a manifestação violenta da política (Brasil, 2025).

Sob a perspectiva jurídica, o Direito Internacional Humanitário (DIH), conforme interpretado pelo Comitê Internacional da Cruz Vermelha (CICV), aplica-se a situações de conflito armado com base em sua realidade fática, independentemente de declaração formal de guerra ou de seu reconhecimento (CICV, 2024). Esse entendimento reforça que a caracterização da Guerra não depende da terminologia empregada, mas da presença concreta de seus elementos constitutivos observáveis, em consonância com os critérios clausewitzianos.

A inflação semântica da guerra e seus efeitos analíticos

Embora a definição clássica estabeleça parâmetros relativamente claros, o emprego contemporâneo do termo "guerra" é marcado por uma notável ampliação semântica, frequentemente dissociada dos pressupostos teóricos e normativos que a estruturam. Nos campos acadêmico e estratégico, observa-se a proliferação de expressões que empregam o termo para descrever fenômenos heterogêneos, desde conflitos armados até disputas informacionais, econômicas e políticas conduzidas sem o emprego organizado da violência.

O Glossário das Forças Armadas brasileiras, por exemplo, apresenta quarenta e oito expressões que incorporam o termo "guerra", abrangendo táticas, sistemas bélicos, motivações, formas de condução e níveis de comprometimento nacional ou internacional (Brasil, 2015). Embora tal diversidade possua valor heurístico, essa flexibilização semântica introduz relevantes dificuldades analíticas, especialmente quando se busca delimitar os marcos éticos e jurídicos aplicáveis a fenômenos que não envolvem o uso organizado da violência e, portanto, nem sempre classificáveis como guerra, como é o caso da guerra cognitiva.

Tal indistinção torna-se particularmente deletéria quando equipara a competição política e suas ramificações ao conflito armado, fenômenos distintos quanto aos meios empregados, aos efeitos produzidos e aos regimes normativos aplicáveis. A banalização da expressão "guerra" para descrever ações de influência, desinformação ou manipulação cognitiva em contextos abaixo do limiar do conflito armado contribui para a diluição dos limiares normativos que estruturam as relações interestatais, o DIH e a ética da Guerra.

A Doutrina Militar de Defesa reconhece essa complexidade e introduz os conceitos de "Zona Cinza", "Contínuo de Competição" e "Ações Híbridas", que descrevem embates estratégicos frequentemente conduzidos abaixo do limiar do conflito armado e caracterizados por ambiguidades nas intenções e nos recursos empregados. Ademais, reafirma que a Guerra, em sentido estrito, permanece associada ao emprego organizado da violência como instrumento político (Brasil, 2025).

Portanto, essa expansão semântica amplia o conjunto de objetos de análise, contribuindo para a caracterização e o diagnóstico das disputas contemporâneas. Contudo, o uso impreciso do vocábulo "guerra" tende a obscurecer a distinção entre fenômenos qualitativamente distintos, dificultando a análise ética e a adequada atribuição de responsabilidades.

A dimensão cognitiva como instrumento histórico da política e da guerra

A dimensão cognitiva, entendida como o espaço no qual se desenvolvem os processos de percepção, interpretação e tomada de decisão, sempre ocupou um papel relevante na Política, assim como na Guerra. A persuasão, o engano, a propaganda e a manipulação da percepção acompanham os conflitos humanos, sendo reconhecidos por autores clássicos como instrumentos legítimos da ação política e militar.

Sun Tzu enfatizou a superioridade estratégica da vitória obtida pela submissão do inimigo sem o emprego direto da força, afirmando que "a melhor estratégia é promover a rendição inimiga sem nem mesmo ter lutado" (Sun Tzu, 2018, p. 37). De modo semelhante, Maquiavel reconhecia a importância da gestão da percepção pública, do manejo do temor e da construção da legitimidade como elementos fundamentais para a manutenção do poder político (Maquiavel, 1999).

O desenvolvimento tecnológico contemporâneo não altera essa natureza fundamental, mas, como observam Deppe e Schaal (2024), amplia significativamente o alcance, a velocidade e os efeitos dessas práticas. De fato, a inovação associada à guerra cognitiva reside na capacidade de "realizar ataques cognitivos de forma rápida e anônima dentro do ambiente informacional, utilizando plataformas digitais e tecnologias disruptivas emergentes" (NATO *Allied Command Transformation* – NATO, 2024, tradução nossa).

Assim, ações destinadas a influenciar a cognição humana podem ser compreendidas como instrumentos úteis em contextos de competição política ou como parte integrante do esforço de guerra, visando "minar a integridade dos processos políticos em sociedades democráticas (...) por meio de esforços coordenados nas esferas política, militar, econômica e de informação" (Deppe; Schaal, 2024, p. 1).

A distinção analítica fundamental reside no contexto em que essas práticas se desenvolvem, e não nos meios utilizados ou nos alvos visados. Quando integradas ao emprego organizado da violência, tais ações constituem recursos integrados ao esforço de Guerra; enquanto, quando conduzidas abaixo desse limiar, permanecem no domínio da competição política, ainda que possam produzir efeitos profundamente danosos.

A Guerra Cognitiva como problema conceitual contemporâneo

A crescente atenção dedicada à chamada guerra cognitiva reflete o reconhecimento da centralidade da dimensão cognitiva nas disputas contemporâneas. Conforme observam Claverie e du Cluzel (2020), o conceito emerge da integração de capacidades informacionais, psicológicas e tecnológicas destinadas a influenciar percepções e processos decisórios em contextos de competição estratégica e guerra.

O *Allied Command Transformation* da Organização do Tratado do Atlântico Norte reconhece o caráter exploratório do conceito de guerra cognitiva e a ausência de consenso quanto aos seus limites e natureza, embora ressalte sua importância estratégica (NATO, 2024). De modo semelhante, Deppe e Schaal (2024) identificam a guerra cognitiva como o emprego de recursos destinados a produzir efeitos cognitivos em indivíduos e populações, tanto em contextos bélicos quanto fora deles.

Walker (2024), por seu turno, ao tratar de conceitos afetos às Operações de Informação, observa a carência de padronização teórica que suscita uma névoa decorrente da "generalização e banalização de conceitos, desafiando o estabelecimento de percepções entre civis e militares, mesmo nos níveis mais altos do pensamento estratégico" (Walker, 2024, p. 11).

Essa indeterminação conceitual é agravada pela tendência de elevar métodos e meios à condição de fenômenos autônomos de conflito, obscurecendo sua natureza instrumental ao examinar a guerra cognitiva como um ato singular. Essa ambiguidade compromete a capacidade analítica e decisória das lideranças políticas e militares, além de dificultar a adequada aplicação dos regimes jurídicos e éticos pertinentes.

A interferência russa em processos eleitorais nos Estados Unidos e em países europeus, amplamente documentada (Rid, 2020; Paul; Matthews, 2016), evidencia a existência de campanhas cognitivas destinadas a influenciar populações sem o emprego articulado da força militar. Por seu turno, o conflito na Ucrânia demonstra a integração dessas práticas ao esforço de guerra, com operações coordenadas de desinformação, manipulação narrativa e controle e exploração do ambiente informacional acompanhando as operações militares (Kofman; Starke, 2023). Esses eventos ilustram empiricamente a distinção entre o emprego de recursos cognitivos em contextos de competição política e sua integração ao esforço de guerra, corroborando a necessidade de diferenciá-los analiticamente.

Campanhas cognitivas e ações cognitivas: uma proposta analítica

Diante desses óbices conceituais, propõe-se compreender a guerra cognitiva não como uma tipologia autônoma de conflito, mas como um conjunto de recursos que podem ser empregados em dois contextos distintos e inter-relacionados: a política e a guerra. Tais práticas podem ocorrer abaixo do limiar do conflito armado ou integradas diretamente ao emprego organizado da força militar.

De um lado, essas práticas podem ocorrer em embates conduzidos abaixo do limiar do conflito armado, envolvendo operações de influência, coerção diplomática e manipulação informacional. Essas atividades, doravante denominadas campanhas cognitivas, inserem-se no domínio da política, da diplomacia e das relações internacionais e não configuram, por si só, atos de guerra. De outro lado, os mesmos meios podem ser empregados como instrumento preparatório, ou parte do esforço coordenado de guerra, prejudicando a capacidade decisória do adversário e com vistas à sua derrota.

Nessa condição, passam a constituir ações cognitivas, integradas ao emprego organizado da violência e subordinadas aos objetivos políticos da guerra.

Em ambos os casos, os objetivos estão relacionados à "exploração da cognição humana e da tecnologia para interromper, minar, influenciar ou modificar a tomada de decisões humanas" (Deppe; Schaal, 2024, tradução nossa), diferenciando-se apenas quanto ao contexto em que são conduzidos e, por isso, atraindo regimes jurídicos e éticos distintos.

Essa abordagem preserva o cerne ontológico da teoria clausewitziana ao mesmo tempo que reconhece a crescente centralidade da dimensão cognitiva nas disputas contemporâneas, sem incorrer na imprecisão decorrente da expansão indiscriminada do termo "guerra". Dessa forma, fornece base analítica mais precisa para a compreensão e avaliação ética do emprego contemporâneo dos recursos cognitivos.

A Ética na Política e na Guerra Cognitiva

A distinção entre campanhas cognitivas e ações cognitivas implica diretamente a análise ética. Max Weber observa que a ação política é orientada por indagações a respeito da retidão dos atos, considerando a intenção, o contexto político, as consequências e a possível responsabilização, reconhecendo que a consecução de objetivos tidos como legítimos pode envolver o emprego de meios moralmente ambíguos e potencialmente danosos, como a própria Guerra (Weber, 1967).

Quando conduzidas no contexto da Guerra, as ações cognitivas submetem-se aos regimes éticos e jurídicos aplicáveis a esta, incluindo as normas do DIH. Por outro lado, quando conduzidas fora desse contexto, como campanhas cognitivas, permanecem no domínio da ética política, da diplomacia e das relações internacionais, sem se submeterem aos constrangimentos normativos específicos.

O principal desafio analítico e normativo reside na zona de transição, na qual práticas cognitivas podem contribuir para a escalada em direção ao conflito armado sem configurar, isoladamente, atos de Guerra. A expansão semântica do termo "guerra" e a indistinção conceitual associada a esses fenômenos

obscurecem a aplicação adequada dos preceitos éticos e jurídicos, reforçando a necessidade de distinções analíticas claras para sua correta avaliação.

Conforme orienta o CICV, o DIH é aplicável "a situações de conflito armado, um estado de hostilidades de fato que não depende nem de uma declaração, nem do reconhecimento da existência de uma 'guerra'" (CICV, 2024, p. 5). Assim, fundamenta-se na análise fática da existência de conflito armado, independentemente de sua formalização, vinculando sua identificação à presença concreta dos elementos constitutivos da guerra. Esse entendimento fornece base conceitual sólida para a análise ética da guerra cognitiva, ao permitir distinguir entre o emprego de recursos cognitivos em contextos de guerra ou competição política, estabelecendo o arcabouço analítico necessário para a avaliação de suas implicações éticas, conforme será desenvolvido nas seções seguintes. Dessa forma, cumpre-se o primeiro objetivo específico, ao enquadrar comparativamente as ações cognitivas em contextos de guerra e as campanhas cognitivas em contextos de competição política, estabelecendo a base conceitual necessária para a análise dos fundamentos éticos, como será desenvolvido a seguir.

O problema da Ética no contexto da "guerra cognitiva": campanhas cognitivas e ações cognitivas

Conforme observado na primeira seção deste trabalho, o enfoque atribuído à guerra cognitiva refere-se à sua aplicação no ambiente da estratégia e, portanto, relacionada com a obtenção de superioridade militar. De todo modo, a resposta à questão sobre como a ética imiscui-se na guerra cognitiva reclama a conjugação de outros fatores, que extrapolam o ambiente dos estudos de segurança e defesa, no qual, segundo Pinto e Laterza (2025), a guerra cognitiva é analisada como parte da guerra híbrida e da doutrina militar.

Assim, as questões de ordem filosófica, entre as quais se encontram os problemas éticos, ingressam no contexto de estudo da guerra cognitiva, mesmo porque os aspectos essenciais da sociedade e da cultura são os meios sobre os quais as "armas" cognitivas operam, e não o fazem desprovidas dos pressupostos filosóficos em voga. Ademais, a presença dos instrumentos da guerra cognitiva nos conflitos armados implica na ampliação dos estudos ético-filosóficos da

guerra, por consistir em uma fronteira que ultrapassa os instrumentos geradores de efeitos cinéticos.

Disso resulta a possibilidade de divisão da análise dos desafios éticos relativos à guerra cognitiva sob duas abordagens, sendo a primeira voltada aos problemas diretamente relacionados à ordem política, de natureza filosófica, localizados no âmbito das "campanhas cognitivas", e a segunda, situada no momento da guerra propriamente, considerada como "ação cognitiva". Sob o segundo aspecto, a guerra cognitiva esbarra no Direito Internacional Humanitário, cujos princípios podem vir a ser violados em decorrência do uso indiscriminado dessa ferramenta agregada aos combates armados.

A guerra cognitiva vem sendo frequentemente descrita como o sexto domínio nos conflitos da atualidade, ao lado dos domínios terrestre, marítimo, aéreo, espacial e cibernético. No âmbito dos estudos desenvolvidos pela OTAN, Claverie (2022) enfatiza a função estratégica da guerra cognitiva, classificando-a como uma das maneiras utilizadas por especialistas no intuito de orientar ou alterar o raciocínio humano com o objetivo de conquistar superioridade militar. Entretanto, o conceito de guerra cognitiva é também acadêmico, máxime considerando que a temática abarca não somente o ambiente militar, propriamente ligado aos conflitos armados, mas a seara política, na qual o intento do emprego das distorções ocasionadas pela guerra cognitiva é gerar impacto nas sociedades democráticas (Deppe; Schaal, 2024).

Os ataques cognitivos, não sendo algo necessariamente novo, operam por meio de manobras ofensivas deliberadas, focadas na percepção, nas crenças, nos interesses, nas decisões e nos comportamentos dos seres humanos (Claverie, 2022). Sendo o "campo de batalha" a mente humana, podem ser identificadas como fragilidades a inflexibilidade cognitiva, a necessidade de pertencimento social e a excitação emocional, como comportamentos que suscetibilizam a influência e a manipulação, (Deppe; Schaal, 2024).

O estudo da ética no ambiente da guerra cognitiva, sob o viés acadêmico, refere-se à filosofia da mente e da epistemologia que, conforme Pinto e Laterza (2025), possui como questão central o questionamento de como a verdade é construída e manipulada cognitivamente. Como ponto de convergência nesta abordagem, os autores apontam o reconhecimento quanto à moldagem da realidade a partir dos elementos históricos e culturais. A divergência, por seu turno, é estabelecida entre o posicionamento relativista, de um lado, amparado

pelo pensamento pós-moderno, conforme o qual a verdade é uma construção, e o realismo epistemológico, de outro, para o qual a verdade não é um dado relativo, ou moldável conforme ideologias ou preferências individuais.[2]

De todo modo, é importante considerar que a realidade, vinculada à verdade, não pode ser compreendida exclusivamente como construção histórica ou cultural. Para estudar a ética na guerra cognitiva, deve-se considerar a unidade da realidade e do conhecimento. Como afirma Lavelle (2023), o mundo material é um dado objetivo, definido pelo espaço e pelo tempo e que permanece constantea pesar das influências culturais.

A compreensão dessa divergência entre o realismo epistemológico e as correntes relativistas contemporâneas exige um breve recuo histórico. Parte significativa das bases do pensamento moderno pode ser associada ao desenvolvimento do nominalismo no século XIV, especialmente a partir da obra de Guilherme de Ockham (1295–1349). A crítica nominalista aos universais e ao realismo aristotélico-tomista produziu consequências profundas para a filosofia, para a teoria do conhecimento e, posteriormente, para a própria compreensão da moralidade e do direito.[3]

---

[2]Para fins de auxiliar na compreensão dessa dicotomia e de seu impacto no estudo da guerra cognitiva, é relevante destacar que, em termos filosóficos, as ciências teóricas se dividem entre as ciências naturais, as ciências matemáticas e a metafísica. As ciências naturais relacionam-se com os sentidos, concentrando-se nas qualidades comuns dos fenômenos observados. As ciências matemáticas são lógicas e formais, focadas na quantidade e abstraindo as qualidades do sensível. Finalmente, a metafísica possui como objeto de estudo o ser enquanto ser. Não se interessa pelas qualidades gerais ou individuais do ser, ou pela quantidade, mas pela estrutura do ser, ou aquilo de que tudo o que é participa. A metafísica refere-se à ontologia do ser e a negação dessa ontologia resulta no niilismo. De outro lado, a possibilidade de conhecer é o objeto da epistemologia, cuja negação leva ao ceticismo. A filosofia contemporânea, essencialmente vinculada à linguagem, é herdeira da dialética transcendental kantiana, tendo se dividido nas vertentes continental, ou hermenêutica, e peninsular, ou analítica. Dessa mesma cisão pós-kantiana surgem o positivismo e o romantismo. Todas essas correntes contemporâneas possuem em comum a crítica da metafísica clássica e a unidade do todo da realidade. Por isso, compreender essa postura é essencial para o estudo das distorções cognitivas verificadas nos dias em curso.

[3]A referência ao nominalismo é fundamental para a compreensão da guerra cognitiva na atualidade. O nominalismo difundiu a ideia de que os universais não possuem existência real, sendo apenas nomes dados às coisas. Desse modo, sendo o traço central da guerra cognitiva contemporânea a disputa pelo significado das palavras, torna-se límpida a relação ora estabelecida. Se conceitos como "verdade", "democracia", "liberdade" ou até "fato" são reduzidos a rótulos moldáveis conforme interesses estratégicos, o campo de batalha deixa de ser apenas territorial ou econômico

No âmbito do debate sobre os universais, Ockham rejeita a existência de essências universais objetivas, sustentando que os universais consistem apenas em termos da linguagem utilizados para designar múltiplos indivíduos (Culleton, 2011). Assim, os conceitos gerais não corresponderiam a realidades objetivas, mas a signos empregados para ordenar a experiência. Como observa Villey (2019), os termos universais funcionam como instrumentos lógicos para conotar fenômenos singulares, e não como expressões de naturezas comuns efetivamente existentes. Essa mudança conceitual contribuiu para deslocar o foco do conhecimento das essências para os indivíduos, influenciando profundamente o desenvolvimento posterior da filosofia moderna.

O nominalismo transformou o Direito e a Moral ao substituir a natureza das coisas pela vontade individual e pelo positivismo. Enquanto o pensamento clássico (aristotélico-tomista) via o bem como algo cognoscível pela razão na própria realidade, o nominalismo de Ockham define a lei moral como um imperativo de obediência. A ética, portanto, deixa de ser o desenvolvimento da natureza humana (teleologia) para se tornar um sistema de regras e deveres.

Essa transformação epistemológica possui implicações diretas para o ambiente informacional contemporâneo. Em um contexto caracterizado pela multiplicação de narrativas concorrentes e pela fragmentação da autoridade epistêmica, torna-se mais difícil distinguir entre verdade, interpretação e manipulação, sendo essa a condição explorada pelas campanhas cognitivas.

Conforme observa Pinheiro (2021, p.122), a decomposição da metafísica funda uma outra forma de valoração "que não é simplesmente a substituição de velhos valores por novos [...], mas se trata da atividade subjetiva de *criar valores*." A utilização dessa fragilidade, observada em especial no cerne da sociedade ocidental contemporânea, apresenta-se como uma via fácil de entrada para as distorções cognitivas. A fragilidade apontada pode ser explorada de forma sistemática por algoritmos, influenciadores ou grupos ideológicos, que reforçam vieses e alimentam deformidades cognitivas, como a

e passa a ser semântico. Na prática, isso significa que vencer uma guerra hoje pode depender menos de destruir o inimigo e mais de redefinir os termos do debate público, fragmentando consensos e explorando a plasticidade dos significados. O nominalismo, levado ao extremo cultural, favorece um ambiente em que narrativas competem sem referência estável, tornando a manipulação informacional uma arma tão poderosa quanto qualquer tecnologia militar.

relativização indevida da autoridade epistêmica e a equivalência entre opinião e conhecimento.

No ambiente das "campanhas cognitivas", por conseguinte, a desconstrução da verdade figura como um meio voltado ao enfraquecimento da vontade individual, de grupos específicos ou dos decisores políticos. Considerando que, consoante Claverie (2022), a cognição corresponde à atuação cerebral diante das informações extraídas do mundo, em um ambiente de distorções constantes, a própria ética tende a se apresentar de forma igualmente distorcida. Conforme observa Ortega y Gasset (2002, p. 48) "a característica do momento é que a alma vulgar, sabendo que é vulgar, tem a coragem de afirmar o direito da vulgaridade e o impõe em toda parte." Isto porque, continua o autor, "a massa faz sucumbir tudo o que é diferente, egrégio, individual, qualificado, especial. Quem não for como todo mundo, quem não pensar como todo mundo, correrá o risco de ser eliminado".

À pergunta norteadora – como a ética se imiscui na guerra cognitiva – pode-se responder, em um primeiro momento, que no tocante às campanhas cognitivas, relacionadas às práticas políticas, a atribuição de valor ético às ações deflagradas nesse contexto mostra-se duvidosa, seja diante da dificuldade de justificar a reta intenção no ato de manipular a mente dos indivíduos, seja em função da vulgaridade das massas, capaz de corromper a realidade, de maneira a facilitar a moldagem das opiniões de acordo com os mais diversos interesses presentes na convivência humana.

Mesmo em meio a um conflito armado, as campanhas cognitivas podem gerar efeitos deletérios, em relação aos quais dificilmente podem ser alegadas razões éticas. Em 2025, por exemplo, a Rússia empreendeu mais uma campanha conhecida como *Doppelgänger*[4], com a finalidade de difundir conteúdos destinados a influenciar eleitores alemães (Jones, 2025). Esta prática consiste em uma tática de desinformação, que opera a partir da clonagem de sites de meios de comunicação social, comprando domínios semelhantes e imitando o estilo de apresentação, a fim de promover a divulgação de artigos falsificados, posteriormente espalhados pelas demais redes sociais. Nesse caso

[4] *Doppelgänger:* é uma palavra de origem alemã que significa "duplo ambulante". Em histórias e filmes pode indicar um duplo idêntico, enquanto na psicologia se relaciona com a ideia de alter ego, ou uma versão alternativa de si mesmo.

específico, o intento russo era influenciar as eleições alemãs, de maneira a buscar enfraquecer o apoio do Ocidente à campanha ucraniana.

Por outro lado, as ações cognitivas integradas ao combate podem resultar na violação de princípios fundamentais, como a proporcionalidade e a distinção entre combatentes e não combatentes. É importante notar, contudo, que a conformidade com o Direito Internacional Humanitário (DIH) não esgota a dimensão ética do conflito, visto que o DIH é um corpo normativo com fundamentos próprios. Portanto, a análise ética extrapola o mero cumprimento das "leis da guerra", devendo ser buscada tanto na conduta e nas escolhas individuais dos combatentes quanto nas decisões do estrato político-estratégico que orientam a condução das hostilidades.

Isto posto, a utilização de exemplos pode funcionar como instrumento útil para a compreensão do apontamento ora firmado. O DIH corresponde ao *jus in bello*, ou direito da guerra, aplicado durante um conflito armado. No estudo da ética na guerra, focado na moralidade e não na legalidade, correntes ortodoxas entendem que os dois momentos da guerra, isto é, o *jus ad bellum* e o *jus in bello* são distintos, de forma que mesmo uma guerra injusta pode ser lutada de forma justa, e vice-versa, sendo essa a posição de Michael Walzer (2003). De outro lado, o pensamento revisionista sobre a ética na guerra promove a ligação entre os dois momentos citados, de maneira que uma guerra injusta implicará, necessariamente, em um combate injusto, sendo este o pensamento de Jeff McMahan (2009).

Retomando o problema das ações cognitivas, a desinformação e a propaganda utilizadas em Ruanda, em 1994, demonstram como esse tipo de recurso é capaz de gerar graves violações, como o genocídio perpetrado. Durante o conflito, a *Rádio Télevision Libre des Mille Collines* e jornais ligados ao governo difundiram informações falsas de que a minoria tutsi era "inimiga interna" e representava uma ameaça militar iminente (Zimbardo, 2024). Embora o massacre de civis consista em uma violação direta do DIH, a questão da ética e do uso da ação cognitiva situa-se, justamente, no problema da escolha deliberada, firmada no nível estratégico, de falsear a realidade, a fim de insuflar ou perpetuar um conflito.

De outro lado, pode ocorrer a efetiva interseção entre os preceitos de ordem ética e o Direito Internacional Humanitário, como é o caso do uso da perfídia, proibida pelo Artigo 37 do Protocolo Adicional I às Convenções de

Genebra (ICRC, 2015). A perfídia pode ser considerada como uma forma de distorção cognitiva, pois, diferente da camuflagem ou do estratagema, ocorre quando um combatente simula uma condição de proteção (como ser um civil ou estar ferido) para trair a confiança do adversário e obter vantagem militar.

Esse recurso foi sistematicamente empregado pelo Estado Islâmico (EI) em contextos de guerra urbana, como na Batalha de Mosul, entre 2016 e 2017 (Amnesty International, 2017). Durante o cerco à cidade, o grupo utilizou o disfarce de civis em fuga, o transporte de armamentos em ambulâncias e falsas rendições para atrair e atacar as forças iraquianas e da coalizão. Tais táticas não apenas violam o DIH, mas representam uma degradação ética profunda, pois exploram a própria humanidade do adversário para transformá-la em vulnerabilidade tática.

Ambos os exemplos demonstram a dificuldade de se conciliar as ações cognitivas com a ética. Embora a norma jurídica e o preceito ético coincidam em certos casos, o que permite a repressão a distorções graves, a desinformação, por sua própria natureza, visa a confundir, afastando-se de uma conduta eticamente amparada. No cenário atual, a guerra cognitiva exige estudos mais profundos, pois, ao dissolver a autoconsciência reflexiva e crítica, o ser humano perde a capacidade de superar ilusões coletivas e julgar o seu tempo. Consequentemente, anula-se o senso da verdade e a distinção entre o real e o simulado. Nesse contexto, o dilema ético da guerra cognitiva transcende a legalidade das ações, atingindo a preservação das condições epistemológicas que sustentam o próprio julgamento moral.

Considerações Finais

Diante do exposto, é possível considerar que a guerra cognitiva tensiona os próprios limites conceituais e normativos da Guerra, exigindo não apenas atualização doutrinária, mas um enfoque filosófico. Se, de um lado, ela compartilha com a guerra clássica a finalidade política, nos termos clausewitzianos, por outro, desloca o centro do confronto para a esfera da cognição, operando, com frequência, abaixo do limiar do conflito armado e alheia aos marcos jurídicos consolidados. Isso não implica na ausência da ética, mas na necessidade de explicitar quais referenciais éticos são adotados e como se aplicam a práticas que não produzem, necessariamente, efeitos cinéticos,

muito embora possam gerar danos profundos à autonomia, à deliberação pública e à soberania decisória. Assim, mais do que expandir indefinidamente o conceito de guerra, impõe-se reafirmar seus contornos para que o juízo ético não se dilua em ambiguidades semânticas.

Ademais, a incorporação da ética ao debate sobre a guerra cognitiva demanda uma abordagem na qual seja possível articular filosofia moral, teoria política e estudos estratégicos, de forma a se reconhecer que a manipulação deliberada da cognição humana não constitui mero instrumento técnico, mas ato dotado de implicações sociais de amplo espectro. A assimetria informacional, a instrumentalização de vulnerabilidades psicológicas e o emprego de tecnologias digitais de influência configuram práticas que podem comprometer valores estruturantes das sociedades democráticas, mesmo quando ausentes efeitos cinéticos. Nesse sentido, a investigação proposta visa a contribuir para a delimitação de critérios analíticos capazes de fornecer subsídios para a distinção entre persuasão legítima e coerção cognitiva, entre influência estratégica e manipulação indevida, bem como entre competição política ordinária e modalidades de conflito propriamente ditas. Essa distinção conceitual viabiliza não apenas a precisão teórica, mas a capacidade institucional de formular respostas proporcionais e juridicamente fundamentadas no âmbito da segurança e da defesa.

Referências

AMNESTY INTERNATIONAL. *At Any Cost:* The Civilian Catastrophe in West Mosul, Iraq. London: Amnesty International Ltd, 2017. Disponível em: https://www.amnesty.org/en/latest/campaigns/2017/07/at-any-cost-civilian-catastrophe-in-west-mosul-iraq/. Acesso em: 11 mar. 2026.

BRASIL. Ministério da Defesa. *Doutrina Militar de Defesa: MD51-M-04.* Brasília, DF: Ministério da Defesa, 2025.

BRASIL. Ministério da Defesa. *Glossário das Forças Armadas: MD35-G-01.* Brasília, DF: Ministério da Defesa, 2015.

CLAUSEWITZ, C. von. *Da guerra.* Tradução de Michael Howard e Peter Paret. São Paulo: Martins Fontes, 2010.

CLAVERIE, B. What is cognition? And how to make it one of the ways of the war? In: CLAVERIE, Bernard; PRÉBOT, Baptiste; BUCHLER, Norbou; DU CLUZEL, François. *Cognitive warfare*: the future of cognitive dominance. NATO Collaboration Support Office, 2022. p. 4–17. Disponível em: https://hal.science/hal-03635907v1/file/NATO-CSO-CW%202022-03-01%20%28US%29%20Claverie.pdf. Acesso em: 12 mar. 2026.

CLAVERIE, B.; DU CLUZEL, F. *Cognitive warfare:* the advent of a new domain of warfare. Norfolk: NATO Innovation Hub, 2020.

CICV. COMITÊ INTERNACIONAL DA CRUZ VERMELHA. *How is the term "armed conflict" defined in international humanitarian law?* Opinion paper. Geneva: ICRC, 2024. Disponível em: https://www.icrc.org/sites/default/files/document_new/file_list/armed_conflict_defined_in_ihl.pdf. Acesso em: 18 fev. 2026.

CULLETON, A. *Ockham e a Lei Natural.* Florianópolis: Editora da UFSC, 2011.

DEPPE, C; SCHAAL, G. S. *Cognitive warfare:* a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. Frontiers in Big Data, Lausanne, v. 7, 2024. Disponível em: https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full. Acesso em: 26 dez. 2025.

ICRC. INTERNATIONAL COMMITTEE OF THE RED CROSS. *Convenções de Genebra de 12 de agosto de 1949.* Genebra: ICRC, 2015. Disponível em: https://www.icrc. org. Acesso em: 12 mar. 2026.

JONES, M. G. Operações de desinformação da Rússia ressurgem antes das eleições alemãs. *Euronews,* 22 jan. 2025. Disponível em: https://hal.science/hal-03635907v1/file/NATO-CSO-CW%202022-03-01%20%28US%29%20Claverie.pdf. Acesso em: 12 mar. 2026.

KOFMAN, M.; STARKE, E. *Russian military strategy and Ukraine:* operational art, cognitive warfare, and information confrontation. Washington, DC: Carnegie Endowment for International Peace, 2023.

LAVELLE, L. *A intimidade espiritual.* Tradução de Christian Lesage. Campinas: Vide Editorial, 2023.

MAQUIAVEL, N. *O Príncipe.* Tradução de Olívia Bauduh. São Paulo: Nova Cultural, 1999.

MCMAHAN, J. *Killing in the War.* New York: Oxford University Press, 2009.

NATO. *Allied Command Transformation develops the cognitive warfare concept to combat disinformation and defend against cognitive warfare*. Norfolk, VA: NATO Allied Command Transformation, 2024. Disponível em: https://www.act.nato.int/article/cogwar-concept/. Acesso em: 27 dez. 2025.

ORTEGA Y GASSET, J. *A Rebelião das Massas.* Tradução de Marylene Pinto Michael. São Paulo: Martins Fontes, 2002.

PAUL, C.; MATTHEWS, M. *The Russian "firehose of falsehood" propaganda model:* why it might work and options to counter it. Santa Monica: RAND Corporation, 2016.

PINHEIRO, V. S. *A Crise da Cultura e a Ordem do Amor:* ensaios filosóficos. São Paulo: É Realizações Editora, 2021.

PINTO, E. M.; LATERZA, R. Q. *Guerra cognitiva.* Velho General, 6 mar. 2025. Disponível em: https://velhogeneral.com.br/wp-content/uploads/2025/03/Guerra-cognitiva-v2.pdf. Acesso em: 12 mar. 2026.

RID, T. *Active measures:* the secret history of disinformation and political warfare. New York: Farrar, Straus and Giroux, 2020.

SUN TZU. *A arte da guerra.* Tradução de Jia Sun Costa. São Paulo: Buzz Editora, 2018.

UNITED STATES. *Senate Select Committee on Intelligence. Russian active measures campaigns and interference in the 2016 U.S. election.* Washington, DC: U.S. Senate, 2020.

VILLEY, M. *A Formação do Pensamento Jurídico Moderno.* Tradução de Cláudia Berliner. São Paulo: Martins Fontes, 2019.

WALKER, M. *Operações de informação: névoa de conceitos.* Maringá: Viseu, 2024.

WALZER, M. *Guerras Justas e Injustas.* Tradução de Waldéia Barcelos. São Paulo: Editora Martins Fontes, 2003.

WEBER, M. A política como vocação. In: GERTH, H. H.; MILLS, C. W. (org.). *Max Weber: ensaios de sociologia*. Rio de Janeiro: Livros Técnicos e Científicos, 1967. p. 55-89. Disponível em: https://www.bresserpereira.org.br/index.php/search?searchword=weber&ordering=newest&searchphrase. Acesso em: 17 fev. 2026.

ZIMBARDO, P. *O Efeito Lúcifer*: Como pessoas boas se tornam más. Tradução de Tiago Novaes Lima. 13. ed. Rio de Janeiro/São Paulo: Editora Record, 2024.

Parte II

Segurança e Defesa na Era Digital: desafios cognitivos, educacionais e operacionais

Plataformas digitais, (des)informação e a mobilização do 8 de janeiro: um Estado do Conhecimento[1]

Gabriel Carlos dos Reis Costa Dias
Nádia Xavier Moreira
Viviane Machado Caminha

Introdução

O dia 8 de janeiro de 2023 marcou a história recente da República Federativa do Brasil como um ponto de tensão na estabilidade de suas instituições democráticas. Brasília, a capital federal planejada para ser o centro decisório do país, amanheceu sob uma atmosfera atípica, carregada de tensões acumuladas.

Milhares[2] de indivíduos, impulsionados por um inconformismo radical com o resultado do pleito presidencial de 2022, haviam se deslocado para a cidade, concentrando-se nas imediações do Quartel-General do Exército Brasileiro, situado no Setor Militar Urbano, a aproximadamente oito quilômetros da Praça dos Três Poderes. Esse acampamento, tolerado e mantido por semanas, serviu como o incubador logístico e ideológico para o que viria a ser o maior ataque físico às sedes dos poderes constituídos desde a redemocratização

A cronologia dos fatos, detalhada no Relatório Final da Comissão Parlamentar Mista de Inquérito (CPMI) e corroborada por relatórios da intervenção na Segurança Pública do Distrito Federal, revela uma escalada de violência que desafiou os protocolos de segurança existentes. A marcha,

[1] Neste artigo, foram utilizadas as ferramentas ChatGPT, da OpenAI, para revisão gramatical e estruturação de parágrafos, e NotebookLM, do Google, para resumo de artigos e organização de ideias do corpus de análise, com validação integral do conteúdo pelos autores.

[2] No relatório da Comissão Mista Parlamentar de Inquérito (Brasil, 2023a) não há uma precisão da quantidade de pessoas que participaram dos atos de 8 de janeiro. Em mensagens da Agência Brasileira de Inteligência na manhã do dia 8 de janeiro indicava-se a estimativa da Secretaria de Segurança Pública (SSP) de 3.000 (três mil) pessoas e 101 ônibus que teriam chegado à Brasília. Já no início da tarde há a informação de uma mensagem enviada ao Governador do Distrito Federal, na qual o Secretário Executivo da SSP informa que havia em Brasília 150 ônibus. Dessa forma, utilizamos a expressão "milhares de pessoas" a qual também foi utilizada no relatório do interventor na Segurança Pública do Distrito Federal (Brasil, 2023b)

iniciada por volta das 13h, deslocou-se pela via N1, acompanhada pela Polícia Militar do Distrito Federal. Durante este trajeto, a materialidade da ameaça já se fazia presente: apreensões realizadas no percurso identificaram um arsenal improvisado composto por facões, estilingues, esferas metálicas, balaclavas, material incendiário e outros instrumentos ofensivos, indicando que a mobilização não possuía caráter pacífico, mas sim uma intenção beligerante latente.

A iminência do colapso do sistema de segurança tornou-se evidente às 14h25, momento em que a primeira linha de revista policial, situada próxima ao "Buraco do Tatu", foi rompida pela turba. A progressão foi rápida e agressiva. Menos de vinte minutos depois, às 14h43, a linha de contenção principal, composta por gradis e efetivo policial na Avenida das Bandeiras, sucumbiu diante da superioridade numérica e da disposição violenta dos manifestantes. O uso de granadas de gás lacrimogêneo e outros instrumentos de menor potencial ofensivo mostrou-se insuficiente para deter o avanço, que culminou na invasão do Congresso Nacional, do Palácio do Planalto e do Supremo Tribunal Federal (STF).

A descrição fenomenológica da invasão revela um padrão de destruição simbólica e material. No Congresso Nacional, a ocupação do Salão Negro e das cúpulas permitiu o acesso aos plenários e gabinetes, resultando na depredação de obras de arte e mobiliário histórico. No Palácio do Planalto, a barreira de proteção na altura do Ministério da Justiça foi violada, permitindo o acesso à rampa principal e, subsequentemente, ao Gabinete da Presidência da República.

No STF, a destruição atingiu o plenário, com o arrancamento de poltronas, danos ao busto de Ruy Barbosa e o alagamento proposital das instalações. A desocupação dos prédios, iniciada às 16h25 e concluída no início da noite, resultou em um quadro de devastação que exigiu resposta imediata e contundente do Estado.

A descrição "nua e crua" desses acontecimentos desperta não apenas comoção social, mas uma urgência analítica para a academia, especialmente para o campo da Segurança e Defesa. O evento suscita diversos questionamentos estruturais, dentre eles: Quais foram as dinâmicas de mobilização que permitiram a convergência de milhares de pessoas com o intento de atacar as instituições?

A relevância deste estudo reside na necessidade de transcender a análise jornalística imediata e adentrar na reflexão científica estruturada. O 8 de janeiro não foi um evento isolado, mas o clímax de um processo de corrosão institucional e radicalização política (Queiroz; Barboza; Souza, 2024).

Para o pesquisador da área de Segurança e Defesa, torna-se imperativo observar como a comunidade acadêmica tem processado, categorizado e interpretado estes eventos. A produção científica atua como um espelho crítico, permitindo identificar quais interpretações estão sendo consolidadas, quais aspectos estão sendo escrutinados e, crucialmente, quais lacunas permanecem inexploradas.

Justifica-se, ainda, este trabalho pela posição singular do autor, que vivenciou os eventos como policial legislativo na proteção do Senado Federal. A metodologia do Estado do Conhecimento permite, neste contexto, um distanciamento epistemológico necessário. Ao analisar o evento através das lentes de outros pesquisadores, é possível mitigar o viés da experiência traumática direta e construir uma análise objetiva sobre os eventos. Este estudo busca, portanto, não apenas catalogar o que foi produzido, mas sintetizar o conhecimento acumulado.

Construção do corpus de análise

A metodologia adotada para a elaboração deste capítulo é o Estado do Conhecimento, fundamentada nas proposições teóricas de Morosini e Fernandes (2014). Diferente de uma revisão bibliográfica tradicional, o Estado do Conhecimento foca na identificação, registro e categorização de produções científicas em uma área delimitada e num recorte temporal específico. O objetivo é conduzir a uma reflexão e síntese crítica sobre como o conhecimento está sendo construído.

Nesta perspectiva, o conhecimento não é entendido como uma verdade estática ou neutra, mas como uma produção histórico-cultural situada no tempo e no espaço, atravessada por dinâmicas de poder. Ao aplicar esta metodologia ao 8 de janeiro, busca-se compreender como a academia brasileira e internacional está construindo o conhecimento acerca desse evento, quais disputas simbólicas e ideológicas permeiam essas análises e como diferentes campos do saber dialogam ou conflitam na interpretação dos fatos.

Seguindo o percurso metodológico de Morosini e Nascimento (2021) buscou-se a seleção das fontes e bases de dados, a delimitação de um recorte temporal, os descritores e sintaxe de busca, os critérios de inclusão e exclusão e a sistematização e categorização.

A construção do corpus fundamentou-se em busca estruturada no Google Acadêmico, base selecionada por apresentar maior abrangência de resultados sobre o tema em comparação a repositórios especializados (CAPES, SciELO). O recorte temporal compreendeu o período de janeiro de 2023 a abril de 2025.

Utilizaram-se os descritores "8 de janeiro" AND invasão para a produção nacional, e "january 8" AND invasion AND brazil AND riot para a internacional. Da busca inicial, que retornou 655 registros, aplicaram-se critérios de inclusão para selecionar apenas produções com o evento como objeto central (artigos, teses, livros e *policy papers*), resultando em um corpus final de 70 obras. Mediante leitura lateralizada, os trabalhos foram classificados em cinco eixos temáticos, sendo selecionada para este capítulo a subcategoria plataformas digitais e (des)informação, a fim de entender as dinâmicas de mobilização que culminaram com os ataques de 8 de janeiro.

Plataformas digitais e (des)informação

Nessa subcategoria os estudos giram em torno da análise do papel desempenhado pelas plataformas digitais como arenas multifacetadas de construção, circulação e disputa de narrativas políticas. Parte-se do reconhecimento de que tais espaços não operam apenas como meios de comunicação, mas configuram ecossistemas informacionais dinâmicos, nos quais a desinformação desempenha função central.

Essa centralidade das redes no processo político e comunicacional contemporâneo pode ser compreendida a partir da noção de ciberterritórios e ciberterritorialidades, introduzida por Martinuzzo e Anciães Darriba (2023). Para os autores, trata-se de uma expansão da dimensão existencial humana, constituindo um "quarto âmbito existencial, um *bios* midiático" (Martinuzzo;Anciães Darriba, 2023, p. 6). Nesse *bios* midiático, a natureza dos dados pessoais, em plataformas como o Twitter se transforma, tornando-se publicizáveis e sujeitos a intenso escrutínio à medida que o conteúdo viraliza

(Rota; Nicodemo, 2023). Essa fusão entre o pessoal e o público na esfera digital é uma característica marcante das redes sociais. Nesse sentido, as redes sociais digitais tornam-se territórios cibernéticos relevantes, operando não apenas como suporte, mas como território simbólico e relacional.

Sob tal ótica, a circulação de informações manipuladas ou falsas, muitas vezes sistematicamente direcionada, revela-se capaz de reconfigurar o debate público, influenciar percepções e comportamentos sociais, bem como fomentar processos de mobilização – inclusive de natureza antissistêmica – cujos efeitos podem comprometer a estabilidade da ordem democrática.

Taxonomia da desinformação

Mendes, Sanglard e Costa (2024) oferecem uma contribuição teórica consistente ao examinarem os fundamentos conceituais indispensáveis à compreensão da dinâmica desinformacional associada aos atos de 8 de janeiro. Segundo os autores, a desordem informacional configura-se pela ampla disseminação de conteúdos "problemáticos ou duvidosos" (Mendes; Sanglard; Costa, 2024, p.121), cuja natureza varia conforme o grau de veracidade e a intencionalidade subjacente à sua veiculação

Baseando-se na taxonomia do fenômeno, Mendes, Sanglard e Costa (2024) delineiam, a partir de outros autores, o espectro da desordem informacional em três eixos: o compartilhamento de conteúdo inverídico por mero desconhecimento (*misinformation*); a fabricação e difusão intencional de mentiras visando o desgaste de alvos específicos (*disinformation*); e a instrumentalização maliciosa de dados reais e privados para destruir reputações (*malinformation*)..

Essa taxionomia ganha densidade na análise de Souza e Leal (2024), ao situarem o fenômeno das *fake news* dentro de uma perspectiva histórica e comunicacional mais ampla. Para as autoras, ainda que a circulação de falsos conteúdos remonte a períodos como a Antiguidade – a exemplo do uso de escritos apócrifos para comprometer reputações políticas –, as *fake news* contemporâneas[3] assumem características específicas: mimetizam a estética do

[3] De Assis Cordeiro *et al.* associam as fake news a distorções eleitorais contemporâneas, como o Brexit (referendo para saída dooReino Inido da União Européia) e as eleições presidenciais dos EUA, em 2016, e do Brasil, em 2018.

jornalismo tradicional (Martinuzzo;Anciães Darriba, 2023), ocultam-se entre informações verdadeiras e são orientadas por forte apelo emocional.

Além disso, destacam-se pelo uso planejado em contextos de alta exposição política, explorando a viralização em redes digitais e moldando a opinião pública com base em sentimentos como indignação e revolta. Tais conteúdos, mesmo que eventualmente imprecisos ou sem fonte confiável, adquirem legitimidade discursiva justamente por ativarem crenças preexistentes dos indivíduos e operarem em um ambiente de disputa narrativa constante.

Nesse novo arranjo informacional, a perda da hegemonia do jornalismo tradicional desempenha papel relevante (Luiz, 2023). A erosão do monopólio informativo da imprensa tradicional é explicada por Tavares (2017, *apud* Souza; Leal, 2024) através de uma tríplice fratura: o nivelamento tecnológico, que transformou o cidadão comum em emissor; a perda da capacidade institucional dos jornais de filtrarem o debate público (*gatekeepers*[4]); e a falência do modelo de objetividade, visto que a audiência passou a desvalorizar a isenção em prol de narrativas que confirmem suas crenças prévias

Esse movimento de deslegitimação não se restringe ao campo teórico, mas se materializa em interações concretas nas plataformas digitais. Souza et al. (2023) identificaram, por exemplo, comentários de usuários que não apenas criticavam o conteúdo veiculado, mas incentivavam que outros deixassem de seguir a página de um jornal, recorrendo a adjetivos depreciativos para qualificar a mídia. Tais manifestações evidenciam como a desconfiança se traduz em ações simbólicas e coletivas, reforçando a erosão da autoridade jornalística no ecossistema informacional contemporâneo.

Câmaras de Eco

A partir de alguns estudos, Mendes, Sanglard e Costa (2024) observam que é nesse ecossistema informacional assimétrico que emergem as denominadas câmaras de eco — espaços digitais caracterizados pela filtragem seletiva de conteúdos, que tendem a reforçar convicções pré-existentes.[5] Essa dinâmica de

[4]"porteiros" em tradução livre, mas contextualmente referem-se a protetores da conformidade.

[5]A adesão ao discurso maculado por notícias falsas está menos ancorada em critérios lógicos e objetivos e mais associada a estruturas cognitivas e afetivas dos indivíduos (Mendes; Sanglard;

retroalimentação cognitiva favorece tanto o enrijecimento de posicionamentos quanto a intensificação da radicalização, além de potencializar a disseminação de desinformação no interior desses agrupamentos.

Conforme a análise de Garrossini *et al*. (2023), o fenômeno das mobilizações iniciado em 2013, com as jornadas de junho e o Movimento Passe Livre, passou por um processo de apropriação que envolveu coleta e tratamento de dados, mapeamento de perfis e segmentação em comunidades digitais, inicialmente concentradas no Facebook. Esse rearranjo comunicacional teria contribuído para a transformação da imagem de mobilizações plurais em manifestações mais homogêneas, visualmente identificadas por símbolos patrióticos e alinhadas a agendas da direita.

Para conceituar o isolamento cognitivo em redes, Matsuda *et al.* (2025) explicam que as câmaras de eco operam como um filtro algorítmico e social. Nesse ambiente, o indivíduo é retroalimentado por narrativas alinhadas ao seu viés ideológico, sofrendo uma drástica redução no acesso a visões de mundo contraditórias ou dissonantes. No campo político, isso ocorre quando a orientação ideológica do conteúdo recebido coincide com a orientação do conteúdo compartilhado, criando um ciclo de retroalimentação sustentado por diferentes elementos interligados.[6]

A análise empírica desses autores, focada especificamente no Twitter/X durante os Atos de 8 de janeiro de 2023 (dados coletados entre 8 e 10 de janeiro), confirma a existência dessas estruturas na prática. A pesquisa combinou análise

---

Costa;2024) Essa dinâmica é referendada por Souza e Leal (2024), ao argumentarem que as bases da atual desordem política são pavimentadas, primordialmente, nos domínios cultural e mental. A engenharia dessa radicalização é potencializada pelos fluxos comunicacionais do ecossistema digital, caracterizado por um paradoxo: a sobrecarga de dados coexiste com um déficit de capacidade analítica por parte dos usuários. Sob a égide da pós-verdade, a validação coletiva afasta-se de balizas factuais, tornando a opinião pública cativa de apelos passionais e vieses ideológicos (o que as autoras resgatam como o efeito narcotizante das mídias). É nesse cenário pautado pela mobilização de afetos que a arquitetura das plataformas digitais se revela um vetor ambíguo. Se, por um lado, o engajamento virtual tenta satisfazer a necessidade intrínseca das comunidades de partilhar poder — dinâmica que Martins (2002, *apud* Evangelista; Quaresma, 2024) define como a própria condição de vitalidade da participação cidadã —, por outro, essa mesma energia participativa pode ser capturada por fluxos de desinformação.

[6]Como exemplo, Matsuda *et al.* (2025) destacam que o Twitter/X, pela amplitude de usuários e volume de discussões políticas, é especialmente propenso à formação de câmaras de eco, nas quais o compartilhamento seletivo reforça visões específicas e intensifica a polarização

de redes para identificação de comunidades, avaliação de posicionamento político e estudo de sentimentos, revelando uma polarização[7] evidente na plataforma. Os usuários tendiam a interagir predominantemente com pessoas de orientação ideológica semelhante, e os debates giravam em torno do apoio ou da rejeição ao ato e às medidas adotadas.

O isolamento cognitivo nestas plataformas opera por meio do que Castro e Cavalcante (2024),[8] amparadas em Recuero, definem como microesferas públicas. O design algorítmico incentiva uma segregação baseada em alinhamento político, erguendo barreiras informacionais intransponíveis onde o dissenso é bloqueado e apenas o consenso intragrupo consegue trafegar

Dados empíricos, trazidos por Bertanha e De Araujo (2024), validam essa tese ao apresentarem a linha do tempo[9] com a evolução do Twitter durante os atos de 8 de janeiro, apontaram que as discussões eram mais frequentes no interior de cada grupo[10] do que entre eles, indicando um distanciamento comunicativo entre usuários com posicionamentos políticos divergentes – evidência da presença de bolhas de conversação nas redes analisadas.

Visando analisar possíveis conexões entre a desinformação digital e a mobilização de movimentos contrários à ordem democrática, Martinuzzo e Anciães Darriba (2023) investigaram[11] a disseminação de notícias falsas relacionadas à eleição presidencial de 2022, com atenção especial à articulação comunicacional que precedeu os atos de 8 de janeiro.

---

[7]Em termos emocionais, prevaleceram expressões de raiva e aborrecimento, potencializadas por trocas de acusações e retóricas inflamadas, que reforçaram a predominância de emoções negativas. Além disso, a análise demonstrou que os *retweets* ampliam a homogeneidade temática dentro das comunidades, intensificando a dinâmica de reforço característica das câmaras de eco.

[8]Analisando as interações no X nos meses de janeiro, fevereiro e março de 2023

[9]Essa linha do tempo foi resultado do pipeline pelo *pipeline* desenvolvido por Silva; Araujo e Correa (2024) que permitiu a identificação de 436.640 perfis (nós) e 1.164.952 interações (arestas) ao longo de 24 horas do dia 8 de janeiro, resultando na formação de 4.847 *clusters.*

[10]Os autores utilizaram ferramentas de visualização que explicitavam a formação de grupos (*clusters*) classificados como pró-Lula, pró-Bolsonaro e neutros/indefinidos, além de "nuvens de palavras" para identificar os termos mais citados tanto na rede como um todo quanto nos principais grupos.

[11]O corpus do estudo consistiu nas averiguações realizadas pelo Projeto Comprova, uma iniciativa de jornalismo colaborativo voltada à verificação de conteúdos de veracidade duvidosa que viralizam nas redes sociais. De acordo com os dados analisados pelos autores, as apurações realizadas durante o período eleitoral resultaram na publicação de 378 reportagens investigativas. Dentre os conteúdos verificados, 96,7% foram classificados como falsos ou enganosos.

Os autores delimitaram seu corpus ao intervalo compreendido entre o dia anterior ao primeiro turno das eleições, em 1º de outubro, e o encerramento das apurações eleitorais pelo projeto Comprova, em 17 de dezembro de 2022. O conjunto de material analisado totalizou 110 registros de *fake news* verificados ao longo desse período.[12]

Complementando essa perspectiva, Luiz (2023) examinou o conjunto de desinformações verificadas pela agência "Aos Fatos" entre os dias 8 de janeiro e 6 de abril de 2023, observando a prevalência de conteúdos que, embora baseados em imagens reais,[13] são descontextualizados por meio de legendas enganosas, cortes seletivos ou manipulações narrativas.

Mobilização digital

Souza e Leal (2024), ao analisarem a comunicação no ambiente digital que antecedeu os eventos de 8 de janeiro, por sua vez, concluíram que a disseminação de desinformações, ocorrida em um ecossistema de ódio, constituiu o principal método de construção da violência simbólica contra as instituições públicas, a qual resultou na invasão das sedes dos três Poderes em Brasília.[14]

De Assis Cordeiro *et al.* (2024) complementam essa perspectiva argumentando que a eficácia da desinformação reside em sua capacidade de mimetizar a realidade. Para que as narrativas fraudulentas sejam assimiladas como verdadeiras, os emissores as ancoram em elementos factuais da conjuntura

[12]A repercussão desses conteúdos, segundo os dados analisados, gerou um total de 100.624.032 interações – incluindo compartilhamentos, curtidas, comentários e visualizações – e esteve centrada em temas como acusações de fraude eleitoral e ataques direcionados ao Tribunal Superior Eleitoral (TSE) e ao Supremo Tribunal Federal (STF). Ainda assim, os autores alertam que essa quantidade representa apenas a uma pequena parte da circulação desinformacional, já que redes fechadas como WhatsApp e Telegram impõem barreiras técnicas ao monitoramento sistemático (Martinuzzo; Anciães Darriba, 2023).

[13]Em muitos casos, a peça desinformativa não é fabricada do zero, mas construída a partir da distorção parcial da realidade, o que reforça sua aparência de veracidade. A operação de tirar uma imagem ou evento do seu tempo ou circunstância original – prática comum nesse tipo de conteúdo – acaba por gerar enunciados falaciosos, ainda que visualmente autênticos.

[14]Grischke (2024) afirma que a concretização de 8 de janeiro ilustra a tênue fronteira entre a violência simbólica e a violência física: quando legitimada socialmente, a retórica transborda o discurso e se materializa em ações concretas contra a ordem democrática.

política, social ou econômica, manipulando essas premissas reais para conferir validade a conclusões enganosas.

Para Mendes, Sanglard e Costa (2024), os episódios analisados devem ser compreendidos no contexto da chamada sociedade da desinformação, marcada pela presença endêmica de narrativas falsas que se articulam por meio de uma lógica multiplataforma. Tal configuração não apenas amplia o alcance dos conteúdos, como também intensifica seu impacto, favorecendo a organização de comunidades digitais em torno de crenças coletivas, frequentemente dissociadas da veracidade factual da informação.

Nesse cenário, as plataformas digitais assumem papel estratégico na reconfiguração da esfera pública contemporânea. Longe de atuarem como intermediárias neutras, tais infraestruturas tecnológicas moldam as dinâmicas de interação entre usuários e produtores de conteúdo, influenciando diretamente quais informações circulam, quem as consome e de que maneira esses fluxos são amplificados no ecossistema digital.[15]

Contudo, há que se ressaltar que, as mesmas plataformas que facilitaram a mobilização para atos como os de 8 de janeiro também foram palco de iniciativas em defesa da ordem constitucional. À luz do conceito de *continuum on-line/off-line,*[16] Evangelista e Quaresma (2024) observam que a participação nas redes sociais é uma extensão da vida cotidiana e pode estar diretamente ligada ao fortalecimento ou ao enfraquecimento democrático, a exemplo dos acampamentos e da própria invasão de 8 de janeiro.

Na esfera da mobilização prática, Calza (2024) demonstra que, nas eleições presidenciais de 2022, mensagens disseminadas em grupos de *WhatsApp* e *Telegram*[17] vinculados à direita articularam enquadramentos narrativos voltados a questionar a legitimidade do processo eleitoral e a sustentar a mobilização de apoiadores por um longo período. Essa comunicação,

[15] Por exemplo, os algoritmos de recomendação personalizam o *feed* de informações dos usuários com base em seus comportamentos anteriores, o que pode levar a uma visão limitada do mundo e à perda de controle sobre o conteúdo recebido. (Matsuda *et al.,* 2025).

[16] O conceito de *continuum on-line-off-line* refere-se à compreensão de que as interações virtuais não estão dissociadas da vida cotidiana, mas constituem uma extensão dela, influenciando e sendo influenciadas por eventos no mundo físico. (Evangelista; Quaresma, 2024)

[17] Scheren et al. (2024) indicam que diante da intensa fiscalização e implementação de controle das plataformas comumente utilizadas por esses grupos, houve uma migração para plataformas alternativas como o *Telegram*, a qual possui características favoráveis.

estruturada segundo a lógica dos *collective action frames,*[18] manteve redes ativas e alinhadas em torno de pautas antidemocráticas antes, durante e após o pleito, servindo de base discursiva para os atos de 8 de janeiro. Esse enquadramento narrativo contribuiu para articular um repertório de ação coletiva capaz de transpor o ambiente digital e se materializar em atos coordenados no espaço físico.

Scheren *et al.* (2024) em estudo de caso sobre grupos no *Telegram* evidenciaram que, em determinados ecossistemas políticos, a narrativa religiosa e a noção de patriotismo se entrelaçam de modo a reforçar identidades políticas exclusivas. Em paralelo, a percepção de ameaça representada por ideologias associadas a outros países – como o temor da adoção de um regime alinhado ao modelo venezuelano – foi explorada como elemento retórico para sustentar demandas por medidas de força.

Nessas construções discursivas, atores coletivos se autodefinem como "representantes legítimos do povo" e atribuem às Forças Armadas um papel central de garantidoras da integridade nacional, reproduzindo um enquadramento que opõe aliados e adversários em termos existenciais.

A centralidade assumida pelas plataformas digitais na reconfiguração da esfera pública está intimamente relacionada à transformação estrutural da própria internet. Esse processo acompanha a transição de uma web originalmente aberta –pautada por ideais de descentralização, interoperabilidade e acesso livre – para ambientes digitais cada vez mais fechados, organizados em torno de ecossistemas proprietários sob controle de grandes conglomerados tecnológicos. Esses ambientes são moldados por interesses comerciais e estratégias de autorregulação que buscam, ao mesmo tempo, ampliar lucros e evitar a intervenção estatal. (Mendes; Sanglard; Costa, 2024)

Nesse sentido, Santos, V. V. V. (2024, p.97) argumenta que as grandes empresas de tecnologia, por meio das escolhas algorítmicas que estruturam as redes sociais, influenciam diretamente o "canal comunicativo" e o "contexto de produção das performatividades linguísticas online". Atuando como extensões do sujeito, essas plataformas contribuem para usos predatórios da linguagem, favorecendo a proliferação de desinformação e a subversão de discursos e identidades. Os próprios *designs* algorítmicos modulam as escalas e os efeitos

[18]Enquadramentos de ação coletiva em tradução livre.

dos atos performativos, determinando as regras de expressão em ambientes digitais — processo que está diretamente vinculado às permissividades impostas ou negadas por cada arquitetura algorítmica.

Como resultado, essas plataformas acabaram por reproduzir assimetrias sociais, reforçar bolhas cognitivas e fomentar a viralização de conteúdos desinformativos. Nesse processo, tornaram-se instrumentos de intimidação contra adversários, de silenciamento de vozes dissidentes e de promoção de agendas particulares, frequentemente disfarçadas sob a retórica de mobilizações coletivas. (Souza; Leal, 2024; Mendes; Sanglard; Costa, 2024)

Além disso, as *affordances* (as potencialidades de interação que o próprio design sugere ao usuário) são calibrados para restringir a agência individual em favor do engajamento. Consequentemente, esse modelo estrutural atua como um catalisador para dinâmicas discursivas nocivas, facilitando desde o linchamento virtual e a difamação até a propagação orquestrada de notícias falsas. (Santos, V.V.V. 2024)

A mobilização de determinados grupos organizados no Brasil, especialmente a partir de estratégias coordenadas no ambiente digital, evidenciou como essas ferramentas foram empregadas na articulação de ações contrárias à ordem democrática. A observação sistemática dessas interações digitais também demonstra que, para além da retórica, tais grupos empregaram as plataformas como canais de convocação e organização logística para ações presenciais.

A partir da perspectiva das representações sociais, como discutido por Castro e Cavalcante (2024), a disputa de narrativas sobre o 8 de janeiro pode ser compreendida como um processo de ancoragem e objetivação. A ancoragem opera ao reduzir ideias novas ou desconfortáveis a categorias já conhecidas pelo grupo, enquadrando-as dentro de um sistema de crenças pré-existente. No caso, os grupos progressistas enquadraram os eventos como atos criminosos que deveriam ser punidos, enquanto segmentos alinhados à direita atribuíram a violência a supostos "infiltrados" de esquerda, deslocando a culpa para fora de seu grupo (Castro; Cavalcante, 2024; Rota; Nicodemo, 2023). Já a objetivação, que transforma conceitos abstratos em realidades tangíveis, manifestou-se na concretização de figuras de "amigo" e "inimigo", convertendo opositores políticos em ameaças existenciais. Esse mecanismo não apenas reforça a

coesão interna, mas também orienta a mobilização e as demandas políticas de cada campo narrativo (Scheren et al., 2024).

Essa disputa semântica também é observável no nível da linguagem empregada nas redes. Rota e Nicodemo (2023), ao analisarem publicações no Twitter/X entre 8 e 9 de janeiro de 2023, identificaram expressões que buscavam provocar uma instabilidade semântica no conceito de liberdade, atribuindo-lhe um caráter irrestrito e dissociado de seus limites sociais. Paralelamente, assim como Castro e Cavalcante (2024), detectaram o uso de narrativas que associavam os atos de vandalismo a "infiltrados da esquerda", estratégia voltada à transferência de responsabilidade e reforço da coesão grupal.[19] A aplicação de análise de *n*-gramas[20] revelou que tais construções semânticas apresentavam elevado grau de padronização, evidenciando como determinadas estruturas linguísticas são replicadas para sustentar e difundir enquadramentos narrativos específicos.

No mesmo sentido, Souza et al. (2023) indica que as interações nas mídias sociais são influenciadas por padrões anteriores de reforço, moldados pelas práticas e valores predominantes no ambiente cultural em que os usuários estão inseridos. Esse condicionamento influencia desde o tipo de conteúdo que atrai atenção até as formas de engajamento, como curtir, comentar ou compartilhar.

Do virtual para o real

Quando essa dinâmica se articula a objetivos coletivos claros, ela favorece a formação de uma coesão grupal que, em contextos específicos, pode se converter em mobilização real. Essa coesão, retomada no trabalho Souza *et*

[19]Nesse contexto, observa-se que tais deslocamentos narrativos funcionam como estratégias nas quais eventos negativos são reinterpretados de modo a proteger a imagem do grupo e preservar sua unidade interna. Essa manobra discursiva, ao mesmo tempo em que desvia o foco de possíveis falhas ou excessos próprios, fortalece a percepção de um adversário comum, alinhando-se à lógica de objetivação descrita anteriormente.

[20]Conforme explicitado por Rota e Nicodemo (2023) n-gramas correspondem a uma técnica de processamento de linguagem natural empregada na análise textual, que consiste na extração de sequências contínuas de *n* unidades (tokens), como palavras, letras ou fonemas. O valor de *n* define o tamanho da sequência extraída. No contexto da análise, o recurso foi utilizado para calcular as frases mais recorrentes associadas a termos específicos – como "liberdade" e "infiltrados" – nas publicações do Twitter/X relativas aos atos de 8 de janeiro.

al. (2023) a partir de outros estudos, contribui para compreender como grupos – mesmo inicialmente conectados apenas por meios digitais – podem aderir rapidamente a ações coordenadas no mundo real quando impulsionados por uma causa percebida como comum.

Scheren *et al.* (2024) identificaram trocas de mensagens que tratavam de deslocamentos coordenados para Brasília, acompanhadas de apelos por medidas de exceção e, em casos mais extremos, de incentivos à prática de atos materiais contra alvos institucionais. Essa capacidade de articular fluxos comunicacionais voltados à ação imediata evidencia como *affordances* específicas das plataformas podem ser instrumentalizadas para converter engajamento on-line em eventos físicos de grande escala.

Parte significativa das mensagens analisadas tinha por finalidade enfraquecer a legitimidade de opositores e despertar sentimento de insegurança e urgência entre os participantes. Essa estratégia, orientada para estimular respostas rápidas e alinhadas a um grupo identitário, reflete padrões de comunicação de polarização e radicalização (amigo vs. inimigo). A persistência dessa lógica de ameaça iminente mantém elevado o nível de mobilização e reforça o vínculo entre os membros da rede.

Parte dessa dinâmica se sustenta no uso intensivo de tecnologias automatizadas, como os chamados robôs digitais – essas ferramentas artificiais são capazes de replicar conteúdos em larga escala, simulando engajamento orgânico e fraudando a percepção de relevância de certos atores ao subverterem o ranqueamento algorítmico. Conforme destacam Souza e Leal (2024), esses mecanismos não apenas criam a ilusão de popularidade de determinados perfis, como também funcionam como catalisadores do engajamento humano, ao ativar um efeito de contágio e incentivar a adesão a conteúdos já previamente impulsionados.

Por outro lado, conforme tratado por Evangelista e Quaresma (2024) há ainda que se considerar o papel de influenciadores digitais, que não apenas incentivam a participação de seus seguidores, mas também contribuem para definir as pautas e direcionar o sentido das mobilizações. Utilizando seu alcance expressivo e capacidade de engajamento, esses atores convertem a insatisfação social em ações concretas e ampliam o impacto das narrativas em diferentes espectros político-ideológicos.

O resultado é um ambiente informacional em que a velocidade e a abrangência da disseminação das chamadas *fake news* convergem com interesses políticos específicos, sustentados por estratégias comunicacionais sensacionalistas, com forte apelo emocional, especialmente em torno de temas como religião, moralidade e corrupção.

Para Grischke (2024), a desinformação, quando amplificada pelas redes, passou a condicionar o comportamento dos indivíduos por meio de mecanismos de pertencimento e mobilização coletiva.

No contexto brasileiro, essa lógica culminaria na organização dos atos de 8 de janeiro de 2023, cuja articulação nas redes foi precedida por mensagens codificadas, como a chamada "Festa da Selma", que circularam dias antes em grupos de *WhatsApp* orientando a ocupação de prédios públicos e convocando manifestantes a clamar por uma intervenção militar. O uso da expressão, que faz alusão à saudação "Selva", tradicionalmente utilizada por setores do Exército, revela a apropriação simbólica de elementos militares. (Grischke, 2024)

No mesmo sentido, De Assis Cordeiro *et al.* (2024) argumentam que os acontecimentos de 8 de janeiro de 2023 estão intimamente relacionados à falta de memória e de verdade sobre o passado brasileiro, bem como à ausência de pensamento crítico e à obediência cega a grupos saudosistas do regime militar.

Respostas a desinformação

A gravidade dos atos ocorridos em 8 de janeiro de 2023 também reabriu o debate jurídico acerca dos limites da liberdade de expressão frente aos crimes cibernéticos praticados por meio de plataformas digitais. Lopez Pelaez e Mendonça (2024) destacam que segundo Supremo Tribunal Federal, esse direito, embora essencial, não é absoluto, devendo ser ponderado com outros valores constitucionais, especialmente quando utilizado para propagar desinformação, incitar a violência ou promover discursos de ódio.

Nesse contexto, os autores entendem que os crimes cibernéticos associados à desinformação política[21] expõem lacunas normativas e operacionais ainda existentes na legislação brasileira.

[21]Como disparos em massa, manipulação algorítmica e disseminação de *fake news*.

Nesse cenário, Forster *et al.* (2021 *apud* Grischke, 2024) apontam que a resposta do Estado brasileiro à proliferação de notícias falsas ainda é incipiente quando comparada ao cenário internacional, onde já se observam progressos mais consolidados tanto na formulação de regulações públicas quanto na promoção do letramento midiático.

A questão da regulamentação das mídias sociais emerge como um tema inadiável, que transcende o ambiente legislativo e demanda engajamento amplo da sociedade. Nesse cenário, Garrossini *et al.* (2023) apontam que o debate se estrutura em torno de dois blocos com visões antagônicas: enquanto o Supremo Tribunal Federal e forças progressistas advogam por maior controle e responsabilização das plataformas digitais, as grandes empresas de tecnologia e as bancadas conservadoras, majoritárias no Congresso Nacional, resistem a esse avanço regulatório.

Nessa direção, De Assis Cordeiro *et al.* (2024) evidenciam que a mitigação do fenômeno desinformacional requer a ponderação entre múltiplos direitos e garantias[22] bem como a observância das decisões do Supremo Tribunal Federal, como a que declarou a inconstitucionalidade do artigo 19 do Marco Civil da Internet, e dos desdobramentos legislativos em curso nas esferas administrativa e penal.

Oa autores concluem que a consolidação democrática e a preservação da lisura eleitoral no Brasil exigem uma abordagem multidimensional, que vai além dos ajustes no ordenamento jurídico-penal. Para os autores, é igualmente necessário que os responsáveis por episódios recentes sejam efetivamente responsabilizados, e que a superação desses desafios se construa por meio de uma atuação conjunta entre a sociedade civil, o poder público, as instituições e as plataformas digitais.

Para além do arranjo regulatório e sancionatório, a mitigação da desinformação exige políticas públicas de formação cidadã e de educação midiática. Nesse sentido, Castro e Cavalcante (2024), a partir de outros estudos, sistematiza cinco eixos de ação que deslocam o foco exclusivamente punitivo para uma estratégia de capacitação, participação e corresponsabilização entre Estado, escolas, sociedade civil e plataformas:

[22]Como a liberdade de expressão, o acesso à informação, a livre manifestação do pensamento, o direito à indenização por danos decorrentes de violações à intimidade, à vida privada, à honra e à imagem.

O eixo alfabetização midiática e informacional capilarizada[23] dialoga diretamente com a necessidade de romper rotinas de consumo em bolhas e de reduzir vulnerabilidades a *affordances* que privilegiam engajamento acrítico (Santos, 2024).

A elaboração de estratégias de mitigação exige uma abordagem multissetorial. Conforme resgatado por Castro e Cavalcante (2024), é imperativo que o Estado atraia a academia, a sociedade civil organizada e centros de excelência em pesquisa para formularem conjuntamente os protocolos de educação midiática e enfrentamento à desinformação.

O eixo formação docente e atualização curricular prevê a capacitação de professores do ensino fundamental e médio em alfabetização midiática, produção de materiais de apoio e inserção do tema nos currículos de jornalismo e de pedagogia. Em termos analíticos, esse eixo atua na base cultural do reforço comportamental (Souza *et al.,* 2023), ensinando práticas de checagem, comparação de fontes e reconhecimento de enquadramentos.

Na produção de conteúdos públicos e abertos incentiva-se a criação e difusão de recursos audiovisuais gratuitos para escolas e comunidades. A lógica é inundar o ecossistema com bens informacionais de qualidade, disputando atenção nos mesmos circuitos em que circulam conteúdos manipulados – inclusive nos aplicativos e formatos mais usados pelos estudantes.

Já no eixo fortalecimento da gestão democrática e dos laços comunitários, percebe-se que do ponto de vista da teoria das representações sociais (Castro; Cavalcante, 2024), trata-se de reduzir a objetivação do "inimigo" e criar espaços de exposição ao dissenso que diminuam a rigidez das ancoragens.

Em conjunto, esses eixos reorientam a política pública do controle a *posteriori* para a prevenção por competências, sem excluir responsabilização. Conectam-se, ainda, às respostas da sociedade civil as agências de *fact-checking,* as quais operam como instrumento imediato de verificação no *feed* (Luiz, 2023), enquanto as ações educativas ampliam a capacidade de uso dessas

[23]Conforme apontado pelo autor, o enfrentamento à desinformação requer uma ação estatal coordenada que transcenda o âmbito de um único ministério. É essencial instituir programas de letramento midiático que integrem o governo federal, os demais entes e a sociedade civil organizada em uma rede conjunta de cooperação.

checagens e incentivam a diversificação de fontes, condição necessária para sair das microesferas de auto-confirmação (Castro; Cavalcante, 2024).

Como aponta Luiz (2023), tais iniciativas adicionam uma camada de responsabilidade ao jornalismo contemporâneo. Diante da descentralização dos fluxos comunicativos – nos quais indivíduos, grupos e robôs operam como produtores e retransmissores de conteúdo –, o jornalismo também pode passar a exercer a função de aferidor da veracidade das informações que circulam em redes sociais e aplicativos de mensagens. Nesse sentido, a checagem de fatos torna-se, na *práxis*, um dos instrumentos mais imediatos de enfrentamento à desinformação, atuando como ponte entre a liberdade de expressão e a preservação da verdade no espaço público digital.

Em síntese, marco normativo, alfabetização midiática e *fact-checking* não são trilhas concorrentes, mas camadas complementares de uma mesma política de integridade informacional. Nesse sentido, abre-se a possibilidade de pesquisas futuras examinarem de modo sistemático a articulação desses mecanismos como instrumentos de prevenção à disseminação de desinformação e, sobretudo, de educação crítica para o uso consciente das mídias sociais, em consonância com suas *affordances*.

Além disso, identifica-se como lacuna a escassez de estudos comparativos que quantifiquem os resultados de políticas públicas implementadas em outros países para a contenção da desinformação. A análise de experiências externas poderia oferecer subsídios valiosos para a formulação de medidas preventivas mais eficazes no Brasil.

Considerações Finais

Como apresentado nas seções anteriores, neste trabalho, buscou-se o levantamento do que já vem sendo produzido pela academia para identificar, registrar e categorizar os enfoques predominantes sobre o evento de 8 de Janeiro. Desta forma, com o uso da metodologia de estado do conhecimento, foi possível construir o *corpus* de análise desta pesquisa a partir da seleção dos descritores escolhidos e dos critérios de seleção de base, estudos e de temporalidade definidos.

A identificação permitiu reconhecer setenta produções sobre o tema, divididas entre artigos, *policy brief*, resumos, capítulos de livro, dissertações, teses e livros, revelando uma grande quantidade de pesquisas acadêmicas de um evento recente na história brasileira. Isso demonstra a relevância do tema na academia reflexo do interesse da sociedade em compreender esse fenômeno.

O registro permitiu a organização do corpo de pesquisa com a produção da bibliografia anotada, facilitando a consulta e análise das produções identificadas e a categorização dessas. Essas etapas formaram a espinha dorsal da metodologia empregada e permitiram, após utilização de critérios de exclusão, a reflexão e síntese dos estudos classificados na subcategoria plataformas digitais e (des)informação

O Estado do Conhecimento realizado permitiu mapear não apenas a volumetria da produção acadêmica sobre o 8 de janeiro, mas, sobretudo, as disputas epistemológicas que permeiam sua interpretação. A análise qualitativa do eixo selecionado revela que a academia superou o estágio de diagnóstico do evento como baderna para compreendê-lo como um fenômeno de arquitetura sociotécnica.

A síntese dos achados aponta para uma convergência teórica crucial: o reconhecimento de que as *affordances* das plataformas e a lógica algorítmica proprietária atuaram como vetores de governança comportamental. Mais do que canais de comunicação, as redes operaram como câmaras de eco onde a radicalização foi monetizada e a violência simbólica, transmutada em ação física. A literatura indica, portanto, que o 8 de janeiro foi um produto do *design* atual das plataformas, que privilegia o engajamento polarizado em detrimento da esfera pública democrática.

A contribuição analítica deste estudo reside ainda na articulação sistêmica das lacunas e caminhos para a resposta democrática. Embora a literatura mais avançada já reconheça a necessidade de esforços conjuntos, o enfrentamento estatal à desordem informacional tem recaído, frequentemente, em medidas operacionais estanques e compartimentadas. A síntese aqui construída busca superar essa fragmentação prática: conclui-se que o marco normativo (regulação), a alfabetização midiática (educação) e o *fact-checking* (verificação) não são trilhas concorrentes, mas camadas complementares e interdependentes de uma arquitetura unificada de integridade informacional.

A alfabetização midiática capilarizada proposta por Castro e Cavalcante (2024), por exemplo, não substitui a necessidade de responsabilização jurídica conforme tratado por Lopez Pelaez e Mendonça (2024), mas fornece a imunidade cognitiva necessária para que a sociedade navegue pelas *affordances* das plataformas sem sucumbir aos seus vieses de confirmação. Da mesma forma, a checagem de fatos atua como contenção imediata no *feed*, enquanto a regulação impõe limites à arquitetura algorítmica proprietária que lucra com a desinformação

Portanto, para a agenda futura de pesquisa, sugere-se ultrapassar o diagnóstico do conteúdo das *fake news* para investigar a articulação sistêmica desses mecanismos. Ademais, a necessidade de aprofundar estudos comparativos internacionais indica a urgência de compreender como outras democracias consolidadas têm desenhado e integrado essas camadas de resposta institucional. O desafio que se impõe não é apenas punir os atos passados, mas desenhar um ecossistema digital onde a educação crítica e a regulação das plataformas operem em consonância para blindar a esfera pública contra novas ondas de radicalização algorítmica.

Referências

BERTANHA, M. de C.; DE ARAUJO, R .M. *Linha do tempo eleições presidenciais 2022*: evolução da rede social Twitter durante o 8 de janeiro de 2023. In: SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO (SBSI), 20., 2024, Juiz de Fora. *Anais [...].* Porto Alegre: Sociedade Brasileira de Computação, 2024. p. 339–344. Disponível em: https://doi.org/10.5753/sbsi_estendido.2024.238947. Acesso em: 29 abr. 2025.

BRASIL. Congresso Nacional. Comissão Parlamentar Mista de Inquérito dos Atos de 8 de Janeiro. R*elatório final da Comissão Parlamentar Mista de Inquérito dos Atos de 8 de Janeiro.* Brasília, DF, 2023. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento/download/264ac824-5d02-4463-b446-25eb22f4c96b. Acesso em: 20 maio 2025.

BRASIL. Gabinete do Interventor Federal na Segurança Pública do Distrito Federal. *Relatório sobre os fatos ocorridos no dia 8 de janeiro de 2023.*

Brasília, DF, 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/interventor-na-seguranca-do-df-apresenta-relatorio-sobre-ataques-de-8-de-janeiro. Acesso em: 25 maio 2025.

CASTRO, G. L. de; CAVALCANTE, C. V. Representações sociais sobre 8 de janeiro de 2023 no X (Twitter). *Contribuciones a las Ciencias Sociales,* [S. l.], v. 17, n. 10, p. e11310, 2024. Disponível em: https://doi.org/10.55905/revconv.17n.10-070. Acesso em: 29 abr. 2025.

CALZA, B. Collective action on WhatsApp and Telegram: the framings that laid the ground for the invasion of the Three Powers Plaza, Brazil, on January 8, 2023. *In:* VON BÜLOW, M.; AVRITZER, L.; SANTANA, E. (org.). *Democracy under attack.* Cham: Springer, 2024.

DE ASSIS CORDEIRO, G.; GIACOMINI CORREIA, H.; MUNARETTO PEREIRA, M.; MENDES FIRMIANO, N.; DE POLI, C. M. Fascistização, fake news e atos antidemocráticos no Brasil. *Caderno PAIC,* 2024. Disponível em: https://cadernopaic.fae.edu/cadernopaic/article/view/576. Acesso em: 30 abr. 2025.

EVANGELISTA, R.; QUARESMA, F. Uma espada de dois gumes. *Contracampo,* v. 43, n. 2, 2024. Disponível em: https://doi.org/10.22409/contracampo.v43i2.59707. Acesso em: 29 abr. 2025.

GARROSSINI, D. F.; SANTOS, F. A. dos; TONHÁ, J. V. A.; GUIMARÃES, P. H. E. O papel das redes sociais digitais na mobilização política. *Journal of Latin American Communication Research*, v. 11, n. 1, p. 34–48, 2023. Disponível em: https://doi.org/10.55738/journal.v11i1p.34-48. Acesso em: 29 abr. 2025.

GRISCHKE, L. L. "Festa da Selma". *Princípios,* [S. l.], v. 43, n. 170, p. 222–238, 2024. Disponível em: https://doi.org/10.14295/principios.2675-6609.2024.170.012. Acesso em: 29 abr. 2025.

LOPEZ PELAEZ, L. N.; MENDONÇA, D. L. de. Crimes cibernéticos e os limites da liberdade de expressão. *In:* CONGRESSO ACADÊMICO

CIENTÍFICO DO UNIFESO, 9., 2024, Teresópolis. *Anais [...].* Teresópolis: UNIFESO, 2024.

LUIZ, T. C. O combate à desinformação. *Galáxia*, v. 48, 2023. Disponível em: https://doi.org/10.1590/1982-2553202362879. Acesso em: 29 abr. 2025.

MARTINUZZO, J. A.; ANCIÃES DARRIBA, V. Terrorismo, ciberterritórios e fake news. *Liinc em Revista,* [S. l.], v. 19, n. 1, 2023. Disponível em: https://doi.org/10.18617/liinc.v19i1.6238. Acesso em: 29 abr. 2025.

MATSUDA, W. T.; CASELI, H. de M.; VALEJO, A. D. B.; IASULAITIS, S. Câmaras de eco políticas. P2P e *Inovação,* v. 11, n. 2, 2025. Disponível em: https://doi.org/10.21728/p2p.2025v11n2e-7398. Acesso em: 29 abr. 2025.

MENDES, C. M.; SANGLARD, F. N.; COSTA, V. S. da. Desinformação e democracia. Estudos *Semióticos*, v. 20, n. 2, p. 119–136, 2024. Disponível em: https://doi.org/10.11606/issn.1980-4016.esse.2024.218951. Acesso em: 29 abr. 2025.

MOROSINI, M. C.; FERNANDES, C. M. B. Estado do conhecimento. *Educação Por Escrito*, v. 5, n. 2, p. 154–164, 2014.

MOROSINI, M. C.; NASCIMENTO, L. M. do; NEZ, E. de. Estado de conhecimento: metodologia na prática. *Revista Humanidades e Inovação,* v. 8, n. 55, p. 70–81, 2021.

QUEIROZ BARBOZA, E. M. de; SOUZA, C. B. M. de. Democracia em risco. In: IMMORDINO, M.; GULLO, N.; CELONE, C. (org.). D*emocrazia diritti umani e sviluppo sostenibile.* Napoli: Editoriale Scientifica, 2024.

ROTA, A. R.; NICODEMO, T. L. Arquivos pessoais e redes sociais. *Estudos Históricos*, v. 36, n. 79, p. 44–67, 2023.

SANTOS, V. V. V. dos. Big techs e algoritmos. *Revista Linguagem em Foco,* v. 15, n. 3, p. 97–114, 2024.

SCHEREN, M. L.; RODRIGUES, V. S.; LÓPEZ ZAMORA, G. D.; CESARINO, L.; NASCIMENTO, L. F.; FONSECA, P.; BARRETO, T. Métodos mistos para a antropologia digital. *Horizontes Antropológicos,* v. 30, n. 68, 2024. Disponível em: https://doi.org/10.1590/1806-9983e680407. Acesso em: 29 abr. 2025.

SILVA, L. J.; ARAUJO, R. M. de; CORREA, A. G. D. Pipeline para monitoramento de discussões políticas*. In*: BRAZILIAN WORKSHOP ON SOCIAL NETWORK ANALYSIS AND MINING (BRASNAM), 13., 2024, Brasília. *Anais [...].* Porto Alegre: Sociedade Brasileira de Computação, 2024.

SOUZA, D. M. M.; BORGES, E. E.; SOUZA, F. M. dos S.; MARQUES, M. L. F.; BORRI, V. Comportamento em redes sociais. *Cuadernos de Educación y Desarrollo*, v. 15, n. 7, 2023.

SOUZA, R. M. V. de; LEAL, M. de J. D. R. *Redes sociais e desinformação. Journal of Latin American Communication Research*, v. 11, n. 1, p. 4–17, 2024.

Competências em inteligência artificial e ensino profissional em segurança e defesa: articulações conceituais e experiências na Escola Superior de Defesa

Aline Barbosa Xavier Muniz
Patrícia Pontes Bezerra
Lorena Hermenegildo de Oliveira

Introdução

A pesquisa parte da constatação decisiva de que as novas ferramentas digitais capazes de produzir textos, resumos e sugestões em poucos segundos já fazem parte do cotidiano acadêmico e profissional, e seu impacto não se limita à velocidade de execução de tarefas. Em instituições voltadas à Segurança e Defesa, em que o rigor metodológico e a responsabilidade pública são valores estruturantes, essas ferramentas introduzem oportunidades e riscos que precisam ser tratados com métodos, critérios e orientação pedagógica.

Nesse diapasão, as competências no uso das tecnologias para o ensino profissional em Segurança e Defesa fomentam discussões que envolvem a capacitação, as legislações e as ações práticas de integração da inteligência artificial generativa (IAGen) no processo formativo. Em termos acessíveis, trata-se de entender que "saber usar" mobiliza conhecimentos, habilidades, atitudes e valores em situações reais. Para isso, investiga-se como preservar a "voz autoral" e o pensamento crítico no processo de escrita quando há apoio de tecnologias que estruturam argumentativas ou revisões de texto.

A discussão aborda a conjuntura jurídica brasileira quanto ao impacto da IA na sociedade, especialmente no tocante ao emprego da tecnologia nas rotinas educativas no campo da Defesa que, por sua natureza particular e imprescindível, demanda diretrizes claras de autorregulação e de políticas internas. Aproxima essas discussões da experiência concreta da Escola Superior de Defesa (ESD), descrevendo iniciativas recentes que funcionam como laboratório institucional

de aprendizagem. Esses exemplos conduzem a caminhos possíveis para integrar inovação pedagógica com cultura institucional, liderança e planejamento.

Nesse ensejo discursivo, as temáticas são relevantes para o transcurso formativo do profissional em Segurança e Defesa, que esteja alinhado às mudanças tecnológicas e preserve o sentido amplo da ação educativa, que é promover conhecimento para transformar a sociedade.

A importância das competências para o uso da IAGen

As máquinas fascinam o ser humano há séculos e, com o avanço tecnológico, passaram a potencializar a produtividade das atividades humanas. O deslumbramento diante dessas novas tecnologias articula-se à ideia de Ser, Fazer e Pensar em maior escala — isto é, de um humano progressivamente mais produtivo. Tal perspectiva pode abarcar a realização mais célere de tarefas, a redação mais ágil de artigos ou a análise acelerada de dados em investigações científicas. Contudo, não se pode perder de vista que o *fazer humano* deve permanecer no centro das ações colaborativas que envolvem o uso de inteligências artificiais generativas, uma vez que nuances interpretativas, percepções contextuais e juízos ponderativos constituem atributos genuinamente humanos (Mollick, 2025).

Nesse devir epistemológico, as reflexões sobre o uso responsável, ético, com voz autoral e singularidade de escrita estão no centro das publicações que tratam do tema do uso da IAGen no campo da educação. Dentro dessas investigações, este estudo se limitará, neste primeiro momento, a dois atributos da discussão: i) competências no uso da IAGen para a escrita científica; e ii) o *prompt* como uma forma de comunicação com a IAGen.

As competências são compreendidas como a articulação entre conhecimentos, habilidades, atitudes e valores que, integrados, constituem estruturas cognitivas orientadoras do uso da IAGen. O conceito de competência adotado nesta investigação filia-se à corrente construtivista, por compreender que tais dimensões emergem da interação entre o indivíduo e os processos de construção do conhecimento, concretizando-se em ações efetivamente competentes (Bezerra; Muniz, 2024). A relação entre competências e o uso da IAGen na escrita científica tem sido explorada em diversos estudos, especialmente por meio da formulação de quadros referenciais de competências

que articulam saberes essenciais à utilização crítica e qualificada dessas tecnologias (Burneo *et al.,* 2025; Chiu, 2025).

Com base em uma análise qualitativa da pesquisa bibliométrica (Moresi, 2022) com a expressão de busca "*Generative Artificial Intelligence" OR "enerative AI" OR "ChatGPT" OR "generative pre-trained transformer" OR "genai") AND "scientific writing" OR "academic writing" OR "scholarly writing" OR "research writing"AND "competenc*" OR "skills" OR "literacy" OR "AI literacy" OR "digital competenc*"AND "professional education" OR "vocational education" OR "higher education" OR "military education" OR "defense education" OR "security studies",* foi obtido um total de 93 (noventa e três) documentos que, após a delimitação excepcionando a área médica e limitando o tipo de documento em artigo, artigos de conferência e artigos de revisão, resultou em 76 (setenta e seis) documentos.

A partir das palavras-chave dos artigos foram elencados dois grupos, o primeiro referente a competências e o segundo a IAGen. Grupo 1: competência; habilidade; literacia; proficiência; quadro de competências; autorregulação; competência digital; pensamento crítico e avaliação. E o grupo 2: IAGen; ChatGPT e LLM. Esses grupos foram determinantes como critério de inclusão dos artigos selecionados com a presença de pelo menos um dos termos de cada grupo. Foram selecionados desta maneira 15 artigos que fundamentaram um quadro de competências norteadoras da pesquisa.

O quadro de competência apresenta seis domínios com três competências associadas que, a partir de ações de mapeamento na Instituição, podem gerar capacitação do corpo permanente. Além das dimensões e competências, foi incluída uma relação com a escrita científica no campo da Segurança e Defesa, ou seja, como essas competências descritas podem impactar a pesquisa dentro do campo específico.

Quadro 1 – Matriz de Competências em IAGen aplicadas ao campo da Segurança, Desenvolvimento e Defesa - SDD (continua)

Dimensão	Competência	Alinhamento de conteúdo	Aplicabilidade no campo da SDD
AI Literacia	Compreensão estrutural	Funcionamento básico de LLMs;	Interpretação qualificada de *outputs* em análises estratégicas
	Limitações epistemológicas	Reconhecimento de alucinações; Identificação de vieses;	Mitigação de riscos informacionais;
	Consciência sistêmica	Impacto da IAGen na produção do conhecimento;	Adequação de protocolos institucionais;
Competência Técnica de Interação	Formulação de comandos	Clareza; Contextualização; Definição de objetivo	Uso estruturado da IAGen em análises estratégicas.
	Iteratividade estratégica	Refinamento progressivo;	Redução de ambiguidades em cenários críticos;
	Controle de *output*	Parametrização de formato	Adequação a normas técnicas institucionais
Competência Cognitiva-Crítica	Avaliação de Conteúdo	Checagem factual; Consistência argumentativa	Validação de informações em contextos sensíveis
	Pensamento independente	Capacidade de discordar do *output*	Preservação da autonomia decisória;

Dimensão	Competência	Alinhamento de conteúdo	Aplicabilidade no campo da SDD
Competência em Produção Acadêmica Mediada por IAGen	Planejamento assistido	Organização argumentativa	Produção de artigos com temas estratégicos;
	Revisão e Refinamento	Melhoria de coesão; Correção gramatical crítica	Aprimoramento de feedback;
	Integração autoral	Manutenção da voz acadêmica;	Garantia de autoria responsável em documentos estratégicos
Competência Ética e Integridade Acadêmica	Transparência	Declaração de uso da IAGen;	Uso responsável em ambientes de informação sensível
	Responsabilidade acadêmica	Diferenciação entre auxílio e substituição	Conformidade com padrões éticos institucionais
	Conformidade institucional	Respeito a políticas de segurança informacional	Observância de protocolos informacionais
Autorregulação e Governança do Uso da IA	Gestão da Dependência	Evitar substituição cognitiva contínua	Uso controlado em ambientes de alto risco
	Metacognição	Reflexão sobre quando usar IAGen;	Desenvolvimento de autonomia intelectual estratégica
	Planejamento Estratégico de Uso	Escolha adequada da ferramenta	Uso seguro da IA em cenários de escrita no campo SDD.

Fonte: Elaborado pelos autores (2026).

A análise dos documentos selecionados evidencia que o debate sobre o uso da IAGen no ensino superior tem transitado entre uma abordagem instrumental para uma perspectiva centrada em competências, de modo que a disponibilidade de ferramentas como ChatGPT não garante melhoria na aprendizagem. O fator determinante é, em verdade, o desenvolvimento de

uma literacia em IA, compreendida como a capacidade de entender o uso da ferramenta a partir de implicações epistemológicas da tecnologia (Kim, 2025; Deep; Chen, 2025)

A literacia em IAGen inclui uma compreensão técnica, avaliação crítica e consciência ética, o que gera a necessidade de compreender o funcionamento básico dos modelos de linguagem para evitar uma relação acrítica com os *outputs*, que podem gerar a dependência cognitiva (Hossain; Biswas; Khan, 2025). Assim, essa competência aparece como essencial (*core competency*) para uso acadêmico responsável da IAGen (Fitzek; Bârgăoanu, 2025; Nwagbara, 2025).

O pensamento crítico aplicado à avaliação de conteúdo gerado por IAGen demonstra que o uso orientado da ferramenta pode fortalecer habilidades analíticas, desde que mediado pedagogicamente e, por outro lado, o uso superficial pode comprometer a integridade acadêmica e reduzir o engajamento cognitivo. O mesmo ponto é reforçado por Gonzales et al., (2025) ao indicar que estudantes que avaliam criticamente os *outputs* apresentam maior autonomia intelectual. Dessa forma, a competência crítico-cognitiva envolve verificar fatos, identificar incoerências e julgar a adequação epistemológica das respostas geradas.

No campo da produção textual, a IAGen pode apoiar planejamento, organização e revisão textual (Dinh, 2025), mas a voz autoral é um fator nevrálgico que deve ser observado. Em uma atitude metacognitiva, uma das ações é comparar seus próprios textos, antes e depois do uso da IAGen e questionar sua autoidentificação na linguagem. O indivíduo se vê no texto escrito, tem sua perspicácia autoral analisada e constata se a sua escrita se mantém fiel a sua voz autoral.

Assim, a competência textual mediada por IAGen não se reduz à melhoria estilística, mas envolve integração consciente da ferramenta ao processo argumentativo. A dimensão ética e de integridade acadêmica aparece de forma transversal quando se discute a necessidade de redefinir critérios avaliativos diante da presença da IAGen, da regulação por princípios de equidade e de transparência e a necessidade de políticas institucionais claras para orientar práticas éticas. Dessa forma, a competência ética envolve distinguir apoio legítimo de substituição indevida, declarar o uso da ferramenta e respeitar normas institucionais (Kim; Danilina, 2025; Zhao; Cox; Chen, 2025).

Esse ecossistema que interliga humano/IAGen na atividade acadêmica, especificamente na escrita científica no campo da educação profissional em Segurança e Defesa, agrega dimensões que não operam isoladamente. Forma-se um constructo de competências, no qual o domínio técnico precisa ser equilibrado por maturidade cognitiva e compromisso institucional. O desafio contemporâneo está posto, não há como proibir o uso da IAGen, mas o caminho é estruturar trilhas de aprendizagem que preservem a autonomia intelectual e fortaleçam a qualidade da produção acadêmica.

Esses caminhos formativos sugerem correlações com ações transversais na instituição que podem incluir desde a validação das competências apresentadas a cursos de capacitação, ações formativas diversas, incentivos a capacitações externas, participação em eventos direcionados às reflexões sobre o uso da IAGen no ambiente acadêmico.

Dessa maneira, as competências atuam como norteadoras de políticas internas sobre o uso da IAGen na escrita científica e trazem um arcabouço conceitual de dimensão construtivista das competências, alinhando aos objetivos organizacionais e aos anseios individuais que permeiam o uso responsável da IAGen no campo investigativo da Segurança e Defesa.

Prompt: uma comunicação assertiva humano/IAgen

Os processos de iteração com a IAGen pressupõem diálogos conversacionais que vão além de uma simples pergunta e resposta. A iteração é um devir comunicacional entre homem e IAGen com o objetivo de fortalecimento colaborativo (Molenaar, 2022). É um ecossistema, um ciclo de ações interagir-analisar-reformular-interagir. Neste complexo conversacional, o humano é o centro do processo e a IAGen atua como um agente colaborativo.

Nesse conceito de iteração, a formulação de um *prompt* é o caminho para diálogos produtivos, "um *prompt* é um texto de entrada (*input*) que direciona o padrão de resposta do modelo de IAGen, podendo conter instruções, contexto histórico ou metodológico, exemplos de conteúdo desejado e até restrições de formatação" (Sampaio; Figueiredo, 2025, p.12). Existem diversas técnicas de construção de *prompt*, *zero-shot, one-shot, contextual prompting, self-consistency* (Boonstra, 2025). A técnica da cadeia de pensamento é uma delas e consiste em fornecer ao modelo exemplos contendo pares estruturados de

entrada, etapas intermediárias de raciocínio e resposta final, a ideia é separar o raciocínio em etapas (decompor) como normalmente se resolve um problema matemático (Knoth et al., 2024).

Wei *et al*. (2022) demonstram que essa estratégia potencializa o desempenho de modelos de larga escala em tarefas de raciocínio aritmético, simbólico e de senso comum, sobretudo quando ultrapassam aproximadamente 100 (cem) bilhões de parâmetros. O uso da cadeia de pensamento pode resultar em ganhos de desempenho, transparência do processo decisório e, quando relacionado a rastreabilidade, facilita o envio de dados estruturados por diálogos.

Então, a ferramenta de IAGen pode entender melhor quando conversamos usando a técnica? A resposta é sim, pois o autor reforça que são incluídas etapas intermediárias e são fornecidas janelas interpretáveis, ou seja, a IAGen pode filtrar soluções erradas e fornecer apenas as corretas, podendo ser facilmente adaptável por meio da linguagem humana e, por fim, todas as IAGen respondem bem a este tipo de *prompt*. Nesse sentido, a comunicação Humano/IAGen para se tornar assertiva, pode se utilizar desta técnica de *prompt* que inclui dentre outros aspectos, a clareza, a especificidade e o contexto (Sampaio; Figueiredo, 2025).

Entretanto, o papel do humano não pode se reduzir a criar formas de comunicação com a IAGen, mas estar no centro do processo criativo da escrita científica e da comunicação de forma mais ampla (Mollick, 2025). Para tanto, diversas revistas científicas possuem orientações claras de transparência, rastreabilidade e formas de uso da IAGen nas produções acadêmicas, o que fortalece a estrutura de rigor, de autoria e de liberdade acadêmica.

Para além das revistas e eventos de divulgação científica, são necessárias legislações, orientações governamentais e direcionamentos institucionais que deem conta dessa inovação nos processos educacionais e possam conduzir ao uso equitativo, humanizado, e que a IAGen seja um elemento para diminuir desigualdades, fortalecer as redes de pesquisa e fomentar a ciência para a humanidade.

Marcos regulatórios:documentos normativos em IA

O uso da Inteligência Artificial é uma temática da qual toda a comunidade internacional se encontra em fase de adaptação, especialmente no tocante à

legislação para regulamentar os limites, as diretrizes e as responsabilidades pelo seu mau uso. Até o momento, o Brasil não possui lei em sentido estrito que regule de forma apropriada o uso de Inteligência Artificial (IA) nos diversos âmbitos de sua aplicabilidade, permanecendo as discussões sobre sua regulamentação no nível de projeto de lei.

O Projeto de Lei nº 2338 foi proposto em 03 de maio de 2023 no Plenário do Senado Federal – o primeiro a ser proposto sobre a temática –, o qual, em seu artigo 1º, §1º, inciso II, excepciona os regramentos ali dispostos às tecnologias desenvolvidas e utilizadas única e exclusivamente para fins de defesa nacional (Brasil, 2025). Isto é, o referido projeto volta-se para a regulamentação da IA no sentido de conferir proteção a direitos individuais, notadamente quanto às temáticas de direito do consumidor, direito de saúde, do comércio em geral, do exercício empresarial, das responsabilizações cíveis, dentre outros aspectos afastados do campo da Segurança e Defesa nacional

No mesmo sentido, tramita na Câmara dos Deputados o segundo projeto já apresentado – o Projeto de Lei nº 1797 –, proposto em 14 de maio de 2024, com vistas a estabelecer normas gerais para o desenvolvimento, a implementação e o uso responsável da Inteligência Artificial, tendo, inclusive, atribuído definição legal à IA:

> Art. 2º (...)
> Parágrafo único. Define-se como inteligência artificial a habilidade de um sistema computacional com diferentes graus de autonomia e adaptabilidade após sua implantação, desenhado para inferir como atingir um dado conjunto de objetivos, explícitos ou implícitos, por meio de dados de entrada provenientes de humanos ou de máquinas, com o objetivo de produzir previsões, conteúdos, recomendações ou decisões que possam influenciar o ambiente virtual ou real, nos termos da regulamentação. (Brasil, 2024)

No mesmo projeto, em seu artigo 6º consta a criação do Conselho Nacional sobre Inteligência Artificial, classificado como órgão consultivo interministerial, coordenado pelo Ministério da Justiça e Segurança Pública, contando com a integração da Autoridade Nacional de Proteção de Dados, do Banco Central do Brasil, da Casa Civil da Presidência da República, do Ministério do Desenvolvimento, Indústria, Comércio e Serviços, da Advocacia-Geral da União, e da Ordem dos Advogados do Brasil (Brasil, 2024).

Em 31 de janeiro de 2025, foi proposto no Senado o Projeto de Lei nº 04/2025 que, ao fazer alterações substanciais no Código Civil, criou um Capítulo disciplinando a Inteligência Artificial. No entanto, limita-se o texto a dispor acerca da não discriminação em relação às decisões, às condições de transparência e de governança, atribuição de responsabilidade civil, dentre outros princípios e regras não aplicáveis à Segurança Nacional.

Não obstante a preocupação legislativa em regulamentar a aplicação da IA no âmbito do direito do consumidor, do direito penal, do direito administrativo, dentre tantos outros segmentos, resta evidenciado que a Defesa Nacional possui um regime de excepcionalidade, o que transfere ao Ministério da Defesa e às instituições militares a responsabilidade de autorregulamentação de suas tecnologias disruptivas.

Para suplantar a falta de legislação em sentido estrito, assim como várias instituições e órgãos brasileiras,[1] o Ministério da Defesa expediu a Portaria nº 3.063/GM/MD, de 22 de julho de 2021, atuando como o sucedâneo disciplinador da Política de Ciência, Tecnologia e Inovação de Defesa ao estabelecer que o desenvolvimento de capacidades operacionais deve estar intrinsecamente ligado ao fortalecimento do ensino e da pesquisa (Brasil, 2021).

Esta norma centraliza a necessidade de formação de competências voltadas para a autonomia tecnológica, um conceito que permeia a educação profissional ao exigir que o militar não seja apenas um operador de sistemas, mas um gestor do conhecimento capaz de garantir a soberania nacional diante de algoritmos de alta complexidade (Brasil, 2021).

No mesmo ato normativo, conferiu às Forças Armadas o dever de editar "atos específicos complementares para a implementação da Política de Ciência, Tecnologia e Inovação de Defesa de que trata esta Portaria" (Brasil, 2021).

Cumprindo tal determinação, a Marinha do Brasil, por meio da Portaria nº 122/CTMRJ, de 30 de junho de 2023, estabeleceu as diretrizes da Política de Inovação do Centro Tecnológico da Marinha no Rio de Janeiro (CTMRJ). Foi atribuído ao órgão de gestão tecnológica a incumbência de educação técnica e profissional que promova a capacitação em tecnologias críticas e a gestão da propriedade intelectual (Brasil, 2023).

[1]Vide o Ato Normativo nº 808, do Superior Tribunal Militar.

Enquanto Instituição Científica, Tecnológica e de Inovação, o CTMRJ, preconiza que o ensino profissional deve ser pautado na interação entre pesquisadores e o setor produtivo, facilitando a transferência de tecnologia e o desenvolvimento de sistemas de IA voltados à engenharia naval e defesa cibernética (Brasil, 2023). A norma enfatiza que o capital intelectual da instituição deve ser incentivado por meio de estímulos à pesquisa e ao desenvolvimento, consolidando um ambiente de ensino onde a inovação não é acessória, mas componente estruturante da carreira militar naval.

Na Força Aérea Brasileira, a educação profissional em segurança e defesa é regida por normas que fortalecem o ecossistema de inovação aeroespacial. A Portaria UNIFA nº 70/AGI, de 14 de dezembro de 2023, aprova a Política de Inovação da Universidade da Força Aérea, definindo diretrizes para a organização e gestão dos processos de inovação tecnológica (Brasil, 2023).

A Universidade da Força Aérea, ao atuar como o centro de pensamento estratégico da Aeronáutica, estabelece que sua política deve estimular o empreendedorismo e a proteção das criações inovadoras dentro dos seus currículos de pós-graduação. Isso significa que o ensino profissional para os oficiais da FAB passa a exigir competências em gestão da inovação, no qual a IA é tratada como um ativo de capital intelectual.

Complementando esta visão, a Portaria CCA-SJ nº 55/AFPI, de 29 de maio de 2025, do Centro de Computação da Aeronáutica de São José dos Campos, foca na atualização das práticas de desenvolvimento e cooperação para inovação, sendo uma organização técnica de grande avanço para a defesa nacional, orientando que a educação profissional deve focar no desenvolvimento sustentável de softwares e na segurança da informação, competências imprescindíveis para o uso seguro de IAGen em missões de comando e controle (Brasil, 2025).

No Exército Brasileiro, a Portaria EME/CEx nº 1.318, de 14 de maio de 2024, aprovou a Diretriz Estratégica de Inteligência Artificial, materializando a aplicação prática desses conceitos no ensino militar (Brasil, 2024). A diretriz preconiza que a educação profissional deve fomentar a compreensão da IA como um sistema de suporte à decisão que opera com variados graus de autonomia, mas que jamais poderá substituir o juízo crítico humano (Brasil, 2024).

Esta correlação educacional é fundamental, pois estabelece que a formação do militar deve incluir a correta análise de dados e o emprego ético dos algoritmos, de modo a preparar o militar para supervisionar processos de inferência que possam influenciar tanto o ambiente virtual quanto o real. O Exército Brasileiro, ao normatizar o uso de IA, impõe ao seu sistema de ensino o desafio de integrar a inovação com a doutrina militar tradicional, garantindo que o uso de ferramentas de IAGen ocorra sob o princípio da centralidade da pessoa humana e da segurança de infraestruturas críticas.

Assim, a correlação entre as políticas de inovação da UNIFA, do CTMRJ e do CCA-SJ, somadas às diretrizes do Ministério da Defesa e do Exército, revelam que o ensino profissional em Segurança e Defesa nas Instituições Militares está sendo reconfigurado para o século XXI.

As normas convergem para a criação de um militar altamente qualificado, cuja formação técnica em IA é acompanhada por uma sólida base em ética e segurança jurídica, na qual a integração desses marcos regulatórios assegura que o desenvolvimento de sistemas inteligentes nas Forças Armadas seja acompanhado por um processo educacional contínuo, capaz de absorver as rápidas transformações tecnológicas sem comprometer os princípios de proteção dos direitos humanos e de soberania nacional.

Desse modo, a educação profissional emerge não apenas como um processo de instrução, mas como uma ferramenta estratégica de defesa, onde a literacia em IA e a inovação tecnológica são os novos requisitos para o exercício do poder nacional em ambientes cada vez mais automatizados e complexos.

Práticas pedagógicas no uso da IAgen na educação profissional em Segurança e Defesa

O caminho percorrido que possibilita tornar um conhecimento escolar envolve o fazer pedagógico. É nesse sentido que é possível descrever uma "cultura escolar", na qual se identificam conceitos, linguagem, papéis e regras próprias. O contexto no qual essa cultura é, ao mesmo tempo reificada e fortalecida é a escola, sendo, portanto, "uma organização com identidade própria, marcada por uma cultura que resulta da história, das tradições, das práticas e das interações dos seus atores." (Nóvoa, 1995, p.28).

A análise da apropriação do uso da IAGen em uma cultura escolar específica — no caso, o campo da Educação Profissional em Segurança e Defesa — será realizada por meio da descrição das práticas pedagógicas desenvolvidas na Escola Superior de Defesa nos últimos três anos. Importa destacar que o campo da Segurança e Defesa é profundamente impactado por um ambiente caracterizado como volátil, incerto, complexo e ambíguo (VUCA), conceito difundido no âmbito estratégico a partir do final do século XX, especialmente em contextos militares e organizacionais (Whiteman, 1998). Nesse enquadramento, volatilidade refere-se à velocidade e intensidade das mudanças; incerteza, à imprevisibilidade dos eventos; complexidade, à multiplicidade de variáveis interdependentes; e ambiguidade, à dificuldade de interpretação dos cenários e de suas possíveis consequências.

Como decorrência, instituições formativas inseridas nesse ecossistema não apenas precisam responder com celeridade aos estímulos externos, mas desenvolver capacidades adaptativas, cognitivas e decisórias compatíveis com tais dinâmicas. Nesse cenário, a incorporação da IAGen nas práticas pedagógicas não representa mera inovação tecnológica, mas configura-se como estratégia formativa orientada à preparação de profissionais capazes de atuar de maneira crítica, responsável e competente em ambientes de elevada instabilidade e transformação contínua.

Dandeker (1994) afirma que a capacitação dos tomadores de decisão pode proporcionar uma atuação que vai além de uma gestão da violência e a Educação Profissional em Segurança e Defesa desenvolvida na Instituição é envolta de valores que despertam o saber crítico, o rigor acadêmico e a pesquisa científica direcionada a temas de interesse Nacional. O Ensino de Defesa, neste ambiente escolar, é amparado pelo conceito mais amplo da Educação de Segurança e Defesa.

Os primeiros passos nas competências no uso de IAgen

A Escola Superior de Defesa (ESD) foi criada em 1º de outubro de 2021, por meio do Decreto Presidencial n° 10.806, de 23 de setembro de 2021. A instituição, ligada ao Ministério da Defesa (MD), realiza estudos, pesquisas, extensão, difusão, ensino e intercâmbio, em temas de interesse da Defesa Nacional, com foco prioritário nos servidores civis dos Poderes Executivo,

Legislativo e Judiciário e de instituições de interesse da Defesa, atendendo, também, os militares das Forças Armadas e Auxiliares.

Uma Instituição cuja missão é "desenvolver atividades acadêmicas em temas de interesse da Defesa Nacional, considerados os campos de segurança e desenvolvimento" é instada por diversos *stakeholders* a incorporar temáticas em seu processo de ensino. No caso das competências no uso de IAGen não se trata apenas de uma nova temática, mas de uma mudança paradigmática que atinge todos os campos sociais, com impactos sem precedentes. Assim, o primeiro processo foi direcionar os olhares aos docentes e discentes da escola, a partir do reconhecimento dos marcos legais e teóricos que já foram construídos sobre competências e IAGen e apresentados na seção anterior deste capítulo.

A abordagem inicial foi realizada a partir do reconhecimento dos espaços de formação continuada já existentes na instituição. A ESD possui em seu calendário escolar uma atividade intitulada Semana Pedagógica, cuja finalidade é "familiarizar os docentes da Escola Superior de Defesa (ESD) com modernas práticas pedagógicas e padronizar procedimentos para a condução do ano letivo".

Assim, em 2022, a primeira semana pedagógica tratou de Inovação e o campo da Defesa; em 2023 Competências e o Ensino de Defesa; em 2024 Inteligência Artificial (IA) e Ambiente Virtual de Aprendizagem (AVA) Moodle; em 2025 Competências em IA para a escrita acadêmica e, finalmente em 2026 Orientação de Trabalhos de Conclusão de Curso em tempos de IA. Considerando que a ESD tem cinco anos de existência, em quatro desses anos a temática em IA foi objeto das reflexões do corpo docente.

Uma outra atividade significativa do processo de desenvolvimento das competências de uso em IAGen foi a promoção de Oficinas de Ferramentas em IA. A partir de 2024, foram idealizadas e executadas as oficinas destinadas em um primeiro momento aos docentes e, em seguida, aos discentes. Fruto dessas ações, a ESD incorporou no principal documento normativo destinado aos discentes, o "Guia do Aluno", a previsão do uso da IA para elaboração dos trabalhos de conclusão de curso.

As atividades de capacitação mostraram-se significativas para o desenvolvimento de competências no uso da IAGen, à luz da perspectiva construtivista de Philippe Zarifian (2001), segundo a qual a competência se

constitui na mobilização responsável de saberes diante de situações concretas de trabalho. Nessa abordagem, o "evento" — entendido como aquilo que irrompe no cotidiano profissional e exige interpretação e resposta — torna-se elemento central para a produção da competência, pois convoca o sujeito a agir com autonomia e discernimento. Assim, o uso da IAGen não se reduz à apropriação técnica de uma ferramenta, mas configura-se como um campo de eventos que demandam responsabilidade, julgamento e tomada de decisão. Desse modo, o desenvolvimento de competências implica simultaneamente o crescimento organizacional e o fortalecimento dos indivíduos, ampliando sua capacidade de responder de forma crítica e ética aos desafios emergentes do trabalho mediado por tecnologias inteligentes.

A transposição didática na educação profissional em Segurança e Defesa

A ciência da informação propõe uma cadeia conceitual entre dado, informação e conhecimento, cuja hierarquia já foi superada por Nonaka e Takeuchi (1995), a partir da conversão do conhecimento tácito em explícito. A forma caótica com que os dados chegam a alunos e professores parece colocar em xeque o trabalho pedagógico. No entanto, a análise pretendida neste capítulo é que se trata muito mais de acompanhar e prospectar do que controlar e negar o processo de apropriação e uso ético e consciente dos conhecimentos obtidos e gerados pela IAGen. O que não significa que algumas perguntas não surjam, dentre elas, como saber que foram os alunos os autores dos trabalhos; como manter o pensamento crítico diante das reflexões que são propostas nas aulas; como verificar que as entregas foram realmente feitas pelos alunos.

Os docentes e equipe pedagógica imbuídos das formações oferecidas, das ferramentas didáticas e do objetivo de manter o papel inalienável do ensino de Defesa promoveram mudanças nas práticas anteriormente adotadas. As disciplinas dos cursos não somente permitiram o uso das ferramentas de IAGen, como também consideram o uso como parte desse processo, inclusive para a escrita do trabalho de conclusão de curso existente em três dos onze cursos da ESD. Ressalta-se que a transposição didática aqui apresentada é ancorada no conceito de Chevallard, para o qual:

> Um conteúdo de saber, ao ser designado como saber a ensinar, sofre um conjunto de transformações adaptativas que o tornam apto a ocupar um lugar entre os objetos de ensino. O trabalho que transforma um objeto de saber a ensinar em objeto de ensino chama-se transposição didática (1991, p. 39).

O trabalho de transposição didática envolve, portanto, uma prática docente de apropriação crítica e adaptação das atividades pedagógicas já consolidadas na ESD. Nesse sentido, destacam-se materiais previamente produzidos e ofertados aos discentes, como: vídeos instrucionais, totalmente elaborados por IAGen; avatares criados também por IAGen; além de etapas orientadas de escrita acadêmica para os trabalhos de conclusão de curso com o emprego de ferramentas de IA. Tais iniciativas demandaram intenso engajamento da equipe pedagógica, que, por meio da atuação articulada com docentes e discentes, buscou constituir um ambiente formativo favorável às adaptações necessárias, preservando, simultaneamente, a identidade institucional. Assim, a inovação tecnológica não se sobrepõe à cultura escolar, mas a tensiona criativamente, reafirmando que a centralidade do processo educativo permanece no agir pedagógico intencional.

Considerações Finais

A incorporação de novas ferramentas digitais de apoio à escrita, à organização de ideias e à produção de conteúdo no ensino profissional em Segurança e Defesa é uma questão acadêmica e institucional. Observa-se que o uso qualificado desses recursos depende da formação de quem a utiliza, significando desenvolver capacidades de leitura crítica, verificação de informações, clareza na comunicação, responsabilidade sobre o que se escreve e consciência dos limites do apoio tecnológico. Em contextos ligados à Segurança e Defesa, essa exigência é premente, pois a qualidade da análise, a precisão dos argumentos e o cuidado com informações sensíveis são elementos que possuem relevância institucional.

Nesse sentido, a experiência apresentada pela Escola Superior de Defesa é relevante por demonstrar um caminho possível: começar com ações formativas, promover o debate interno, ajustar normas e acompanhar práticas reais de uso. Esse movimento gradual favorece aprendizado institucional e evita tanto a adoção irrefletida quanto a rejeição improdutiva.

Para avançar, algumas ações se mostram estratégicas, tais como consolidar programas permanentes de capacitação para docentes e discentes; estabelecer orientações sobre transparência no uso dessas ferramentas em trabalhos acadêmicos; criar critérios de avaliação que valorizem o raciocínio, a autoria e a justificativa das escolhas; e incentivar materiais didáticos e exercícios voltados à análise crítica de conteúdos produzidos com apoio digital. É recomendável, também, manter espaços de observação e revisão contínua das práticas, de modo que a instituição possa ajustar suas normas e métodos diante de novos desafios.

Dessa forma, a inovação no ensino profissional em Segurança e Defesa precisa estar vinculada à formação crítica, à responsabilidade institucional e ao compromisso com a qualidade acadêmica. É nessa convergência entre prudência, ensino e propósito público que se encontra a principal contribuição desta agenda para o campo da Segurança e Defesa.

Referências

BEZERRA, P.P.; MUNIZ, A.B.X. Explorando a evolução do conceito de competências: da teoria à prática. *In:* CAMINHA,V. M.; NASCIMENTO, C. P. *Abordagens em Segurança, Desenvolvimento e Defesa:* a pesquisa no LAB-SDD. Brasília: Projeção, 2024, p. 83-101.

BOONSTRA, L. *Prompt Engineering.* Google, 2025. Disponível em: https://encurtador.com.br/ntMr. Acesso em: 15 jan. 2026.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Centro de Computação da Aeronáutica de São José dos Campos. *Portaria CCA-SJ nº 55/AFPI*, *de 29 de maio de 2025.* Atualiza a Política de Inovação do CCA-SJ. São José dos Campos: CCA-SJ, 2025. Disponível em: https://shre.ink/AGVt. Acesso em: 15 jan. 2026.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Universidade da Força Aérea. *Portaria UNIFA nº 70/AGI, de 14 de dezembro de 2023.* Aprova a Política de Inovação da Universidade da Força Aérea. Rio de Janeiro: UNIFA, 2023. Disponível em: https://shre.ink/AGV3. Acesso em: 15 jan. 2026.

BRASIL. Ministério da Defesa. Comando da Marinha. Centro Tecnológico da Marinha no Rio de Janeiro. *Portaria nº 122/CTMRJ*, *de 30 de junho de 2023.* Estabelece as Diretrizes da Política de Inovação do CTMRJ. Rio de Janeiro: CTMRJ, 2023. Disponível em: https://shre.ink/AGVG. Acesso em: 15 jan. 2026.

BRASIL. Ministério da Defesa. Comando do Exército Brasileiro. P*ortaria 1.318, de 14 de maio de 2024.* Aprova a Diretriz Estratégica de Inteligência Artificial para o Exército Brasileiro (EB20-D02.031). Disponível em: https://shre.ink/AGVi. Acesso em: 15 jan. 2026.

BRASIL. Ministério da Defesa. *Portaria nº 3.063, de 22 de julho de 2021.* Aprova a Política de Ciência, Tecnologia e Inovação de Defesa. Disponível em: https://shre.ink/AGVz. Acesso em: 15 jan. 2026.

BRASIL. *Projeto de Lei nº 1797/2024.* Estabelece normas gerais para o desenvolvimento, implementação e uso responsável de sistemas de Inteligência Artificial, com o objetivo de proteger os direitos humanos e a garantia de sistemas seguros e confiáveis em benefício da pessoa humana. Brasília, DF: Câmara dos Deputados, 2024. Disponível em: https://shre.ink/AGVP. Acesso em: 15 jan. 2026.

BRASIL. *Projeto de Lei nº 2338/2023.* Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília, DF: Senado Federal, [2025]. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=3106629&filename=Avulso%20PL%202338/2023. Acesso em: 15 jan. 2026.

BRASIL. *Projeto de Lei nº 04/2025.* Dispõe sobre a atualização da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), e da legislação correlata. Brasília, DF: Senado Federal, [2025]. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9889356&ts=1772122267271&disposition=inline. Acesso em: 15 jan. 2026.

BRASIL. Superior Tribunal Militar. *Ato Normativo nº 808.* Institui o Guia de Diretrizes e Boas Práticas no Uso de Soluções de Inteligência Artificial Generativa na Justiça Militar da União. Brasília, DF: STM, 2024. Disponível em: https://shre.ink/AGNk. Acesso em: 15 jan. 2026.

BURNEO, P.; COSTA, A.P.;PINHO, I.; MUNIZ, A.B.X.; MORESI, E.A.D. Competence frameworks for exploring generative AI in education. *In:* Prokopis, A. (ed.). *Artificial Intelligence (AI) in Social Research.* Oxfordshire, UK: CABI, 2025. p.160-175.

CHIU, T. K. F. AI literacy and competency: definitions, frameworks, development and future research directions. *Interactive Learning Environments*, v. 33, n. 5, p. 3225-3229, 2025. Disponível em: https://www.tandfonline.com/doi/full/10.1080/10494820.2025.2514372. Acesso em: 19 jan. 2026.

DANDEKER, C. New Times for the Military: Some Sociological Remarks on the Changing Role and Structure of the Armed Forces of the Advanced Societies. *The British Journal of Sociology***,** vol. 45, no. 4, 1994, p. 637-654. Disponível em: https://www.jstor.org/stable/i225027. Acesso em: 12 fev. 2026.

DEEP, P. D.; CHEN, Y. The role of AI in academic writing: impacts on writing skills, critical thinking, and integrity in higher education. *Societies,* v. 15, p. 247, 2025. Disponível em: https://www.mdpi.com/2075-4698/15/9/247. Acesso em: 17 fev. 2026.

DINH, C. T. Undergraduate English majors' views on ChatGPT in academic writing: perceived vocabulary and grammar improvement. *FWU Journal of Social Sciences,* v. 19, n. 1, p. 1-11, 2025. Disponível em: https://shre.ink/AGV8. Acesso em: 11 fev. 2026.

FITZEK, S.; BÂRGĂOANU, A. Introducing large language models in communication and public relations education: a mixed-methods pilot study. *International Journal of Artificial Intelligence in Education,* 2025. Disponível em: https://d-nb.info/1370568223/34. Acesso em: 15 fev. 2026.

GONZALES, J. D. R. et al. Evaluation of the impact of ChatGPT on the development of research skills in higher education. *International Journal of Learning, Teaching and Educational Research*, v. 24, n. 4, p. 370-390, 2025. Disponível em: https://shre.ink/AGN7. Acesso em: 23 jan. 2026.

HOSSAIN, Z.; BISWAS, M. S.; KHAN, G. AI literacy of library and information science students: a study of Bangladesh, India and Pakistan.

Journal of Librarianship and Information Science, 2025. Disponível em: https://shre.ink/AGVp. Acesso em: 7 fev. 2026.

KIM, J.; DANILINA, E. Towards inclusive and equitable assessment practices in the age of GenAI: revisiting academic literacies for multilingual students in academic writing. *Innovations in Education and Teaching International*, v. 62, n. 2, p. 1-5, 2025. Disponível em: https://encurtador.com.br/Yhwt. Acesso em: 28 jan. 2026.

KIM, J. Exploring students' perspectives on Generative AI-assisted academic writing. *Education and Information Technologies*, 2025. Disponível em: https://link.springer.com/article/10.1007/s10639-024-12878-7. Acesso em: 14 fev. 2026.

KNOTH, N.; TOLZIN, A. JANSON, A.; LEIMEISTER, J.M. AI literacy and its implications for prompt engineering strategies. *Computers and Education: Artificial Intelligence*. v.6 2024. Disponível em: https://www.sciencedirect.com/science/article/pii/S2666920X24000262. Acesso em: 22 jan. 2026.

MOLENAAR,I. Towards hybrid human-AI learning technologies. *European Journal of Education*, v.57, p. 632-645, 2022. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/ejed.12527. Acesso em: 15 fev. 2026.

MOLLICK, E. *Cointeligência*: a vida e o trabalho com IA. Rio de Janeiro: Intrínseca, 2025.

MORESI, E.A.D. PINHO, I.; COSTA, A.P. How to Operate Literature Review Through Qualitative and Quantitative Analysis Integration? *Computer Supported Qualitative Research (WCQR 2022)*. Disponível em: https://link.springer.com/chapter/10.1007/978-3-031-04680-3_13. Acesso em: 15 fev. 2026.

NONAKA, I.; TAKEUCHI, H. *Criação de conhecimento na empresa*: como as empresas japonesas geram a dinâmica da inovação. Rio de Janeiro: Campus, 1997.

NÓVOA, A. *As organizações escolares em análise.* Lisboa: Publicações Dom Quixote, 1995.

NWAGBARA, U. U. From curiosity to dependency: Nigerian students' perspectives on AI integration in academic research. *Journal of Academic Ethics*, v. 23, n. 4, p. 2051-2068, 2025. Disponível em: https://eric.ed.gov/?id=EJ1485441. Acesso em: 14 fev. 2026.

SAMPAIO, R. C.; FIGUEIREDO, D. *Prompts (Infalíveis!) para Pesquisa Acadêmica com Inteligência Artificial* (Coleção Para Bebês). Teresina: EDUFPI, 2025.

WEI, J.; WANG, X.; SCHUURMANS, D.; BOSMA, M.; ICHTER, B.; XIA, F.; CHEN, E. H.; CHOWDHERY, A.; LE, Q. V.; CHIANG, Y.; ZHOU, D. *Chain-of-Thought Prompting Elicits Reasoning in Large Language Models*. arXiv, 2022. Disponível em: https://arxiv.org/abs/2201.11903. Acesso em: 18 fev. 2026.

WHITEMAN, W. E. Training and educating army officers for the 21st century: implications for the United States military academy. Carlisle, PA: US Army War College, 1998.

ZARIFIAN, P. *Objetivo competência: por uma nova lógica.* São Paulo: Atlas, 2001.

ZHAO, X.; CHEN, X.; COX, A. Exploring the affordances of generative AI in academic writing for disabled students. In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 58., 2025, Maui, Hawaii. *Proceedings [...]*. 2025. p. 4941-4948. Disponível em: https://shre.ink/AGN8. Acesso em: 17 fev. 2026.

ZHAO, X.; COX, A.; CHEN, X. The use of generative AI by students with disabilities in higher education. *The Internet and Higher Education*, v. 66, art. 101014, 2025. Disponível em: https://www.sciencedirect.com/science/article/pii/S1096751625000235. Acesso em: 17 fev. 2026.

Guerra Remota:
emergência, fundamentos teóricos e dificuldades conceituais à luz do Estado do Conhecimento

André Barros de Oliveira
Viviane Machado Caminha
Nádia Xavier Moreira

Introdução

O fenômeno da guerra é uma constante na história e, conquanto sua natureza – conflito político resolvido pelo emprego da violência – nunca tenha mudado, sua condução assimila diferentes métodos (Worcester, 2015; Rossiter, 2021). A definição tradicional da natureza da guerra foi elaborada por Clausewitz (1996, p. 75), no seu livro Da guerra: "A guerra é, portanto, um ato de força para obrigar o nosso inimigo a fazer a nossa vontade". Trata-se da resolução do conflito político por meio do emprego da violência, isto é, "uma continuação das relações políticas realizada com outros meios" (Clausewitz, 1996, p. 98). Por essa perspectiva, a guerra é um instrumento violento da política.

Nesse sentido, a natureza política da guerra resiste aos desenvolvimentos tecnológicos que a instrumentalizam, ao menos até o estágio em que o próprio ser humano ou o Estado sejam removidos completamente da sua condução:

> [...] a natureza da Guerra é eterna e como tal imutável por qualquer processo de Transformação [...]. Assim, até que a Guerra possa ser travada de forma completamente remota, removendo o fator humano do campo de batalha, muitos destes aspectos serão eternos e estarão omnipresentes na conflitualidade hostil. Todavia, tendências como a imposição da vontade sobre o adversário sem o confronto físico (através da Guerra Remota); por atores sem monopólio legítimo do uso da força; sem risco; de forma autónoma por máquinas, fazem perspectivar alterações qualitativas na natureza da Guerra. Por isso, a remoção destas inevitabilidades da equação da Guerra, dará lugar a outras formas de conflito em dimensões políticas, económicas, informacionais e tecnológicas, podendo transformar a natureza fundamental da Guerra (Vicente, 2013, p. 14).

A perspectiva da imposição da vontade política sem contato físico entre combatentes humanos se avizinha em razão do rápido desenvolvimento tecnológico da era presente, de forma que termos como guerra remota (*remote warfare*), guerra de drones (*drone warfare*) e guerra autônoma (*autonomous warfare*), já frequentam os estudos da conflituosidade contemporânea (Worcester, 2015; Rauta, 2021; Garcia *et al*., 2025). Especificamente quanto à guerra remota, essa é um produto da belicosidade do século XXI, marcada pelo incremento de artefatos tecnológicos operados com efetividade a longas distâncias (Rogers, 2023).

Como observado, esse imenso avanço tecnológico acumulado e incorporado aos embates militares ainda é incapaz de alterar a natureza da guerra, mesmo se travada apenas remotamente, porquanto o objetivo de submeter a vontade alheia continua sendo seu motor. "O processo social que conforma, situa e usa tecnologia está fora do âmbito da teoria da guerra. É esta a razão pela qual a tecnologia não é tematizada explicitamente em qualquer capítulo ou seção do Da guerra de Clausewitz (1984)" (Duarte, 2012, p. 30).

No entanto, a guerra, no sentido de *warfare,*[1] sofre constante influência da tecnologia. "A tecnologia tem transformado a guerra mais do que qualquer outra variável [...]. Da Idade da Pedra à era nuclear, ela tem impulsionado a evolução da guerra (Roland, 2016, p. 22, tradução nossa).[2] A tecnologia é o instrumento da guerra remota:

> Nos últimos anos, as principais tecnologias amplamente utilizadas no âmbito da defesa têm sido os drones e os softwares de inteligência artificial (IA). A guerra na Ucrânia parece ser a representação contemporânea de um verdadeiro mostruário do potencial atingido pelos drones e pelos artefatos e treinamentos que seu uso envolve.

[1]Embora a língua portuguesa traduza "*war*" e *"warfare*" indistintamente como "guerra", na língua inglesa esses termos designam fenômenos distintos. Enquanto *"war*" refere-se à Guerra em seu aspecto político (*World War I, World War II, Cold War, Vietnam War, Iraq and Afghanistan War*), "*warfare"* designa a prática da guerra e alude ao caráter ou meio de condução da guerra (*proxy warfare*, *hybrid warfare, irregular warfare, cyberwarfare, remote warfare, drone warfare*). Nesse sentido, tal como a guerra é um instrumento da política, a guerra remota (*remote warfare*) é um instrumento da Guerra (*war*).

[2]Texto original: "Technology has changed warfare more than any other variable .... From the Stone Age to nuclear age, technology has driven the evolution of warfare" (Roland, 2016, p. 22).

> Os diversos drones, tanto de reconhecimento quanto de ataque, que sobrevoam o território ucraniano intensificaram ainda mais a tendência de disputa por meio da superioridade tecnológica, especialmente nos céus (Saint-Pierre; Zorzo, 2023, p. 274).

Assim, o objetivo do presente capítulo é discutir o conceito de guerra remota enquanto via de intervenção militar. Para tanto, utilizou-se uma abordagem metodológica de cunho qualitativo, tendo como instrumento de coleta de dados a revisão da literatura, operacionalizada por meio da aplicação da metodologia Estado do Conhecimento, tal como proposto por Morosini, Nascimento e Nez (2021).

O texto encontra-se estruturado a partir da elaboração de uma breve contextualização da emergência da guerra remota, seguida pela operacionalização do método, formação do *corpus* de análise e sua divisão em duas categorias: abordagem ampla e estrita. E, na parte final, refletimos sobre a teoria levantada em cotejo com a realidade dos conflitos contemporâneos.

Contexto da emergência da Guerra Remota

Os Estados Unidos (EUA) reagiram aos ataques terroristas de 11 de setembro de 2001, no seu território, por meio da declarada "Guerra ao Terror", que se desdobrou em campanhas militares no Afeganistão (2001) e no Iraque (2003). Essas intervenções, contudo, trouxeram-lhes dissabores. Contrariando as previsões político-militares, as 2.324 baixas no Afeganistão e as 4.598 no Iraque sinalizaram, para os EUA, um período pós-11 de setembro caracterizado por atoleiros militares e impasses políticos. A dificuldade americana de encerrar suas intervenções militares estava novamente evidenciada (Rogers, 2023).

> A história demonstra também que as intervenções militares americanas têm uma tendência de se tornarem permanentes [...] Mais de duas décadas após a primeira intervenção no Iraque, forças americanas ainda permanecem no território. Os combates no Afeganistão duram há mais de uma década. Simultaneamente, a USAF ainda ajuda a defender a Coreia do Sul, mais de 60 anos após o conflito na Península (Vicente, 2013, p. 22).[3] A maneira americana de fazer a guerra, "segundo uma forte tendência tecnológica, procurando por um lado contrariar a

[3]USAF é o acrônimo de *United States Air Force*, a Força Aérea americana.

> inferioridade numérica, ao mesmo tempo que saciam a crescente aversão por baixas em combate" (Vicente, 2013, p. 16), não funcionara a contento. Uma nova estratégia tornou-se imprescindível para a continuidade do empenho americano na Guerra ao Terror.

A eleição de Barack Obama em 2008 marcou o início dessa nova abordagem. Em sua campanha eleitoral, Obama prometeu retirar as forças armadas americanas das campanhas terrestres expedicionárias (*no boots on the ground*) que comprometiam o apoio público à Guerra ao Terror. Estava em curso uma transformação profunda na maneira americana de fazer a guerra, na qual o uso de drones emergia como o principal instrumento dessa inovação – "*bots in the sky [...] replace boots on the ground"* (Gertz, 2014, p. 92). De fato, graças às operações remotas, frequentemente apoiadas por drones, as baixas americanas diminuíram enquanto os conflitos se alastravam na Somália, Filipinas, Iêmen, Líbia, Paquistão e em todo o Sahel (Rogers, 2023).

A guerra remota, portanto, respondeu à pretensão política americana de diminuir baixas em intervenções militares (Walker, 2018) e hoje abarca uma série de sistemas de ataques precisos e capacidades correlatas – principalmente plataformas não tripuladas – para entregar força letal de forma remota (Rossiter, 2023b). As razões políticas e estratégicas da emergência da guerra remota estão bem assentadas na literatura, resta indagar acerca do seu conceito.

Operacionalização do método

A guerra remota se apresenta como um fenômeno complexo, cujo conceito ainda é objeto de disputa na academia. Não obstante, aspectos teóricos definidores do fenômeno podem ser extraídos a partir dos textos publicados sobre o tema. A operacionalização desse estudo se deu por meio da metodologia "Estado do Conhecimento". Portanto, a revisão teórica aqui proposta objetiva construir um estado do conhecimento sobre a guerra remota, adotando as seguintes fases para catalogação e análise dos textos: a) identificação; b) registro; c) categorização; d) reflexão; e e) síntese sobre a produção científica em determinado espaço de tempo (Morosini; Nascimento; Nez, 2021).

Inicialmente, a pesquisa do termo "guerra remota" no Google Acadêmico retornou 75 trabalhos, enquanto "*remote warfare*" 1990.[4] Em razão

[4]Essas pesquisas ocorreram em maio de 2025.

da quantidade bem maior de material disponível, optou-se pela utilização do termo indutor em inglês. Uma delimitação da busca em torno do conceito mostrou-se fundamental para o intento de descrever uma teoria básica do fenômeno. Dessa forma, o termo indutor escolhido foi uma combinação de "*remote warfare*" *and* "*conceptual analysis*", o qual gerou 53 resultados no Google Acadêmico e nenhum resultado nas bases Biblioteca Digital Brasileira de Teses e Dissertações - BDTD, Catálogo de Teses e Dissertações Capes, Rede Scielo e Revista Brasileira de Estudos de Defesa - RBED, já o correlato em português "guerra remota" e "análise conceitual" não gerou resultados nessas plataformas.

Quadro 1 - Resultados das pesquisas nos sistemas de busca

Termo indutor	Sistema de busca	Resultado inicial	Resultado final
"remote warfare" and "conceptual analysis"	Google acadêmico	53	15
	bdtd.ibict.br	0	-
	periodicos.capes.gov.br	0	-
	search.scielo.org	0	-
	rbed.abedef.org	0	-
"guerra remota" e "análise conceitual"	Google acadêmico	0	-
	bdtd.ibict.br	0	-
	periodicos.capes.gov.br	0	-
	search.scielo.org	0	-
	rbed.abedef.org	0	-

Fonte: Elaborado pelos autores (2026).

Em seguida, descartaram-se os trabalhos que sequer mencionavam guerra remota em seu título ou resumo, restando um total de 15 textos, que passaram a compor o *corpus* de análise, subdividido em duas categorias analíticas ou blocos temáticos. Não se utilizou delimitação temporal pois o fenômeno investigado é consensualmente datado no pós-11 de setembro de 2001.

O primeiro bloco desses estudos adota uma abordagem ampla do termo "guerra remota", ou seja, trata de múltiplos fenômenos não se reduzindo ao emprego do poder aéreo. O segundo bloco temático corresponde a uma abordagem estrita, focada essencialmente no desenvolvimento de tecnologias

de atuação remota, sobretudo drones e emprego do poder aéreo por tropas próprias.

Quadro 2 - *Corpus* de análise (continua)

Bloco Temático Discussão Teórica sobre Guerra Remota: abordagem ampla				
Nº	**Ano**	**Autor**	**Título**	**Livro/Revista**
1	2016	ABBOTT, Chris; HATHORN, Steve; HICKIE, Scott	The Remote Warfare Digest	London: Oxford Research Group, 2016
2	2018	ADELMAN, Rebecca A.; KIERAN, Kieran.	Re-Conceptualizing Cultures of Remote Warfare: Editors' Introduction	Journal of War & Culture Studies
3	2021	WATTS, Tom F. A.; BIEGON, Rubrick	Revisiting the remoteness of remote warfare: US military intervention in Libya during Obama's presidency	Defence Studies
4	2021	BIEGON, Rubrick; RAUTA, Vladimir; WATTS, Tom F. A.	Remote warfare–buzzword or buzzkill?	Defence Studies
5	2021	STODDARD, Ed; TOLTICA, Sorina	Practising remote warfare: Analysing the remote character of the Saudi/UAE intervention in Yemen	Defence Studies
6	2021	RIEMANN, Malte; ROSSI, Norma	Remote warfare as "security of being": reading security force assistance as an ontological security routine	Defence Studies
7	2021	RAUTA, Vladimir	A conceptual critique of remote warfare	Defence Studies
8	2021	TRENTA, Luca	Remote killing? Remoteness, covertness, and the US government's involvement in assassination	Defence Studies
9	2022	BIEGON, Rubrick; WATTS, Tom F. A.	Remote warfare and the retooling of American primacy	Geopolitics

Bloco Temático Discussão Teórica sobre Guerra Remota: abordagem ampla				
Nº	**Ano**	**Autor**	**Título**	**Livro/Revista**
10	2023	ROGERS, James; GOXHO, Delina	Light footprint—heavy destabilising impact in Niger: why the Western understanding of remote warfare needs to be reconsidered	International Politics
11	2023	WASIUTA, Olga	Konceptualizacja zdalnej wojny: przeszłość, teraźniejszość i przyszłość	In: SKRZYNSKI, Tomasz; JASTRZEBSKI, Jaroslaw. Polityka - wojskowość - bezpieczeństwo. Księga jubileuszowa z okazji 40-lecia działalności naukowej Profesora Romana Kochnowskiego.
12	2023	ROGERS, James	Rethinking remote warfare	International Politics
Bloco Temático Discussão Teórica sobre Guerra Remota: abordagem estrita				
1	2018	WALKER, David M.	American Military Culture and the Strategic Seduction of Remote Warfare	Journal of War & Culture Studies
2	2020	ZEITLIN, Michael	“An Entirely New Method of Conducting War at a Distance” The First World War and the Air War of the Future.	In: ADELMAN, Rebecca A.; KIERAN, David (Ed.). Remote Warfare: New Cultures of Violence
3	2023	ROSSITER, Ash	AI-enabled remote warfare: sustaining the western Warfare paradigm?	International Politics

Fonte: Elaborado pelos autores (2026).

Análise conceitual: abordagem ampla

O estudo proposto se inicia com os textos do primeiro bloco, ordenados pela data de publicação. A pesquisa Abbott, Hathorn e Hickie (2016), como o próprio título sugere (*The Remote Warfare Digest*), pretende-se um resumo das possibilidades de guerra remota. Os autores argumentam que, durante a Guerra Fria, os EUA empregaram forças especiais, agentes secretos, mercenários e exércitos por procuração como uma estratégia para contornar o controle parlamentar e a opinião pública. Isso evoluiu durante os períodos da Guerra ao Terror e das Guerras no Afeganistão e Iraque, nas quais, ao lado das forças convencionais, foram utilizados drones armados, operações cibernéticas ofensivas e vigilância em massa. Apesar desse trabalho confirmar a utilização de drones e ataques cibernéticos como os elementos disruptores da conflituosidade moderna, sua definição da guerra remota incorpora distintas atividades: a) operações com forças especiais; b) atuação de empresas militares e de segurança privadas; c) veículos não tripulados e sistemas de armas autônomas; d) guerra cibernética; e e) inteligência, vigilância e reconhecimento. A todas elas o texto dirige as mesmas críticas: falta de transparência, ausência de supervisão legal e internacional, presença de dilemas éticos e abusos dos direitos humanos.

Adelman e Kieran (2018) resgatam a Declaração de Postura da Força Aérea dos Estados Unidos de 2008. Essa declaração afirma que as missões de combate americanas cobrem todo o planeta, incluindo os domínios do ar, do espaço e do ciberespaço, de forma interdependente. Assegura ainda que os bombardeiros e mísseis de longo alcance são a garantia máxima da segurança dos Estados Unidos. A opção por uma abordagem inicial baseada naquela declaração tem o objetivo de ilustrar uma tendência equivocada dos estudos históricos e contemporâneos da guerra remota: a preponderância da identificação da guerra remota com a guerra de drones, embora isso não configure um equívoco completo já que os drones representam uma das inovações militares mais importantes do século XXI.

Entretanto, os autores ressaltam que esse foco restrito na guerra de drones minimiza o impacto dos demais tipos de violência realizados à distância, com igual ou maior letalidade, a exemplo dos bombardeios aéreos e guerra cibernética. Essa redução também implica uma teorização histórica da guerra remota tão antiga quanto a própria aviação. Retomando a declaração de 2008,

o artigo conclui que os militares provavelmente pensavam a guerra remota com mais complexidade e diversidade do que os estudiosos dessa violência.

Watts; Biegon (2021) procuram problematizar o distanciamento (*remoteness*) na qualidade de elemento constitutivo da guerra remota. Enquanto o estudo da distância física (*physical distance*) é mais antigo, o estudo do caráter do distanciamento (*remoteness*) na guerra é objeto da investigação atual:

> Este artigo defende uma definição inovadora da distanciamento (remoteness) da guerra remota (remote warfare) como o grau de distanciamento socio-psicológico do público em relação às realidades da violência política travada a uma distância física do território continental dos Estados Unidos, mediado pela condição de espectador do uso da força militar (Watts, Biegon, 2021, p. 509, tradução nossa).[5]

Como se observa da leitura da definição exposta, o distanciamento da guerra remota não se resume apenas à distância física dos combatentes ou ao uso de tecnologias, ele possui também propriedades psicológicas e sociais. Daí porque o papel do espectador é fundamental.[6] Tendo em vista a intervenção americana na Líbia, durante o governo Obama, marcada pela contenção legislativa da ação militar, os autores argumentam que a diminuição do espetáculo em torno da "Operation Odyssey Lightning" ajuda a explicar o crescente distanciamento do público americano em relação à intervenção militar na Líbia. A dinâmica envolvida com tal "afastamento" também firma a temporalidade e o âmbito geográfico aparentemente cada vez mais amplo de algumas guerras contemporâneas.

Biegon; Rauta; Watts (2021, p. 427) argumentam que a linguagem do estudo da violência política recebeu um influxo terminológico e conceitual

---

[5]Tesxto original: This paper makes the case for a novel definition of the remoteness of remote warfare as the degree of the public's socio-psychological detachment from the realities of political violence fought at a physical distance from the continental United States, as mediated through spectatorship of the use of military force (Watts, Biegon, 2021, p. 509).

[6]As guerras distantes têm raízes históricas que remontam ao período colonial das potências ocidentais e correspondem a uma estratégia útil para privar o público do conhecimento e envolvimento emocional. Uma sondagem de 2011, por exemplo, sugeriu que metade do público americano acreditava que as guerras no Afeganistão e no Iraque – as maiores e mais notórias intervenções militares recentes dos EUA – tinham feito pouca diferença nas suas vidas (Watts; Biegon, 2021).

imenso na última década. A (re) invenção de conceitos é evidenciada por termos como: "grey zone warfare", "hybrid warfare", "liquid warfare", "post-heroic warfare", "proxy war(fare)", "surrogate warfare", "vicarious warfare" e naturalmente "remote warfare". Com relação à guerra remota, há pouca avaliação conceitual e sua aplicação permanece ateórica, muito embora os estudos adotem alguma definição como ponto de partida para avaliações teóricas e empíricas mais amplas. A partir da noção de jargão (*buzzword*),[7] os autores avaliam a introdução do termo no campo semântico da violência política contemporânea, um processo no qual a adição de novos referentes fez com que o conceito fosse além de seu foco original na tecnologia, se desdobrando em cinco grandes campos de estudos: (1) a ética, a legalidade e as experiências do uso de diversas tecnologias de armas; (2) as representações culturais e as consequências das tecnologias de guerra remota; (3) a delegação e a privatização da guerra; (4) a transparência, a eficácia e os custos humanos das recentes operações ocidentais de contraterrorismo e estabilização; e (5) a lógica geopolítica e os efeitos sociopolíticos da guerra remota.

Ainda, segundo o texto, um embate principal se apresenta. Por um lado, uma compreensão tecnocêntrica da guerra remota, que se concentra no impacto de diversas tecnologias de armas. Por outro lado, uma compreensão mais orientada para os resultados da guerra remota, que amplia o debate para estudar um conjunto amplo de agentes e práticas que compartilham o efeito de distanciar as forças do combate na linha de frente, a exemplo da terceirização ou apoio a agentes locais. E mesmo dentro da visão tecnocêntrica, mais rigorosa no emprego do termo, a indefinição conceitual não deixa claro se a unidade básica de interesse é o drone, a arma autônoma ou a guerra cibernética. Essa indefinição tende a se acentuar pois tanto a guerra cibernética quanto as armas autônomas, por exemplo, têm sido apontadas como uma face distinta do conflito, a demandar separação em relação aos estudos sobre guerra remota.

Tematicamente, os cinco ramos da pesquisa em guerra remota abordaram um conjunto comum de questões: há algo de novo na tendência recente de distanciamento entre forças terrestres convencionais e combates

[7] *Buzzwords* tendem a capturar e refletir o *zeitgeist*. Elas ajudam a definir os tópicos quentes de um determinado momento. Embora isso sugira que elas podem ter um grau de efemeridade, também podem ser maneiras convenientes de iniciar uma nova conceituação (Biegon; Rauta; Watts, 2021).

na linha de frente? O que explica essa tendência? Como as diversas formas de distanciamento criadas por esse processo são vivenciadas por diferentes públicos? A intervenção à distância é ética e eficiente? Quais são os efeitos da intervenção à distância na política, na sociedade, no direito e na cultura?

O principal ponto de divergência em relação a esses cinco ramos é o peso relativo dado ao estudo da tecnologia em relação à delegação na guerra. Apesar disso, os autores concluem que a guerra remota já se consolidou no estudo da violência política, tendo se enraizado em uma variedade de contextos disciplinares e profissionais, tornando-se um jargão (*buzzword*) usado não apenas por acadêmicos, mas também por formuladores de políticas e profissionais.

Stoddard e Toltica (2021) partem de um foco diferente do tradicional – centrado no Ocidente e sobretudo nos EUA – para examinar a intervenção de Arábia Saudita e Emirados Árabes Unidos no Iêmen desde 2015. Essa intervenção adotou, simultaneamente, o emprego de poder aéreo, forças especiais, combatentes privados e parceiros locais, ou seja, esses países preferiram adotar táticas remotas para limitar o emprego de suas tropas terrestres e, assim, reduzir os riscos inerentes. Ao contrário das intervenções ocidentais, os objetivos dos sauditas e dos Emirados Árabes Unidos não estão primariamente relacionados ao combate ao terrorismo nem se baseiam em motivações humanitárias, mas são impulsionadas por ameaças à segurança compartilhadas, especialmente a ascensão militar do Irã. O conceito que os autores oferecem é amplo e envolve um conjunto de práticas que, variadas em suas configurações táticas, produzem o mesmo efeito estratégico de promover os interesses políticos de um Estado sem o desdobramento de um grande número de suas forças terrestres convencionais.

Riemann e Rossi (2021) sugerem uma análise da guerra remota por meio da perspectiva de segurança ontológica, em vez da sobrevivência (*security as survival*), o foco está na segurança do eu (*the security of the self*). O papel da SFA britânica (*Security Force Assistance*) é destacado como uma dimensão imaterial da guerra, uma maneira de reforçar o engajamento global *(global engagement identity*) do Reino Unido sem dispensar efetivo militar, por meio do fortalecimento de aliados e parceiros locais. Trata-se de um modo de intervenção à distância para a qual os autores atribuem o seguinte conceito: "[...] a guerra remota constitui uma tentativa de recriar ordem e hierarquia para manter ameaças à distância, estabelecer rotinas e estabilidade e (re)estabelecer

uma narrativa autobiográfica coerente." (Riemann; Rossi, 2021, p. 494, tradução nossa).[8]

O artigo seguinte, de Rauta (2021), discute uma análise conceitual da guerra remota e aponta que o termo se refere a realidades tão distintas que sua compreensão se torna bastante confusa, prejudicando até o progresso das pesquisas e a desejável acumulação do conhecimento. Campo semântico (*semantic field*), na linguística, designa um domínio de palavras relevantes em áreas específicas, e o significado de cada uma é constituído pelas relações entre elas, de forma que a redefinição de uma implica a das outras.

A "guerra remota" está, assim, bem situada no campo semântico amplo da violência política como um termo que designa o distanciamento da guerra e contribui para a democratização do debate sobre a guerra. Não atingiu, contudo, o *status* de conceito – conjunto de propriedades atribuídas ao termo –, por lhe faltar um valor analítico próprio em relação aos outros termos existentes que fazem afirmações semelhantes. O debate sobre "guerra remota" tem se concentrado amplamente na suposta novidade do termo em detrimento do conceito. E esse termo se refere a quase tudo que diz respeito à conflituosidade do século XXI, desde a competição entre grandes potências até a inteligência artificial, e, ao final, se reduz a imensa complexidade a um debate sobre distância, vista como facilitador, condição e contexto.

Nesse sentido, Rauta (2021) postula que um olhar sobre os diferentes modos pelos quais a "guerra remota" foi estudada mostra que ela é, simultaneamente, uma forma de lutar, um modo de intervenção, o futuro das guerras, um modo de consumir e visualizar a guerra, um novo domínio de batalha e uma medida de como a conduta legal/ética da guerra sucumbiu ao determinismo tecnológico (*techno-dominance*). Como a literatura sobre "guerra remota" dá tanta importância ao seu adjetivo central, ela não dispensa muita atenção ao que falta para transformar o termo em um conceito: uma descrição robusta de suas propriedades constituintes e como estas são configuradas para dar significado.

[8] Texto original: "[...]remote warfare is an attempt to recreate order and hierarchy to keep threats at a distance, establish routines and stability, and (re)establish a coherent autobiographical narrative" (Riemann; Rossi, 2021, p. 494).

O estudo de Trenta (2021) traz para a discussão da guerra remota os assassinatos encomendados pelo governo americano e israelense como ferramenta da sua política externa. O conceito se amplia para incluir, além dos meios mais ou menos remotos, o caráter mais ou menos dissimulado do emprego desses meios. O assassinato do General Qassem Soleimani, chefe da Guarda Revolucionária do Irã, foi conduzido de forma ostensiva, com o pleno reconhecimento público, já o assassinato de Mohsen Fakhrizadeh, cientista nuclear iraniano, pelo Mossad, foi realizado por meio do uso de uma metralhadora assistida por IA e operada a 1.600 quilômetros de distância, ou seja, por meio dissimulado. Esses assassinatos demonstram o interesse dos governos em atingir seus objetivos políticos utilizando tecnologia superior, de maneira mais ou menos dissimulada, mas evitando uma confrontação direta.

Biegon e Watts (2022) analisam a geopolítica americana por meio da guerra remota. A violência americana passa por um processo de "remotificação" (*remotification*) explicitada de duas maneiras: 1) nova tecnologias e substitutos para promover segurança com o mínimo de militares em campo; 2) distância entre EUA e sítios subalternos de suas intervenções. Esse processo decorre tanto da diminuição do apoio público às intervenções em larga escala no estrangeiro quanto da acirrada competição estratégica com a China. Essa mudança vai além do uso de novas tecnologias como drones e inteligência Artificial e inclui múltiplas modalidades de intervenção remota, tais como Forças de Operações Especiais, atividades de cooperação em segurança e empresas privadas de segurança. Esse estudo estabelece a guerra remota como um dos termos usados para estudar a violência política contemporânea, a política externa americana e as relações internacionais contemporâneas. O texto definiu de guerra remota: "[...] como uma estratégia de segurança que combina múltiplas modalidades 'remotas' de intervenção militar, com o objetivo de gerar distanciamento físico e político entre o agente interveniente e os locais de emprego da força" (Biegon; Watts, 2022, p. 950, tradução nossa).[9]

Rogers e Goxho (2023) argumentam que a noção de guerra remota como uma intervenção caracterizada pela "pegada leve" *(light footprint*), de baixo risco e distante, dependente do poder aéreo, das novas tecnologias, das operações especiais, de parceiros locais e de terceirizados (*proxies and*

[9][...]as a strategy of security management that blends multiple 'remote' modalities of military intervention to generate physical and political distance between an intervening agent and the sites(s) of its use of force" (Biegon; Watts, 2022, p. 950).

surrogates), precisa ser reavaliada por lhe faltar justamente o caráter de leveza. Os autores estudaram as intervenções no Níger em 2019 e 2021, por meio da análise de documentos e entrevistas semiestruturadas realizadas com militares, conselheiros, agentes de inteligência e atores locais e internacionais da sociedade civil envolvidos na operação. A conclusão, nesse caso, é que os mecanismos de guerra remota se proliferaram para uma multiplicidade crescente de atores estatais, com interesses variados e que, por meio da ação conjunta, geraram a saturação da zona de conflito e tiveram um impacto "pesado" para Níger.

O trabalho seguinte retrata a visão de uma autora polonesa, alheia ao convencional eixo EUA-Reino Unido e ambientada na fronteira com a Rússia, Olga Wasiuta (2023). Citando o uso pela Rússia de uma variedade de táticas de guerra híbrida,[10] incluindo desinformação, ataques cibernéticos e manipulação de entidades políticas na Europa. A guerra remota, portanto, situa-se num horizonte mais amplo de uma ordem internacional em (re) construção, onde os métodos tradicionais de conflito estão sendo suplantados por estratégias sofisticadas, indiretas e tecnológicas, que trazem implicações significativas para a segurança global e o futuro da governança democrática.

A autora afirma que o conceito não é novo, mas ganhou relevância devido aos avanços tecnológicos que facilitam operações militares precisas e de baixo custo sem o envio de forças terrestres substanciais. Sua definição, bastante ampla, aproxima-se da noção de guerra híbrida, pois ambas desafiam suposições antigas sobre o *locus* do conflito, transformando o campo de batalha em uma extensa rede de combates híbridos que combinam medidas cinéticas e não cinéticas em vários domínios, incluindo os informacionais e os cibernéticos. Além disso, o conceito engloba uma mudança mais ampla na natureza do conflito em si. A guerra remota confunde os limites convencionais entre guerra e paz, à medida que incidentes intermitentes e aparentemente isolados de ataques cibernéticos, ataques de drones e operações especiais se acumulam para formar um *continuum* de conflito que desafia as normas internacionais estabelecidas e as definições legais de guerra.

Rogers (2023) situa a guerra remota no espectro da intervenção por meio de drones armados, forças especiais e apoio a atores locais, longes do

[10]A noção de "guerra híbrida" se refere a uma conjunção de guerra irregular, convencional e terrorismo, presentes simultaneamente, assim como os agentes e as tecnologias empregadas nesse contexto complexo (Krishnan, 2022).

escrutínio público. Duas frases do Presidente Obama chamam bastante atenção acerca do caráter desse tipo de ação: a primeira de que o problema "com o programa de drones não era o fato de causar um número desproporcional de vítimas civis [...], mas o fato de passar a criar a ilusão de que não se tratava de guerra [...] O aparato passou a tornar-se excessivamente fácil" (Rogers, 2023, p. 782–783, tradução nossa);[11] a segunda foi repetida 16 vezes nos últimos dois anos do seu mandado "*no boots on the ground in Syria*" (Rogers, 2023, p. 782–783). Estava revelado, segundo o articulista, o caráter leve, democraticamente distanciado, indireto, limitado e remoto do envolvimento militar americano. Entretanto, como um produto da guerra americana ao terror do início do século XXI, em contexto de pouca restrição ao uso da força, a guerra remota já nasceu desafiando as restrições do direito internacional.

Análise conceitual: abordagem estrita

Os textos seguintes se convergem para uma visão mais estrita da guerra remota. O primeiro, de David M. Walker (2018), traz a perspectiva do determinismo tecnológico, representado atualmente pelo poder aéreo. O autor alega que esse determinismo foi incorporação às Forças Armadas americanas desde o início do século XIX, quando o currículo da incipiente Academia Militar já abordava a guerra como um problema a ser resolvido por meio do racionalismo científico.

Essa visão resistiu ao século XX porquanto, mesmo contra todas as evidências factuais, teóricas e militares, os estrategistas americanos ainda insistiam na ideia de que o emprego adequado do poder aéreo era fator decisivo para a vitória. Walker (2018) assinala que as esperanças atuais depositadas nos veículos aéreos não tripulados, ou drones, constituem a próxima interação dessa velha lógica consubstanciada na Teoria do Bombardeio Estratégico para destruir pontos decisivos. Assim, o autor evidencia a prevalência do uso de drones como a estratégia militar americana no Oriente Médio para combater organizações terroristas, durante o primeiro mandato do presidente Obama. Essa estratégia tinha por objetivo reduzir o emprego de forças terrestres,

[11]Texto original: "with the drone programme was not that it causes an inordinate amount of civilian casualties […], but that it starts giving you the illusion that it's not war […] The machinery started becoming too easy".(Rogers, 2023, p. 782-783).

implicando uma crescente dependência americana dos drones para bombardeios estratégicos.

Bombardeios à distância foram utilizados no final da Guerra do Vietnã e propiciaram poucas perdas entre operadores, mas não garantiu a vitória. Já na Guerra do Golfo, 1990-1991, a mesma estratégia foi empregada e seu sucesso impulsionou a ênfase no poder aéreo, bem como o desenvolvimento de uma nova doutrina - Operações Baseadas em Efeitos - por meio da qual os objetivos políticos eram alcançados com o atingimento de alvos precisos e sem envolvimento de grande contingente terrestre. A percepção americana após o 11 de setembro seguiu nesses moldes e possibilitou um grande avanço no emprego de drones pelos governos Bush e Obama, considerados uma solução tecnológica para a guerra.

Zeitlin (2020) faz uma genealogia da guerra de drones contemporânea até visões militares históricas, do início do século XX, quando os teóricos da aviação militar anteciparam a dificuldade de poupar alvos civis em bombardeios aéreos. O advento da aviação, especialmente bombardeios aéreos, elevou a habilidade de matar à distância a um patamar sem precedentes históricos. Dessa forma, a guerra remota realiza tanto o desejo humano profundo de matar remotamente, mas também explicita que, para o detentor da tecnologia, as vítimas civis pouco importam.

Por último, Rossiter (2023a) destaca a emergência dos sistemas autônomos baseados em Inteligência Artificial (IA). De início, o autor reflete que a guerra remota já começa a perder suas vantagens comparativas à medida que os concorrentes também adotam sistemas de precisão e desenvolvem suas contramedidas. Os entusiastas da Inteligência Artificial advogam justamente que ela trará de volta a vantagem perdida na guerra remota porquanto associada a um ganho de efetividade na cadeia decisória:

> A autonomia (autonomy), nesse contexto decisório, significa que o sistema possui a capacidade de decidir de forma independente entre diferentes cursos de ação. A delegação da tomada de decisão a sistemas autônomos tem o potencial de gerar ganhos substanciais de eficiência entre as etapas da kill chain, comprimindo o tempo necessário entre a identificação de um alvo e sua destruição" (Rossiter, 2023a, p. 825, tradução nossa).[12]

[12] Texto original: (a)utonomy in this decisionmaking context means that the system has ability to independently decide among different courses of action. Delegated decision-making to

O autor critica essa visão porque, em primeiro lugar, o impacto da IA é superestimado e ignora as vulnerabilidades associadas à confiança em seus sistemas, e, em segundo lugar, o seu emprego implica métodos de guerra antiéticos para o paradigma ocidental, como massificação sem precisão (*mass over precision*) ou sistemas autônomos letais *(lethal autonomous weapons systems LAWS*).

Reflexão crítica e cotejo com a realidade

"No campo de batalha, não vi um único soldado ucraniano. Apenas drones. Só os vi quando me rendi. Apenas drones, e há muitos deles. Não venham. Trata-se de uma guerra de drones." – soldado russo rendido (Bondar, 2025, p.1, tradução nossa).[13] Esse testemunho retrata a perplexidade de um combatente convencional ao ingressar em um "campo de batalha" e se deparar com um ataque de máquinas; o primeiro contato humano ocorreu apenas após sua rendição. Trata-se, para o controlador do drone, da realização da utopia da guerra sem risco e, para o seu inimigo, do pesadelo de uma batalha contra robôs, só vista, até então, em filmes de ficção científica. A guerra de drones, nesse sentido, é distópica porque evoca "cenários distópicos típicos de filmes de ficção científica, marcados por uma inevitável insurreição de robôs, por um insensível, implacável e incontrolável exército de máquinas, avançando em ondas sucessivas contra quaisquer grupos dispersos de combatentes humanos que ousem enfrentá-los" (Gertz, 2014, p. 93, tradução nossa).[14]

Ademais, a circunstância retrata o microcosmos de uma guerra remota ao trazer à luz muitas das características abordadas nos textos que compõem o *corpus* de análise, a saber: ataque à distância segura (Zeitlin, 2020; Wasiuta, 2023; Rogers, 2023), controle remoto (Walker, 2018; Zeitlin, 2020; Rossiter, 2023), ausência de tropas no campo de batalha (Zeitlin 2020; Rogers, 2023), e

autonomous systems has the potential for substantial efficiencies between stages of the kill chain, compressing the time it takes from identifying a target to destroying it (Rossiter, 2023a, p. 825).

[13]Texto original: "On the battlefield I did not see a single Ukrainian soldier. Only drones. I saw them [Ukrainian soldiers] only when I surrendered. Only drones, and there are lots and lots of them. Guys, don't come. It's a drone war" - Surrendered Russian soldier (Bondar, 2025, p. 1).

[14] "nightmare scenarios of many a sci-fi film of an inevitable robot uprising, of an unfeeling, uncaring, unstoppable army of robots marching in wave after wave toward whatever disparate groups of human resistance fighters would dare to challenge them" (Gertz, 2014, p. 93).

pouco risco e escrutínio público (Abbott; Hathorn; Hickie, 2026; Trenta, 2021; Rogers, 2023). Explicita também a assimetria dessa guerra, na qual todas as vantagens favorecem o atacante (Rogers; Goxho, 2023).

Outro exemplo desponta em contexto político diverso, mas igualmente dialoga com a teoria aqui levantada. Israel lançou a "Operation Rising Lion" contra o Irã no dia 13 de junho de 2025, ocasião em que, segundo alega, destruiu instalações nucleares e metade dos mísseis balísticos e lançadores iranianos. Pelo menos duas dúzias de cientistas nucleares e altos comandantes militares foram assassinados em suas casas, escritórios e bunkers. Israel utilizou bombardeios aéreos, drones e infiltrou agentes no território inimigo. O Irã reagiu com seus mísseis e drones. E, ao final, após 12 dias de combates, a população civil pagou o maior preço com um saldo de 29 mortos em Israel, e mais de 1.000 no Irã, e milhares de feridos em ambos os lados (Pace, 2025).

As características desse conflito também coincidem, em grande parte, com aquelas atribuídas pela literatura à guerra remota: emprego de bombardeios aéreos (Walker, 2018; Adelman; Kieran, 2018; Zeitlin, 2020; Stoddard; Toltica, 2021; Rogers; Goxho, 2023) e drones (Abbott; Hathorn; Hickie, 2016; Adelman; Kieran, 2018; Walker, 2018; Trenta, 2021; Rogers; Goxho, 2023; Rogers, 2023), infiltração de agentes secretos no território inimigo (Abbott; Hathorn; Hickie, 2016), ausência de tropas expedicionárias (Stoddart; Toltica, 2021; Watts; Biegon, 2021; Biegon; Watts, 2022; Rogers, 2023), assassinatos encomendados (Trenta, 2021) e transferência do ônus para a população civil (Zeitlin, 2020).

Já uma aproximação dos elementos teóricos com a prática da guerra cibernética pode ser encontrada no bojo do conflito Irã x Israel/EUA. Nos idos dos anos 2010, as centrífugas de enriquecimento de urânio do Irã foram danificadas por um *worm* chamado Stuxnet. Apesar da autoria incerta, o objetivo político de conter o programa nuclear iraniano foi alcançado, "sendo o primeiro caso conhecido de um ataque à rede de computadores a promover danos físicos a infraestruturas estratégicas além das fronteiras lógicas nacionais" (Marini; Pederneiras; Moita, 2024, p. 170).

Um ativo estratégico caro ao Irã foi sabotado sem o ingresso de tropas estrangeiras em seu território (*no boots on the ground*). Esse episódio evidencia características da guerra remota pela modalidade cibernética, onde se provocou danos cinéticos sem a utilização de tropas expedicionárias, mas por meio da

infiltração ou cooptação de agentes no território inimigo que possibilitaram a inserção do *worm* nos computadores iranianos, provavelmente por meio da porta USB (Marini; Pederneiras; Moita, 2024).

Interessante notar a confirmação da teoria clássica da natureza da guerra – política por outros meios – em um contexto de guerra puramente tecnológica, pois, ainda que sua autoria jamais tenha sido reivindicada por qualquer país,

> [...] o Stuxnet pode ser caracterizado como um ato de guerra, de acordo com a percepção clausewitziana, ao levar em consideração que fora um ato político com o intuito de impor seu propósito ao oponente [...] Desse modo, conclui-se que este *worm* funcionou como sendo a continuação da política por outros meios, estes tecnológicos, para impor a sua vontade ao país persa (Marini; Pederneiras; Moita, 2024, p. 175).

Essa breve contextualização histórica demonstra que as práticas de condução da guerra atual guardam relação direta com o núcleo duro do conceito de guerra remota presente no *corpus* de análise (*no boots on the ground*), seja pela utilização de drones, seja pela via da guerra cibernética. E mesmo na abordagem mais estrita, observa-se uma correlação da teoria com os conflitos no território ucraniano e iraniano, saturados pelo emprego de drones. O crivo da realidade, portanto, parece confirmar a teoria.

Retomando a proposta inicial da discussão teórica, nota-se que a abordagem ampla do conceito tem a vantagem de alargar as possibilidades críticas, sobretudo éticas e legais, à conflituosidade contemporânea, mas gera uma sobreposição conceitual em relação a outros termos do campo de estudo da guerra, tal como guerra cibernética (*cyber warfare*), guerra por procuração (*proxy warfare*), sub-rogação e privatização da guerra (*surrogate warfare*), guerra líquida (*liquid warfare*) e guerra vicária (*vicarious warfare*), tal como apontado por Stoddard e Toltica (2021). Esses atravessamentos expõem a procura acadêmica por conceitos capazes de explicar a novidade de intervenções de força baseadas em três premissas: aversão democrática ao risco, tecnologia e redes (Demmers; Gould, 2021).

Quanto ao marco temporal, ele emerge bem definido no *corpus* de análise. Não obstante durante a Guerra Fria ter sido comum o emprego de Forças Especiais, Agentes Secretos, Mercenários e Exércitos por procuração para travar guerras longe dos olhos do público, a gênese da guerra remota é usualmente atribuída à Guerra ao Terror e às guerras subsequentes associadas

no Afeganistão e no Iraque pós 11/9 (Abbott; Hathorn; Hickie, 2016). Essa mesma opinião é compartilhada por Trenta (2021), Biegon; Watts (2022), Rogers; Goxho (2023), Wasiuta (2023), Rogers (2023), Walker (2018) e Zeitlin (2021). A aversão ao risco mostrou-se um componente social relevante (Watts; Biegon, 2021; Biegon; Rauta; Watts, 2021; Stoddard; Toltica, 2021; Wasiuta, 2023; Rogers, 2023).

Cabe uma reflexão, no entanto, sobre a importante questão da distância enquanto qualificadora da guerra remota. Do combate corpo a corpo ao bombardeio aéreo, a arte de matar (*the killing process*) passou por diferentes pontos ao longo do espectro de distância (Grossman, 2009).“[...] a guerra de drones não é tão nova, nem tão distante, nem tão distinta, nem tão indiferente, nem tampouco tão isenta de riscos. Em outras palavras, [...] o distanciamento constitui uma constante na história da guerra — que sempre se desenvolveu, em grau crescente, de forma remota” (Jeangène Vilmer, 2023, p. 913, tradução nossa).[15]

Entretanto, se a “arte” de matar, em seu percurso histórico, passou por diferentes pontos ao longo do espectro de distância, cabe indagar qual seria, afinal, a novidade própria da guerra remota contemporânea. A novidade que emerge é, paradoxalmente, essa mesma distância, porém atualizada por uma conjugação de tecnologias, estratégias e condições políticas que, se empregadas separadamente não definem uma era na condução da guerra, todavia, se combinadas, mostram-se relevantes para a definição de um campo de estudo da conflituosidade contemporânea.

Nesse perspectiva, além da ausência de tropas no terreno (*no boots on the ground*), é possível extrair do *corpus* de análise os seguintes elementos definidores da guerra remota: emprego massivo de armamentos não tripulados (Abbott; Hathorn; Hickie, 2016; Adelman; Kieran, 2018; Biegon; Rauta; Watts, 2021; Stoddard; Toltica, 2021; Walker, 2018; Zeitlin, 2020; Trenta, 2021; Biegon; Watts, 2022; Rogers; Goxho, 2023; Rogers, 2023; Rossiter, 2023a) e guerra cibernética (Abbott; Hathorn; Hickie, 2016; Adelman; Kieran, 2018; Biegon; Rauta; Watts, 2021; Wasiuta, 2023).

[15]Texto original: “[...] drone warfare is not so new, not so distant, not so different, not so indifferent, and not so riskless. In other words, [...] distancing is a constant in the history of warfare—which has always, to an increasing extent, been remote” (Jeangene Vilmer, 2023, p. 913).

De igual modo a utilização de operações especiais e empresas privadas (Abbott; Hathorn; Hickie, 2016; Biegon; Rauta; Watts, 2021; Stoddard; Toltica, 2021; Biegon; Watts, 2022; Rogers; Goxho, 2023; Rogers, 2023), apoio a grupos locais (Biegon; Rauta; Watts, 2021; Stoddard; Toltica, 2021; Riemann; Rossi, 2021; Biegon; Watts, 2022), pouco escrutínio público (Watts; Biegon, 2021; Biegon; Rauta; Watts, 2021; Stoddard; Toltica, 2021; Biegon; Watts, 2022; Wasiuta, 2023; Rogers, 2023) e aversão ao risco (Watts; Biegon, 2021; Biegon; Rauta; Watts, 2021; Stoddard; Toltica, 2021; Wasiuta, 2023; Rogers, 2023).

Considerações Finais

Em que pese o caráter inicial do presente estudo, baseado em número reduzido de textos, percebe-se, pelas reiteradas características colhidas do *corpus* de análise, a emergência de uma teoria sobre a guerra remota caracterizada pelo emprego restrito de tropas no *front* (*no boots on the ground*). Esse emprego econômico de tropas se dá, primordialmente, em razão da tecnologia ou pela utilização de interpostos combatentes, assinalando uma correspondente abordagem teórica estrita ou ampla do fenômeno.

O conceito que emerge, no entanto, é ambíguo e, em grande parte, mostrou-se coincidente com outros termos adotados para designar fenômenos específicos da condução da guerra contemporânea (*warfare*). Por esse motivo, parte da doutrina entende que guerra remota ainda não define um conceito, mas corresponde a um termo, um campo de estudos amplo (Rauta, 2021) ou um jargão – *buzzword* (Biegon *et al*., 2021). Ainda assim, uma carga semântica forte se associa ao termo guerra remota, a denotar uma ação militar bem distante ou, ao menos, controlada à distância. Isso significa que, mesmo na ausência de um conceito preciso, os estudos publicados sob essa terminologia se identificam por aspectos comuns e apontam importantes implicações ético-legais.

A discussão mais premente corresponde à incorporação de Inteligência Artificial aos armamentos não tripulados. À imensa dificuldade de regular a utilização remota dos armamentos, agora se soma a paulatina substituição da própria operação humana pela IA, a desafiar a imputação de responsabilidade pela violência resultante. A guerra remota, em suma, satisfez inicialmente à pretensão das grandes potências de exercer a coerção imperialista sem arriscar

suas tropas no terreno. Contudo, devido ao barateamento das tecnologias, os instrumentos dessa guerra se disseminaram para nações menos ricas e grupos não estatais, permitindo que esses agentes também exerçam violência.

Dessa forma, a guerra remota constitui um grande campo aberto para os estudos futuros na área da conflituosidade moderna, a demandar aprofundamentos acerca do papel do combatente, seu perfil físico e psicológico, a imputação de responsabilidade perante o direito, o poder crescente das ameaças não estatais e a completa desumanização do combate.

Referências

ABBOTT, C; HATHORN, Steve; HICKIE, Scott. *The Remote Warfare Digest. Remote Control Project.* London: Oxford Research Group, 2016.

ADELMAN, R. A.; KIERAN, David. Re-Conceptualizing Cultures of Remote Warfare: Editors' Introduction. *Journal of War & Culture Studies*, v. 11, n. 1, p. 1-4, 2018.

ADELMAN, R. A.; KIERAN, David. Introduction: Rethinking Killing at a Distance. *In*: ADELMAN, Rebecca A.; KIERAN, David (org.). *Remote Warfare*: New Cultures of Violence. Minneapolis: U of Minnesota Press, 2020.

BIEGON, R.; RAUTA, V.; WATTS, T. F. A. Remote warfare–buzzword or buzzkill? *Defence Studies*, v. 21, n. 4, p. 427-446, 2021.

BIEGON, R.; WATTS, T. F. A. Remote warfare and the retooling of American primacy. Geopolitics, v. 27, n. 3, p. 948-971, 2022.

BONDAR, K. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare.* Washington: Center for Strategic and International Studies, 2025. Disponível em: https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare. Acesso em 04 jun. 2025.

CLAUSEWITZ, C. *Da guerra.* São Paulo: Martins Fontes, 1996.

DEMMERS, J.; GOULD, L. The Remote Warfare Paradox: Democracies, Risk Aversion and Military Engagement. *In:* MCKAY, Alasdair; WATSON, Abigail; KARLSHØJ-PEDERSEN, Megan (Ed.). *Remote Warfare*: Interdisciplinary Perspectives. Bristol: E-International Relations publishing, 2021. p. 34-47.

DUARTE, E. E. A conduta da guerra na era digital: conceitos, políticas e práticas. In: SILVA FILHO, E. B.; MORAES, R. F. de. (Org.). *Defesa nacional para o século XXI:* política internacional, estratégia e tecnologia militar. Rio de Janeiro: Ipea, 2012.

GARCIA, M. S. A. *et al*. The Impact of Revolution 4.0 on International Law and Arms Regulation (2016-2024). *Review of Contemporary Philosophy,* v. 24, n. 1, p. 280-288, 2025.

GERTZ, N. *The Philosophy of War and Exile*: From the Humanity of War to the Inhumanity of Peace. London: Palgrave Macmillan, 2014.

GROSSMAN, D. *On killing*: The psychological cost of learning to kill in war and society. New York: Back Bay Books, 2009.

JEANGÈNE VILMER, J.-B. Not so remote drone warfare. *International Politics*, London: Palgrave Macmillan, v. 60, n. 4, p. 897–918, 2023.

KRISHNAN, A. Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict: A Comparison. *Journal of Strategic Security,* v. 15, no. 4, p. 14-31, 2022.

MARINI, A. N. L.; PEDERNEIRAS, L. C.; MOITA, S. T. A guerra cibernética sob a ótica de Clausewitz: um estudo de caso sobre o Stuxnet. *Malala, Revista Internacional de Estudos sobre o Oriente Médio e Mundo Muçulmano, v*. 12, n. 15, p. 159-178, 2024.

MOROSINI, M. C.; NASCIMENTO, L. M. do.; NEZ, E. de. Estado de Conhecimento: metodologia na prática. *Revista Humanidades e Inovação,* v. 8, n. 55, p. 70-81, ago. 2021.

PACE, M. Europe's failure to take decisive action on Middle Eastern issues erodes its global credibility: Israel-Iran: A Fragile Ceasefire and the Shape of Regional Power. *Italian Institute for International Political Studies (ISPI)*

Online, 2025. Disponível em: https://www.ispionline.it/en/publication/israel-iran-a-fragile-ceasefire-and-the-shape-of-regional-power-212331. Acesso em: 1 jul. 2025.

RAUTA, V. A conceptual critique of remote warfare. *Defence Studies*, v. 21, n. 4, p. 545-572, 2021.

RIEMANN, M.; ROSSI, N. Remote warfare as "security of being": Reading security force assistance as an ontological security routine. *Defence Studies*, v. 21, n. 4, p. 489-507, 2021.

ROGERS, J. Rethinking remote warfare. *International Politics*, v. 60, n. 4, p. 781-789, 2023.

ROGERS, J; GOXHO, D. Light footprint — heavy destabilising impact in Niger: why the Western understanding of remote warfare needs to be reconsidered. *International Politics*, v. 60, n. 4, p. 790-817, 2023.

ROLAND, A. *War and technology:* A very short introduction. New York: Oxford University Press, 2016.

ROSSITER, A. Changing Participation in War: Is a Paradigmatic Shift Underway? *Journal of Military and Strategic Studies*, v. 21, n. 1, 2021.

ROSSITER, A. AI-enabled remote warfare: sustaining the western Warfare paradigm? *International Politics,* v. 60, n. 4, p. 818-833, 2023a.

ROSSITER, A. Military technology and revolutions in warfare: priming the drone debate. *Defense & Security Analysis,* v. 39, n. 2, p. 253-255, 2023b.

SAINT-PIERRE, H. L.; ZORZO, M. Tecnologias e despersonalização da violência. In: SAINT-PIERRE, Héctor Luis; LEANDRO, I. A.; MEI, E. (orgs.). *Entre as assombrações do passado e as sementes do futuro: Notas sobre a defesa do Sul Global.* São Paulo: Fundação Perseu Abramo; Hucitec; Cultura Acadêmica Editora, 2023. p. 272-288.

STODDARD, E.; TOLTICA, S. Practising remote warfare: Analysing the remote character of the Saudi/UAE intervention in Yemen. *Defence Studies,* v. 21, n. 4, p. 447-467, 2021.

TRENTA, L. Remote killing? Remoteness, covertness, and the US government's involvement in assassination. *Defence Studies*, v. 21, n. 4, p. 468-488, 2021.

VICENTE, J. P. N. *Da Guerra Remota à Desumanização do Poder Aéreo, a Interferência e a Interação Humana no Futuro da Guerra.* Tese de Doutorado. Lisboa: Universidade NOVA de Lisboa, 2013.

WALKER, D. M. American Military Culture and the Strategic Seduction of Remote Warfare. *Journal of War & Culture Studies*, v. 11, n. 1, p. 5-21, 2018.

WASIUTA, O. Konceptualizacja zdalnej wojny: przeszłość, teraźniejszość i przyszłość. *In*: SKRZYNSKI, Tomasz; JASTRZEBSKI, Jaroslaw. *Polityka - wojskowość - bezpieczeństwo. Księga jubileuszowa z okazji 40-lecia działalności naukowej Profesora Romana Kochnowskiego.* Cracóvia: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego w Krakowie, 2023. p. 522-541.

WATTS, T. F. A.; BIEGON, R. Revisiting the remoteness of remote warfare: US military intervention in Libya during Obama's presidency. *Defence Studies*, v. 21, n. 4, p. 508-527, 2021.

WORCESTER, M. Autonomous Warfare-A Revolution in Military Affairs. *ISPSW Strategy Series*: Focus on Defence and International Security, v. 340, p. 44-53, 2015.

ZEITLIN, M. An Entirely New Method of Conducting War at a Distance The First World War and the Air War of the Future. In: ADELMAN, R. A; KIERAN, D. (Ed.). *Remote Warfare:* New Cultures of Violence. Minneapolis: University of Minnesota Press, 2020.

Parte III

Estado, Governança e Defesa: perspectivas atuais

Mídias sintéticas em conflitos armados:
tensões ao comando e controle e ao Direito Internacional Humanitário[1]

Matheus Henrique de Souza
Rômulo Ferreira dos Santos
Jaime de Melo Gama da Silva

Introdução

Na história da guerra, o atrito franco entre tropas foi gradualmente substituído por manobras evasivas e estratégias, motivo pelo qual sobram relatos históricos da projeção sistemática de poder por meio da desinformação. Ocorre que a guerra de informação de outrora estava limitada à prática estatal, porque não contava com métodos robustos de produção de mídias. As recentes evoluções tecnológicas, particularmente no campo da inteligência artificial (IA) generativa, alteram profundamente essa realidade, porque ampliam a escala, a velocidade e a qualidade dessas práticas e, em certa medida, permitem a participação da população civil.

Nesse contexto, os conflitos armados ampliaram sua área de atuação também para o ciberespaço, no qual começam a despontar registros do emprego de mídias sintéticas, com a clara intenção de impactar as operações militares. Essa nova fase da guerra de informação destaca riscos operacionais e políticos, na medida em que afetam a credibilidade de autoridades e de instituições, fragilizando as fronteiras seguras entre o real e o sintético. A eficiência desses novos usos da IA suscita debates sobre a maior dificuldade em diferenciar o civil e o combatente nos conflitos armados, porque agora a participação nas hostilidades pode ser difusa; o que impõe também repensar o alcance da jurisdição penal internacional.

[1] Neste artigo, foi utilizada a ferramenta ChatGPT (GPT-$^{5.5}$) como apoio à geração de ideias, à revisão gramatical, à indicação de fontes para leitura e à tradução. O conteúdo intelectual, as interpretações, as conclusões e a redação final foram integralmente elaborados, revisados e validados pelos autores, que assumem total responsabilidade pelo trabalho apresentado.

Nesse sentido, as *deepfakes*, que são uma espécie maliciosa do gênero mídias sintéticas, iniciam uma nova geração de instrumentos que adensam a névoa da guerra, por atingirem o que se entendia como referenciais seguros da verdade: vídeos, fotos e áudios. As consequências dessas simulações altamente verossímeis em conflitos armados vão além do mero engano, porque podem fraudar ordens ilegítimas ou criar um falso arcabouço de informações que sustentam decisões complexas. Esse impacto pode ser percebido na função de combate Comando e Controle (C^2), porque ela é elemento estruturante da ação militar, tanto no que diz respeito ao processo de tomada de decisão, quanto no que se refere às estruturas que culminam no cumprimento das ordens.

Para além disso, a IA generativa está difundida na sociedade e qualquer pessoa pode tornar-se um editor de mídia de alta qualidade, o que concede à população civil poder de influenciar efetivamente na guerra de informação nos conflitos armados. Com isso, a aplicação do estatuto de proteção à população civil, consagrado no Direito Internacional Humanitário (DIH), fica tensionada quando se percebe o potencial dessas mídias de provocar hostilidades tão significativas quanto as causadas pelos combatentes. Essa nova realidade faz com que os tipos penais consagrados no Direito Penal Internacional passem a ser repensados para abarcar essa evolução dos fatos sociais, porquanto as mídias sintéticas tendem a aumentar o potencial de simulações que caracterizariam o cometimento do crime de guerra de perfídia.

Diante desse contexto, surge o seguinte questionamento: como o uso malicioso de mídias sintéticas, especialmente *deepfakes*, nos conflitos armados contemporâneos afeta o exercício da função de combate C^2 e tensiona a aplicação das normas do DIH e do Direito Internacional Penal? Para respondê-lo, adotou-se inicialmente uma abordagem analítico-conceitual para delimitar o fenômeno das mídias sintéticas, seguida de uma análise dogmático-jurídica do marco normativo internacional aplicável aos conflitos armados. Busca-se, assim, examinar em que medida os efeitos operacionais descritos tensionam categorias jurídicas clássicas, bem como identificar os limites e as possibilidades de responsabilização no plano internacional.

Para isso, o primeiro tópico do capítulo examina o fenômeno apontado, ou seja, o uso malicioso de mídias sintéticas para influenciar os conflitos armados, o que restou materializado na *deepfake* veiculada em 2022 contra o presidente ucraniano Volodymyr Zelensky. O segundo tópico examina os

impactos desse fenômeno na função de combate C², para demonstrar como o desgaste da verdade factual dificulta o exercício da autoridade, tanto no que diz respeito à credibilidade das ordens transmitidas, quanto na tomada de decisão nublada por informações inseguras. Por fim, o terceiro tópico examina as questões de direitos humanos suscitadas e que tensionam o DIH, além das constatações de que a jurisdição da Corte de Haia pode ser ampliada para abarcar ações praticadas no ambiente cibernético.

Mídias sintéticas e guerra de informação no conflito armado russo-ucraniano

O dicionário de Oxford declarou "pós-verdade" como a palavra do ano de 2016 (Dunker *et al*., 2018, p. 7), definida, em tradução própria, como "relacionado a circunstâncias nas quais as pessoas respondem mais a sentimentos e crenças do que aos fatos". Os autores estabelecem que a pós-verdade é consequência direta das transformações promovidas na pós-modernidade, tempo em que debates relevantes questionaram a verdade como valor absoluto, permitindo o esgarçamento dos limites aceitáveis que separam os fatos das opiniões. Nesse cenário de relativização da verdade e, consequentemente, da credibilidade das fontes de informação, as mídias sintéticas produzidas por IA generativa surgem como uma arma poderosa com potencial para fragilizar o que se entendia por "verdade".

As transformações tecnológicas promovidas a partir do final do século XX já impuseram cuidados no trato com a informação, particularmente no que diz respeito aos riscos de fraudes praticadas por meios cibernéticos. Nesse tempo, as imagens (estáticas ou vídeos) e áudios desfrutavam de uma aura de segurança, haja vista que demandavam um conhecimento profundo de design para serem manipulados com qualidade – fazendo com que fossem raros os casos de fraudes. Esse tempo ficou para trás, porque segundo Schick (2020, p. 9), com o surgimento das *deepfakes* – um tipo de mídia sintética (áudio, imagens e vídeo manipulados ou totalmente gerados por IA) produzida com fins maliciosos –, surge o potencial para transformar qualquer pessoa com um smartphone, mesmo com pouco conhecimento em design, em um produtor de vídeos de alta qualidade.

Esse tipo de mídia impulsiona a complexa guerra de informação contemporânea, em que Estados fazem usos políticos e militares da cultura de pós-verdade para modificar a percepção da história à medida em que ela acontece. Essa guerra não surge com a IA, como aponta o registro do governo britânico de que a Rússia conduziu operações dessa natureza em uma escala massiva para afastar sua responsabilidade pela queda do voo MH-17, da Malaysia Airlines, que ocorreu em 2014 (Schick, 2020, p. 12). Todavia a IA agrava esse cenário, no qual as mídias sintéticas despontam como ferramentas que podem difundir e tornar mais efetivo esse tipo de operação, o que contribui para o agravamento da crise da confiança no século XXI.

A guerra de informação está intimamente relacionada com os conflitos armados contemporâneos, que passam a se projetar no espaço cibernético, onde os efeitos maliciosos das *deepfakes* ganham relevância como instrumentos de corrosão da credibilidade das autoridades e dos processos decisórios. À medida que os conflitos armados evoluem, passando da guerra de atrito que marcou a 1ª Guerra Mundial para as manobras militares que evitaram esse atrito na 2ª Guerra Mundial (Simioni, 2025, p. 209), o exercício da autoridade tornou-se mais complexo. No cenário que surge após as guerras mundiais, particularmente com a relevância que ganha o ambiente cibernético nos conflitos, o domínio da informação projeta poder capaz de influenciar os rumos dos conflitos armados, porque condiciona o comportamento das massas e tem o potencial de provocar mudanças sociais relevantes.

Por isso, a doutrina militar mais atual trata a informação como recurso essencial, componente do que se entende como ambiente operacional, ao incluir o ambiente cibernético como um dos domínios de operação possível (junto do terrestre, marítimo, aéreo e espacial) e a informação como uma das três dimensões que impactam nesse ambiente – além da física e da humana (Brasil, 2025, p. 2-2). A dimensão informacional tem sua importância destacada na doutrina militar, porque o seu uso eficaz pode enganar, confundir e influenciar a vontade de combater. Essa característica da informação fica nítida no caso paradigmático selecionado para este estudo, em que a *deepfake* produzida contra o presidente ucraniano pretendeu, além de enganar a tropa (e a população) sobre a rendição, corroer a confiabilidade da população nos meios de comunicação do país (Akkus, 2025, p. 19).

O portal CNN Brasil (Metz, 2022) noticiou que em 16 de março de 2022 tornou-se viral no Facebook um vídeo *deepfake* em que o presidente ucraniano, Volodymyr Zelensky, apresenta uma falsa rendição à Rússia. Ainda segundo o portal, o autor da falsificação empregou estratégias para esconder a qualidade ruim da falsificação, como diminuir a resolução do vídeo (o que esconde as imperfeições) e a utilização do brasão de armas ucraniano como elemento de credibilidade. Não há indícios de que a fraude tenha impactado na movimentação de tropas, porém o caso tornou-se notório, porque um hacker teria inserido um texto noticiando o vídeo durante uma transmissão ao vivo da emissora *TV Ukraine 24* (Cluley, 2022).

Diante da repercussão, o então Chefe da Política de Segurança da Meta, Nathaniel Gleicher, informou no mesmo dia (16 de março de 2022) que a equipe reviu e removeu o vídeo rapidamente, por considerá-lo manipulado/enganoso, além de ter notificado os pares de outras plataformas. Apesar da baixa qualidade da película, sua transmissão em uma emissora de TV, além da viralização em rede social, motivou a manifestação do presidente Zelensky, que veio à público recusar a autoria do vídeo (*Institute of Mass Information*, 2022). Uma análise comparativa rápida entre a mídia sintética e uma foto real permitem perceber que, neste caso, a falsificação poderia ser facilmente identificada pelo observador comum.

Embora pobre, a fraude atinge um objetivo estratégico muito importante na guerra de informação: descredibilizar, em qualquer medida, os canais de comunicação e o próprio líder do país. Falsificações dessa natureza dificilmente serão recebidas como ordens pelas tropas, todavia essas falsificações podem ser lembradas em futuros pronunciamentos autênticos de autoridades, levantando dúvida e incerteza sobre sua veracidade. Essa desconfiança da fonte pode ser particularmente prejudicial se acarretar demora na reação a informações críticas, que demandam respostas urgentes, como a evacuação de áreas com risco iminente de serem atingidas pelo conflito armado.

O caso de *deepfake* que envolveu Volodymyr Zelensky não foi o único desse conflito armado, como mostra o caso do pronunciamento do presidente russo anunciando uma mobilização em massa das forças russas em maio de 2023 e do anúncio do representante do Departamento de Estado dos EUA autorizando o uso de armas americanas no conflito russo-ucraniano em maio de 2024, ambos *deepfakes*. Também sobram registros de usos civis e políticos, tanto de

cheapfakes (edições mais simples e de baixo custo, sem uso de IA avançadas) quanto de *deepfakes*, como as largamente empregadas na comunicação digital do primeiro mandato presidencial de Trump nos EUA (Schick, 2020, p. 58-60). Como um dos exemplos, Schick (2020, p. 60) aponta a publicação que marcou a transição, no *twitter* do Presidente Trump, das *cheapfakes* para as *deepfakes*, quando ele compartilhou em 2020 um vídeo de Joe Biden apoiando a sua candidatura ao dizer "Nós só podemos reeleger Donald Trump".

O uso de mídias sintéticas nos contextos narrados tende a aumentar, porque elas foram revolucionadas pelas *Generative Adversarial Networks* (GANs), que possibilitaram a geração de *deepfakes* hiper-realistas, que desafiam a distinção entre o real e o fabricado. Essa tecnologia, embora tenha aplicações legítimas em entretenimento, medicina e pesquisa, tornou-se um instrumento geopolítico de desinformação com impactos diretos em processos eleitorais e estabilidade democrática. Segundo Liu *et al*. (2025, p. 1), as GANs estão no centro da revolução das *deepfakes*, pois permitem tanto a criação de novos conteúdos quanto a manipulação de conteúdos existentes.

A precisão crescente desses modelos, especialmente quando combinados com modelos de difusão (*Diffusion Models*), intensifica o desafio de detectar falsificações, exigindo sistemas de verificação cada vez mais sofisticados. Os detectores de *deepfakes* treinados em ambientes laboratoriais falham em identificar falsificações políticas reais, especialmente as compartilhadas em redes sociais. Isso leva à conclusão de que o uso de GANs e técnicas correlatas amplia o alcance da manipulação geopolítica, ameaçando a confiança pública e a estabilidade institucional (Lin *et al*., 2025, p. 26). Por fim, destacam que o jogo de gato e rato entre geradores de *deepfakes* e detectores alimenta uma corrida tecnológica com profundas implicações éticas e políticas (Liu *et al*. 2025, p. 13).

Assim, os estudos convergem em apontar que as GANs são hoje ferramentas centrais tanto na criação quanto no combate às *deepfakes*, configurando um campo estratégico na geopolítica digital contemporânea. O uso político de mídias sintéticas redefine o cenário da informação, propaganda e guerra cibernética, exigindo regulamentações internacionais, desenvolvimento ético de IA e educação midiática como medidas urgentes de mitigação. Isso evidencia a necessidade de modelos mais generalizáveis e resistentes à

manipulação adversarial, sobretudo diante do uso político de mídias sintéticas (Abbasi *et al*., 2025, p. 14).

Diante dos desafios emergentes, cresce de importância que os Estados estabeleçam medidas, no ambiente cibernético, para prevenir usos maliciosos, detectar ataques antecipadamente, responsabilizar infratores e mitigar os danos provocados aos cidadãos e às instituições. Na esteira desses objetivos, é importante destacar a necessidade de que a Doutrina Militar Terrestre se aprofunde sobre o uso de mídias sintéticas no contexto de conflitos armados, a fim de evitar que causem danos às operações militares. Isso, porque os fatos destacados neste capítulo relatam o uso de *deepfake* com o intuito imediato de transmitir informações ou ordens falsas, podendo produzir o efeito mediato de descredibilizar as autoridades, dificultar a tomada de decisão e tornar inseguros os meios de comunicações.

Quando mídias sintéticas se pretendem verdadeiras para transmitir informações ou ordens em um conflito armado, elas criam dúvidas sobre toda a infraestrutura de comunicações, tornando-a insegura. As dúvidas quanto à veracidade das ordens emitidas fragilizam a autoridade, gerando retardos no acatamento dos imperativos, e a nuvem de informações falsas nubla a percepção correta e atual do contexto tático, dificultando o processo decisório que precede a emissão das ordens. Por isso é importante compreender os impactos que as mídias sintéticas causam à função de combate C², que é composta justamente por autoridade, processo decisório e infraestrutura. Esse é o objetivo do capítulo seguinte.

Desafios das mídias sintéticas à função de combate Comando e Controle

Existe uma dificuldade conceitual na definição do que é "verdade", especialmente no que diz respeito aos fatos do cotidiano, que podem ser percebidos de forma distinta a depender do observador. Quando analisou a relação entre verdade e política, Arendt (2000, p. 548) diferenciou a verdade matemática, científica e filosófica (aquela derivada da razão) da verdade factual (que registra os fatos ocorridos no mundo, mas que depende, para isso, de testemunho e registro para comprovar sua existência). Para a autora, a verdade factual é relevante no reino da política, porque os fatos influenciam o comportamento

das pessoas, mas eles não podem ser pressupostos ou comprovados pela lógica, o que faz com que a sua existência esteja constantemente em disputa.

A disputa pela existência dos fatos é terreno fértil para as mídias sintéticas, que conseguem modificar ou criar registros e testemunhos com muito mais facilidade do que desacreditar uma constatação lógica. A título de exemplo, uma deepfake teria maior credibilidade ao tentar comprovar que dois mais dois são quatro ou ao inserir uma fala não pronunciada em um vídeo previamente registrado? Como apontou a própria Arendt (2000, p. 548, tradução livre), "fatos e eventos são coisas infinitamente mais frágeis que axiomas, descobertas, teorias – mesmo as mais especulativas – produzidas pela mente humana".

Ocorre que o C², assim como a política, tem como pressuposto epistemológico a verdade factual, pois depende de uma percepção precisa e atualizada do ambiente operacional, que não pode ser obtida por meio da lógica, mas pela comprovação dos fatos. Por outro lado, a política possui uma histórica relação de distanciamento da verdade (Arendt, 2000, p. 545), enquanto o C² depende indissociavelmente dela (atualizada, diga-se de passagem, pois mesmo o atraso em sua transmissão pode tornar falsa a informação). Nesse sentido, a *deepfake* produzida contra o presidente ucraniano é particularmente alarmante, pois evidencia uma progressão: do uso histórico da mentira para fins políticos para um uso estratégico da mentira de alta qualidade, voltado a adensar a névoa da guerra.

Neste ponto, é importante a imersão no conceito de C² para aprofundar o argumento de que ele opera sob a lógica da verdade factual, e que por isso será profundamente impactado pelo uso de mídias sintéticas nos conflitos armados. Partindo da literatura estrangeira, o Departamento de Defesa dos Estados Unidos da América o define como o "exercício da autoridade e direção por um comandante devidamente designado sobre as forças atribuídas para o cumprimento da missão" (Hoehn; Campbell; Bowen, 2022, p. 1). O conceito americano está centrado na autoridade, mas implícita também no processo prévio para a tomada de decisão e as estruturas necessárias para garantir que essas decisões, transformadas em ordens, culminem no êxito das missões – somente assim a autoridade pode ser exercida, para além de estar simplesmente constituída.

Na doutrina do Exército Brasileiro, o C² conta com três componentes que se relacionam de forma cíclica, tendo em vista o caráter dinâmico dos conflitos armados, o que torna constante a necessidade de direcionamento das ações. A autoridade (i) recebe as informações que permitem o exercício do controle e materializa o comando ao emanar as decisões. O processo decisório (ii) envolve processar as informações para garantir uma decisão coerente com o contexto tático, além de transformá-las em ordens; para tal, é preciso estruturar o fluxo de informações que pressupõe o processo intelectual da decisão, além de estabelecer mecanismos que garantam a execução das ordens emanadas. Para esses fins, a infraestrutura (iii) é indispensável, haja vista a complexidade no trâmite de informações em um conflito armado, particularmente na atual fase da guerra, que ocorre em áreas descentralizadas e complexas, o que demanda enfoque em pessoal, equipamento, doutrina e tecnologia (Brasil, 2023, p. 1-3).

No Estado de Direito, inaugurado com a Revolução Francesa, a autoridade só pode ser legitimada formalmente no âmbito do ordenamento jurídico em que se insere, e não pode ser pressuposta logicamente por nenhum critério (seja ele força, genialidade, liderança, ou qualquer outro). No Brasil, a autoridade é estruturada em níveis de antiguidade e protegida pelas prerrogativas da hierarquia, conforme estabelecido no § 1º do art. 14 da Lei nº 6.880/1980 (Estatuto dos Militares) e no art. 24 do Decreto-Lei nº 1.001/1969 (Código Penal Militar). O sistema hierárquico das Forças Armadas visa garantir o cumprimento das ordens, estabelecendo que a autoridade competente detém o poder de direcionar a ação dos militares diretamente subordinados (no que seja pertinente à vida castrense e nos limites da legalidade, conclusão que decorre do estado de necessidade coativo previsto no art. 38 do Código Penal Militar).

Isso significa dizer, apropriando-se dos ensinamentos de Bobbio (2014a, p. 60), que a autoridade no Brasil não é definida pela lógica jusnaturalista, porque a sua validade não depende de ser o ato que a constituiu reconhecido como justo, mas de uma lógica positivista, porque basta ser válido juridicamente o ato que constitui um militar em autoridade para que seja considerado justo. Para esclarecer, propomos a compreensão de que o ato de conduzir homens para o cumprimento do dever é chamado de "liderança" em uma acepção jusnaturalista, quando é estudada na ciência militar e incentivada no cotidiano, e de "autoridade" na acepção positivista, quando trata do que estabelece o ordenamento jurídico vigente. Em outros termos, a liderança é material,

relacionada com a pessoa, enquanto a autoridade é formal, relacionada com o ato jurídico que a constituiu.

Ao se estabelecer que a autoridade é constituída formalmente, chega-se à constatação dos riscos que as mídias sintéticas apresentam ao seu exercício. O exercício da autoridade, materializado em ordens, produz verdades factuais, comprovadas de forma empírica; o que implica que, falseado a transmissão de uma ordem juridicamente legal, como a *deepfake* do Zelensky, a aparência de verdade formal supera a eventual contradição lógica material. Portanto, ainda que o subordinado entendesse que a rendição não fosse correta, ao constatar a veracidade da ordem, seu cumprimento torna-se um imperativo, não uma faculdade, cujo descumprimento implica no Brasil em ilícito penal (arts. 149, 169, 196, 374, todos do Código Penal Militar, para citar alguns).

Além dos riscos relacionados ao cumprimento de ordens falsas, como apontado até então, as mídias sintéticas também impactam o processo decisório no que diz respeito às informações que fundamentam as decisões. Nesse ponto é importante diferenciar a ordem, que viabiliza a direção das ações dos subordinados no sentido do cumprimento do dever, da informação, que é a verdade factual propriamente dita, definida na doutrina militar como os "dados e fatos que foram organizados e comunicados de forma coerente e com significado, e a partir dos quais se pode tirar conclusões" (Brasil, 2023, p. 2-9). É nesse ponto que as mídias sintéticas mais podem adensar a névoa da guerra, diante da possibilidade de produzir informações falsas em larga escala e da crescente qualidade dessas fraudes.

Existe uma relação indissociável entre o conceito militar de informação e a consciência situacional, que se ramifica em dois campos: a percepção precisa e atualizada do ambiente operacional em que se atua; e o reconhecimento da importância de cada elemento em relação à missão atribuída. A consciência situacional trata da produção de informações no conflito armado, mas de uma perspectiva mais ampla, abarcando também a gestão dessa informação e os meios e técnicas que a produzem, com o fim de garantir uma visão do ambiente operacional que melhor direcione a tomada de decisão. Por isso a doutrina estabelece que quanto mais precisa a percepção, melhor; mas não só isso, que essa percepção seja entregue às pessoas certas e no momento oportuno (Brasil, 2023, p. 2-9).

A importância da consciência situacional surge da constatação de que os conflitos armados estão envoltos em uma névoa de incerteza, na qual não só as prospecções se tornam difíceis (na guerra impera o acaso), mas as emoções constantemente assumem o lugar da razão na tomada de decisões (Clausewitz, 1832, p. 109). Isso, porque a informação na guerra é pouco confiável e momentânea (Clausewitz, 1832, p. 129), afinal de contas sobram relatos históricos do uso da desinformação nesses períodos, como a prática da Alemanha nazista, durante a Segunda Guerra Mundial, de transmitir informações falsas por estações rádio, visando que elas fossem replicadas pela BBC inglesa (Bender, 2025, p. 226). O que muda com as mídias sintéticas atuais é: a qualidade, que dificulta a distinção do real; a facilidade de produção, que aumenta a sua ocorrência; e a difusão desse tipo de manipulação para autores não estatais, o que dificulta a sua identificação e responsabilização.

Até aqui foram analisados os riscos das mídias sintéticas para dois componentes do C^2, a autoridade e o processo decisório, com o intuito de destacar que quando empregadas de forma maliciosa (exemplo das *deepfakes*) visam não apenas enganar, mas desorganizar. A autoridade pode ser descredibilizada diante da possibilidade de transmissão de ordens falsas, o que pode gerar atraso no cumprimento das ordens verdadeiras; e a névoa da guerra, que naturalmente atrapalha o processo decisório, pode ficar mais obscura se houver necessidade constante de separar o conteúdo real do sintético. O terceiro componente, a infraestrutura, desponta com potencial para mitigar esses riscos, desde que a preocupação com a segurança seja tratada como prioridade inegociável.

A Doutrina Militar Terrestre já estabeleceu cultura organizacional e procedimentos para garantir a troca de informações seguras em hipóteses de emprego finalístico (defesa da pátria), sob o título de Medidas de Proteção Eletrônica (Brasil, 2014, p 1-3). No âmbito da infraestrutura, despontam como técnicas que podem diminuir os riscos de que transitem mídias sintéticas fraudulentas nos meios de comunicações oficiais: o emprego de criptografia manual e digital nas mensagens, a criptografia dos dados nas transmissões físicas e os procedimentos de autenticação entre os operadores. Todavia, a eventual eficiência da guerra cibernética impõe considerar o risco de que mídias dessa natureza transitem nos meios oficiais (militares ou não), como foi o caso da *deepfake* do presidente ucraniano noticiada em uma emissora de TV do país.

Por isso, é importante que a preocupação com a integridade da informação esteja em todo o seu fluxo, para que os militares que participam dele adotem métodos de detecção de mídias sintéticas na transmissão/recepção de informações. Um desses métodos é baseado em características artesanais, em que a observação visual crítica da mídia, por quem tenha permissão para visualizá-la, busca falhas perceptíveis no processo de geração de imagens, como olhos de cor diferentes, dentes desenhados de forma grosseira ou outras assimetrias (Verdoliva, 2020, p. 10). Outro método seria também empregar tecnologias de aprendizado profundo para identificar as mídias sintéticas, buscando as impressões digitais artificiais das arquiteturas GAN ou incorreções na manipulação dos frames de vídeos (Verdoliva, 2020, p. 11), entre outras técnicas.

É fato que esses métodos de detecção serão muito desafiados para acompanhar a evolução das tecnologias de geração de mídias sintéticas, como apontam Chesney e Citron (2019, p. 1787), pela dificuldade de superar a geração cada vez melhor, que implicará na necessidade constante de atualizações. Ainda assim, esforços nesse sentido evitam prejuízos decorrentes de falsificações grosseiras, de modo que, alinhados com as técnicas de autenticação e criptografia, ajudam no combate a esse tipo de ataque. Disso surge a importância de que sejam incentivados no âmbito do Sistema Tático de Comunicações, para que os militares no nível tático sejam vetores de identificação de fraudes.

Quadro 1 – Impactos operacionais das mídias sintéticas nos componentes do C² (continua)

Componente	Vetor de impacto	Efeito operacional provável	Linhas de mitigação
Autoridade	Falsificação de pronunciamentos e ordens e erosão de confiança	Atraso no acatamento, contestação da legitimidade e ruído na cadeia de comando	Protocolos de autenticação, canais redundantes e *challenge–response* operacional
Processo decisório	Insumos informacionais manipulados e "névoa" de falsidades	Decisão sob premissas falsas e aumento de fricção e tempo de decisão	Verificação multi-fonte, critérios de confiabilidade e células de OSINT/ forense

Componente	Vetor de impacto	Efeito operacional provável	Linhas de mitigação
Infraestrutura	Compromete/ contamina os meios de transmissão	Amplifica o risco ao longo do fluxo informacional	Criptografia, autenticação, detecção/forense e governança de segurança

Fonte: Elaborado pelos autores (2026).

Diante dos desafios trazidos pelo uso malicioso das mídias sintéticas para o C² (Quadro 1), cresce de importância identificar e desmentir com oportunidade esse tipo de conteúdo, a fim de garantir que os elementos subordinados cumpram apenas ordens verdadeiras e que as autoridades decidam baseadas apenas em verdades factuais legítimas. Ocorre que para mitigar a difusão do uso malicioso de mídias sintéticas em conflitos armados, para além de estabelecer procedimentos operacionais que diminuam sua influência, é preciso responsabilizar os autores que cometem crimes com a produção desse tipo de conteúdo. Esse debate sobre responsabilização poderia ter como foco o ordenamento jurídico interno, centrado nos crimes autorais, contra a proteção de dados ou contra a honra, mas como o plano de fundo deste trabalho são os conflitos armados, o campo de estudo não pode ser outro, senão o DIH. É sobre o que trata o próximo capítulo.

Tensões das mídias sintéticas ao Direito Internacional Humanitário e ao Direito Internacional Penal

Bobbio (2014a, p. 48) ensina que as normas jurídicas podem ser submetidas a três diferentes valorações: quanto à justiça (correspondência aos valores que inspiram um ordenamento jurídico), eficácia (se é ou não seguida pelos destinatários) ou validade (existência da regra). Com base nessa distinção, Bobbio (2014a, p. 55, *apud* Verdross, 1950, p. 98-99) apresenta que a justiça é de interesse do filósofo da moral, a eficácia é interesse do sociólogo, cabendo ao teórico do direito a competência para compreender a forma do direito e a conexão intrínseca das normas positivas (sua validade). Com base nisso, fica estabelecido que o presente capítulo limitar-se-á à área do teórico jurídico, o que permite adotar como pressuposto epistemológico a validade das normas jurídicas internacionais nessa nova fase difusa da guerra de informação.

É importante esclarecer que não é a validade *strictu sensu* (no sentido de vigência) das normas internacionais que está em análise, mas a sua capacidade de acompanhar os desafios que as mídias sintéticas criam para os conflitos armados sem permitir o surgimento de lacunas. Essa análise, que está inserida no campo do Direito Internacional Público, concentra-se em dois ramos distintos: o DIH, em que se debatem os costumes e limites da guerra; e o Direito Internacional Penal, em que se estabelece a responsabilização de quem comete crimes de maior gravidade, em desrespeito a esses costumes e limites. Delimitado o objeto de estudo do capítulo, o primeiro passo é esclarecer se os produtores de mídias sintéticas maliciosas podem ser tratados como partes no conflito, o que define o seu estatuto de proteção e os deveres no âmbito do DIH.

É o Direito de Genebra, subdivisão do DIH, que estabelece estatutos protetivos, os quais estão materializados nas quatro Convenções de Genebra, de 12 de agosto de 1949, bem como nos seus dois Protocolos Adicionais, como mais bem desenvolvido em trabalho anterior (Bender; Souza, 2025, p. 133). O conceito de combatente consta do art. 13 da Primeira Convenção de Genebra, assim entendidos (de modo geral) os membros das forças armadas e de milícias que tomem parte nas hostilidades. Por outro lado, os civis gozam de proteção contra os efeitos nefastos dos conflitos armados, exceto se participarem diretamente das hostilidades e enquanto durar essa participação, conforme consta no art. 51 do Protocolo Adicional I às Convenções de Genebra.

Ocorre que as normas internacionais não estabelecem o que significa a participação direta nas hostilidades, a qual justificaria a perda temporária (durante a prática da hostilidade) da proteção da população civil. Quem fornece um entendimento sobre esse conceito é a Comitê Internacional da Cruz Vermelha (Melzer, 2009, p. 46), que o identifica como a prática individual (direta ou indiretamente, a depender da natureza e do grau do envolvimento) de meios e métodos destinados a causar dano ao inimigo. Para enquadrar uma conduta como participação direta nas hostilidades, o guia interpretativo da Cruz Vermelha aponta três elementos constitutivos, quais sejam:

> 1. o ato deve ser suscetível de afetar adversamente as operações militares ou a capacidade militar de uma parte em um conflito armado ou, alternativamente, de infligir morte, ferimentos ou destruição a pessoas ou bens protegidos contra ataques diretos (limiar de dano); e 2. deve haver um nexo causal direto entre o ato e o dano que provavelmente resultará desse ato ou de uma operação militar coordenada da qual

> esse ato constitua parte integrante (causalidade direta), e 3. o ato deve ser especificamente concebido para causar diretamente o limiar de dano exigido, em apoio a uma parte no conflito e em detrimento de outra (nexo beligerante) (Melzer, 2009, p. 46, tradução livre).

O uso de desinformação para ocultar aspectos importantes de operações militares é um procedimento normalizado na guerra, como afirmam Chesney e Citron (2019, p. 1783) citando os esforços dos Aliados para enganar o Eixo quanto à localização da invasão na Normandia, em junho de 1944 (ficou conhecida como Operação Guarda-costas). Ocorre que as mídias sintéticas possuem potencial para agravar essa prática e impactar significativamente operações militares, como apontam Chesney e Citron (2019, p. 1776), ao exemplificarem que uma *deepfake* mostrando soldados assassinando civis inocentes em uma zona de guerra pode ocasionar ondas de violência; ou um vídeo que anuncia falsamente um ataque de mísseis em uma cidade, pode provocar grave pânico. As estratégias de desinformação impulsionadas pelas mídias sintéticas possuem dimensões sistêmicas, difíceis de mensurar, mas com potencial de causar hostilidades tão violentas quanto as da própria guerra.

Isso permite reconhecer, voltando aos três elementos constitutivos apontados pela CICV, que as mídias sintéticas possuem "limiar de dano", porque podem impactar diretamente as operações militares, inclusive culminando em mortes ou ferimentos. Acontece que é muito difícil reconhecer a "causalidade direta" entre a mídia e o suposto impacto à guerra, porque os seus efeitos são especulativos e abstratos, difíceis de antecipar ou mensurar – além de ser difícil isolar de outros fatos igualmente importantes que podem acontecer concomitantemente. Também é difícil estabelecer um "nexo beligerante" nesse caso, particularmente quando é produzida por civis, justamente porque os efeitos da produção e veiculação de uma mídia sintéticas não são tão óbvios quanto o disparo de uma arma de fogo – é possível produzir uma mídia com efeitos maliciosos, mas é difícil diferenciar a estratégia de guerra da mera manifestação pública de opinião.

Vale ressaltar, porém, que as vítimas desse tipo de estratégia de desinformação não são apenas os combatentes, porque a população civil também é afetada não só em sua percepção da realidade, mas eventualmente pelas externalidades negativas que decorrem dessa mídia, como uma onda de violência. Por isso é que Akkus (2025, p. 18) aponta que é difícil compatibilizar

o uso de *deepfakes* em conflitos armados com o dever de proteção à população civil positivado no art. 48 do Protocolo I adicional às Convenções de Genebra. Sendo assim, o uso de *deepfakes* em conflitos armados pode violar a proteção da população civil se por si só caracterizar uma operação militar (há autores que defendem essa possibilidade – Akkus, 2025, p. 18, *apud* Dunstein, 2016), ou se ocorrer no contexto de uma, como em uma campanha de desinformação que antecede uma invasão (como ocorreu na ocupação de Manchúria pelo exército imperial japonês em 1931 – obviamente com método arcaico, sem a *deepfake*).

Por isso, a participação direta nas hostilidades por meio da produção/veiculação de mídias sintéticas está no universo das possibilidades, mas é de tão difícil caracterização, que a suspensão da proteção garantida aos civis deve ser excepcional para evitar decisões precipitadas pela névoa da guerra. Diferentemente de quem pega em armas para alvejar um combatente inimigo, o civil que emprega desinformação não deve perder o status de pessoa protegida nem passar a ser considerado combatente, o que significa que não é autorizado que contra ele sejam praticadas as hostilidades características da guerra. Isso não significa que o uso de mídias sintéticas na guerra deva ficar impune, mas para isso existe a responsabilização *a posteriori*, feita com a adequada análise jurídica do fato, o que leva à segunda parte desta argumentação.

Quando o estudo direciona para a análise da responsabilização criminal por atos praticados em conflitos armados (internacionais ou não), em decorrência da afirmação de que contra o criador ou veiculador de mídias sintéticas não se deve praticar hostilidades, invariavelmente direciona para o Direito Internacional Penal. Husek (2017, p. 43) ensina que esse ramo do Direito Internacional Público é um campo amplo de estudo que abarca a punição de criminosos internacionais, a persecução dos crimes internacionais, a cooperação judiciária entre Estados e o funcionamento de Tribunais Penais Internacionais. Nesse oceano temático, a relação intrínseca que o objeto de estudo tem com a guerra indica que o recorte feito neste segundo grande argumento será sobre a jurisdição da Corte de Haia, inaugurada pelo Estatuto de Roma de 1998, o único Tribunal Penal Internacional instaurado com a finalidade de permanência (Husek, 2017, p. 336).

Não existe uma previsão específica sobre o uso de mídias sintéticas em conflitos armados (Akkus, 2025, p. 13), o que é de certa forma óbvio, tendo em vista o descompasso temporal entre essas tecnologias e a redação do Estatuto

de Roma. Ainda assim, a ausência de previsão expressa não pode implicar em uma lacuna, porque a completude de um ordenamento jurídico impõe o uso da integração para adequar as normas aos fatos sociais novos, como ensina Bobbio (2014b, p. 138). Isso viabiliza que Akkus (2025, p. 13) aponte a possibilidade de que uma *deepfake* possa caracterizar a prática de perfídia, proibida pelo art. 37 do Protocolo I adicional às Convenções de Genebra e considerada crime de guerra previsto no art. 8º, § 2º, alínea b, inciso XI do Estatuto de Roma.

Para definir perfídia, a definição da Convenção de Genebra é mais indicada, por ser mais descritiva, pois estabelece que é a prática de hostilidades em sequência a um ato de boa-fé para com o adversário, seja por traição ou por fazer entender que o adversário teria direito à proteção, ou de que estaria obrigado a conceder a proteção ao adversário. Os exemplos apresentados pela norma referem-se a um ofensor que leva o adversário a não usar a força por meio de uma das seguintes simulações: falsa intenção de negociar sob bandeira de rendição ou armistício; falsa incapacidade ou enfermidade; falsa condição de pessoal civil; ou uso indevido de sinais de proteção reconhecidos, como os de pessoal de saúde. Por outro lado, a norma internacional, no § 2º do art. 37 em questão, diferencia a perfídia dos estratagemas (permitidos), que são os atos que visam induzir a erro o inimigo para que aja com imprudência, mas sem simular boa-fé ou fazer uso malicioso dos estatutos de proteção do Direito de Genebra, como a camuflagem e as informações falsas.

Percebendo que a informação falsa pode tanto caracterizar um crime de perfídia, quanto um estratagema normal de guerra, fica claro que a diferença entre os dois reside na distorção da boa-fé ou no uso dos estatutos protetivos como pretexto para a prática de hostilidades. Avançando no cenário visualizado por Akkus (2025, p. 9), caracterizaria perfídia o ato de civil que produz uma *deepfake* em que um comandante do país X ordena rendição aos seus homens, apenas para que os adversários do país Y acreditem e avancem suas tropas sem preocupação e sejam alvejados pelo exército de X (não rendido). Por outro lado, seria um mero estratagema a *deepfake* que mostra de forma realista a destruição da principal fortificação do exército adversário, o que Akkus (2025, p. 10) aponta como uma operação psicológica normal, porém baseada em mídia sintética.

Diante disso, o vídeo *deepfake* contra o presidente Zelensky, divulgado em 2022, flerta perigosamente com a tipificação de perfídia, porque poderia

ter impactado a movimentação do adversário, levando soldados russos a avançarem no território, até descobrirem a falsidade da rendição após serem alvejados pelo exército ucraniano. É claro que, como já tratado e constatado por Akkus (2025, p. 17), o episódio em questão fez uso de uma falsificação ruim, de difícil credibilidade, motivo pelo qual não repercutiu no campo de batalha – afastando a responsabilização do seu criador/veiculador por perfídia. Porém, como também já fora tratado neste estudo, as mídias sintéticas são tecnologias em ascensão, cuja qualidade tende a melhorar exponencialmente, permitindo que falsificações dessa natureza possam repercutir nos conflitos armados concretamente.

Diante das tensões possíveis (Quadro 2), resta constatar que as soluções para os desafios criados pelas mídias sintéticas são complexas, até porque as *deepfakes* não são problemas exclusivos do DIH, porque tensionam também os ordenamentos jurídicos internos, em diversas áreas além da criminal (Akkus, 2025, p. 14). A título de exemplo, existem fronteiras abertas relacionadas ao uso de IA no campo da propriedade intelectual, que carece de um estatuto jurídico de suas saídas. Esses desafios somam-se a outros que as arquiteturas baseadas em IA impõem ao domínio da paz e da segurança internacionais, como destacado em trabalho anterior que evidenciou a lacuna de *hard law* específica para sistemas de armas letais autônomas (Dos Santos *et al*., 2025, p. 83).

Quadro 2 – Tensões jurídicas e pontos críticos de responsabilização (DIH/DIP) (continua)

Eixo jurídico	Categoria	Como o fenômeno tensiona	Gargalo
DIH	Distinção (civil/ combatente)	Participação civil difusa em operações informacionais com efeitos relevantes	Identificar quando há participação direta e por quanto tempo
DIH	Participação direta nas hostilidades	Dificuldade de enquadrar atos informacionais com efeitos indiretos/difusos	Causalidade direta, nexo beligerante e mensuração do dano
DIP	Perfídia (crime de guerra)	Simulações verossímeis podem instrumentalizar confiança/boa-fé e enganar o adversário	Elementos subjetivos, probatórios e prova de intenção e resultado

Eixo jurídico	Categoria	Como o fenômeno tensiona	Gargalo
Jurisdição	Responsabilização internacional	Possível ampliação/ repensar alcance diante de condutas cibernéticas	Atribuição padrões de prova, cooperação e preservação de evidência

Fonte: Elaborado pelos autores (2026).

Por isso, Chesney e Citron (2019, p. 1789) discutem soluções tecnológicas e jurídicas e ressaltam as dificuldades de proibir as *deepfakes*, principalmente pelos danos causados à liberdade de expressão, uma vez que não são sempre criminosas, embora sempre maliciosas. Partindo da análise dos autores, é possível introduzir uma hipótese superficial de solução: impor que as *deepfakes* sejam veiculadas com o esclarecimento de suas intenções, algo similar ao tratamento dado às publicidades ocultas impulsionadas por plataformas digitais (Simas; Souza Júnior, 2018, p. 24). Assim, as *deepfakes* veiculadas sem intenção esclarecida causariam dano considerado *in re ipsa*, em que a reparação civil decorreria da simples existência do fato ilícito somada ao seu nexo de causalidade com o envolvido, já que pretendia maliciosamente se passar pela verdade.

Com isso, resta constatar que o emprego de mídias sintéticas no contexto de conflitos armados, como registrado na guerra russo-ucraniana, tende a aumentar e se agravar na medida em que a qualidade das *deepfakes* aprimorar-se-á. Por isso o DIH e o Direito Internacional Penal continuarão a ser tensionados por casos concretos que corroem a dicotomia combatente/civil e influenciam a ocorrência de hostilidades graves. Para isso, o princípio da distinção no DIH precisa ser reforçado, a fim de evitar violações a direitos fundamentais; e, como indica Akkus (2025, p. 26), os novos métodos e usos da guerra cibernética indicam que a jurisdição da Corte de Haia precisa ser repensada.

Considerações Finais

Os conflitos armados observados nesse início de século XXI, como o russo-ucraniano, inserem-se em um contexto de emprego massivo de tecnologias no campo de batalha, dentre as quais ganha destaque o uso de mídias sintéticas para acentuar as operações informacionais. Cresce de importância,

por isso, compreender como essa nova realidade desafia o exercício da função de combate C² e tensiona tanto o princípio da distinção no DIH, quanto a tipificação da perfídia no Direito Internacional Penal. Esse olhar para o uso malicioso das mídias sintéticas (exemplificada com as *deepfakes*) nos conflitos armados oportuniza uma análise multidisciplinar, que aponta as interseções entre a doutrina militar operacional e as normas jurídicas limitadoras e punitivas das hostilidades.

É importante destacar que o uso de mídias sintéticas em conflitos armados não é hipotético, porque já conta com exemplos concretos, como o caso das *deepfakes* envolvendo o presidente ucraniano Volodymyr Zelensky. Essa prática encontra terreno fértil nos conflitos armados, porque eles se orientam com base em uma versão da verdade que Arendt chama de factual, ou seja, aquela que para ter credibilidade demanda a comprovação da sua existência por documentos e/ou testemunhos. Por isso, com o crescente potencial das mídias sintéticas de apresentar provas falsas com extremo realismo, a névoa da guerra se torna mais obscura, devido ao impacto direto na credibilidade das autoridades e instituições.

No âmbito desses impactos, são crescentes os desafios ao exercício do C², porque a consciência situacional (vetor importante dessa função de combate) também se orienta pela verdade factual e depende, portanto, da credibilidade da informação e da integridade da cadeia de comando. Cabe ressaltar que as mídias sintéticas despontam como riscos cibernéticos de que decisões sejam tomadas com base em informações manipuladas, ou de que ordens falsas sejam recebidas como verdadeiras. Por isso, as *deepfakes* (espécie de uso malicioso de mídias sintéticas) agravam as preocupações quanto à legitimidade/credibilidade das autoridades e à integridade do processo decisório que culmina em ordens.

Esses desafios operacionais jogam luz às tensões jurídicas que surgem dessa nova guerra de informação, na qual os civis estão cada vez mais envolvidos (pela proliferação de tecnologias de IA generativa) e suas ações impactam cada vez mais o teatro de operações. Diante desse novo cenário, a distinção entre combatentes e civis torna-se ainda mais complexa, o que não significa que o estatuto de proteção às pessoas civis deva ser desrespeitado, mas reforçado para impedir violações aos direitos humanos nos conflitos armados. Esse reforço pode ser buscado, quando presentes os requisitos, na responsabilização jurídica das pessoas que fazem uso malicioso de mídias sintéticas perante o Tribunal

Penal Internacional, quando praticarem atos pérfidos, ou seja, que simulem boa-fé ou estatutos protetivos com o fim de praticar hostilidades.

Diante do exposto, resta observar que o impacto do uso malicioso de mídias sintéticas em conflitos armados reverbera nas doutrinas militar e jurídica e estabelece um elo entre fenômenos tecnológicos, operacionais e normativos. Essa visão multidisciplinar atende ao objetivo geral proposto e indica que as transformações materiais da sociedade contemporânea impulsionam discussões sobre operações militares ao mesmo tempo que tensionam os marcos regulatórios jurídicos. Isso reforça a percepção de que a guerra é um fenômeno social complexo, que pelos seus efeitos nefastos tanto impulsiona os estudos militares, quanto demanda regulações jurídicas humanitárias.

Quanto a limitações do estudo, esta pesquisa: (i) não se pretende exaustiva, nem esgota soluções técnico-operacionais de proteção da informação no ciclo de C^2; (ii) não realiza mensuração empírica dos efeitos operacionais (quantificando impacto em tempos de decisão, taxa de cumprimento de ordens ou escalada de hostilidades); e (iii) concentra-se no plano normativo internacional, reconhecendo que a jurisdição internacional é complementar e que as respostas domésticas (cíveis e penais) apresentam desafios adicionais.

À luz do exposto, recomenda-se aprofundar: (i) modelos de atribuição em operações informacionais com mídias sintéticas (cadeias de custódia digital, padrões de rastreio e vínculo entre criador, disseminador e efeitos); (ii) padrões de prova e autenticação aplicáveis a evidências audiovisuais em ambientes de conflito (incluindo critérios técnico-periciais mínimos e "doutrina de autenticação" no C^2); (iii) deveres e responsabilidades de plataformas e intermediários (detecção, rotulagem, remoção e preservação de metadados para responsabilização), considerando tensões entre segurança, liberdade de expressão e necessidades humanitárias; e (iv) a adequação tipológica de categorias do DIH/DIP diante de efeitos difusos, especialmente em torno de participação direta nas hostilidades e perfídia em ecossistemas cibernético-informacionais.

Referências

ABBASI, M.; VAZ, P. J. A.; SILVA, J. Comprehensive Evaluation of Deepfake Detection Models: Accuracy, Generalization, and Resilience to Adversarial Attacks. *Applied Sciences*, v. 15, n. 3, p. 1225, 2025. DOI: https://doi.org/10.3390/app15031225. Acesso em: 1 fev. 2026.

AKKUS, B. Deepfakes and the Geneva Conventions: Does Deceptive AI-Generated Misinformation Directed at an Enemy During Armed Conflict Violate International Humanitarian Law? A Critical Discussion. *Laws*, v. 14, n. 6, p. 83, 2025. DOI: https://doi.org/10.3390/laws14060083. Acesso em: 26 jan. 2026

ARENDT, H. *The Portable Hannah Arendt.* New York: Penguin Books, 2000.

BENDER, J. M.; DE SOUZA, M. H. O princípio da distinção no direito internacional humanitário e a guerra dos drones: repensando a definição de alvos legítimos a partir do conflito russo-ucraniano. *Revista O Comunicante,* v. 1, n. 1, p. 131–141, dez. 2025. Disponível em: https://www.escom.eb.mil.br/index.php/sistemas/revistas/summary/4-revista/14-revista-2025. Acesso em: 26 jan. 2026.

BENDER, J. *O que você ainda não sabe sobre 1964*: ideologia & polarização na Guerra Fria do Brasil. Curitiba: Appris, 2025.

BOBBIO, N. *Teoria da norma jurídica*. Tradução de Ariani Bueno Sudatti e Fernando Pavan Baptista. 5. ed. São Paulo: Edipro, 2014a.

BOBBIO, N. *Teoria do Ordenamento Jurídico.* Tradução de Ari Marcelo Solon. 2. ed. São Paulo: Edipro, 2014b.

BRASIL. Decreto nº 4.388, de 25 de setembro de 2002. Promulga o Estatuto de Roma do Tribunal Penal Internacional. *Diário Oficial da União*, 26 set. 2002, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2002/d4388.htm. Acesso em: 26 jan. 2026.

BRASIL. Decreto nº 42.121, de 21 de agosto de 1957. Promulga as Convenções concluídas em Genebra, a 12 de agosto de 1949, destinadas a proteger as vítimas da guerra. *Diário Oficial da União,* 9 set. 1957, Rio

de Janeiro, RJ. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1950-1969/d42121.htm. Acesso em: 26 jan. 2026.

BRASIL. Decreto nº 849, de 25 de junho de 1993. Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados. *Diário Oficial da União*, 28 jun. 1993, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0849.htm. Acesso em: 26 jan. 2025.

BRASIL. Decreto-Lei nº 1.001, de 21 de outubro de 1969. Código Penal Militar. *Diário Oficial da União*, 21 out. 1969, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/6880.htm. Acesso em: 26 jan. 2026.

BRASIL. Exército Brasileiro. *Comando e Controle***.** Manual de Campanha EB70-MC-10.205. 1ª ed. Aprovado pela Portaria – COTER/C Ex nº 331, de 20 de setembro de 2023. Brasília, DF: Comando do Exército, 2023.

BRASIL. Exército Brasileiro. *Medidas de Proteção Eletrônica*. Caderno de Instrução EB70-CI-11.403. 1ª ed. Aprovado pela Portaria – COTER nº 1, de 14 de fevereiro de 2014. Brasília, DF: Comando de Operações Terrestres, 2014.

BRASIL. Exército Brasileiro. *Operações*. Manual de Campanha MC 3.0. 6ª ed. Aprovado pela Portaria – COTER/C Ex nº 527, de 24 de abril de 2025. Brasília, DF: Comando do Exército, 2025.

BRASIL. Lei nº 6.880, de 9 de dezembro de 1980. Dispõe sobre o Estatuto dos Militares. *Diário Oficial da União*, 11 dez. 1980, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6880.htm. Acesso em: 26 jan. 2026.

CHESNEY, R.; CITRON, D. K. Deep fakes: a looming challenge for privacy, democracy, and national security. *California Law Review,* v. 107, n. 6, p. 1753–1819, 2019. Disponível em: https://ssrn.com/abstract=3213954. Acesso em: 23 jan. 2026.

CLAUSEWITZ, C. von. *Da guerra.* Tradução de Luis Carlos Nascimento e Silva do Valle. Rio de Janeiro: Biblioteca do Exército, 1984.

CLULEY, G. *Deepfake President Zelensky calls on Ukraine to surrender, as TV station hacked.* Bitdefender Blog, 17 mar. 2022. Disponível em: https://www.bitdefender.com/en-us/blog/hotforsecurity/deepfake-president-zelensky-calls-on-ukraine-to-surrender-as-tv-station-hacked. Acesso em: 26 jan. 2026.

DUNKER, C.; SAFATLE, V.; SILVA JUNIOR, N. da; KUPERMANN, D. (org.). *Ética e pós-verdade.* São Paulo: Dublinense, 2018.

DOS SANTOS, R. F. *et al.* A Inteligência Artificial e o Direito Internacional: desafios e oportunidades na regulação de tecnologias emergentes. IOSR *Journal of Business and Management*, v. 27, n. 9, p. 78–89, 2025. Disponível em: https://www.iosrjournals.org/iosr-jbm/papers/Vol27-issue9/Ser-3/I2709037889.pdf. Acesso em: 1 fev. 2026.

HOEHN, J. R.; CAMPBELL, C.; BOWEN, A. S. *Defense primer: what is command and control?* Washington, DC: Congressional Research Service, 2021. Disponível em: https://apps.dtic.mil/sti/html/trecms/AD1132997/. Acesso em: 26 jan. 2026.

HUSEK, C. R. *Curso de direito internacional público.* 14. ed. São Paulo: LTr Editora, 2017.

INSTITUTE OF MASS INFORMATION. Ukraina 24 TV's ticker tape hacked, streaming fakes about Zelenskyy's "capitulation". 16 mar. 2022. Disponível em: https://imi.org.ua/en/russias-crimes/ukraina-24-tvs-ticker-tape-hacked-streaming-fakes-about-zelenskyys-capitulation. Acesso em: 26 jan. 2026.

LIN, G.; LIN, L.; WALKER, C. P.; SCHIFF, D. S.; HU, S. *Fit for purpose? Deepfake detection in the real world*. arXiv preprint, 2025. Disponível em: https://arxiv.org/abs/2510.16556. Acesso em: 1 fev. 2026.

LIU, B.; LIU, B.; ZHU, T.; DING, M. A review of deepfake and its detection: from generative adversarial networks to diffusion models. *International Journal of Intelligent Systems,* v. 2025, n. 1, art. 9987535, 2025. DOI: https://doi.org/10.1155/int/9987535. Acesso em: 1 fev. 2026.

MELZER, N. *Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law.* Geneva: International Committee of the Red Cross, 2009.

METZ, R. *Facebook remove vídeo falso de Zelensky rendendo-se à Rússia.* CNN Brasil, 16 mar. 2022. Disponível em: https://www.cnnbrasil.com.br/internacional/facebook-remove-video-falso-de-zelensky-rendendo-se-a-russia/. Acesso em: 26 jan. 2026.

SCHICK, N. *Deepfakes: the coming infocalypse.* London: Hachette UK, 2020.

SIMAS, D. C. de S.; SOUZA JÚNIOR, A. M. de. Sociedade em rede: os influencers digitais e a publicidade oculta nas redes sociais. *Revista de Direito, Governança e Novas Tecnologias*, v. 4, n. 1, p. 17–32, 2018. DOI: https://doi.org/10.26668/IndexLawJournals/2526-0049/2018.v4i1.4149.

SIMIONI, A. A. C. Uma visão da evolução das guerras modernas: a ameaça da guerra cibernética no conflito de quarta geração. *Revista Marítima Brasileira,* v. 131, n. 01/03, p. 202-221, 2011. Disponível em: https://portaldeperiodicos.marinha.mil.br/index.php/revistamaritima/article/view/7067. Acesso em: 23 jan. 2026.

VERDOLIVA, L. Media forensics and deepfakes: an overview. *IEEE journal of selected topics in signal processing*, v. 14, n. 5, p. 910-932, 2020. Disponível em: https://ieeexplore.ieee.org/abstract/document/9115874. Acesso em: 23 jan. 2026.

Centralização das compras públicas de defesa: governança, eficiência e o caso do Exército Brasileiro[1,2]

Marcelo Batista Soares Barroso
Peterson Ferreira Silva

Introdução

O presente estudo examina a centralização das compras públicas de defesa como instrumento de governança, eficiência administrativa e modernização logística, tomando como estudo de caso a experiência do Exército Brasileiro. Para tanto, estrutura-se metodologicamente segundo os pressupostos do Estado do Conhecimento (Morosini; Kohls-Santos; Nez, 2021), buscando mapear, sistematizar e analisar criticamente a produção científica nacional e internacional sobre centralização administrativa e sua aplicação na gestão pública de defesa. O objetivo central foi compreender em que medida os modelos teóricos de centralização dialogam com os resultados concretos alcançados pelo Exército Brasileiro, especialmente na racionalização de processos, na otimização de recursos e no fortalecimento da governança institucional no campo das compras públicas.

A investigação buscou identificar como as abordagens conceituais presentes na literatura especializada se traduzem em impactos administrativos,

[1] Versão preliminar foi apresentada no V ERABED Sudeste, na modalidade híbrida, em 7 de outubro de 2025. As ideias e pontos de vista deste texto expressam o pensamento de seus autores, sendo de inteira responsabilidade deles, não representando necessariamente posições oficiais de qualquer órgão ou entidade do governo brasileiro.

[2] Neste artigo, foi utilizada a ferramenta Google NotebookLM (Gemini) como apoio à organização do corpus bibliográfico, à análise preliminar de resumos, à identificação de padrões temáticos e à categorização de referências. O conteúdo intelectual, as interpretações, as conclusões e a redação final foram integralmente elaborados, revisados e validados pelos autores, que assumem total responsabilidade pelo trabalho apresentado.

logísticos e institucionais quando aplicadas a organizações complexas e intensivas em recursos, como as Forças Armadas. Nesse sentido, o estudo buscou analisar simultaneamente as interpretações acadêmicas e os resultados empíricos observados na implementação do modelo centralizado no Quartel-General do Exército (QGEx). A partir desse diálogo, pretende-se analisar as potencialidades, os limites, as tensões e as lições institucionais decorrentes da centralização das compras públicas de defesa.

Com base no referencial metodológico de Morosini e Fernandes (2014), a pesquisa identifica os núcleos teóricos predominantes, os padrões interpretativos e as lacunas investigativas que configuram o campo de estudo sobre centralização administrativa. A sistematização do corpus bibliográfico permite não apenas mapear as abordagens existentes, mas também situar a experiência do Exército Brasileiro em um contexto comparado, favorecendo interpretações mais amplas e rigorosas sobre eficiência, governança e modernização no setor público de defesa.

O estudo insere-se em um processo mais amplo de modernização administrativa do Estado brasileiro, iniciado com as reformas institucionais da década de 1990. O marco inaugural desse ciclo foi o Plano Diretor da Reforma do Aparelho do Estado (PDRAE), de 1995, que consolidou os fundamentos da Nova Administração Pública (NAP) no país. Inspirada por essa agenda, a administração pública brasileira passou a adotar princípios como eficiência, eficácia, foco em resultados e *accountability* como vetores de reorganização da máquina estatal (Bresser-Pereira, 1998).

No setor de defesa brasileiro, essa orientação traduziu-se em iniciativas institucionais e normativos estratégicos de racionalização da gestão e a modernização da administração militar.

A criação do Ministério da Defesa, em 1999, representou um marco na tentativa de integrar a atuação das Forças Armadas sob uma coordenação única centralizada. Esse processo foi aprofundado com a instituição do Estado-Maior Conjunto das Forças Armadas (EMCFA) e da Secretaria de Produtos de Defesa (SEPROD), ambos criados em 2010, com o objetivo de promover a integração interforças, coordenar aquisições estratégicas e fortalecer a governança logística. Em setembro de 2019, foi aprovada a Diretriz de Obtenção Conjunta de Produtos de Defesa (PRODE) e de Sistemas de Defesa (SD), com a finalidade

de orientar as aquisições da administração central do Ministério da Defesa e das Forças Armadas em bases cooperativas e integradas.

Nesse contexto, a literatura especializada destaca que a criação do Ministério da Defesa representou uma inflexão institucional relevante no modelo brasileiro de governança da defesa, ao estabelecer um centro civil de coordenação estratégica e de planejamento de capacidades militares. Para Rudzit e Nogami (2010), a institucionalização da defesa como política pública setorial, subordinada ao poder civil, insere-se no processo mais amplo de consolidação do Estado democrático e de racionalização das políticas de segurança nacional. Já Bruneau e Tollefson (2014) argumentam que a criação do Ministério da Defesa e, posteriormente, do Estado-Maior Conjunto das Forças Armadas, contribuiu para a reconfiguração das relações civil-militares no Brasil, reduzindo prerrogativas corporativas e fortalecendo mecanismos institucionais de coordenação, planejamento e controle, ainda que persistam desafios relacionados à capacitação técnica da burocracia civil e à integração efetiva dos sistemas de gestão.

Adicionalmente, a instituição da Secretaria de Produtos de Defesa (SEPROD) e a aprovação da Diretriz de Obtenção Conjunta de Produtos de Defesa e de Sistemas de Defesa reforçam a orientação estratégica para a racionalização das aquisições militares e para a indução de arranjos cooperativos interforças. Conforme Bruneau e Tollefson (2014), a modernização da governança da defesa no Brasil tem sido acompanhada pela ampliação do arcabouço normativo e pela valorização de instrumentos de coordenação central, em consonância com modelos internacionais de gestão de capacidades militares. Nesse sentido, a literatura converge ao apontar que a integração institucional, a padronização de processos e a centralização seletiva das compras estratégicas constituem vetores fundamentais para o aumento da eficiência, da transparência e da efetividade operacional, desde que sustentados por capacidades estatais robustas e por estruturas administrativas profissionalizadas (Rudzit; Nogami, 2010; Bruneau; Tollefson, 2014).

No âmbito do Exército Brasileiro, observa-se a adoção de medidas normativas que reafirmam o compromisso institucional com a racionalização da gestão e a modernização da administração pública militar. A Portaria nº 295-EME, de 2014 (Brasil, 2014), instituiu a Diretriz de Racionalização Administrativa no Exército, orientando as Organizações Militares à adoção de

práticas voltadas à eficiência, à padronização de processos e à melhor alocação dos recursos públicos. Em continuidade a esse esforço institucional, a Portaria nº 442-EME, de 2017 (Brasil, 2017), estabeleceu a criação do Almoxarifado Central no âmbito do Quartel-General do Exército, como estrutura unificada de apoio logístico. A esse movimento somam-se outros marcos relevantes: a Portaria EME/C Ex nº 325, de 22 de fevereiro de 2021 (Brasil, 2021), que aprovou a Diretriz de Implantação da Centralização do Sistema de Transporte do QGEx; a Portaria EME/C Ex nº 891, de 13 de outubro de 2022 (Brasil, 2022a), que definiu os procedimentos, responsabilidades e prazos para a centralização das licitações e aquisições de bens e serviços comuns, não finalísticos, na Divisão de Licitações da Base Administrativa do QGEx; e a Portaria nº 1.525, de 14 de maio de 2025 (Brasil, 2025), que estabeleceu a centralização dos processos de pagamento de pessoal das Organizações Militares do QGEx na mesma Base Administrativa, consolidando-a como núcleo operacional da governança administrativa local.

O tema assume especial relevância diante da conjuntura fiscal brasileira. A compressão das despesas discricionárias, somada ao crescimento rígido das despesas obrigatórias, restringe progressivamente a capacidade de investimento e manutenção das Forças Armadas. A projeção de esgotamento do espaço fiscal até 2033 (Brasil, 2022b) evidencia a necessidade de modelos de gestão capazes de reduzir custos, eliminar redundâncias, aumentar transparência e elevar a eficiência no uso de recursos públicos. Nesse cenário, a centralização administrativa emerge como estratégia institucional imprescindível para sustentabilidade orçamentária e eficiência operacional da Defesa.

Esse debate articula-se ao corpo teórico sobre governança pública, que destaca que processos de centralização tendem a fortalecer a coordenação institucional, melhorar o controle interno, aprimorar a padronização de procedimentos e maximizar o uso compartilhado de recursos (Serrão, 2017; Procópio; Oliveira Junior, 2021; Pires, 2004).

A criação do Almoxarifado Central do QGEx, inaugurado em 2021, consolidou a transição de um modelo descentralizado e oneroso para uma estrutura integrada e orientada por resultados (Tinoco Junior, 2021).

Nesse debate, o Almoxarifado Virtual Nacional (AVN) destaca-se como exemplo paradigmático de inovação em compras públicas. Estudos evidenciam que sua adoção gerou ganhos de escala e racionalização na Polícia Rodoviária

Federal (Affonso; Ogawa, 2021), redução de preços e previsibilidade de consumo no Exército Brasileiro (Inácio, 2024), e agilidade operacional no Comando da Aeronáutica (Maciel, 2024; Gomes, 2024).

O caso do QGEx evidencia que a centralização pode elevar a eficiência administrativa, aprimorar o controle de estoques, reduzir custos e fortalecer o planejamento e a transparência das compras públicas, contribuindo de forma concreta para o debate sobre a modernização da gestão no setor de defesa.

Introdução à metodologia do Estado de Conhecimento

Conforme delineado por Morosini et al. (2021), a metodologia estrutura-se em três etapas fundamentais, Bibliografia Anotada, Bibliografia Sistematizada e Bibliografia Categorizada. Neste trabalho, uma quarta fase, a Bibliografia Propositiva foi apresentada. A inclusão dessa etapa adicional representa uma evolução em relação à proposta original, ao conferir ao Estado do Conhecimento um caráter analítico e construtivo ainda mais pronunciado, superando a lógica de uma revisão meramente descritiva e posicionando-o como instrumento para gerar proposições, tensionar modelos vigentes e orientar agendas de pesquisa e de gestão (Morosini; Kohls-Santos, 2021). No campo dos Estudos de Defesa, essa abordagem também tem sido empregada para mapear a inserção de temas emergentes na produção acadêmica nacional (Caminha, 2024). O Quadro 1 sintetiza as etapas metodológicas adotadas.

Quadro 1 – Etapas do Estado de Conhecimento

ETAPAS	DEFINIÇÕES
1. Bibliografia Anotada	Identificação e seleção, a partir da pesquisa por descritores, dos materiais que farão parte do corpus de análise.
2. Bibliografia Sistematizada	Leitura flutuante dos resumos dos trabalhos para a seleção e o aprofundamento das pesquisas, a fim de elencar os que farão parte da análise e escrita do estado do conhecimento.
3. Bibliografia Categorizada	Reorganização do material selecionado, ou seja, do corpus de análise e reagrupamento destes em categorias temáticas.
4. Bibliografia Propositiva	Organização e apresentação de, a partir da análise realizada, proposições presentes nas publicações e propostas emergentes a partir da análise.

Fonte: Kohls-Santos, P.; Morosini, M. C. (2021), p. 127.

Para garantir consistência e rastreabilidade na gestão do corpus, empregaram-se o Zotero, responsável pela organização das referências, controle de duplicações e sistematização dos metadados, e o Google NotebookLM, ferramenta de inteligência artificial aplicada à análise textual, que permitiu a leitura automatizada de resumos, objetivos e métodos, apoiando a definição dos eixos temáticos.

A constituição do corpus foi guiada por critérios de rigor metodológico e pertinência temática, considerando o caráter estratégico da centralização administrativa no Exército Brasileiro e a natureza interdisciplinar do objeto, que articula administração pública, logística institucional, compras governamentais e Defesa Nacional. A Biblioteca Digital de Teses e Dissertações (BDTD/IBICT) foi selecionada como base central para a busca de dissertações e teses, em virtude de sua capilaridade nacional e vínculo com programas *stricto sensu* avaliados pela CAPES. O Catálogo de Teses e Dissertações e o Portal de Periódicos da CAPES foram utilizados como fontes complementares, permitindo acesso a trabalhos revisados por pares e indexados em periódicos de excelência.

Em complemento, o Google Acadêmico e o Google Books foram empregados como instrumentos de rastreamento ampliado, especialmente úteis para localizar obras de circulação internacional, capítulos de livros, estudos não indexados em bases tradicionais e autores de alta frequência de citações. Embora apresentem menor curadoria científica, essas plataformas mostraram-se fundamentais para captar tendências emergentes e lacunas teóricas ainda não plenamente incorporadas a repositórios institucionais. Foram também consultadas bases especializadas, como SciELO e a Revista Brasileira de Estudos de Defesa (RBED), cuja linha editorial se orienta pela interseção entre políticas públicas, segurança internacional, poder militar e governança estratégica.

No plano prático-aplicado, incorporaram-se os repositórios da ENAP e os anais de eventos como ENABED e ERABED, que concentram estudos sobre inovação na gestão pública, logística governamental e análise de políticas em contextos complexos; bem como os repositórios da Escola Superior de Defesa (ESD), da Escola Superior de Guerra (ESG) e da Escola de Comando e Estado-Maior do Exército (ECEME), que conferem ancoragem institucional e prática ao corpus, ao reunir produções de oficiais, pesquisadores e gestores diretamente envolvidos na transformação administrativa da Defesa.

A seleção dos descritores estruturou-se em três eixos conceituais: Eficiência Administrativa e Racionalização, Governança Logística e Inovação e Gestão em Estruturas de Defesa. A partir desses eixos, foram elaboradas expressões compostas em português e inglês, combinadas por operadores booleanos (“AND”), tais como “centralização administrativa” AND “forças armadas” e “administrative centralization” AND “armed forces”. Foram excluídos descritores genéricos e termos isolados, como “gestão pública” ou “Exército”, por gerarem elevado ruído informacional e retornarem estudos alheios ao foco na centralização da gestão e nas compras públicas de defesa.

O levantamento inicial identificou 3.090 produções científicas. A partir de critérios de aderência temática, consistência metodológica e relevância estratégica, entendida como capacidade de dialogar com a agenda de governança e eficiência na Defesa, o corpus foi progressivamente refinado até alcançar 18 trabalhos selecionados, entre teses, dissertações, artigos e estudos técnicos. Foram excluídos 3.072 documentos, em geral por apresentarem abordagem genérica de gestão pública, foco estritamente jurídico ou histórico, ausência de percurso metodológico explícito, redundância temática, orientação exclusivamente técnico-operacional ou caráter descritivo sem densidade analítica.

Quadro 2 – Quantitativo de bibliografias encontradas

Base de Dados	Produções Localizadas	Produções Selecionadas
BDTD (IBICT)	71	5
CAPES	1	0
Google Acadêmico	3.002	5
Google Books	3	2
Repositório ESD/ESG	8	4
SciELO / RBED / ABED	0	0
Repositório ENAP	5	2
Total Geral	**3.090**	**18**

Fonte: Elaborado pelos autores (2025).

A etapa de categorização, fundamentada na técnica de análise de conteúdo de Bardin (2011), constituiu o ponto de inflexão entre a sistematização do corpus e a construção de proposições teóricas. A partir da leitura aprofundada das 18 produções selecionadas, consolidaram-se três grandes eixos temáticos. O primeiro, Eficiência Administrativa e Racionalização Logística, reúne seis estudos que analisam estratégias de centralização de processos, serviços e compras sob a perspectiva da economicidade, da padronização e da redução de custos, em contextos como universidades federais, estruturas administrativas do Exército e bases da Força Aérea (Melo, 2019; Pires, 2020; Porto, 2021; Procópio; Oliveira Junior, 2021; Maciel, 2024; Simões, 2020).

Quadro 3 – Bloco temático Eficiência Administrativa e Racionalização Logística (continua)

Base de Dados	Nº	Ano	Autor(es)	Título	Objetivo	Resultados
BDTD	1	2019	Hallilson Cosmo de Melo	Análise comparativa da execução orçamentária, centralizada vs. descentralizada	Comparar os resultados da execução orçamentária do CCAE (centralizado ou descentralizado).	O modelo descentralizado mostrou-se mais eficiente para os campi interioranos da UFPB.
BDTD	2	2020	Marco Aurélio Gall Pires	Efeitos da centralização do exame de pagamento de pessoal para as OM de Santa Maria	Apresentar os efeitos da centralização do exame de pagamento de pessoal em Santa Maria	Aumentou a eficiência e racionalização; apontada demora na resolução de inconsistências nos pagamentos

Base de Dados	Nº	Ano	Autor(es)	Título	Objetivo	Resultados
Google Acadêmico	1	2021	Juliana Bustamante Porto	A centralização nas aquisições da saúde após a criação do Centro de Aquisições Específicas	Avaliar os impactos percebidos com a centralização das aquisições da saúde no CAE	Redução do tempo de aquisição, melhoria na satisfação dos usuários, ganhos de eficiência nos processos
Google Acadêmico	2	2021	Cassius Eduardo de Souza Procópio, Márcio de Oliveira Júnior	Economicidade no sistema de compras centralizadas no Exército Brasileiro: estudo de caso do modelo utilizado na Guarnição de Brasília	Analisar se o sistema de compras centralizadas gera maior economicidade no Exército Brasileiro	Modelo estatístico comprova maior economicidade nas compras centralizadas em Brasília; sugere replicabilidade nacional
ESG	1	2024	Leonardo Teixeira Maciel	Análise dos impactos da implementação do Almoxarifado Virtual Nacional Base Aérea de Anápolis	Analisar os impactos da implementação do AVN na gestão da cadeia de suprimentos da BAAN	Redução de custos, melhoria na qualidade e velocidade das entregas; sugerida ampliação do AVN para outros itens
ENAP	1	2020	Felipe Guedes Simões	Análise do processo de aquisição realizado no Grupamento de Apoio do Distrito Federal	Mapear e avaliar os processos de compras centralizadas realizados pelo GAP-DF	O estudo mostrou que a centralização das aquisições no GAP-DF gerou benefícios como padronização

Fonte: Elaborado pelo autores (2025).

O segundo eixo, Governança Logística e Inovação, agrega seis trabalhos que tratam da centralização como instrumento de governança, integração de sistemas, serviços compartilhados, adoção de critérios de sustentabilidade e uso de tecnologias da informação em compras públicas e logística de defesa (Zsidisin *et al.*, 2020; Góis; Ouro; Mendonça, 2024; Araújo, 2017; Silveira, 2021; Soares, 2022; Amaral; Silva, 2022).

Quadro 4 – Bloco temático Governança Logística e Inovação

Base de Dados	Nº	Ano	Autor(es)	Título	Objetivo	Resultados
Google Acadêmico	1	2020	George A. Zsidisin; Amanda Bresler; Ben Hazen; Keith F. Snider; Taylor H. Wilkerson	*Research in defense logistics: where are we and where are we going?*	Fornecer uma visão crítica sobre os principais temas de interesse e lacunas na pesquisa em logística de defesa, com foco gestão da cadeia de suprimentos militar	O estudo, com base em painel de especialistas, **indica três direções centrais para o avanço da** área: criação de um repositório unificado, incentivo à produção acadêmica
ENAP	1	2024	Lúcio Góis, Abimael Ouro, Cláudio Mendonça	Compras públicas centralizadas: vantagens e desvantagens à luz dos critérios de sustenta-bilidade	Identificar as vantagens e desvantagens das compras públicas centralizadas à luz dos critérios de sustentabilidade	A pesquisa identificou vantagens da centralização, como economia, padronização e sustentabilidade, mas também apontou riscos, como morosidade e desabaste-cimento

Base de Dados	Nº	Ano	Autor(es)	Título	Objetivo	Resultados
BDTD	1	2017	Grice Barbosa Pinto de Araújo	Modelo de compras na SEPLAG/DF	Analisar o modelo de compras da SEPLAG/DF como órgão central de compras e de caráter normativo	Diagnóstico de um modelo parcialmente centralizado; necessidade de redefinição de processos e uso de sistemas integrados
BDTD	2	2021	Juliana Passos Silveira	Centralização de compras públicas: uma proposta para o IFSul	Propor um modelo de centralização de compras no IFSul conforme nova legislação e diretrizes de governança.	Sugere modelo misto de aquisições; ganhos em escala e processo identificados, com recomendações práticas para estruturação organizacional
BDTD	3	2022	Alexandre R. Soares	Serviços compartilhados e lógicas institucionais no Exército Brasileiro	Analisar os efeitos da centralização do processo de pagamento em um centro de serviços compartilhados na guarnição de Santa Maria	Padronização é fator crítico para o sucesso, mas a lógica burocrática e hierárquica continua predominante

Base de Dados	Nº	Ano	Autor(es)	Título	Objetivo	Resultados
Google Books	1	2021	Carlos Alberto Cintra do Amaral; Sandro Dutra e Silva	Compras públicas para além da economicidade	Discutir modelos de governança das compras públicas que valorizem a centralização como estratégia de fortalecimento da capacidade estatal	Aponta que a centralização pode promover maior controle, profissionalização e integração estratégica das compras públicas

Fonte: Elaborado pelo autores (2025).

O terceiro eixo, Gestão em Estruturas de Defesa, compreende seis estudos que abordam diretamente modelos de aquisição de defesa, estruturas organizacionais de *defence procurement*, interação com a Base Industrial de Defesa e experiências de centralização em forças armadas nacionais e estrangeiras (Auger, 2020; Marques, 2020; Barros; Silva, 2024; Gigante, 2014; Brick, 2014; 2019).

Quadro 5 – Bloco temático Gestão em Estruturas de Defesa

Base de Dados	Nº	Ano	Autor(es)	Título	Objetivo	Resultados
Google Acadêmico	1	2014	Thadeu da Costa Gigante	Compras governamentais: estudo de caso sobre contratações centralizadas pela Marinha	Propor um modelo de contratações centralizadas de serviços comuns para a Marinha	Identificou-se potencial de economia significativa e melhoria nos processos com centralização de contratações

Base de Dados	Nº	Ano	Autor(es)	Título	Objetivo	Resultados
Google Acadêmico	2	2020	Pedro Miguel Mendes Marques	Centralização das Aquisições das Direções Técnicas do CLAFA	Analisar como a centralização dos processos aquisitivos em um único órgão do CLAFA pode melhorar a eficiência	Conclui que a centralização melhora a gestão dos recursos e aumenta a eficiência dos processos
Google books	1	2020	Martin Auger	*Defense Procurement Organizations Worldwide: A Comparison*	Analisar comparativa-mente os diferentes modelos organizacionais de aquisição de defesa entre países industrializados, com ênfase no modelo canadense e possíveis reformas	O modelo canadense é único por envolver múltiplos ministérios e agências de diversos países em que adotam modelos centralizados, por força armada, por corporações civis ou órgãos separados
ESD	1	2024	Felipe Pereira Barros, Manuella Andrade P. de Souza Silva	Desafios e oportunidades para a centralização das aquisições de materiais de emprego militar no âmbito do Ministério da Defesa	Analisar os desafios e oportunidades da centralização de aquisições no MD com foco na defesa antiaérea de média altura	Aponta modelo híbrido com coordenação central no MD e execução por Força Singular; destaca a necessidade de capacitação e superação de entraves legais e técnicos

Base de Dados	Nº	Ano	Autor(es)	Título	Objetivo	Resultados
ESG	2	2014	Eduardo Siqueira Brick	O Mercado das Empresas da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança	Caracterizar o mercado das empresas fornecedoras de produtos de defesa e segurança no Brasil, tanto interno quanto externo.	Identificou a concentração de mercado em poucas empresas, o perfil das empresas fornecedoras, dificuldades enfrentadas na exportação, e as interações com a base logística de defesa. Destacou a importância de uma governança eficaz para o desenvolvimento do setor.
ESG	3	2019	Eduardo Siqueira Brick	A conceptual framework for defense logistics	Estabelecer o domínio do problema de logística de defesa, desenvolvendo um arcabouço conceitual que identifique objetivos, áreas funcionais, componentes estruturais e interfaces com o ambiente externo	Propõe uma definição de Base Logística de Defesa como sistema estratégico para criar e sustentar capacidade militar e tecnológica, além de indicar uma agenda de pesquisa futura.

Fonte: Elaborado pelo autores (2025).

A centralização dos processos de aquisição também se relaciona diretamente com a Capacidade Logística para a Defesa Nacional, prevista na Estratégia Nacional de Defesa. Essa capacidade envolve a articulação das funções logísticas, entre elas suprimentos e transporte, de modo a assegurar

interoperabilidade e atendimento ao interesse da Defesa Nacional (Brasil, 2024).

A literatura indica que a centralização pode gerar ganhos relevantes de eficiência administrativa e racionalização logística, mas não constitui solução universal. Melo (2019) demonstra que, em campi interioranos da UFPB, a descentralização apresentou melhor desempenho, sugerindo que o desenho institucional deve considerar especificidades territoriais e operacionais. Em contrapartida, Pires (2020) e Porto (2021) identificam ganhos de eficiência, redução de prazos e melhoria da capacidade de resposta administrativa em modelos centralizados, ainda que apontem a necessidade de mitigar efeitos colaterais como a lentidão na resolução de inconsistências.

No âmbito militar, os estudos convergem ao evidenciar ganhos de economicidade, padronização e controle. Procópio e Oliveira Jr. (2021) demonstram, por meio de modelo estatístico, que o sistema de compras centralizadas na Guarnição de Brasília produz maior economicidade, com potencial de replicação nacional. Maciel (2024) aponta reduções expressivas de custos e melhoria na velocidade e qualidade das entregas com a implementação do Almoxarifado Virtual Nacional, enquanto Simões (2020) destaca avanços em padronização e controle, mas ressalta gargalos na fase interna e fragilidades no planejamento da demanda, indicando a necessidade de articular centralização com gestão por processos e uso de indicadores.

Desses estudos, infere-se que a centralização, quando sustentada por planejamento, estrutura institucional adequada e instrumentos de monitoramento, configura estratégia consistente para racionalizar estruturas, otimizar fluxos e ampliar a previsibilidade das entregas e dos resultados administrativos, especialmente em cadeias de suprimento complexas, como aquelas associadas às compras públicas de defesa. A principal implicação propositiva, para o caso do Exército Brasileiro, é que processos críticos, tais como aquisições de materiais de emprego militar, logística de apoio administrativo e gestão de almoxarifados, tendem a se beneficiar de modelos centralizados ou híbridos, desde que desenhados com sensibilidade às necessidades das OM apoiadas e dotados de mecanismos ágeis de resposta a demandas específicas.

No eixo Governança Logística e Inovação, as contribuições analisadas reforçam que a centralização deve ser compreendida como componente de uma estratégia ampla de governança pública. Zsidisin et al. (2020), em revisão

crítica sobre logística de defesa, apontam a necessidade de estruturas integradas, repositórios de dados e centros de excelência capazes de coordenar esforços dispersos de aquisição, avaliação e inovação. Embora não discutam diretamente o desenho organizacional da centralização na administração pública, os autores defendem arranjos que, por sua natureza, pressupõem coordenação centralizada para garantir padronização, acúmulo de expertise e governança estratégica.

No contexto brasileiro, Góis, Ouro e Mendonça (2024) demonstram que compras públicas centralizadas geram ganhos em escala, padronização e sustentabilidade, mas ressaltam riscos de morosidade, desabastecimento e perda de autonomia local, concluindo que a decisão entre centralizar ou não deve ser explicitada e justificada nos Estudos Técnicos Preliminares, conforme a Lei nº 14.133/2021. Silveira (2021) destaca que a eficácia da centralização depende da articulação entre os atores envolvidos e da consolidação de estruturas administrativas aptas a coordenar processos complexos, alertando para os riscos de sobrecarga organizacional. Soares (2022) enfatiza a necessidade de capacidades estatais específicas, em especial no uso de tecnologias de informação e na institucionalização de regras claras de coordenação e controle. Amaral e Silva (2022), ao proporem uma abordagem de compras públicas "para além da economicidade", defendem que a centralização, quando combinada à inovação institucional e a modelos colaborativos, pode reforçar a governança, a transparência e a capacidade estratégica do Estado.

A implicação propositiva direta para as compras públicas de defesa é que a centralização deve ser concebida como eixo de uma política de governança logística que integre tecnologias, critérios de sustentabilidade, serviços compartilhados e arranjos colaborativos entre órgãos centrais e unidades executoras. No caso do Exército Brasileiro, isso significa que estruturas como o Almoxarifado Central do QGEx e o Almoxarifado Virtual Nacional podem atuar como plataformas de integração de dados, padronização de catálogos, consolidação de demanda e coordenação com a Base Industrial de Defesa, desde que acompanhadas por mecanismos de transparência, accountability e gestão de riscos.

No eixo Gestão em Estruturas de Defesa, a literatura evidencia que modelos centralizados de aquisição e logística são decisivos para fortalecer a soberania, a continuidade de capacidades críticas e a coerência entre planejamento e execução na área de defesa. Auger (2020) mostra que países

como França e Reino Unido, ao adotarem organismos civis especializados e centralizados – como a Direction générale de l'armement (DGA) e a Defence Equipment and Support (DE&S) – obtêm maior integração entre planejamento, aquisição e logística, ao passo que modelos altamente descentralizados, como o norte-americano, convivem com sobrecustos, atrasos e dificuldades de coordenação, mesmo após sucessivas reformas.

Marques (2020), ao analisar a centralização das aquisições no Comando Logístico das Forças Armadas de Portugal (CLAFA), conclui que a concentração de decisões em uma direção técnica melhora a gestão de recursos e otimiza fluxos administrativos. Brick (2014; 2019), ao conceituar a Base Logística de Defesa (BLD) e ao analisar o mercado de empresas da ABIMDE, destaca que a fragmentação institucional e a ausência de políticas de aquisição articuladas dificultam o fortalecimento da Base Industrial de Defesa, defendendo a centralização das decisões logísticas e de aquisições como requisito para autonomia estratégica e coerência entre planejamento, inovação e sustentação operacional. No contexto brasileiro, Gigante (2014) aponta ganhos de escala, padronização e controle orçamentário com contratações centralizadas na Marinha do Brasil, enquanto Barros e Silva (2024) propõem modelo híbrido, com coordenação central no Ministério da Defesa e execução por uma das Forças Singulares, para atender às exigências de interoperabilidade na defesa antiaérea de média altura, enfatizando a importância da capacitação e da superação de entraves normativos.

Em conjunto, esses achados convergem na valorização da centralização como estratégia para fortalecer a governança, a eficiência e a soberania na área de defesa, em linha com os objetivos deste estudo. No plano propositivo, sugerem que a centralização das compras públicas de defesa, tal como vem sendo ensaiada no Exército Brasileiro por meio do Almoxarifado Central, do Almoxarifado Virtual Nacional e de experiências de compras centralizadas em guarnições, não é apenas uma opção gerencial, mas um caminho necessário para articular planejamento estratégico, racionalização logística e desenvolvimento da Base Industrial de Defesa.

Nesse contexto, a literatura alerta que esse caminho exige capacidades institucionais robustas, qualificação dos quadros, clareza de papéis entre órgãos centrais e unidades executoras e constante aperfeiçoamento dos instrumentos de coordenação, sob pena de reproduzir os riscos de morosidade, rigidez excessiva

e perda de responsividade local identificados em outros países e setores. É a partir dessa síntese que se orienta a análise do caso do Exército Brasileiro e as proposições deste trabalho sobre a centralização das compras públicas de defesa como vetor de governança e eficiência.

Considerações Finais

A centralização da gestão, no âmbito da administração pública de defesa, especialmente no Exército Brasileiro, pode ser entendida como uma resposta estratégica às exigências de eficiência, controle, padronização e racionalidade na aplicação dos recursos públicos.

Nesse sentido, o estudo emerge como alternativa estratégica para enfrentar os desafios impostos pela crescente restrição fiscal, pela necessidade de racionalização de recursos e pela complexidade logística inerente às atividades militares.

Ao longo desta pesquisa, mediante a metodologia do Estado do Conhecimento, constatou-se que o modelo centralizado, desde que bem estruturado e adaptado à realidade organizacional brasileira, tem o potencial de ampliar a capacidade institucional do Estado, reduzir vulnerabilidades logísticas e promover maior integração entre planejamento, execução e controle das atividades administrativas.

A análise das experiências nacionais e internacionais evidencia que os modelos centralizados favorecem maior controle, integração entre instâncias decisórias e redução de custos operacionais. Ao mesmo tempo, destaca-se que sua adoção requer a superação de entraves normativos, a qualificação de recursos humanos e a institucionalização de mecanismos de monitoramento e avaliação. A centralização deve, portanto, ser compreendida não apenas como uma diretriz administrativa, mas como política pública estruturante, voltada à profissionalização da gestão e ao fortalecimento da Base Logística de Defesa.

Conclui-se, por fim, que a centralização da gestão no Exército Brasileiro representa não apenas uma resposta às exigências da administração pública contemporânea, mas também um instrumento de aprimoramento da capacidade estatal, da soberania nacional e da prontidão militar. Tais evidências sustentam a proposição de aprofundamento do modelo centralizado no âmbito da

Defesa, articulado a inovações institucionais e à consolidação de uma cultura organizacional orientada por resultados.

Referências

AFFONSO, B. D. F.; OGAWA, S. B. *Inovação sistemática nas contratações públicas federais*: implantação do Almoxarifado Virtual Nacional no Departamento de Polícia Rodoviária Federal. Brasília: Escola Superior de Guerra, 2021. Disponível em: https://repositorio.esg.br/handle/123456789/1525. Acesso em: 23 jul. 2025.

ARAÚJO, G. *O modelo centralizado de compras como potencializador da melhoria dos processos de aquisições*: estudos de caso da central de compras do Distrito Federal. 2019. Dissertação (Mestrado em Administração Pública) – Instituto Brasiliense de Direito Público, Brasília, 2019. Disponível em: https://bdtd.ibict.br/vufind/Record/IDP-1_76af2469cf84bafe6653483a03ecc0ab. Acesso em: 1 jun. 2025.

AUGER, M. F. *Defense procurement organizations worldwide:* a comparison. Background Paper n. 2019-52-E. Ottawa: Library of Parliament, Parliamentary Information and Research Service, 28 abr. 2020. Disponível em: https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/BackgroundPapers/PDF/2019-52-e.pdf. Acesso em: 1 jun. 2025.

BARDIN, L. *Análise de conteúdo.* São Paulo: Edições 70, 2011.

BARROS, F. P.; SILVA, M. A. P. de S. *Desafios e oportunidades para a centralização das aquisições de materiais de emprego militar no âmbito do Ministério da Defesa:* o caso da defesa antiaérea de média altura (2013–2024). 2024. Trabalho de Conclusão de Curso (Especialização em Altos Estudos em Defesa) – Escola Superior de Defesa, Brasília, 2024. Disponível em: https://repositorio.esg.br/handle/123456789/2107. Acesso em: 1 jun. 2025.

BRASIL. Exército Brasileiro. Portaria nº 295-EME, de 17 dez. 2014. Institui a Diretriz de Racionalização Administrativa no Exército. *Diário Oficial da União, Brasília,* DF, 17 dez. 2014. Disponível em: https://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/01_diretrizes/04_estado-maior_do_exercito/port_n_295_eme_17dez2014_republica%C3%A7%C3%A3o.html. Acesso em: 1 jun. 2025.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. *Portaria nº 442-EME, de 4 dez. 2017.* Cria o Almoxarifado Central do QGEx. Brasília, DF: Exército Brasileiro, 2017.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. *Portaria EME/C Ex nº 891, de 13 out. 2022*. Aprova a diretriz para centralização administrativa dos processos de aquisição de materiais e prestação de serviços comuns das unidades gestoras do Comando do Exército. Brasília, DF: Exército Brasileiro, 2022a. Disponível em: https://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/01_diretrizes/04_estado-maior_do_exercito/port_n_891_eme_13out2022.html. Acesso em: 4 jun. 2025.

BRASIL. *Tesouro Nacional. Relatório de projeções fiscais – 1º semestre de 2022.* Brasília, DF: Tesouro Nacional, 29 jun. 2022b. Disponível em: https://www.tesourotransparente.gov.br/publicacoes/relatorio-de-projecoes-fiscais/2022/20. Acesso em: 1 jun. 2025.

BRASIL. Ministério da Defesa. *Política Nacional de Defesa. Estratégia Nacional de Defesa.* Brasília, DF: Ministério da Defesa, 2024. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_1.pdf. Acesso em: 26 jun. 2024.

BRICK, E. S. A conceptual framework for defense logistics. *Gestão & Produçã*o, v. 26, n. 4, e4062, 2019. DOI: 10.1590/0104-530X4062-19. Acesso em: 1 jun. 2025.

BRICK, E. S. O mercado das empresas da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança – *ABIMDE. Relatórios de Pesquisa em Engenharia de Produção*, Rio de Janeiro, v. 14, n. D6, p. 91–149, 2014. Disponível em: https://www.producao.uff.br/images/rpep/2014/RPEP_D6.pdf. Acesso em: 1 jun. 2025.

BRESSER-PEREIRA, L. C. *Reforma do Estado para a cidadania:* a reforma gerencial brasileira na década de 1990. Brasília: ENAP, 1998.

BRUNEAU, T. C.; TOLLEFSON, S. D. Civil–military relations in Brazil: a reassessment. *Journal of Politics in Latin America*, v. 6, n. 2, p. 107–138, 2014.

CAMINHA, V. M. O *lugar do ensino de defesa nos estudos de defesa no Brasil:* apontamentos a partir do Estado do Conhecimento (2016–2024). 2024. Trabalho de Conclusão de Curso (Curso de Altos Estudos em Defesa – CAED) – Escola Superior de Defesa, Brasília, 2024. Disponível em: https://repositorio.esg.br/handle/123456789/2007. Acesso em: 18 ago. 2025.

GIGANTE, T. da C. *Compras governamentais: estudo de caso sobre contratações centralizadas de serviços comuns pela Marinha do Brasil. 2014*. 160 f. Dissertação (Mestrado em Engenharia de Produção) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2014.

GÓIS, L. M.; OURO, A.; MENDONÇA, C. Compras públicas centralizadas: vantagens e desvantagens à luz dos critérios de sustentabilidade. *Revista do Serviço Público,* v. 75, n. 1, p. 161–181, 2024. DOI: 10.21874/rsp.v75i1.10150. Acesso em: 18 ago. 2025.

GOMES, R. S. dos S. *A efetividade do Almoxarifado Virtual Nacional na cadeia de suprimento de bens não finalísticos do Comando da Aeronáutica à luz do modelo Balanced Scorecard*. 2024. Monografia – Escola Superior de Guerra, Rio de Janeiro, 2024. Disponível em: https://repositorio.esg.br/handle/123456789/2070. Acesso em: 1 jun. 2025.

INÁCIO, L. C. *O Almoxarifado Virtual Nacional e as transformações na gestão de aquisições do Exército Brasileiro*. 2024. Trabalho de Conclusão de Curso – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2024. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/14288. Acesso em: 27 jul. 2025.

KOHLS-SANTOS, P.; MOROSINI, M. C. O revisitar da metodologia do Estado do Conhecimento para além de uma revisão bibliográfica. *Revista Panorâmica Online*, v. 33, p. 123–145, 2021.

MACIEL, L. T. *Análise dos impactos da implementação do Almoxarifado Virtual Nacional no Supply Chain Management da Base Aérea de Anápolis.* 2024. Trabalho de Conclusão de Curso – Escola de Comando e Estado-Maior da Aeronáutica, Rio de Janeiro, 2024. Disponível em: https://www.redebia.direnSri.fab.mil.br. Acesso em: 18 ago. 2025.

MARQUES, P. M. M. *Centralização das aquisições das direções técnicas do CLAFA*. 2020. Trabalho de Investigação Individual – Instituto Universitário Militar, Lisboa, 2020. Disponível em: https://comum.rcaap.pt. Acesso em: 5 jun. 2026.

MELO, H. C. de. *Análise comparativa da execução orçamentária, centralizada versus descentralizada, de campi interioranos da UFPB.* 2019. 113 f. Dissertação – Universidade Federal da Paraíba, João Pessoa, 2019.

MOROSINI, M. C.; FERNANDES, C. M. B. Estado do conhecimento: conceitos, finalidades e interlocuções. *Educação Por Escrito,* v. 5, n. 2, p. 154–164, 2014. DOI: 10.15448/2179-8435.2014.2.18875.

MOROSINI, M. C.; KOHLS-SANTOS, P.; BITTENCOURT, Z. *Estado do conhecimento: teoria e prática*. Curitiba: CRV, 2021.

MOROSINI, M. C.; NASCIMENTO, L. M. do; NEZ, E. de. Estado do conhecimento: metodologia na prática. *Revista Humanidades e Inovação*, v. 8, n. 55, p. 70–81, 2021.

PIRES, M. A. G. *Efeitos da centralização do exame de pagamento de pessoal para as OM de Santa Maria*. 2020. Trabalho de Conclusão de Curso – Escola de Formação Complementar do Exército, Salvador, 2020.

PIRES, S. R. I. *Gestão da cadeia de suprimentos:* conceitos, estratégias, práticas e casos. São Paulo: Atlas, 2004.

PORTO, J. B. *A centralização nas aquisições da saúde após a criação do Centro de Aquisições Específicas.* 2020. 75 f. Trabalho de Conclusão de Curso (Curso Avançado de Comando e Estado-Maior) – Escola de Comando e Estado-Maior da Aeronáutica, Rio de Janeiro, 2020. Disponível em: https://www.redebia.direnri.fab.mil.br. Acesso em: 1 jun. 2025.

PROCÓPIO, C. E. de S.; OLIVEIRA JÚNIOR, M. de. Economicidade no sistema de compras centralizadas no Exército Brasileiro. In: ENCONTRO BRASILEIRO DE ADMINISTRAÇÃO PÚBLICA, 8., 2021, Brasília, DF. *Anais [...].* Brasília, DF: Sociedade Brasileira de Administração Pública, 2021. Disponível em: https://bdtd.ibict.br. Acesso em: 1 jun. 2025.

RUDZIT, G.; NOGAMI, O. Segurança e defesa nacionais: conceitos básicos para uma análise. *Revista Brasileira de Política Internacional,* v. 53, n. 1, p. 5–24, 2010. DOI: 10.1590/S0034-73292010000100001.

SERRÃO, J. R. Gestão de pessoas e racionalização administrativa nas Forças Armadas. *Revista da Escola Superior de Guerra*, v. 32, n. 65, p. 1012–1035, 2017.

SIMÕES, F. G. *Análise do processo de aquisição realizado pela FAB no Grupamento de Apoio do Distrito Federal*. 2020. Trabalho de Conclusão de Curso – Escola Nacional de Administração Pública, Brasília, 2020.

SOARES, A. R. *Serviços compartilhados e lógicas institucionais: estudo de caso do processo de pagamento de pessoal do Exército Brasileiro na Guarnição de Santa Maria.* 2022. 123 f. Dissertação – Universidade Federal de Santa Maria, Santa Maria, 2022.

TINOCO JUNIOR, E. G. O modelo de racionalização administrativa na Base Administrativa do Quartel-General do Exército. *Revista O Gestor,* Brasília, 2021.

ZSIDISIN, G. A.; BRESLER, A.; HAZEN, B.; SNIDER, K. F.; WILKERSON, T. H. Research in defense logistics: where are we and where are we going? Journal of Defense Analytics and Logistics, v. 4, n. 1, p. 3–17, 2020. DOI: 10.1108/JDAL-07-2019-0012.

Resiliência do segmento de armas e munições leves da base industrial de defesa brasileira[1,2]

José Irismar Cabral Junior
Julio Eduardo da Silva Menezes

Introdução

As tensões geopolíticas que caracterizam a primeira metade da década de 2020 têm reconfigurado de maneira significativa as prioridades estatais. Países que, até recentemente, não percebiam a iminência de conflitos bélicos passam a direcionar de forma crescente sua atenção às respectivas indústrias nacionais de defesa, revisitando a necessidade de modernizá-las a fim de assegurar a capacidade de resposta tempestiva a eventuais demandas de suas forças armadas. Nesse contexto, ratifica-se que cada Estado deve preservar o maior grau possível de liberdade de ação, de modo a mitigar vulnerabilidades internas e riscos às ambições externas.

Quando o Estado não se encontra envolvido em conflitos armados, os formuladores de políticas públicas tendem a identificar um suposto excesso de capacidade produtiva nas plantas industriais de material de emprego militar, ainda que tais estruturas tenham sido originalmente dimensionadas para atender às exigências de períodos de guerra. Em contextos de capacidade ociosa, torna-se substancialmente mais difícil justificar investimentos em modernização e expansão da indústria de defesa, sobretudo quando o "rugir dos canhões" deixa de compor o horizonte perceptivo dos tomadores de decisão.

[1]Este estudo é produto do projeto de pesquisa "Políticas públicas, indústria, dualidade e defesa nacional: evidências para uma agenda de desenvolvimento da Base Industrial de Defesa Brasileira", apoiado pela quinta edição do programa PRÓ-DEFESA, financiado pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

[2]Neste artigo, foi utilizada a ferramenta Portugues.AI exclusivamente para verificação ortográfica e de pontuação do texto. O conteúdo intelectual, a estrutura analítica, as interpretações e as conclusões foram integralmente elaborados, revisados e validados pelos autores, que assumem total responsabilidade pelo trabalho apresentado.

No Brasil, país que, por sua localização geográfica, dimensão demográfica e capacidade econômica, se projeta no continente americano como um dos principais líderes regionais, sua indústria de defesa tem enfrentado dificuldades para atender às demandas internas e competir de maneira vantajosa no cenário internacional. Não obstante, dois de seus segmentos constituem exceções relevantes e participam em condições altamente competitivas de nichos específicos dos mercados interno e global: o aeronáutico e o segmento de armas e munições leves.

A investigação que deu origem a este capítulo busca identificar os fatores que explicam a resiliência do segmento de armas e munições leves da Base Industrial de Defesa (BID) brasileira, ao apresentar um histórico consistente de vantagem competitiva no mercado nacional e internacional. Tal desempenho contrasta de maneira significativa com outros segmentos da indústria de defesa nacional, que têm demonstrado dificuldades em alcançar níveis equivalentes de êxito comercial.

O exame realizado justifica-se por quatro razões: (*i*) importância estratégica do segmento de armas e munições leves como insumos básicos das forças de defesa e de forças e instituições de segurança; (*ii*) necessidade de compreender os fatores que sustentam sua resiliência diante de transformações econômicas e políticas; (*iii*) relevância de examinar sua trajetória histórica no âmbito da BID; e (*iv*) escassez de estudos sistemáticos recentes dedicados a esse segmento.

Para a elaboração da investigação, realizou-se pesquisa bibliográfica e documental de caráter exploratório, empregando-se a técnica de revisão da literatura. A escolha dessa abordagem metodológica decorreu da constatação de que há escassa produção científica sistematizada recente sobre o segmento de armas e munições leves, o que evidenciou a necessidade de organizar, comparar e interpretar o conhecimento disponível. A revisão da literatura mostrou-se particularmente adequada porque permitiu: (*i*) identificar tendências históricas relevantes; (*ii*) examinar características estruturais do segmento; (*iii*) mapear fatores de resiliência já discutidos por autores da área; e (*iv*) constituir procedimento apropriado para tratar temas que envolvem dados sensíveis e de acesso restrito, como é o caso da área de defesa.

A pesquisa evidenciou um conjunto de fatores que, ao longo da trajetória histórica da BID, têm sustentado a resiliência do segmento de armas e munições

leves, permitindo-lhe manter desempenho mercadológico competitivo mesmo diante de mudanças estruturais, econômicas e políticas.

No texto que se segue, apresentam-se inicialmente algumas considerações introdutórias e definições necessárias, seguidas de breve histórico da BID, com ênfase nos elementos específicos do segmento de armas e munições leves. Em seguida, elencam-se fatores que contribuíram para a resiliência desse segmento. Por fim, apresentam-se considerações finais e referências bibliográficas que fundamentaram a análise.

Desenvolvimento

Nos últimos anos, o conceito de resiliência ganhou centralidade, especialmente após a pandemia de Covid-19, período em que as cadeias produtivas foram severamente tensionadas e, em muitos casos, mostraram-se incapazes de responder de forma adequada às demandas emergentes. Esse cenário expôs vulnerabilidades significativas e colocou em risco a segurança econômica de países e empresas em escala global. Conforme observa a CNI (2023, p. 194), a resiliência corresponde "à capacidade de rapidamente retomar as condições operacionais em face a eventos inesperados, o que inclui redundância de fornecedores situados em diferentes países e a formação de estoques de segurança". Dessa forma, a literatura especializada afasta a compreensão da resiliência como postura passiva, enfatizando-a como uma capacidade proativa de adaptação, recuperação célere e preservação da autonomia estratégica do Estado. Nessa perspectiva, sob condições de pressão, sistemas, nações ou organizações devem ser capazes de responder de maneira eficaz e emergir mais robustos do período de estresse (ABDI, 2025; IISS, 2025; CNI, 2023; Ambros, 2019).

No que se refere aos marcos regulatórios e às definições jurídicas, a Lei nº 12.598/2012 (Lei da BID) estabelece os principais pilares de governança do setor industrial de defesa. Nessa norma, a BID é definida como o conjunto de organizações, públicas ou privadas, responsáveis por atividades de pesquisa, projeto, desenvolvimento, produção e manutenção de Produtos de Defesa (PRODE). Quando um PRODE, em razão de seu elevado conteúdo tecnológico, dificuldade de obtenção ou caráter essencial, for classificado como de interesse estratégico, passa a ser designado como Produto Estratégico de Defesa (PED).

Para o desenvolvimento e a fabricação desses itens, o Ministério da Defesa (MD) credencia as Empresas Estratégicas de Defesa (EED), como pessoas jurídicas que devem, obrigatoriamente, possuir sede e domínio tecnológico no país, além de garantir que o controle acionário e o direito de voto de grupos estrangeiros não ultrapassem dois terços do total detido por acionistas brasileiros.

A organização setorial da BID varia de acordo com a metodologia adotada pelas principais fontes consultadas. O relatório Diagnóstico: Base Industrial de Defesa Brasileira (Ferreira e Sarti, 2011) estruturou a indústria em sete setores, entre os quais se destaca o setor "Armas e Munições Leves e Explosivos", abrangendo desde armamentos portáteis até insumos explosivos de uso militar. Posteriormente, o estudo Mapeamento da Base Industrial de Defesa (Brasil, 2016), buscando uma caracterização mais minuciosa e sensível à heterogeneidade industrial, reorganizou a BID em oito setores, desdobrando o setor originalmente proposto por Ferreira e Sarti (2011) em duas categorias distintas: "armas e munições leves e explosivos" e "armas e munições pesadas". É nesse primeiro enquadramento classificatório que se insere o recorte analítico adotado nesta pesquisa, centrado especificamente no segmento de armas e munições leves, cuja dinâmica produtiva, trajetória histórica e padrões de competitividade internacional justificam uma investigação aprofundada.

No segmento de armas e munições leves investigado, optou-se por incluir a empresa Condor devido à sua liderança e especialização em tecnologias não letais, em consonância com a classificação adotada por Leske (2016). Embora o segmento seja tradicionalmente associado a armamentos de fogo convencionais como pistolas e revólveres, as fontes consultadas identificam a Condor como empresa âncora devido à sua produção de munições e equipamentos táticos de baixa letalidade e efeito moral, amplamente empregados pelas Forças Armadas em missões de paz das Nações Unidas e em operações internas de Garantia da Lei e da Ordem (GLO).

Breve histórico da BID com foco no segmento de armas e munições leves

A origem do segmento de armas e munições leves da BID tem como marco a instalação da Real Fábrica de Pólvora na região da Lagoa Rodrigo de Freitas, no Rio de Janeiro - RJ, no início do século XIX. A instalação ocorreu

após a transferência da Corte portuguesa para o Brasil, em razão das guerras napoleônicas na Europa. A fábrica foi instalada para atender demandas das armas reais navais e terrestres que protegiam o Reino (ABDI, 2025; Ferreira, 2020; Piva; Filgueiras, 2008).

Com o Brasil independente de Portugal, décadas depois, a Guerra da Tríplice Aliança (1864-1870) demandou armas, munições e equipamentos para as tropas imperiais. Isso fez com que os arsenais e fábricas militares instalados em solo brasileiro aumentassem a produção e se desenvolvessem. No final do século, após a Proclamação da República, os primeiros governos republicanos adotaram a política de importar a maior parte do material de defesa necessário. Mesmo assim, foi criada a Fábrica de Realengo, em 1898, para a produção de armamentos e, em 1909, foi instalada a Fábrica de Piquete, para a produção de pólvora sem fumaça. (Imbel, 2026; ABDI, 2025; Ferreira, 2020; Hilton, 1982)

Nas primeiras décadas do século XX, empresas privadas inicialmente dedicadas a produtos de forjaria e de metalomecânica se estabeleceram e deram início à produção de armas leves. Nesse período, foram criadas a E.R. Amantino e Cia./Boito, a Amadeo Rossi e a Companhia Brasileira de Cartuchos (CBC). Os acontecimentos da Revolução Constitucionalista de 1932 contribuíram para que o governo decidisse instalar fábricas militares no Rio de Janeiro, Juiz de Fora e Curitiba, ampliando a produção nacional de armamentos e munições. Em 1934, foi criada a Fábrica de Canos e Sabres para Armamento Portátil em Itajubá, e, em 1939, foi criada a Forjas Taurus em Porto Alegre. Em meados do século XX, arsenais e fábricas estatais e empresas privadas contribuíram com seus produtos para a mobilização das tropas brasileiras empregadas na Segunda Guerra Mundial (1939-1945) (CBC, 2026; Imbel, 2026; Taurus, 2026; ABDI, 2025; Vieira, 2023; Leske, 2016; Hilton, 1982).

De acordo com Vieira (2023) e Hilton (1982), o controle estatal exercido pelo governo de Getúlio Vargas (1930-1945 e 1951-1954) no setor de defesa foi determinante para restringir a importação de armas leves e de munições e fomentar a fabricação desses produtos por empresas nacionais, fortalecendo o setor. A partir de 1945, com a implantação da Companhia Siderúrgica Nacional, a disponibilidade de aço deu suporte ao desenvolvimento do setor industrial brasileiro como um todo e atraiu capital estrangeiro para o Brasil. A proteção estatal à indústria nacional de defesa e a entrada de capital estrangeiro no país contribuíram para desenvolver capacidades que trouxeram resiliência ao

segmento de armas e munições leves, demonstrada quando a indústria de armas e munições leves foi submetida a desafios de mercado.

Com a incorporação de armamentos, da doutrina e da logística de defesa norte-americana utilizada pela Força Expedicionária Brasileira (FEB) na Segunda Guerra Mundial, o Brasil teve sua indústria de defesa impulsionada, fortalecendo a BID e possibilitando o surgimento de demanda para criação de centros de Pesquisa, Desenvolvimento e Inovação (PD&I) no âmbito das Forças Armadas. A partir desse período, criaram-se vários polos de pesquisa como o Centro Técnico de Aeronáutica (atual Centro Tecnológico da Aeronáutica, CTA), o Instituto de Pesquisa da Marinha (IPqM) e o Centro Tecnológico do Exército (CTEx). Em 1950, foi criado o Instituto Tecnológico de Aeronáutica (ITA) e, em 1959, foi criado o Instituto Militar de Engenharia (IME), que são núcleos de qualificação de recursos humanos para o setor de defesa (ABDI, 2025; Hilton, 1982).

Em meados da década de 1960, políticas públicas voltadas ao fortalecimento da indústria nacional impulsionaram o complexo industrial de defesa. Essas políticas contribuíram para criar, na década de 1970 e nos primeiros anos da década de 1980, ambiente favorável que proporcionou aumento da demanda por produtos de defesa destinados aos projetos estratégicos das Forças Armadas, no contexto de medidas estatais denominadas "Brasil Potência". Ao mesmo tempo, o Brasil passou a participar com maior destaque no mercado internacional de produtos de defesa. Durante a vigência do Acordo Militar Brasil - EUA, no período de 1952 a 1977, o Brasil teve acesso facilitado a equipamentos e tecnologias norte-americanas. Esse acordo, fortemente baseado na aquisição de material de defesa, prejudicou o desenvolvimento autóctone de projetos de defesa (ABDI, 2025).

Nas décadas de 1970 e 1980, o governo desenvolveu diversos programas e ações orientados para o desenvolvimento da infraestrutura nacional e de incentivo à indústria pesada e de base, para gerar capacidade endógena. Nesse ambiente, as Forças Armadas foram contempladas com um orçamento de cerca de 2,1% do PIB anual, o que permitiu, via demanda, o surgimento de empresas e a consolidação de uma indústria de defesa capaz de participar no contexto mundial. Diversas empresas se destacaram no setor de defesa, como Bernardini, Motopeças, Gurgel, Helibrás e Emgepron. No mesmo período, multinacionais como Mercedes-Benz, Ford e Volkswagen ingressaram

no mercado de viaturas militares. Em meados da década de 1970, foi criada a estatal Indústria de Material Bélico do Brasil (Imbel) como resultado da fusão de fábricas do Exército e aproveitando o mercado de produtos de defesa favorável naquele período. Ainda, as empresas da BID conseguiram expandir mercados no exterior, tendo países do Oriente Médio, do Norte da África e da América do Sul como principais clientes (46% das vendas internacionais de material de defesa) e da América do Sul (28% das vendas internacionais de material de defesa). Contudo, em meados da década, a conjuntura econômica mundial tornou-se desfavorável, ao mesmo tempo em que os orçamentos das Forças Armadas foram reduzidos para cerca de 1,5% do PIB, impactando negativamente as vendas nacionais das empresas da BID a partir de então (Imbel, 2026; ABDI, 2025).

De acordo com Ferreira (2020), a demanda internacional por produtos de defesa reduziu-se a partir do fim da Guerra Fria (1947-1991). Além disso, a conjuntura econômica desfavorável no Brasil da década de 1990 se refletiu nos orçamentos dos projetos estratégicos das Forças Armadas, provocando adiamentos e cancelamentos de iniciativas, resultando em queda de desempenho comercial nas empresas da BID brasileira. Apontam-se três causas do declínio da BID na década de 1990: (i) retração do mercado internacional de produtos de defesa; (ii) fim do ciclo de vida dos produtos exportados nos anos anteriores; e (iii) falta de interesse (e de recursos) internacional por produtos mais sofisticados, como a aeronave AMX e o veículo blindado EE T1 Osorio, que poderiam ser produzidos no Brasil. As empresas do segmento de armas e munições leves tiveram dificuldades para alcançar resultados econômicos positivos no período. A baixa escala produtiva e financeira das empresas da BID, além da limitada capacitação tecnológica em alguns setores, trouxeram dificuldades econômicas à indústria de defesa brasileira no final do século XX.

Dalbosco; Cortinhas (2024), Ferreira (2020) e Silva (2015) consideram a criação do MD, em 1999, um momento importante para a retomada do crescimento da BID. A partir de então, estabeleceu-se progressivamente um consistente arcabouço legal, voltado para orientar os atores públicos e privados da indústria de defesa, além de direcionar os processos de desenvolvimento e aquisição do material de defesa. Em 2008, foi aprovada a primeira versão da Estratégia Nacional de Defesa (END), que detalhou e operacionalizou aspectos da então Política de Defesa Nacional (atual Política Nacional de Defesa, PND). Em 2012, foi aprovado o primeiro Livro Branco da Defesa Nacional (LBDN)

e a Lei nº 12.598/2012, a qual gerou claros incentivos à indústria de defesa nacional, sendo considerada um marco regulatório para a implantação da indústria de defesa como indutora do desenvolvimento tecnológico.

A END prioriza setores estratégicos como o nuclear, o cibernético e o espacial, reconhecendo a necessidade de parcerias internacionais para o desenvolvimento da BID e da economia nacional. A Estratégia estrutura programas e projetos de defesa de médio e longo prazos, além de possibilitar que a indústria de segurança seja entendida como um segmento associado da indústria de defesa. Emitem-se diretrizes para médio e longo prazos, com o objetivo de modernizar a estrutura das Forças Armadas em três áreas-chave: monitoramento/controle, mobilidade e presença. Em decorrência, os produtos estratégicos demandados pelas Forças Singulares devem gerar capacidades operacionais que produzam resultados positivos nesses setores prioritários definidos (Dalbosco; Cortinhas, 2024; Ferreira, 2020; Silva, 2015).

A Lei da BID (Brasil, 2012) pretende incentivar o desenvolvimento e a produção de PED e institui o Regime Especial Tributário para a Indústria de Defesa (RETID) para a EED, além de adotar outras medidas de proteção e incentivo à indústria nacional de material de emprego militar. Outras normas editadas no âmbito do MD são também importantes, para compor o arcabouço legal da indústria de defesa. Convém ressaltar a atualização da Política Nacional de Exportação e Importação de Produtos de Defesa - PNEIPD (Brasil, 2018), que estabelece os acordos de compensação comercial, tecnológica e industrial, e a aprovação da Política Nacional da Base Industrial de Defesa – PNBID (Brasil, 2022), que tem objetivos relacionados à CT&I, recursos humanos, redução da dependência tecnológica e industrial externa, aperfeiçoamento da qualidade de bens e serviços de defesa e aumento da competitividade da BID no mercado internacional. Esse conjunto normativo tem potencial de promover o desenvolvimento e o fortalecimento da indústria nacional, atraindo empresas estrangeiras para o setor de defesa brasileiro, instalando subsidiárias ou formando parcerias com empresas nacionais.

O segmento de armas e munições leves

A capacidade de atravessar períodos de maior adversidade nos mercados, decorrentes tanto de fatores econômicos quanto de dinâmicas geopolíticas, constituiu elemento central para que o segmento de armas e

munições leves apresentasse um comportamento distinto em relação a outros setores da indústria de defesa, evidenciando elevada resiliência ao longo de sua trajetória histórica. Esse segmento conseguiu superar dificuldades estruturais ao direcionar esforços à redução de custos e ao desenvolvimento de produtos voltados a nichos específicos, como o segmento de segurança e o mercado de tecnologias não letais. Podem ser elencados aspectos intrínsecos ao segmento que contribuem para sua resiliência, a partir das características gerais da BID sintetizadas por Ferreira (2020):

(i) algumas empresas nacionais foram criadas para atender a demandas específicas das Forças Armadas;

(ii) a indústria de defesa nacional é abrangente e diversificada. Ela varia desde a produção de insumos químicos para explosivos e munições até empresas de setores de maior tecnologia, como aquelas ligadas ao setor nuclear. A BID tem capacidade de desenvolver e produzir, por exemplo, armas, munições leves e pesadas, plataformas terrestres, navais e aéreas, materiais de comunicações e sistemas complexos de uso militar;

(iii) os conglomerados e empresas nacionais são relevantes e têm participação importante no mercado internacional;

(iv) a escala produtiva difere conforme o segmento em análise. Para os segmentos de armas e munições leves, plataformas terrestres e plataformas aeronáuticas, a eficiência em escala pode ser considerada elevada;

(v) a indústria de defesa adquiriu relativa autonomia tecnológica nos segmentos de armas e munições leves, sistemas de artilharia, plataformas aeronáuticas, sistemas de comando e controle, e vem desenvolvendo e acumulando capacidades tecnológicas no setor de propulsão nuclear; e

(vi) no Brasil, existe uma densa infraestrutura educacional, científica e tecnológica com a participação de escolas e centros de pesquisa militares, além de universidades e centros de pesquisa civis, estatais e privados.

Os trabalhos de Leske (2026) e Ferreira (2020) esclarecem que o segmento de armas e munições leves é integrado atualmente por três empresas principais de capital nacional: CBC, que controla a Taurus S.A.; a Condor S.A. Tecnologias Não Letais; e a Imbel. Observa-se que as três indústrias possuem forte participação no mercado internacional de produtos de defesa e segurança. Os mesmos autores assinalam que o segmento é um dos poucos na BID que possui autonomia tecnológica, sendo capaz de suprir as demandas nacionais

e competir fortemente no exterior. A autonomia tecnológica é relevante para o acúmulo de capacidades que trazem robustez e resiliência ao segmento de armas e munições leves, para superar adversidades nos períodos de mercado desafiador.

A CBC é um conglomerado privado que se concentra na fabricação de armas e munições leves e tem sua origem em 1926. Em 1936, a americana Remington Arms e a inglesa Imperial Chemical Industries assumiram o controle acionário da empresa; contudo, em 1979, a CBC foi renacionalizada. No segmento de munições, a empresa participa do mercado nacional na forma de monopólio, com três unidades fabris que exportam cerca de 70% de sua produção total. Em 2007, a CBC adquiriu a alemã Metallwerke Elisenhütte Nassau (MEN) e, em 2009, adquiriu a empresa tcheca Sellier & Bellot, tornando-se uma das líderes mundiais em munições leves e fornecedora de exércitos da Organização do Tratado do Atlântico Norte (OTAN). Antes de ser controlada pela CBC, a Taurus foi adquirida pela norte-americana Smith & Wesson em 1964 e retornou ao controle de acionistas brasileiros em 1977. Em 2015, a CBC adquiriu o controle acionário da Taurus, líder na produção de armas leves, a qual possui três fábricas no Brasil e uma subsidiária nos EUA, o que lhe permite participar fortemente no mercado norte-americano de armas leves (CBC, 2026; Taurus, 2026; Ferreira, 2020; Vieira, 2023).

A Condor tem origem na empresa Química Tupã S.A. Em 1985, a empresa passou a produzir armas, munições e equipamentos não letais e mudou sua denominação para Condor S.A. Indústria Química e, mais recentemente, para Condor Tecnologias Não Letais. Atualmente, a empresa oferece cerca de 160 produtos em mais de 80 países e tem como clientes forças armadas e instituições de segurança pública nacionais e estrangeiras, exportando mais de 70% de sua produção. É considerada uma das empresas líderes mundiais em tecnologias não letais de defesa e segurança (Condor, 2026; Ferreira, 2020).

A Imbel é uma empresa estatal dependente do Tesouro da União, vinculada ao MD, por intermédio do Exército Brasileiro. Ela nasceu da fusão de cinco fábricas do Exército em 1975. As fábricas da Imbel produzem explosivos de uso civil e militar, insumos para munições, armas leves, munições pesadas e material de comunicações e eletrônica. Dentre os produtos comercializados, merece destaque a produção do Fuzil Automático Leve 7.62mm (FAL) sob licença belga e cujas peças ainda são produzidas pela empresa, para atender

demanda do Exército. Atualmente, a Imbel desenvolveu e comercializa a Carabina e o Fuzil IA2, nas versões 5,56mm e 7,62mm, que dotam as Forças Armadas e forças policiais e instituições de segurança brasileiras. (Imbel, 2026; ABDI, 2025; Ferreira, 2020).

A resiliência do segmento de armas e munições leves da BID

Como mencionado, o estudo da evolução da BID possibilita identificar um conjunto de características estruturais que ajudam a compreender melhor o segmento de armas e munições leves. Nesse sentido, da análise realizada, é possível apontar fatores que favorecem o desenvolvimento da resiliência, permitindo que esse segmento superasse sucessivos ciclos econômicos adversos e consolidasse uma posição competitiva no mercado internacional a partir das últimas décadas do século XX. O Quadro 1 apresenta os fatores de resiliência identificados na evolução histórica da BID e que repercutem no segmento de armas e munições leves. É possível que existam outros fatores que proporcionem resiliência e que não tenham sido identificados nas fontes estudadas nesta pesquisa.

Quadro 1 – Fatores de resiliência no segmento de armas e munições leves (continua)

Fatores	Referências
Arcabouço legal e suporte estatal à indústria de defesa	Vieira, 2023; Ávila, 2022; Brasil, 2022, 2018, 2012, 2010, 1965; Pacheco; Pedone, 2016.
Internacionalização ativa e busca por competitividade	Florquin; Oliveira, 2026; Vieira, 2023; Leske, 2016; Ferreira; Sarti, 2011.
Dualidade do mercado e flexibilidade industrial	Condor, 2026; ABDI, 2025; Leske, 2016.
Maturidade empresarial e absorção tecnológica	CTEX, 2026; Vieira, 2023; Leske, 2016; Silva, 2015; Ferreira; Sarti, 2011.
Mecanismos de financiamento e parcerias estratégicas	Imbel, 2026; Finep, 2026; Silva, 2015.
Disponibilidade de recursos humanos	ABDI, 2025; Leske, 2026; Silva, 2015, 2011.

Fonte: Elaborado pelos autores (2026).

De acordo com Vieira (2023) e Pacheco; Pedone (2016), houve restrição à importação de armas e munições em meados do século XX (governo Vargas), dando início a um ciclo de desenvolvimento do setor industrial de defesa. Além disso, a disponibilidade de aço, insumo básico para a indústria metalmecânica, permitiu que empresas estrangeiras, como a italiana Pietro Beretta (adquirida pela Taurus em 1980), se instalassem no Brasil, possibilitando aprendizagem tecnológica e acúmulo de capacidades por empresas nacionais.

Cabe ressaltar o papel do Decreto nº 55.649/1965 que regulou o controle da produção e da venda de armas e permitiu que as empresas brasileiras gozassem de proteção estatal para o desenvolvimento da indústria e capacitação para o mercado internacional. Também central foi o papel da Política Nacional de Exportação de Material de Emprego Militar (PNE-MEM), de 1974, que instituiu incentivos e proporcionou que a indústria de defesa brasileira adquirisse padrão internacional de qualidade para exportar excedentes de produção (Vieira, 2023; Avila, 2022; Brasil, 1965).

Como processo de reorganização do MD, o Decreto nº 7.364/2010 criou formalmente a Secretaria de Produtos de Defesa (SEPROD) e o Departamento de Produtos de Defesa (DEPROD) no âmbito do Ministério, para coordenarem a política da BID e o credenciamento de empresas, entre outras ações de interesse, conforme previa a reorganização da BID sugerida na primeira versão da END. A SEPROD estabelece vínculos com empresas e entidades de classe, como a Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (ABIMDE) e o Sindicato Nacional das Indústrias de Materiais de Defesa (SIMDE), os quais atuam na interlocução com o governo para promover políticas de interesse e apoiar a exportação dos produtos de defesa (Brasil, 2010).

Mais recentemente, a aprovação da Lei da BID, da PNEIPD e da PNBID estabeleceu um arcabouço legal que oferece maior proteção para a indústria de defesa nacional e que reconhece a prioridade que merece o setor industrial de defesa para a estratégia de independência política e de liberdade de ação que o Brasil pretende alcançar no ambiente geopolítico internacional (Brasil, 2022, 2018, 2012).

O conjunto de normas que compõe o arcabouço jurídico brasileiro voltado à BID configura uma estrutura institucional robusta, aplicável a todos os segmentos que a integram. Esse referencial normativo também se estende ao segmento de armas e munições leves, que se beneficia diretamente dos instrumentos de proteção, incentivo e coordenação estatal. Tais dispositivos contribuem para o fortalecimento da capacidade competitiva e da resiliência desse segmento, ao assegurar condições mais estáveis para o desenvolvimento tecnológico, a produção contínua e a inserção internacional da indústria nacional de armas e munições leves.

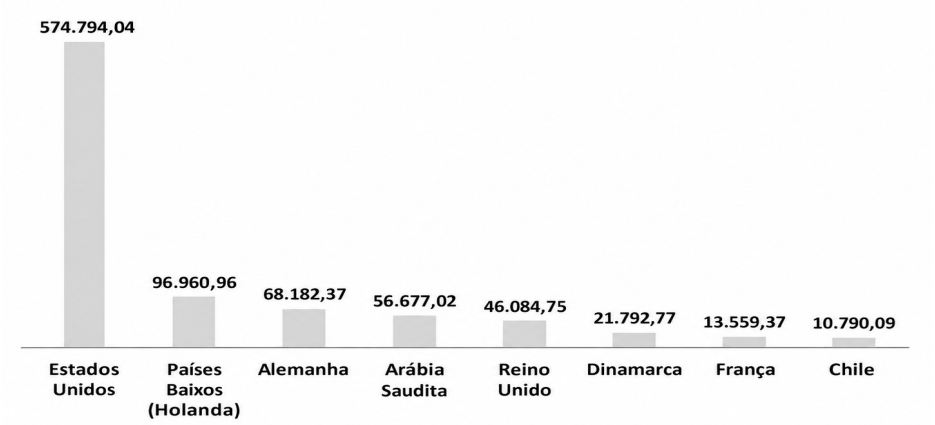
Internacionalização ativa e busca por competitividade

Conforme Ferreira e Sarti (2011), empresas brasileiras também adotaram uma estratégia de internacionalização ativa. Instalaram ou adquiriram unidades nos EUA (Taurus), na Alemanha (CBC) e na República Tcheca (CBC), para cumprir requisitos de proteção industrial dos governos estrangeiros e, ao mesmo tempo, localizar seus produtos mais próximos dos mercados-alvo, reduzindo custos logísticos e de exportação.

Na competição internacional, Leske (2016) ressalta que o segmento de armas e munições leves também aproveita nichos de mercado para produtos de média-alta agregação tecnológica, que são frequentemente negligenciados por grandes conglomerados mundiais, mais interessados na venda de produtos com maior intensidade tecnológica e mais lucrativos. O êxito das estratégias aplicadas pelas empresas brasileiras fica comprovado pelo volume de exportações para países desenvolvidos, como os EUA e nações da Europa.

O Gráfico 1 apresenta dados abertos extraídos do Sistema Comex Stat do Ministério do Desenvolvimento, Indústria, Comércio e Serviços. Os valores de exportação obtidos confirmam as observações comentadas em Leske (2016). Entretanto, como a indústria de defesa tem controle estatal quanto à disponibilidade dos dados, o MDIC não disponibiliza informações consideradas sensíveis, como é o caso dos valores referentes às exportações de pistolas e revólveres, cujos valores exportados não estão agregados aos dados extraídos.

Gráfico 1 – Soma das exportações brasileiras de armas e munições leves de 2021 a 2025 (em USD Mi FOB)

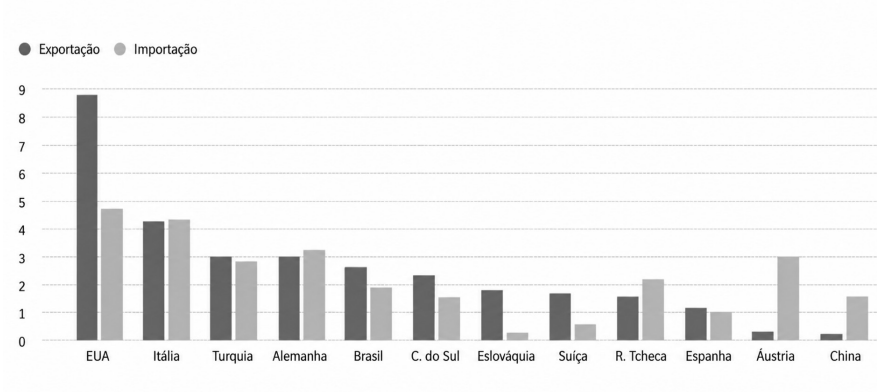


Fonte: Comex Stat /MDIC.
Notas: - dados coletados em janeiro de 2026, sem incluir revólveres e pistolas.
- FOB – *free on board* (frete, seguro e outros encargos por conta do comprador após o embarque).

De acordo com dados apresentados por Florquin e Oliveira (2025) para o Small Arms Survey, o segmento de armas e munições leves demonstra forte inserção externa. Empresas como CBC (Taurus) e Condor exportam mais de 70% de sua produção. Isso corrobora a afirmação de Vieira (2023), que classifica o Brasil como um grande exportador mundial de armas leves. Esse sucesso pode ser explicado pela vitalidade do segmento e pelo menor grau de cerceamento tecnológico imposto, nesse campo, pelos países detentores de indústrias de defesa mais desenvolvidas.

O Gráfico 2 apresenta os principais exportadores de armas leves no período de 2019 a 2024. Destacam-se: Estados Unidos (USD 8,7 bilhões), Itália (USD 4,3 bilhões), Turquia (USD 3 bilhões), Alemanha (USD 2,9 bilhões) e Brasil (USD 2,5 bilhões). Esses cinco países respondem por 54% do total das exportações globais declaradas de armas leves, evidenciando posição predominante dessas economias no mercado internacional.

Gráfico 2 – Principais exportadores mundiais de armas leves (USD Bi), 2019-2024



Fonte: UN Comtrade (s.d.)*, apud* Florquin; Oliveira (2025, p. 5).

Para atender de forma eficiente às demandas externas quanto a prazos, qualidade e custo, as empresas do segmento de armas e munições leves precisam desenvolver atributos característicos de organizações resilientes em seus processos internos e cadeias logísticas. Os resultados alcançados no mercado internacional demonstram que o segmento analisado possui tais atributos, sustentando sua capacidade de adaptação, continuidade produtiva e competitividade global.

Dualidade do mercado e flexibilidade industrial

Segundo Leske (2016), o segmento de armas leves fabrica produtos que podem ser empregados por civis, forças policiais, instituições de segurança pública e empresas privadas de segurança. Esse segmento apresenta uma dualidade de tecnologias e produtos nem sempre encontrada em outros setores da indústria de defesa brasileira, que geram produtos para atender demandas específicas das Forças Armadas. Essa flexibilidade mercadológica e industrial permite que o segmento seja menos dependente das compras das Forças Singulares e supere períodos de reduzidas aquisições estatais com mais facilidade. A autora afirma que as empresas de armas e munições leves aumentam a escala de produção e reduzem custos ao se desvincularem do segmento exclusivo de defesa. Como exemplo de dualidade e flexibilidade industrial, inclui-se o mercado de tecnologias não letais da Condor, que se

destaca globalmente devido à pressão pública pela redução do uso da força nas atividades de segurança pública e de GLO (Condor, 2026; ABDI, 2025; Leske, 2016).

Essa flexibilidade industrial permite que as empresas de armas e munições leves mantenham níveis satisfatórios de desempenho mesmo em contextos de retração orçamentária estatal, que tendem a pressionar fornecedores tradicionais de bens e serviços de defesa. Nesse cenário, a capacidade de atuar simultaneamente no mercado de segurança, no mercado de caça e tiro esportivo e no mercado internacional amplia as alternativas de demanda e reduz a vulnerabilidade do segmento às oscilações das compras governamentais. Assim, a dualidade constitui um elemento estratégico para a sustentabilidade econômica e para o fortalecimento da resiliência das empresas de armas e munições leves no âmbito da BID.

Maturidade empresarial e absorção tecnológica

O estudo da evolução histórica da BID identificou ainda que o segmento de armas e munições leves apresenta maturidade empresarial e tem sido resiliente, uma vez que suas principais empresas estão em operação há mais de quatro décadas. Vieira (2023) destaca um fator peculiar: o processo de "renacionalização" da CBC e da Taurus, ocorrido no final da década de 1970, após as empresas terem sido adquiridas por capital estrangeiro, permitiu que essas empresas retornassem ao controle de capital nacional com acumulado de capacidades tecnológicas e padrões de qualidade de nível mundial. Entretanto, a pesquisa não encontrou indicação de que este movimento tenha ocorrido de forma deliberada, mas o fato é que as empresas brasileiras que foram renacionalizadas haviam passado por processo de aprendizagem tecnológica que permitiu obter vantagem competitiva, para participar do mercado internacional de produtos de defesa e segurança em melhores condições (Vieira, 2023).

No segmento de armas e munições leves, a estrutura de suporte inclui interações com o CTEx e com o Centro de Avaliação do Exército (CAEx). Esses centros prestam serviços científicos fundamentais para superar embargos tecnológicos, tais como: pesquisa e desenvolvimento conjunto, ensaios laboratoriais, apoio técnico, normas técnicas, transferência de tecnologia, ensaios balísticos e metrológicos, testes de armamentos, certificação de produtos

e avaliação de protótipos. Além disso, o desenvolvimento de produtos em conjunto com as Forças Armadas, como ocorreu no caso do Fuzil IA2 da Imbel, tem a capacidade de gerar transbordamento tecnológico, no qual inovações em processos militares podem ser replicadas em plantas destinadas a produtos de segurança (CTEx, 2026; Leske, 2016; Silva, 2015; Ferreira e Sarti, 2011).

Cabe destacar que tanto a Taurus quanto a CBC retornaram ao controle nacional apresentando capacidades tecnológicas superiores às que possuíam antes de sua aquisição por grupos estrangeiros (Vieira, 2023). Essa condição, somada ao suporte institucional oferecido por organizações estatais, especialmente pelos centros de PD&I do Exército Brasileiro, constitui-se um conjunto de fatores que favorece a consolidação de características de resiliência no segmento de armas e munições leves. A combinação entre capacidades tecnológicas acumuladas, aprendizado organizacional e apoio estatal estruturado contribui, assim, para fortalecer a competitividade, a sustentabilidade e a resiliência desse segmento no âmbito da BID.

Mecanismos de financiamento, parcerias estratégicas e disponibilidade de recursos humanos

A resiliência do segmento de armas e munições leves é reforçada por mecanismos de financiamento, especialmente linhas de crédito para produção e inovação oferecidas por instituições como o BNDES e a Finep. Um exemplo relevante é o projeto 2409/2022 da Finep, por meio do qual foram destinados cerca de R$ 175 milhões à Taurus, com prazo de três anos, para o desenvolvimento de novos produtos e processos, a pesquisa de novos materiais e a expansão do Centro Integrado de Tecnologia e Engenharia da empresa. Este foi claramente um financiamento voltado para a inovação industrial. Outro exemplo foi o projeto 0293/23 da Finep com a Condor no valor de cerca de R$ 27,4 milhões, para desenvolver novos produtos e infraestrutura de PD&I visando novos lançadores, granadas, armas, um novo centro de tecnologia e inovação e um centro de instrução, com previsão de ser executado em cerca de 4 anos (Finep, 2026).

Como já comentado, uma referência de parceria estratégica ocorreu entre a Imbel e o Departamento de Ciência e Tecnologia do Exército para o desenvolvimento do Fuzil IA2 5,56mm. A aquisição do lote piloto pelo Exército

Brasileiro permitiu reduzir os custos de desenvolvimento e acumular novas capacidades tecnológicas na empresa (Imbel, 2026; Silva, 2015).

Outro fator que contribui para a resiliência no segmento de armas e munições leves refere-se à disponibilidade de centros de ensino e pesquisa nas Forças Armadas, e de centros de PD&I em universidades e nas próprias indústrias, participantes do Sistema Nacional de Inovação, que oferecem possibilidades para formação de mão de obra qualificada demandada pela indústria de defesa em território nacional. Contudo, a pesquisa de Leske (2016) apresenta dados primários que confirmam dificuldades de obtenção de recursos qualificados no segmento estudado. ABDI (2025) e Silva (2011, 2015) comentam que tem ocorrido evasão desses recursos humanos altamente especializados para empresas internacionais, na busca de melhores condições de trabalho e de salários superiores. O segmento de armas e munições leves não está imune a esta realidade, mas tem conseguido dispor de mão de obra nacional para suprir suas necessidades.

Considerações Finais

Partindo da constatação de que o segmento de armas e munições leves da BID apresenta histórico de vantagem competitiva no mercado internacional, esta pesquisa buscou identificar quais fatores explicam a resiliência demonstrada pelo setor ao longo de sua existência no Brasil, em contraposição a outros segmentos da indústria de defesa. Para isso, realizou-se pesquisa exploratória, empregando revisão bibliográfica e documental, com o objetivo de levantar dados que permitissem identificar, na literatura revisada, indícios e características capazes de elencar os fatores responsáveis pela formação e manutenção da resiliência do segmento analisado. A dificuldade em encontrar literatura recente e em quantidade adequada para investigar o segmento-alvo indicou que a metodologia e as técnicas de pesquisa adotadas foram apropriadas, pois (i) permitiram identificar tendências históricas relevantes; (ii) possibilitaram examinar características da estrutura setorial; (iii) viabilizaram o mapeamento de fatores de resiliência eventualmente apontados por autores da área; e (iv) evidenciaram a existência de barreiras de acesso a dados protegidos e não disponibilizados.

Com base nas fontes reunidas, procedeu-se à análise da evolução histórica do desenvolvimento da BID, buscando identificar os aspectos relacionados à indústria de armas e munições leves. Dessa revisão histórica e da delimitação do universo pesquisado ao segmento alvo, foi possível identificar um conjunto de fatores que contribuem para a resiliência da amostra estudada. Ressalta-se que outros fatores podem existir, mas não foram identificados devido às limitações impostas pela reduzida quantidade de documentos obtidos e fontes disponíveis. Assim, elencam-se como causas de resiliência do segmento de armas e munições leves: (i) a existência de arcabouço legal robusto e suporte estatal consistente; (ii) a inserção das empresas do segmento na competição internacional por meio da criação de filiais ou aquisição de empresas nos mercados-alvo; (iii) o caráter dual dos produtos e das tecnologias empregados pelo segmento, que confere flexibilidade às linhas produtivas para atender tanto aos mercados de defesa quanto aos de segurança; (iv) a maturidade produtiva e a capacidade tecnológica acumulada ao longo da existência das empresas do segmento; (v) a disponibilidade de mecanismos de financiamento com histórico de apoio às indústrias do setor; e (vi) a existência de centros de formação de mão de obra qualificada, ainda que a elevada especialização necessária represente um desafio para o atendimento integral da demanda.

Por fim, a pesquisa também não identificou interação intensa entre o MD e outros órgãos governamentais vinculados ao comércio exterior, à diplomacia e ao desenvolvimento industrial, sugerindo carência de políticas de Estado mais integradas, bem como a pertinência da demanda por investigações futuras nessas direções.

Conclui-se que a resiliência do segmento de armas e munições leves reforça sua posição de destaque e vantagem competitiva na BID brasileira. Para manter esse desempenho, é fundamental desenvolver políticas de Estado mais integradas, superar a falta de interação entre os órgãos governamentais e promover a autonomia tecnológica nacional. Espera-se que esta pesquisa contribua para investigações futuras que aprofundem o conhecimento sobre o segmento estudado para fortalecer a liberdade de ação do Brasil no cenário geopolítico.

Referências

ABDI. *Base industrial de defesa brasileira:* relevância estratégica e políticas públicas. Brasília: FIA/USP, 2025. No prelo.

AMBROS, C. C. Arranjos institucionais e política industrial de defesa: construção de um modelo analítico. *Revista Sul-Americana de Ciência Política,* v. 5, n. 2, p. 301, 15 dez. 2019. Disponível em: https://www.academia.edu/55594580/Arranjos_Institucionais_e_Pol%C3%ADtica_Industrial_de_Defesa_constru%C3%A7%C3%A3o_de_um_modelo_anal%C3%ADtico. Acesso em: 1 jun. 2026.

ÁVILA, C. F. D. Médici, Geisel e as origens da Política Nacional de Exportação de Material de Emprego Militar (PNEMEM), 1973–1974: análise de política externa brasileira. *Revista Brasileira de Ciência Política*, n. 39, e257452, 2022. Disponível em: https://www.periodicos.capes.gov.br/. Acesso em: 1 jun. 2026.

BRASIL. Agência Brasileira de Desenvolvimento Industrial; Instituto de Pesquisa Econômica Aplicada. *Mapeamento da base industrial de defesa.* Brasília: ABDI; Ipea, 2016. Disponível em: https://repositorio.ipea.gov.br/entities/book/cd247fb9-ec27-434d-b7e4-948ccee16de3. Acesso em: 1 jun. 2026.

BRASIL. Decreto nº 11.196, de 10 de agosto de 2022. Institui a Política Nacional da Base Industrial de Defesa – PNBID. *Diário Oficial da União:* Seção 1, Brasília, 11 ago. 2022, p. 3. Disponível em: https://www.in.gov.br/. Acesso em: 1 jun. 2026.

BRASIL. Decreto nº 55.649, de 28 de janeiro de 1965. Dá nova redação ao regulamento aprovado pelo Decreto nº 1.246, de 1º de dezembro de 1936. *Diário Oficial da União:* Seção 1, Brasília, 5 fev. 1965, p. 1455. Disponível em: https://www.in.gov.br/. Acesso em: 1 jun. 2026.

BRASIL. Decreto nº 7.364, de 23 de novembro de 2010. Aprova a estrutura regimental do Ministério da Defesa. *Diário Oficial da União:* Seção 1, Brasília, 24 nov. 2010, p. 1. Disponível em: https://www.in.gov.br/. Acesso em: 1 jun. 2026.

BRASIL. Decreto nº 9.607, de 12 de dezembro de 2018. Institui a Política Nacional de Exportação e Importação de Produtos de Defesa. *Diário Oficial da União*: Seção 1, Brasília, 13 dez. 2018, p. 7. Disponível em: https://www.in.gov.br/. Acesso em: 1 jun. 2026.

BRASIL. Lei nº 12.598, de 21 de março de 2012. Estabelece normas especiais para compras e desenvolvimento de produtos de defesa. *Diário Oficial da União:* Seção 1 (Edição Extra), Brasília, 22 mar. 2012, p. 1. Disponível em: https://www.in.gov.br/. Acesso em: 1 jun. 2026.

CBC – COMPANHIA BRASILEIRA DE CARTUCHOS. *Informações institucionais*. Ribeirão Pires: CBC, s.d. Disponível em: https://www.cbc.com.br/. Acesso em: 19 jan. 2026.

CNI – CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. *Panorama dos desafios brasileiros da indústria de defesa e segurança.* Org. R. G. Carmona. Brasília: CNI, 2023. Disponível em: https://www.portaldaindustria.com.br/. Acesso em: 1 jun. 2026.

CONDOR – CONDOR SOLUÇÕES NÃO LETAIS. *Informações institucionais.* Nova Iguaçu: Condor, s.d. Disponível em: https://www.condornaoletal.com.br/. Acesso em: 19 jan. 2026.

CTEx – CENTRO TECNOLÓGICO DO EXÉRCITO. *Informações institucionais*. Marambaia: CTEx, s.d. Disponível em: https://www.ctex.eb.mil.br/. Acesso em: 19 jan. 2026.

DALBOSCO, M.; CORTINHAS, J. A Estratégia Nacional de Defesa como fomentadora de mudanças nas políticas para a indústria do setor. *Revista Brasileira de Estudos de Defesa,* v. 11, n. 2, p. 319–344, 2024. Disponível em: https://rbed.abedef.org/. Acesso em: 1 jun. 2026.

FERREIRA, M. J. B. Base industrial de defesa brasileira no início do século XXI: expansão e crise. In: DA SILVA, I. J.; ROHENKOHL, J. E. (org.). *Polos de defesa e segurança.* Santa Maria: Ed. UFSM, 2020. p. 197–248.

FERREIRA, M. J. B.; SARTI, F. *Diagnóstico:* base industrial de defesa brasileira. Campinas: ABDI; NEIT-IE-UNICAMP, 2011. Disponível em: https://repositorio.abdi.com.br/. Acesso em: 1 jun. 2026.

FINEP – FINANCIADORA DE ESTUDOS E PROJETOS. *Informações institucionais.* Rio de Janeiro: Finep, s.d. Disponível em: https://www.finep.gov.br/. Acesso em: 19 jan. 2026.

FLORQUIN, N.; OLIVEIRA, V. *The authorized trade in small arms:* Latin America from a global perspective. Geneva: Small Arms Survey, 2025. Disponível em: https://www.smallarmssurvey.org/. Acesso em: 14 jan. 2026.

HILTON, S. E. The armed forces and industrialists in modern Brazil. *The Hispanic American Historical Review*, v. 62, n. 4, p. 629–673, 1982.

IISS – INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. *The military balance* 2025. London: Routledge, 2025.

IMBEL – INDÚSTRIA DE MATERIAL BÉLICO DO BRASIL. *Informações institucionais.* Brasília: Imbel, s.d. Disponível em: https://www.imbel.gov.br/. Acesso em: 19 jan. 2026.

LESKE, A. C. Armas e munições leves e pesadas e explosivos. In: BRASIL. ABDI; Ipea. *Mapeamento da base industrial de defesa.* Brasília: ABDI; Ipea, 2016. p. 31–98.

PACHECO, T.; PEDONE, L. Incentivos governamentais e indústria de defesa. *Revista Brasileira de Estudos de Defesa,* v. 3, n. 2, p. 177–196, 2016.

PIVA, T. C. C.; FILGUEIRAS, C. A. L. O fabrico e uso da pólvora no Brasil colonial. *Química Nova*, v. 31, n. 4, p. 930–936, 2008.

SILVA, Peterson Ferreira da. *A cooperação internacional em programas de produtos de defesa e seus atores:* o caso Brasil e África do Sul no desenvolvimento do míssil A-Darter. 234 f. Dissertação (Mestrado em Relações Internacionais) – Universidade Estadual de Campinas, Campinas, 2011. Disponível em: https://bdtd.ibict.br/vufind/Record/UNICAMP. Acesso em 1 jun. 2026.

SILVA, Peterson Ferreira da. *A política industrial de defesa no Brasil (1999-2014***)**: intersetorialidade e dinâmica de seus principais atores. 445 f. Tese (Doutorado em Relações Internacionais) – Universidade de São Paulo, São Paulo, 2015. Disponível em: https://bdtd.ibict.br/vufind/Record/USP_1b5a2afb63572953e8af465af8e269d7. Acesso em: 1 jun. 2026.

TAURUS – TAURUS ARMAS. *Informações institucionais. S*ão Leopoldo: Taurus, s.d. Disponível em: https://taurusarmas.com.br/. Acesso em: 19 jan. 2026.

VIEIRA, M. T. *Mercado de armas de fogo no Brasil:* construção social de um mercado contestado. São Paulo: Cultura Acadêmica, 2023. DOI: 10.7476/9786559543762.

Planejamento Logístico Estratégico e Análise custo-efetividade:

o caso da operação de combate ao crime organizado na crise de segurança pública do Rio Grande do Norte[1]

Camila Araújo Machado
José Sérgio Marques dos Santos
Luiz Gustavo Celuppi
Carlos Eduardo Gomes
Clayton Mendes da Silva

Introdução

O planejamento logístico é essencial para o sucesso de qualquer operação, especialmente em situações de crise que exigem uma resposta rápida e eficiente das forças de segurança. Nesse contexto, a análise custo-efetividade se torna um fator relevante, pois implica a otimização dos recursos disponíveis e a maximização dos resultados alcançados. Conforme destacado por Christopher (2016), o planejamento logístico eficaz deve garantir a responsividade e a resiliência do sistema, maximizando o valor entregue à sociedade mesmo sob condições extremas.

O papel da logística estratégica na capacidade do Estado de responder a crises complexas, incluindo emergências de segurança pública, é parte relevante constituinte da entrega da administração pública. Segundo Christopher (2016), sistemas logísticos eficientes permitem que instituições públicas atuem com rapidez em cenários de alta incerteza.

De maneira complementar, estudos sobre gestão de cadeias de suprimentos em contextos críticos ressaltam que a coordenação entre múltiplas organizações é um elemento central para o sucesso das operações. De acordo

[1] Neste artigo, foi utilizada a ferramenta OpenAI ChatGPT (GPT-4o) como apoio à revisão gramatical, à tradução e à estruturação de parágrafos do texto. O conteúdo intelectual, as interpretações, as conclusões e a redação final foram integralmente elaborados, revisados e validados pelos autores, que assumem total responsabilidade pelo trabalho apresentado.

com Sheffi (2005), organizações resilientes são aquelas capazes de integrar recursos, informação e processos decisórios de forma adaptativa, reduzindo os impactos de eventos disruptivos e aumentando a capacidade de resposta institucional. Nesse sentido, a aplicação de conceitos de logística estratégica à segurança pública pode ser explorada como uma forma de aprimorar a gestão de crises e a alocação de recursos governamentais.

A pesquisa abrange o contexto do planejamento logístico estratégico e os custos na operação de gerenciamento de crise no Rio Grande do Norte, evento que envolveu o combate ao crime organizado no cenário de crise de segurança pública em 2023. Na ocasião, uma série de ataques orquestrados por uma organização criminosa conhecida como "Sindicato do Crime" exigiu uma ação coordenada entre instâncias federais e estaduais. Essa ação contou com a contribuição conjunta de diversos organismos de segurança pública, entre eles o Sistema Penitenciário Federal (SPF), destacando seu papel na gestão de unidades prisionais de segurança máxima e na resposta a crises no sistema carcerário em nível nacional. Além disso, menciona-se também a atuação da Polícia Penal Federal (PPF) no SPF como parte do Sistema Único de Segurança Pública (SUSP).[2]

Sob a coordenação da Secretaria Nacional de Políticas Penais (SENAPPEN), o Sistema Penitenciário Federal (SPF), estruturado pela Lei 11.671 de 8 de maio de 2008, é um regime especial de execução penal, estruturado com o objetivo de aprimorar o enfrentamento ao crime organizado, mediante o isolamento estratégico de lideranças criminosas e de indivíduos classificados como de elevada periculosidade.[3] Sua atuação se concentra na custódia de presos de alta periculosidade e líderes de organizações criminosas. Trabalhando de forma integrada com outras instituições, o SPF tem contribuído para a redução da criminalidade e para a manutenção da ordem dentro e fora das unidades prisionais em nível nacional.

Em janeiro de 2017, foi criada a Força-Tarefa de Intervenção Penitenciária (FTIP) com o objetivo de resolver e intervir em crises e capacitar servidores locais, alinhando procedimentos de segurança e rotinas administrativas, prevenindo ações criminosas e garantindo a ordem nas

[2]O Sistema Único de Segurança Pública (SUSP) foi instituído pela Lei 13.675, de 11 de junho de 2018.

[3] https://www.gov.br/senappen/pt-br/assuntos/SPF.

unidades prisionais. A FTIP foi regulamentada e desenvolvida por meio dos Convênios de Cooperação Federativa do Ministério da Justiça e Segurança Pública, celebrados com os Estados e com o Distrito Federal, nos termos da Lei 11.473, de 10 de maio de 2007. (Brasil, 2023).[4] A Polícia Penal Federal (PPF) atua no Sistema Penitenciário Federal (SPF) como parte integrante do Sistema Único de Segurança Pública (SUSP), não se limitando à guarda e custódia dos presos, mas também realizando ações preventivas e repressivas de diferentes graus de complexidade, sendo uma delas a Coordenação das ações da FTIP.

Em março de 2023, o Rio Grande do Norte enfrentou uma crise de segurança pública e forte onda de violência que afetou várias cidades do estado. A crise começou no dia 14 de março, com ataques a prédios públicos, incêndios em veículos e ações que causaram pânico na população, resultando em diversos crimes registrados. Os ataques da organização criminosa "Sindicato do Crime" ocorreram como resposta às condições nos presídios, incluindo superlotação e denúncias de violações dos direitos humanos. Uma vez que há ausência do Estado nas unidades prisionais, estas são dominadas pelas organizações criminosas que passam a controlar os fluxos e impedir o acesso às assistências devidas, de maneira geral, refletindo em desordem e insegurança também extramuros, como foi o caso.[5]

Assim, o Governo Estadual solicitou apoio do Governo Federal que, prontamente, entre outras ações, mobilizou reforços à segurança policial ostensiva nas ruas e nas unidades prisionais locais por meio da FTIP, o que resultou em uma redução de 85% dos ataques nos primeiros cinco dias de intervenção. Dez líderes da facção criminosa envolvida foram transferidos

[4]https://www.gov.br/senappen/pt-br/assuntos/noticias/forca-tarefa-de-intervencao-penitenciaria-ftip-da-senappen-inicia-novo-curso-de-capacitacao-em-intervencao-tatica

[5]A Força-Tarefa de Intervenção Penitenciária (FTIP) foi empregada, pela primeira vez no território nacional, no ano de 2017, na Penitenciária de Alcaçuz, situada no Estado do Rio Grande do Norte, em resposta a uma grave crise institucional que culminou na morte de 26 internos. No ano seguinte, em 2018, a FTIP foi novamente mobilizada, desta vez na Penitenciária Agrícola de Monte Cristo, no Estado de Roraima, em decorrência de uma rebelião que resultou em 33 mortes no interior da unidade. Já em 2019, a Força-Tarefa foi acionada em múltiplos contextos de instabilidade em diferentes unidades da federação, destacando-se a atuação no Complexo Penal de Itaitinga, no Estado do Ceará; no Estado do Amazonas, diante de episódios de violência carcerária que culminaram na morte de 55 presos; e no Estado do Pará, onde a FTIP promoveu a retomada e o controle de 13 unidades prisionais, após a ocorrência de 58 mortes no sistema prisional local. (Brasil, 2023).

para penitenciárias federais. A intervenção da FTIP nesses contextos críticos foi marcada por resultados significativos, com destaque para a redução dos índices de criminalidade e das taxas de homicídios nos Estados atendidos, tanto durante quanto após o período de permanência da força. Observou-se, ademais, o restabelecimento da ordem e da disciplina no ambiente carcerário, bem como a implementação de rotinas e protocolos de segurança, com impacto direto na qualificação da gestão penitenciária. (Brasil, 2023).

Além do controle emergencial das crises, a FTIP contribuiu para a introdução de reformas estruturantes voltadas ao fortalecimento da segurança nas unidades prisionais estaduais, deixando como legado a capacitação técnica e a formação continuada de policiais penais mobilizados, por meio de cursos especializados e treinamentos voltados à atuação em contextos de alta complexidade. (Brasil, 2023).

Portanto, este estudo investiga a relação entre custos logísticos e os resultados obtidos em termos de eficácia, eficiência e efetividade da operação. Como destaca Ballou (2006), a logística deve ser compreendida não apenas como um sistema de apoio, mas como elemento estratégico da operação. Este artigo visa preencher lacunas na literatura aplicando conceitos de logística estratégica em operações de segurança pública, com ênfase na mensuração de custos e de desempenho.

A análise se apoia em referencial teórico sobre planejamento logístico estratégico e mensuração de desempenho em segurança pública, incorporando conceitos de eficiência (Charnes; Cooper; Rhodes, 1978), eficácia (Kaplan; Norton, 1996) e efetividade. Utiliza-se abordagem metodológica mista, com ênfase em métodos não paramétricos, para avaliar os impactos da mobilização. A análise da logística e mobilização como vetor estruturante da segurança pública permite a construção de indicadores e diretrizes que subsidiam políticas públicas em contextos de emergência e resposta rápida (Boin et al., 2005), para o que este artigo busca contribuir por meio de um estudo de caso.

Deste modo, o trabalho está estruturado em quatro seções, além da introdução e das considerações finais. A segunda seção apresenta o referencial teórico sobre a mobilização nacional, o planejamento logístico estratégico e a eficiência, eficácia e efetividade de custos. Já a terceira seção expõe a metodologia utilizada na análise dos dados com identificação dos aspectos logísticos da operação, abordando os objetivos, as estratégias, as atividades, os

recursos e os indicadores da operação. Na quarta seção realiza-se a análise dos dados na qual há a observação analítica qualitativa e quantitativa dos custos envolvidos na operação, em que também são descritos os benefícios gerados pela redução da criminalidade e a desarticulação da facção criminosa.

Referencial Teórico

A mobilização nacional é um tema de extrema importância, frequentemente associado à movimentação de pessoas em busca de um objetivo comum, que transcende a simples ideia de um esforço conjunto, assemelhando-se a ações reivindicatórias. É notável a utilização desse termo no discurso cotidiano, refletindo até mesmo em uma expressiva presença nas ferramentas de busca na internet, onde cerca de três milhões de resultados podem ser encontrados. Uma parcela significativa desses resultados, aproximadamente 10%, relaciona-se às medidas governamentais que complementam a logística nacional (Guereschi, 2008).

Nesse contexto, segundo Guereschi (2008), a mobilização nacional é definida como o conjunto de atividades planejadas, orientadas e empreendidas pelo Estado, com o intuito de aprimorar a capacidade do país para realizar ações estratégicas no campo da Defesa Nacional, sobretudo quando enfrentando uma possível agressão estrangeira. O autor cita ainda que, conforme estabelecido na Constituição Federal de 1988, no seu Art. 22, inciso XXVIII, é competência privativa da União legislar sobre a defesa territorial, defesa aeroespacial, defesa marítima, defesa civil e mobilização nacional.

Ainda sobre a mobilização nacional, e para o atendimento aos preceitos da Constituição Federal, é importante que o poder público forneça capacidades adequadas para atingir seus objetivos políticos e coordenar os recursos humanos e materiais necessários para a defesa nacional. A estratégia de manutenção da prontidão das forças armadas e de segurança é crucial para uma mobilização eficiente e os investimentos em defesa são pequenos em comparação com os custos de um conflito (Ramos, 2012).

A gestão de crises tem sido amplamente estudada no campo da administração pública e da segurança internacional. Segundo Boin *et al.* (2005), crises são caracterizadas por elevada incerteza, pressão temporal e necessidade de coordenação interinstitucional, exigindo estruturas organizacionais capazes

de mobilizar rapidamente recursos humanos e materiais. Nesse contexto, a logística e a mobilização assumem papel central no processo de resposta governamental, pois permite organizar fluxos de recursos e informações necessários para estabilizar situações críticas. A literatura destaca que a eficácia da resposta estatal depende, em grande medida, da capacidade de planejamento prévio e da integração entre diferentes níveis de governo.

A literatura sobre gestão pública tem destacado que a logística integrada desempenha papel estratégico na implementação de políticas públicas complexas, especialmente aquelas que envolvem múltiplas organizações governamentais. Segundo Calderaro e Palhares (2011), a logística aplicada ao setor público "não se limita à gestão de recursos materiais, mas envolve também a coordenação de fluxos de informação, pessoas e processos decisórios necessários para a execução das políticas públicas". Nesse sentido, a integração logística contribui para aumentar a capacidade do Estado de responder de forma coordenada a problemas complexos, como crises de segurança pública e situações emergenciais que exigem mobilização rápida de recursos institucionais.

Com a criação do Sistema Nacional de Mobilização – SINAMOB, em dezembro de 2007, veio também a expectativa de que os órgãos que o compõem começassem a executar suas atividades com um planejamento logístico nacional, estabelecido no Plano de Gestão da Secretaria de Ensino, Logística, Mobilização, Ciência e Tecnologia (SELOM). O objetivo do planejamento é identificar soluções para apoiar atividades de gerenciamento de crises, considerando estruturas e capacidades nacionais (Guereschi, 2008).

A utilização do planejamento logístico como uma ferramenta de gestão é defendida também por Giacobo e Ceretta (2010). Os autores afirmam que o planejamento traz melhorias aos processos decisórios, auxiliando os dirigentes na escolha da melhor opção para o alcance dos objetivos. Para isso, defendem ainda que o planejamento seja altamente flexível e que haja uma equipe com profissionais capacitados, com visão gerencial do ambiente interno e externo.

Dito isso, para o atendimento ao planejamento logístico nacional estabelecido pelo SINAMOB, faz-se necessário observar e entender os custos logísticos envolvidos nas operações para promoção da defesa nacional, desde a estratégia para prontidão (capacidade de pronta resposta das organizações) quanto para execução. Assim, utilizaremos o conceito de custo logístico

definido por Segretti *et al.* (2004), em que trata como o consumo dos recursos associados à atividade logística.

A atuação da FTIP também pode ser analisada à luz da logística humanitária, conforme argumentam Tomasini e Van Wassenhove (2009), que a descrevem como a capacidade de responder rapidamente a contextos voláteis por meio da entrega eficiente de assistência crítica a populações vulneráveis.

Referente à recursos logísticos, o Manual de Campanha Logística Militar Terrestre, do Exército Brasileiro, preconiza o uso em conjunto das capacidades logísticas de cada força, o que possibilita uma maximização de disponibilidade de recursos e otimiza atividades de apoio. Esta sinergia pode resultar em maior efetividade das ações, desde que exista uma interoperabilidade doutrinária, ou seja, que todas as Forças tenham os mesmos conhecimentos das atividades logísticas a serem empregadas (Brasil, 2022).

As atividades logísticas a que se referem os parágrafos anteriores estão diretamente ligadas ao conceito de custos logísticos definido por Segretti *et al.* (2004), e nesse sentido, Araujo (2001) corrobora do mesmo entendimento, tratando como custos logísticos todos os recursos relevantes e necessários despendidos em atividades logísticas, não importando o momento e o lugar onde ocorreram.

Diferentemente de outros países, no Brasil, até a década de 1980 os custos logísticos tinham foco nas metodologias e modalidades de transporte e armazenagem de produtos e/ou mercadorias e a partir da década de 1990 iniciaram os estudos científicos objetivando melhorias na administração de materiais e distribuição. Nos estudos que se seguiram, o foco mudou para planejamento, controle, finanças e tecnologia da informação (Cavalcanti *et al.,* 2021).

A análise dos custos logísticos também tem sido objeto de estudos no campo da administração pública, especialmente no que se refere ao impacto desses custos sobre o desempenho das políticas governamentais. Moraes e Gomes (2011) argumentam que o custo logístico em organizações públicas deve ser analisado em conjunto com indicadores de desempenho institucional, uma vez que "a eficiência da cadeia logística governamental depende da capacidade de alinhar recursos financeiros, operacionais e informacionais com os objetivos estratégicos da política pública". Assim, a mensuração dos custos logísticos

torna-se fundamental para avaliar a racionalidade do uso dos recursos públicos e para orientar processos de tomada de decisão.

Considerando que o presente trabalho trata dos custos logísticos de atividades de mobilização nacional, vale esclarecer que estas atividades estão distribuídas em diversas funções logísticas de mesma natureza que são: suprimento, transporte, manutenção, recursos humanos, engenharia, saúde e salvamento. Para utilização dessas funções de maneira eficaz, pelo tomador de decisão, é necessário o uso de ferramentas de Tecnologia da Informação e Comunicação – TIC (Brasil, 2022).

Nesse mesmo contexto, de acordo com Araujo (2001) a mensuração do sistema logístico, a exemplo do conjunto de funções logísticas citado acima, está diretamente relacionada aos custos e à eficiência e eficácia do trabalho. A autora menciona ainda a importância da mensuração na tomada de decisão.

Apesar da disposição de tecnologias e do desenvolvimento destas para análise, algumas decisões ainda são tomadas com base em intuições e esse método pode elevar a taxa de fracasso de uma organização. Para uma tomada de decisão assertiva é necessário ter acesso a informações atualizadas e de fontes confiáveis, tanto das atividades internas quanto externas daquele ambiente de negócio (Dantas, 2013).

Assim, seguindo o mesmo entendimento quanto à mensuração dos custos, para avaliação da eficácia, faz-se necessário considerar variáveis como recursos alocados, acesso à tecnologia, cultura organizacional e desenvolvimento de pessoal, bem como medidas políticas, estratégicas, operacionais e táticas (Farley, 2020). Segundo Novaes (2007), a logística estratégica integra planejamento, execução e controle de fluxos para assegurar desempenho em três níveis: operacional, tático e estratégico. A eficácia está relacionada ao grau de alcance dos objetivos propostos (Kaplan; Norton, 1996); a eficiência refere-se ao uso racional e econômico dos recursos, maximizando a relação custo-benefício (Ballou, 2006); e a efetividade diz respeito ao impacto real das ações na realidade social, considerando mudanças sustentáveis e resultados percebidos pelos beneficiários (Bouckaert e Halligan, 2008).

No campo das políticas públicas de segurança, a avaliação de custo-efetividade tem se consolidado como instrumento importante para orientar decisões governamentais. Estudos apontam que a alocação eficiente de

recursos financeiros é um dos principais desafios enfrentados pelos sistemas de segurança pública. De acordo com Bueno e Lima (2020), a formulação de políticas orientadas para resultados requer mecanismos de avaliação que permitam "relacionar os recursos investidos com os resultados efetivamente alcançados em termos de redução da criminalidade e melhoria da segurança da população" . Essa perspectiva reforça a importância de metodologias capazes de analisar simultaneamente custos operacionais e impactos das intervenções.

A avaliação da efetividade das operações de segurança pública também tem sido analisada em estudos sobre intervenções federais e operações especiais. Diniz, Barbosa e Medeiros (2022), ao analisarem a Operação Arcanjo no contexto das operações de Garantia da Lei e da Ordem, argumentam que a avaliação dessas intervenções deve considerar não apenas indicadores imediatos de redução da criminalidade, mas também efeitos institucionais mais amplos, como o fortalecimento das capacidades operacionais e organizacionais das instituições envolvidas . Dessa forma, a efetividade de operações de segurança pode se manifestar tanto em resultados quantitativos de curto prazo quanto em melhorias estruturais no sistema de segurança pública.

Ainda no contexto das políticas públicas, a mensuração de desempenho deve incorporar indicadores capazes de avaliar a efetividade das intervenções governamentais. Conforme argumentam Bouckaert e Halligan (2008), a efetividade está relacionada também à capacidade das políticas públicas de produzir mudanças duradouras na realidade social, indo além de resultados imediatos ou pontuais. Destaca-se também a importância da logística humanitária na gestão de emergências. Tomasini e Van Wassenhove (2009) afirmam que operações em ambientes de crise exigem elevada flexibilidade logística, capacidade de coordenação interorganizacional e sistemas de informação eficientes.

A literatura recente também tem aproximado os conceitos de logística humanitária e gestão de crises no setor público. Cislaghi *et al*., (2024) destacam que a logística humanitária envolve a mobilização rápida e coordenada de recursos em cenários caracterizados por elevada incerteza e pressão temporal, exigindo flexibilidade organizacional e forte cooperação interinstitucional . Tais características tornam essa abordagem particularmente relevante para operações de resposta a crises de segurança pública, nas quais a capacidade de

mobilização logística pode determinar o sucesso ou fracasso das intervenções governamentais.

A mensuração da efetividade logística, segundo Christopher (2016), exige sistemas de controle baseados em indicadores confiáveis e robustos, o que demanda a coleta sistemática de dados. No Brasil, ainda há carência de estudos aplicados ao setor de segurança pública, sendo a presente análise uma contribuição para a construção dessa base de conhecimento.

A literatura sobre logística em crises, como o Manual de Logística Operacional em Apoio à Defesa Civil (Brasil, 2022), reforça a necessidade de interoperabilidade entre instituições civis e militares. Sheffi (2005) destaca que a resiliência logística depende da coordenação multiescalar e da presença de redes adaptativas. Já Chopra e Meindl (2003) apresentam o conceito de custo total de propriedade (TCO) — que inclui custos diretos, indiretos, tangíveis e intangíveis —, o qual pode ser adotado na modelagem de operações de resposta para garantir decisões mais integradas e eficazes.

A utilização de instrumentos de análise econômica tem se expandido na avaliação de políticas de segurança pública. Odon (2018) argumenta que, em um contexto de restrição fiscal, as políticas de combate ao crime devem ser analisadas sob a perspectiva da alocação eficiente de recursos, priorizando intervenções com maior potencial de impacto sobre a criminalidade e maior retorno social.

Procedimento Metodológico

A efetividade dos custos, na maioria dos casos, consiste em comparar os custos de diferentes alternativas para alcançar o mesmo objetivo. Como este relatório se reporta somente a uma ação e custos já ocorridos na operação de gerenciamento de crise no Rio Grande do Norte, a análise não foi feita por meio das diferentes alternativas ou usando modelos de previsão, posto que não há dados de custos adequados para comparação entre alternativas e para análise de previsão. Deste modo, a análise da eficiência, eficácia e efetividade é feita de maneira diagnóstica, e não preditiva, de modo a observar se a ação atendeu a esses parâmetros, considerando o que se tem à disposição para operação e gastos para esse fim e o objetivo a ser alcançado.

Do ponto de vista dos objetivos, a presente pesquisa pode ser classificada como exploratória e descritiva. Para Gil (2002), a pesquisa exploratória visa proporcionar familiaridade com o problema abordado tornando-o explícito e a descritiva visa demonstrar as características de determinada população ou estabelecimento de relações entre variáveis. A utilização de métodos combinados como qualitativo e quantitativo é defendido por Oliveira (2011). Segundo o autor, nem sempre é possível obter nas pesquisas quantitativas informações, na visão do participante, que são investigadas na qualitativa.

Considerando que uma pesquisa básica gera conhecimentos novos úteis para o avanço da ciência sem aplicação prevista, esta pesquisa é caracterizada como aplicada, pois objetiva gerar conhecimentos para aplicação prática à solução de problemas específicos (Silva; Menezes, 2005). Segundo os autores, na pesquisa quantitativa tudo pode ser quantificável e traduzido em números, opiniões e informações para classificação e análise. Na pesquisa qualitativa é considerada a existência de uma relação dinâmica entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzida em números.

A base de dados utilizada neste estudo foi constituída a partir de registros administrativos e operacionais produzidos pela Secretaria Nacional de Políticas Penais (SENAPPEN) durante a mobilização da Força Penal Nacional na crise de segurança pública do Rio Grande do Norte. As informações referentes à mobilização logística, efetivo empregado, ações executadas e suporte operacional foram obtidas por meio de processos específicos registrados no Sistema Eletrônico de Informações (SEI!) da SENAPPEN, documentos internos interagências, bem como pelos relatórios de missão e relatórios de acompanhamento operacional produzidos no contexto da atuação da Força-Tarefa dentro da Diretoria da Polícia Penal Federal e da Coordenação-Geral de Segurança e Operações. Tais dados foram acessados em virtude da participação direta do autor na coordenação das ações, respeitando-se os limites legais e institucionais para utilização de informações de natureza administrativa em estudos acadêmicos.

Os indicadores de criminalidade e de redução dos eventos violentos foram extraídos de duas fontes principais: relatórios de inteligência produzidos pela Coordenação-Geral de Inteligência Penitenciária da Diretoria da Polícia Penal Federal e pelas Coordenações de Contra-Inteligência da Diretoria de Inteligência Penal da SENAPPEN, sempre em formato agregado, sem

divulgação de elementos sensíveis ou operacionais, e bases de dados abertas disponibilizadas nos portais institucionais da Polícia Civil do Estado do Rio Grande do Norte. A triangulação entre dados internos, informações estratégicas e registros públicos permitiu compor um panorama consistente dos efeitos da intervenção federal, garantindo confiabilidade metodológica sem comprometer o sigilo inerente às atividades de segurança pública e inteligência penitenciária.

Desse modo, para elaboração deste artigo, foram utilizados registros da mobilização logística realizada sob o acompanhamento e controle da Secretaria Nacional de Políticas Penais (SENAPPEN), órgão federal integrado à estrutura do Ministério da Justiça e Segurança Pública, responsável pelo Sistema Penitenciário Federal.

Portanto, para se alcançar o objetivo desse trabalho, fez-se necessário o comparativo de dados de amostras de um ano antes do evento, identificando como se relacionam, assim como observação de antes e depois do evento. Para isso foi utilizado o teste de Wilcoxon, considerado uma extensão do teste dos sinais, só que mais eficiente por utilizar duas amostras relacionadas e identificar a amplitude da diferença entre os pares amostrais (Fávero e Belfiore, 2017).

O contexto da análise envolveu uma crise de segurança pública. Tal crise não só realçou a capacidade de organização das facções criminosas e o perigo que representam para o Estado Democrático de Direito, mas também levantou questões relevantes sobre a importância e necessidade de manter uma força federal em pronto-emprego operacional a fim de coibir a violência e fornecer suporte rápido e eficaz aos Estados quando necessário, retomando o controle e garantindo a segurança da sociedade.

A escolha de utilização da FTIP como ferramenta de repressão imediata aos intentos criminosos em tela abrangeu diversas problemáticas que se apresentaram. Considerada uma "intervenção branca" – quando não há necessidade de disparos de arma de fogo e/ou uso de instrumentos de menor potencial ofensivo – a presença da tropa especializada na Penitenciária Estadual de Alcaçuz representou, por si só, que era chegada a hora de os líderes da organização criminosa cessarem seus desígnios delituosos. Por essa razão, o fato de a pesquisa analisar o contexto da análise custo-efetividade antes e após esse evento de intervenção.

Uma vez publicada a portaria de atuação pelo Ministério da Justiça (Portaria MJSP nº 354, de 13 de abril de 2023 e, depois, prorrogada, Portaria MJSP nº 372, DE 12 de maio de 2023), foram articuladas ações pontuais entre a Coordenação da Força e as autoridades estaduais a fim de refrear os agentes causadores da crise. Desta forma e, como primeiro ato, as agências de inteligência local e o SPF trabalharam para que fosse realizada a transferência dos líderes da organização criminosa de Alcaçuz para presídios federais, no total de 10 transferências.

O impacto das transferências foi rapidamente traduzido em indicadores fornecidos pelo Centro Integrado de Operações de Segurança Pública (SESED/RN): no dia 13 de março, já haviam sido contabilizados 304 ataques; no dia 14, ocorreu a chegada da FTIP ao Estado e a primeira transferência de liderança criminosa para o SPF, seguida de outras nove transferências no dia 16; oito dias após a primeira transferência, cessaram completamente os ataques.

Somadas às transferências, as atuações da Força organizam-se em três eixos: operação (repressiva ou preventiva), treinamento do efetivo mobilizado e instrução ao corpo de servidores locais. Assim, a referida operação, de caráter repressivo, não só envidou esforços de prestar os devidos apoios em fluxos operacionais e administrativos à gestão da Unidade Prisional de Alcaçuz, mas também fomentou e realizou 12 ações de capacitação com temáticas pertinentes ao cenário, visando o controle de possíveis ações ulteriores e compondo um banco de servidores estaduais que poderá agir em situações de crise, motins e rebeliões, gerando 356 vagas em mais de 350 horas/aula. Ainda, a atuação da Força viabilizou a realização de mais de 3 mil atendimentos em saúde e assistenciais nos internos da Unidade Prisional de Alcaçuz.

Destarte, foram utilizados dados secundários oriundos da Secretaria Nacional de Políticas Penais (SENAPPEN) e da Secretaria de Segurança Pública do Rio Grande do Norte, com destaque para estatísticas de crimes violentos e recursos alocados durante a operação. Para análise quantitativa, foi aplicado o teste não paramétrico de Wilcoxon, utilizado para avaliar se há diferenças significativas entre duas condições relacionadas, conforme sugerido por Fávero e Belfiore (2017), comparando pares de observações entre os anos de 2022 e 2023.

A análise se deu por meio da interpretação dos relatórios operacionais da FTIP, observando a articulação logística e os resultados tangíveis. A

triangulação dos dados permitiu inferências sobre a eficiência e indícios de eficácia, embora não tenha sido possível comprovar a efetividade em função do reduzido número de variáveis e da ausência de séries históricas completas.

Resultados e Análise

A análise dos dados revelou uma redução quantitativa nos crimes violentos no Rio Grande do Norte entre o primeiro semestre de 2022 e o mesmo período de 2023. Em que pese demonstrarem-se pouco expressivas as análises no que tange ao estado como um todo, nas cidades da região metropolitana os dados fornecidos apontam significante redução dos crimes dessa natureza, como segue na Tabela 1.

Em relação à análise por municípios da região metropolitana (Tabela 1), observaram-se reduções relevantes nos índices de criminalidade: Mossoró (– 41,7%), Parnamirim (– 44%), São Gonçalo do Amarante (– 21,2%) e Natal (– 12,4%). Esses dados reforçam a hipótese de impacto localizado e possivelmente tático da FTIP. Ainda assim, a ausência de controle por variáveis contextuais impede inferência causal robusta.

Tabela 1 – Percentual da redução de crimes nas cidades da região metropolitana – Redução de CV e CVLI entre Janeiro e Julho de 2023 comparado com o mesmo período de 2022

Município	% de Redução
Natal	12,40%
Mossoró	41,70%
Parnamirim	44,00%
São Gonçalo do Amarante	21,20%
Macaíba	20,80%

Fonte: Elaborada pelos autores (2025).

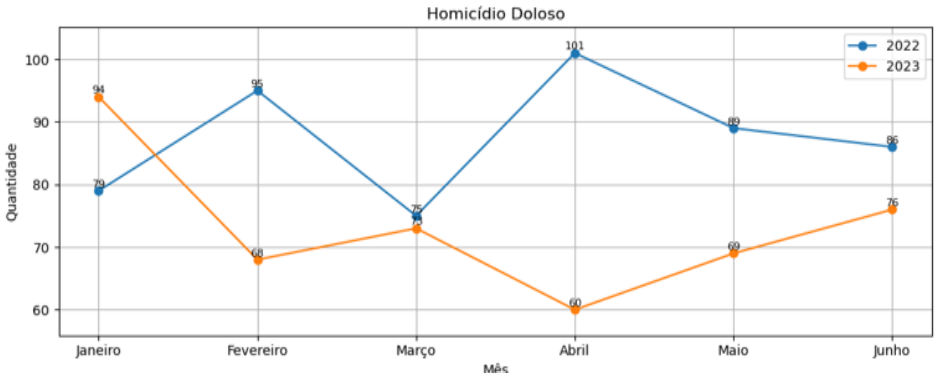
Observações: CV - Crimes Violentos; CVLI - Crimes Violentos Letais Intencionais.

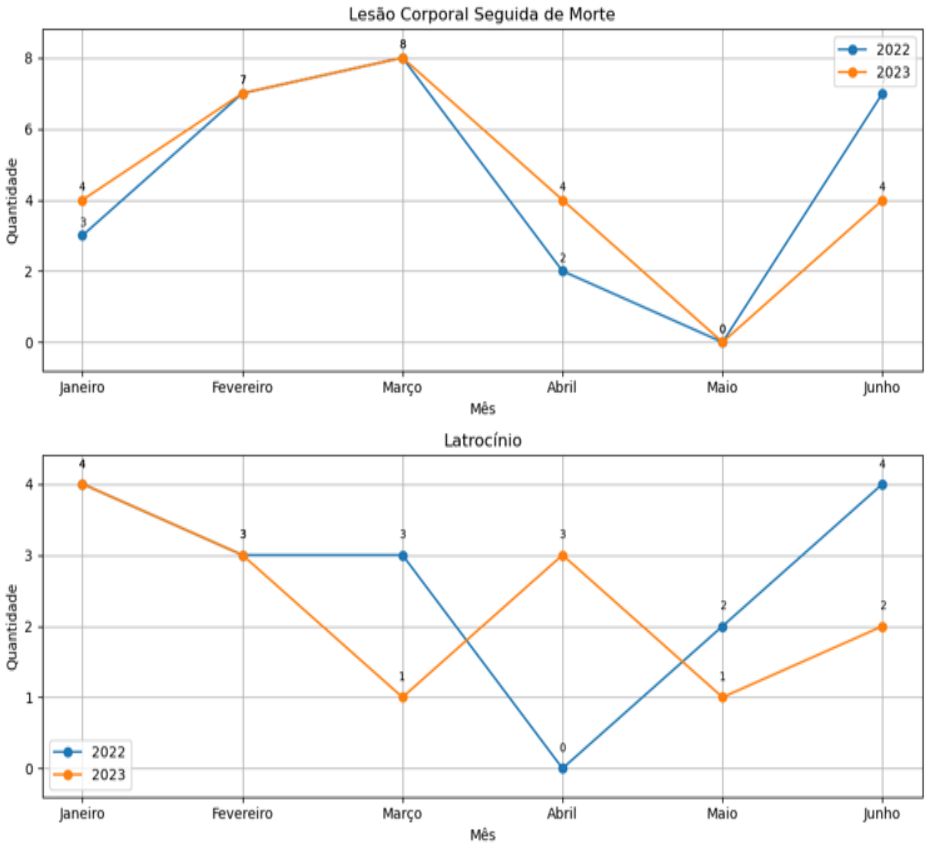
Com base nos dados fornecidos pela Secretaria da Segurança Pública e da Defesa Social, referentes aos indicadores de Crimes Violentos (CV) e Crimes Violentos Letais Intencionais (CVLI) em todo o estado no primeiro semestre de 2022 e de 2023, foi possível obter os seguintes resultados, conforme apresentado no Gráfico 1.

A análise dos dados revelou uma redução quantitativa nos crimes violentos no Rio Grande do Norte entre o primeiro semestre de 2022 e o mesmo período de 2023, conforme Gráfico 1.

Ainda no Gráfico 1, em 2023 houve uma redução consistente dos homicídios dolosos em comparação a 2022. Em janeiro, fevereiro e abril essa redução foi bastante acentuada. Nota-se que abril foi o mês com a maior diferença: redução de 41 casos. Em Lesão Corporal Seguida de Morte, valores muito baixos em ambos os anos. As variações são pequenas e a amostra é muito reduzida (poucos casos absolutos), o que dificulta análises robustas de tendência ou eficácia de políticas públicas com base apenas nesse indicador. No Latrocínio, em janeiro e março de 2023, houve redução significativa em relação a 2022. Abril de 2023 teve aumento em comparação com 2022. Assim como para lesão seguida de morte, os números absolutos são baixos, o que gera alta volatilidade percentual, prejudicando inferências mais sólidas.

Gráfico 1 - Quantidade de crimes violentos e crimes violentos letais intencionais – 1º semestre de 2022 e 2023 (continua)





Fonte: Elaborado pelos autores (2025).

Ainda, considerando as funções logísticas para a manutenção de uma tropa em prontidão, e o planejamento dos recursos disponíveis para a operação, os dados foram divididos em: pessoas (forças e pessoal), equipamento (sistemas, equipamentos e instalações) e prontidão (treinamento e ritmo operacional; manutenção e equipamento; insumos). Neste, assim como no agrupamento dessa divisão, foram realizados testes de sinais de Wilcoxon para análise das amostras relacionadas de indicadores em todo o estado, referentes aos dados em hipóteses dos custos (HC), hipóteses da redução de Crimes Violentos (CV) e Crimes Violentos Letais Intencionais (CVLI) na operação geral (HOG), considerando o mesmo período em 2022 e hipóteses de redução de (CV/CVLI) na operação específica (HOE), somente no primeiro semestre de 2023, buscando em toda análise "parametrizar" quanto à eficácia, eficiência e efetividade da operação.

À luz do exposto acima, as seguintes hipóteses foram testadas:

Hipótese da Operação Específica (HOE) – as séries utilizadas foram: Homicídio Doloso, Lesão Corporal Seguida de Morte e Latrocínio.

Hipótese de Custos (HC) – as séries utilizadas foram: Pessoas (forças e pessoal), Equipamento (sistemas, equipamentos e instalações) e Prontidão (treinamento e ritmo operacional; manutenção e equipamento; insumos);

Hipótese da Operação Geral (HOG) – as séries utilizadas foram: Homicídio Doloso, Lesão Corporal Seguida de Morte e Latrocínio;

Na Tabela 2 apresentamos as análises descritivas das variáveis utilizadas na pesquisa.

Tabela 2 – Análise Descritiva (continua)

Hipótese da Operação Específica (HOE)					
Séries	**Média**	**Desvio Padrão**	**Coeficiente de Variação**	**Valor Mínimo**	**Valor Máximo**
Homicídio Doloso Antes	78,33	13,80	17,62	68	94
Homicídio Doloso Depois	68,33	8,02	11,74	60	76
Lesão Corporal Seguida de Morte Antes	6,33	2,08	32,86	4	8
Lesão Corporal Seguida de Morte Depois	2,67	2,31	86,52	0	4
Latrocínio Antes	2,67	1,53	57,30	1	4
Latrocínio 2023	2	1	50	1	3
Total Antes	87,33	12,86	14,73	78	102
Total Depois	73	7,94	10,88	67	82

Hipótese de Custos (HC)					
Séries	Média	Desvio Padrão	Coeficiente de Variação	Valor Mínimo	Valor Máximo
Pessoas 2022	350.000	0	0	350.000	350.000
Pessoas 2023	505.103,60	170.173,80	33,69	350.000	689.443
Prontidão 2022	0	0	-	0	0
Prontidão 2023	5.846,25	8.068,60	138,01	0	15.590
Equipamento 2022	7.500	0	0	7.500	7.500
Equipamento 2023	3.750	4.008,92	106,90	0	7.500
Total 2022	357.500	0	0	357.500	357.500
Total 2023	514.699,90	173.562,70	33,72	357.500	705.033

Hipótese da Operação Geral (HOG)					
Séries	Média	Desvio Padrão	Coeficiente de Variação	Valor Mínimo	Valor Máximo
Homicídio Doloso 2022	87,50	9,71	11,10	75	101
Homicídio Doloso 2023	73,33	11,48	15,66	60	94
Lesão Corporal Seguida de Morte 2022	4,50	3,27	72,67	0	8
Lesão Corporal Seguida de Morte 2023	4,50	2,81	62,44	0	8
Latrocínio 2022	2,67	1,51	56,55	0	4
Latrocínio 2023	2,33	1,21	51,93	1	4
Total 2022	94,67	8,31	8,78	86	105

Fonte: Elaborada pelos autores (2025).

A Tabela 2 resume as estatísticas de três hipóteses avaliadas na pesquisa: HOE (Hipótese da Operação Específica), HC (Hipótese de Custos) e HOG (Hipótese da Operação Geral). As estatísticas incluem: média, desvio

padrão (DP), coeficiente de variação (CV), valor mínimo e máximo. Em relação à Hipótese da Operação Específica (HOE), ela vai captar mudanças nos indicadores de violência letal antes e depois da operação específica. Ainda na HOE, houve redução média de aproximadamente 10 homicídios dolosos, acompanhada de uma diminuição da variabilidade relativa (CV), sugerindo não apenas redução, mas também maior homogeneidade entre observações; na lesão corporal seguida de morte, houve queda da média, porém o CV aumentou fortemente, indicando maior dispersão relativa; no latrocínio, uma pequena queda na média, com ligeira redução na variabilidade relativa; no total geral, a soma total dos crimes letais caiu, e a dispersão também, o que pode indicar uma eficácia da operação.

Agora, na Hipótese de Custos (HC), que avalia os custos humanos e de materiais da operação, em relação a pessoas, houve aumento considerável no efetivo humano envolvido em 2023 e, ao mesmo tempo, alta variação entre registros; prontidão e equipamento, mostram que em 2023 houve mobilização logística significativa, porém com grande variação, devido a operação; no total, os custos totais aumentaram, mas também variaram bastante, refletindo uma operação com execução heterogênea em termos orçamentários.

Por fim, a Hipótese da Operação Geral (HOG) consiste em uma análise comparativa mais ampla. No caso do homicídio doloso, observa-se uma queda consistente na média, embora a dispersão tenha aumentado ligeiramente. Já a lesão corporal seguida de morte indica que, apesar da estabilidade da média, há grande variação entre as observações. O latrocínio apresentou uma melhora sutil no indicador, acompanhada de maior homogeneidade. Em relação ao total, verificou-se uma redução da criminalidade letal em 2023, mas com aumento na dispersão.

À luz do exposto, para um melhor entendimento da eficiência, eficácia e efetividade, é necessário analisar os resultados do teste de Wilcoxon. A hipótese nula (H_0) do teste para cada um (HOG, HC e HOE) será: A mediana das diferenças entre os pares (ex.: 2023 – 2022) é igual a zero. Ou seja, não há alteração estatisticamente significativa entre os períodos. A hipótese alternativa (H_1) será: A mediana das diferenças entre os pares é diferente de zero. Ou seja, houve alteração estatisticamente significativa entre os períodos.

No caso de haver eficácia - a capacidade de alcançar os objetivos propostos ao final da operação -, deve haver diferença na comparação dos

crimes entre os anos 2022 e 2023. A eficiência, correspondente à relação entre os resultados obtidos e os recursos utilizados para alcançá-los, ou seja, se os recursos utilizados geraram proporcionalmente resultados, não deve haver diferença nos custos dispendidos para a ação entre um ano e outro. Já a efetividade, habilidade de se chegar ao que foi desejado da melhor maneira possível, se verifica na análise antes e após a operação. A Tabela 3 apresenta os resultados para cada hipótese do teste Wilcoxon.

Após realizados os testes, constatou-se que na Hipótese da Operação Específica (HOE) e Operação Geral (HOG), ou seja, comparando os eventos do ano corrente (2023) com o ano anterior (2022), o p-valor é maior que 10% e, por isso, não rejeita a hipótese nula de que não exista diferença nos crimes violentos e crimes violentos letais intencionais referentes aos meses analisados do ano de 2022 e 2023 – embora quantitativamente tenha ocorrido uma diminuição (como evidenciada na Tabela 1), estatisticamente, não há. Ou seja, no mesmo período em comparação, o indicador foi estatisticamente igual e, com isso, não tivemos eficiência, pois não reduziu, estatisticamente, no período considerado.

Nas Hipóteses de análise de Custos (HC) isolados com Pessoal, Prontidão e Equipamento o p-valor é menor que 10% e, dessa forma, rejeita a hipótese nula de que não exista diferença nos custos entre os meses analisados do ano de 2022 e 2023. Ou seja, há diferença entre os custos referentes à operação sendo, nesse aspecto, ineficiente, confirmados pelos resultados das HOE e HOC. Portanto, a operação apresenta ineficiência, pois custos aumentaram (ou mudaram) sem impacto comprovado nos resultados desejados. A análise da efetividade torna-se complicada de se medir, dado o reduzido número de dados para executá-lo, pois ela é definida como impacto de longo prazo e transformação estrutural. Porém, a efetividade implica resultados sustentáveis e custo-efetivos e, dado que não houve eficácia nem eficiência, a efetividade da operação pode estar comprometida. Destarte, a ação analisada não foi efetiva no período analisado.

As ações coordenadas entre SENAPPEN, FTIP e o governo estadual permitiram a redução imediata (quantitativamente) da onda de violência. A transferência de dez líderes da facção para presídios federais foi acompanhada da cessação dos ataques, reforçando a hipótese de eficácia tática da operação. Segundo dados do Centro Integrado de Operações, a redução dos crimes violentos em Mossoró e Parnamirim ultrapassou 40% no primeiro semestre de 2023.

Tabela 3 – Resultados para cada hipótese do teste Wilcoxon

Hipótese da Operação Específica (HOE)			
Séries	**Valor do Teste**	**P-valor**	**Resultado**
Homicídio Doloso	1,572	0,1159	Não rejeita H_0
Lesão Corporal Seguida de Morte	-0,342	0,7324	Não rejeita H_0
Latrocínio	0,649	0,5164	Não rejeita H_0
Total	1,572	0,1159	Não rejeita H_0

Hipótese de Custos (HC)			
Séries	**Valor do Teste**	**P-valor**	**Resultado**
Pessoas	-1,982	0,0474*	Rejeita H_0
Prontidão	-1,732	0,0833**	Rejeita H_0
Equipamento	2	0,0455*	Rejeita H_0
Total	-1,982	0,0474*	Rejeita H_0

Hipótese da Operação Geral (HOG)			
Séries	**Valor do Teste**	**P-valor**	**Resultado**
Homicídio Doloso	0	1	Não rejeita H_0
Lesão Corporal Seguida de Morte	1,387	0,1655	Não rejeita H_0
Latrocínio	0,816	0,4142	Não rejeita H_0
Total	1,387	0,1655	Não rejeita H_0

Fonte: Elaborada pelos autores (2025).

Observações: Significância estatística: * = 5% ; ** = 10%. A hipótese nula (H_0) para cada um (HOG, HC e HOE) será: A mediana das diferenças entre os pares (ex.: 2023 – 2022) é igual a zero. Ou seja, não há alteração estatisticamente significativa entre os períodos. A hipótese alternativa (H_1) será: A mediana das diferenças entre os pares é diferente de zero. Ou seja, houve alteração estatisticamente significativa entre os períodos.

Complementarmente, foram realizadas 12 ações de capacitação com mais de 350 servidores, além de mais de 3 mil atendimentos assistenciais e de saúde, fortalecendo a capacidade institucional local. Essas ações refletem o entendimento de Farley (2020) sobre o valor da logística como vetor de desenvolvimento organizacional em segurança pública.

Os resultados observados estão alinhados com evidências apresentadas na literatura internacional sobre intervenções emergenciais em segurança pública e naquelas que indicam que operações governamentais destinadas à estabilização de crises frequentemente produzem efeitos imediatos na redução da violência, mas nem sempre apresentam resultados estatisticamente significativos no curto prazo.

Segundo Boin *et al.* (2005), intervenções emergenciais devem ser analisadas não apenas pelo impacto imediato nos indicadores quantitativos, mas também pelos efeitos institucionais que produzem na capacidade de resposta do Estado. Elementos como capacitação de pessoal, fortalecimento das estruturas organizacionais e melhoria da coordenação interinstitucional podem representar ganhos relevantes para a gestão pública, ainda que esses resultados não sejam plenamente capturados pelos indicadores tradicionais de desempenho.

Considerações Finais

A análise realizada sobre a operação de resposta à crise de segurança pública no Rio Grande do Norte em 2023 permitiu compreender com maior profundidade os desafios inerentes à articulação logística em contextos de emergência e violência generalizada. A mobilização da Força-Tarefa de Intervenção Penitenciária (FTIP), sob a coordenação da SENAPPEN, demonstrou capacidade tática de resposta imediata, com redução quantitativa dos crimes violentos e estabilização da ordem nas unidades prisionais, sobretudo por meio da transferência de lideranças criminosas e da adoção de medidas de capacitação e suporte institucional.

Entretanto, os resultados estatísticos oriundos do teste de Wilcoxon não foram suficientes para comprovar eficácia ou eficiência de maneira robusta. Ainda que tenha havido variações numéricas positivas, especialmente nas cidades da região metropolitana como Mossoró e Parnamirim, tais variações

não alcançaram significância estatística. Do ponto de vista dos custos, foi possível identificar um aumento expressivo nos recursos humanos e logísticos empregados, o que, sem a devida correspondência nos resultados esperados, compromete a avaliação da eficiência da operação.

A efetividade, por sua vez, foi dificultada de ser mensurada de forma conclusiva, em razão da ausência de séries históricas longas e do caráter pontual da intervenção. Ainda assim, os dados qualitativos sugerem avanços estruturantes, como a capacitação de servidores e a reestruturação das rotinas operacionais nas unidades prisionais, elementos que podem gerar impactos positivos de médio e longo prazo.

A fim de que sejam desenvolvidas análises ulteriores nas operações semelhantes e, com o intuito de aprimorar as atuações em situações de crise, sugere-se que sejam elaborados relatórios analíticos integrados entre os Estados – sobretudo àqueles que passaram por situações de intervenção, e a União, de maneira a facilitar a busca por indicadores e a formulação de diagnósticos para otimizar as ações de mesma natureza.

Ainda, como não foi possível realizar integralmente as hipóteses estatísticas devido à baixa amostragem dos indicadores, propõe-se que pesquisas futuras considerem não apenas os dados relativos ao semestre, mas também os do ano completo. Além disso, recomenda-se ampliar a análise para além dos anos de 2022 e 2023, incorporando informações de períodos anteriores. Igualmente, sugere-se analisar casos similares para que possam ser avaliadas as alternativas adotadas e analisados modelos prognósticos e de previsão de custos. Para aprimorar a análise de efetividade, recomenda-se a ampliação da coleta de dados ao longo do tempo, incluindo variáveis contextuais, sociais e econômicas. Sugere-se ainda a aplicação de modelos como DEA ou regressão descontínua para aprofundamento metodológico.

Referências

ARAUJO, A. O. Gestão estratégica de custos logísticos. In: CONGRESSO BRASILEIRO DE CUSTOS, 8., 2001, São Leopoldo, RS. *Anais [...]*. São Leopoldo: UNISINOS, 2001. Disponível em: https://anaiscbc.emnuvens.com.br/anais/article/view/2943. Acesso em: 10 out. 2023.

BALLOU, R. H. *Gerenciamento da cadeia de suprimentos:* logística empresarial. Porto Alegre: Bookman, 2006.

BOIN, A.; T HART, P.; STERN, E.; SUNDELIUS, B. *The Politics of Crisis Management:* Public Leadership Under Pressure. Cambridge: Cambridge University Press, 2005.

BOUCKAERT, G.; HALLIGAN, J. *Managing Performance: International Comparisons.* London: Routledge, 2008.

BUENO, S.; LIMA, R. S. *Política nacional de segurança pública orientada para resultados:* desafios de financiamento e custo-efetividade. Brasília: IPEA, 2020. (Texto para Discussão, n. 2605). Acesso em: 12 out. 2023.

BRASIL. Exército Brasileiro. *Manual de Campanha Logística Militar Terrestre. EB70-* MC-10.238. 2. ed. Brasília, DF: MD, 2022.

BRASIL. Secretaria Nacional de Políticas Penais. *Institucional*. Brasília: SENAPPEN, 2023. Disponível em: https://www.gov.br/senappen/pt-br/acesso-a-informacao/institucional. Acesso em: 3 out. 2023.

CALDERARO, F.; PALHARES, F. A contribuição da logística integrada às decisões de gestão das políticas públicas. *Revista de Administração Pública*, v. 45, n. 1, p. 207–236, 2011. DOI: https://doi.org/10.1590/S0034-76122011000100010.

CAVALCANTI, H. da S.; GOMES, J. da S. O.; LOPES, K. K. J.; SOUZA, N. A. de; CAMPELLO, M. Uma breve análise sobre a evolução da logística. In: CAMPELLO, M. et al. (org.). *Logística:* contribuições para melhorias na produção e nos resultados. Guarujá: Científica Digital, 2021. p. 64-81. DOI: 10.37885/210303726.

CHARNES, A.; COOPER, W. W.; RHODES, E. Measuring the efficiency of decision-making units. *European Journal of Operational Research*, v. 2, n. 6, p. 429–444, 1978. DOI: https://doi.org/10.1016/0377-2217(78)90138-8

CHOPRA, S.; MEINDL, P. *Gerenciamento da cadeia de suprimentos:* estratégia, planejamento, e operação. São Paulo: Pearson, 2003.

CHRISTOPHER, M. *Logistics & supply chain management*. Harlow: Pearson, 2016.

CISLAGHI, Tatiane et al. Logística humanitária: práticas e desafios em tempos de tensões geopolíticas, desigualdades sociais e crise ambiental. *Organizações em Contexto*, v. 20, n. 40, p. 127-164, 2024

DANTAS, E. B. *A importância da pesquisa para a tomada de decisões.* Brasília: UnB, 2013.

DINIZ, A. M. T.; BARBOSA, K. N. S.; MEDEIROS, D. R. Efetividade e eficiência das operações de garantia da lei e da ordem: o caso da Operação Arcanjo. *Revista Debates,* v. 16, n. 2, p. 145-169, 2022

FÁVERO, L. P.; BELFIORE, P. *Manual de análise de dados:* estatística e modelagem multivariada com Excel®, SPSS® e Stata®. Rio de Janeiro: Elsevier Brasil, 2017.

FARLEY, R. M. *Space Force:* ahead of its time or dreadfully premature? Washington, DC: Cato Institute, 2020. (*Policy Analysis*, n. 904).

GIACOBO, F.; CERETTA, P. S. Planejamento logístico: uma ferramenta para o aprimoramento do nível de serviço. In: SEMEAD, 6., 2003, São Paulo. *Anais [...]* São Paulo: FEA-USP, 2003. Disponível em: https://www.researchgate.net/profile/Paulo-Ceretta/publication/267950288_v_v_i_i_s_planejamento_logistico_uma_ferramenta_para_o_aprimoramento_do_nivel_de_servico/links/552bbd3f0cf29b22c9c1e04d/v-v-i-i-s-planejamento-logistico-uma-ferramenta-para-o-aprimoramento-do-nivel-de-servico.pdf. Acesso em: 13 out. 2023.

GIL, A. C. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Atlas, 2002.

GUERESCHI, J. F. A criação do sistema nacional de mobilização. *Revista da Escola Superior de Guerra*, v. 24, n. 50, p. 131-152, 2008.

KAPLAN, R. S.; NORTON, D. P. *The balanced scorecard*. Boston: Harvard Business School Press, 1996.

MORAES, M. C.; GOMES, L. F. Custo logístico e desempenho em cadeias de suprimentos públicas. *Organizações em Contexto,* v. 17, n. 1, p. 95-118, 2011.

NOVAES, A. G. *Logística e gerenciamento da cadeia de distribuição:* estratégia, operação e avaliação. 3. ed. Rio de Janeiro: Elsevier, 2007.

ODON, T. I. Segurança pública e análise econômica do crime. *Revista de Informação Legislativa*, v. 55, n. 218, p. 33-62, 2018. Disponível em: https://www12.senado.leg.br/ril/edicoes/55/218/ril_v55_n218_p33.pdf. Acesso em: 8 set. 2025.

OLIVEIRA, M. F. de. *Metodologia científica*: um manual para a realização de pesquisas em Administração. Catalão: UFG, 2011. 72 p.

PIMENTEL, M.; PEREIRA, A. M. Análise benefício-custo de políticas de segurança pública: o caso do Espírito Santo. *Revista Brasileira de Economia,* v. 77, n. 2, p. 147-176, 2023

RAMOS, C. E. de F. A importância da mobilização nacional sobre os ombros de gigantes. *Coleção Meira Mattos: revista das ciências militares*, n. 27, p. 87-106, 2012. Disponível em: https://colecaomeiramattos.com.br/CMM/article/view/230/215. Acesso em: 12 out. 2023.

SILVA, E. L da.; MENEZES, E. M. *Metodologia da pesquisa e elaboração de dissertação*. 4. ed. Florianópolis: UFSC, 2005.

SHEFFI, Y. *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage.* Cambridge: MIT Press, 2005.

SEGRETI, J. B.; FARBER, J. C.; MONDINI, L. C. A importância da gestão estratégica de custos logísticos. In: CONGRESSO BRASILEIRO DE CUSTOS, 11., 2004, Porto Seguro, BA. *Anais [...]*. São Leopoldo: Associação Brasileira de Custos, 2004. Disponível em: https://anaiscbc.emnuvens.com.br/anais/article/view/2281. Acesso em: 29 mar. 2026.

TOMASINI, R.; VAN WASSENHOVE, L. *Humanitarian Logistics*. London: Palgrave Macmillan, 2009.

Mudanças climáticas, segurança nacional e resiliência: o exemplo da Operação "Taquari II" (2024)

Thiago Abreu de Figueiredo
Cintiene Sandes Monfredo Mendes
José Roberto Pinho de Andrade Lima

A ampliação do conceito de segurança e a Escola de Copenhague

A ampliação do conceito de segurança constitui um dos principais debates teóricos das Relações Internacionais no período pós-Guerra Fria. Nesse contexto, a contribuição da Escola de Copenhague, especialmente a partir dos trabalhos de Barry Buzan e Ole Wæver, tornou-se essencial para uma abordagem mais ampla e multidimensional da segurança, que desse conta de compreender e abordar processos mais diversificados e complexos para além do fenômeno da guerra.

Segundo essa perspectiva, a segurança deve ser analisada em diferentes setores: militar, político, econômico, societal e ambiental. A abordagem da segurança nesse contexto representa uma ruptura com a visão tradicional, que restringia a segurança ao campo militar, e permite compreender como diferentes tipos de ameaças podem comprometer a estabilidade dos Estados e das sociedades, bem como as respostas do Estado à sensibilidade e vulnerabilidade a fatores que atualmente correspondem aos impactos da interdependência complexa (Keohane; Nye, 1973). A inclusão do setor ambiental é particularmente relevante para a análise das mudanças climáticas, pois reconhece que a degradação ambiental e os desastres naturais podem gerar instabilidade política, crises econômicas e conflitos sociais a ponto de mobilizarem as estruturas do Estado como forma de resposta para a estabilização.

A partir da Escola de Copenhague também se desenvolveu o conceito de securitização, que se tornou central nos estudos de segurança contemporâneos. A securitização refere-se ao processo pelo qual determinados temas passam a ser tratados como questões de segurança, justificando a adoção de medidas extraordinárias para enfrentá-los. Esse processo não ocorre automaticamente,

mas depende de construções políticas e discursivas, dos interesses do Estado em transformar determinados fenômenos em securitizados a partir de seus impactos sociais, econômicos ou políticos.

No caso das mudanças climáticas, observa-se um processo crescente de securitização, na medida em que eventos climáticos extremos passam a ser tratados como ameaças à estabilidade social e à capacidade de governança dos Estados. Esse processo permite a mobilização de recursos excepcionais e a participação de instituições tradicionalmente associadas à defesa, como as Forças Armadas, em operações de resposta a desastres naturais e crises humanitárias.

Paralelamente à ampliação do conceito de segurança promovida pela Escola de Copenhague, desenvolveu-se a abordagem da Segurança Humana, que desloca o foco da segurança do Estado para o indivíduo. Esse conceito foi desenvolvido no âmbito do Programa das Nações Unidas para o Desenvolvimento e representa uma mudança significativa na forma de compreender a segurança.

A segurança humana enfatiza que a segurança não deve ser medida apenas pela ausência de guerras ou conflitos militares, mas pela capacidade de garantir condições mínimas de sobrevivência, dignidade e qualidade de vida para as populações. Essa abordagem inclui diferentes dimensões, como segurança alimentar, segurança sanitária, segurança ambiental, segurança econômica e segurança pessoal.

No contexto das mudanças climáticas, a segurança humana torna-se particularmente relevante, pois os impactos dos desastres naturais afetam diretamente a vida das pessoas, comprometendo moradia, alimentação, acesso à água, saúde e renda. Assim, operações de resposta a desastres ambientais devem ser compreendidas não apenas como ações de defesa civil ou logística militar, mas como políticas de segurança humana, voltadas à proteção da população.

Essa perspectiva amplia o papel do Estado e das instituições de defesa, que passam a atuar também em missões humanitárias, operações de ajuda emergencial e reconstrução de infraestruturas, reforçando a interdependência entre segurança, desenvolvimento e políticas públicas.

Outro conceito fundamental para compreender a transformação da segurança no século XXI é o conceito de resiliência, amplamente discutido por Cecilia Fjäder (2014). No contexto da globalização, caracterizado por interdependência e riscos sistêmicos, a segurança não pode mais ser baseada apenas na prevenção de ameaças, pois muitas crises são inevitáveis, como desastres naturais, pandemias e crises econômicas globais.

A resiliência refere-se à capacidade de sistemas, instituições e sociedades de resistir a choques, adaptar-se a novas condições e recuperar-se rapidamente após crises. Diferentemente da lógica tradicional da segurança, que busca evitar a ocorrência de ameaças, a resiliência parte do pressuposto de que crises ocorrerão e que o mais importante é garantir a continuidade do funcionamento da sociedade.

Nesse sentido, a segurança nacional passa a ser entendida como a capacidade de manter o funcionamento das estruturas essenciais da sociedade, como infraestrutura de transporte, sistemas de energia, comunicações, abastecimento de alimentos e água, serviços de saúde e governança. A proteção dessas infraestruturas críticas torna-se um elemento central da segurança contemporânea.

A incorporação da resiliência às políticas de segurança representa, portanto, uma mudança de paradigma, na qual a segurança deixa de ser apenas proteção contra ameaças e passa a ser capacidade de gestão de crises.

Mudanças climáticas, segurança nacional e resiliência: conceitos-chave

As mudanças climáticas configuram um processo prolongado de transformação do clima terrestre, impulsionado tanto por fatores naturais quanto, de forma mais acentuada, pela intensificação das atividades humanas, a partir do fim dos anos 1940 e início dos anos 1950 (Angus, 2016).

Desde então, o acúmulo de gases de efeito estufa tem intensificado fenômenos como o aumento das temperaturas médias, as alterações nos regimes de precipitação, a acidificação dos oceanos e a maior recorrência de eventos climáticos extremos,[1] dentre outros (Nelles; Serrer, 2020). Essas dinâmicas se

[1] São eventos climáticos extremos ondas de calor e de frio, precipitações intensas (chuva ou neve), tempestades de granizo ou gelo, secas prolongadas, ciclones tropicais e extratropicais,

inserem no conjunto de desafios cada vez mais complexos, interconectados e heterogêneos do Antropoceno,[2] período caracterizado pela influência decisiva da ação humana sobre o planeta e por transformações aceleradas nos sistemas naturais e socioecológicos (Palazzo, 2022).

Nesse cenário, as mudanças climáticas vêm comprometendo de forma crescente a estabilidade global (Góes; Couto, 2021) e impondo a necessidade de reconfigurações profundas em diferentes dimensões da vida em sociedade (Palazzo, 2022). A literatura científica converge no entendimento de que o agravamento do aquecimento global tende a alterar, de maneira significativa, a frequência, a intensidade e a distribuição geográfica dos eventos climáticos extremos (Shepherd, 2023), com repercussões severas para a segurança humana[3] em escala planetária (Price; Pitts; Van Roekel, 2021) e consolidando-se como um dos principais desafios do século XXI, uma vez que ameaçam a segurança dos Estados e a própria sobrevivência humana no planeta (Giddens, 2010).

Essa dinâmica entre o clima e a segurança está alinhada com o crescimento expressivo no número de desastres climáticos registrados em todo o mundo (WMO, 2024), os quais demandam a participação cada vez mais frequente das Forças Armadas nas respostas estatais às suas consequências (Andrade Lima; Figueiredo, 2025). Um exemplo emblemático dessa atuação

---

ressacas e tornados (Shepherd, 2023).

[2]O Antropoceno pode ser compreendido como uma nova era geológica que sucedeu ao Holoceno, vigente nos últimos 10 a 12 mil anos. Introduzido formalmente nos debates científicos e ambientais, a partir dos anos 2000, esse conceito expressa a ideia de que a ação humana se tornou a principal força geológica capaz de moldar o futuro do Sistema Terrestre. Embora comumente associado à Revolução Industrial no final do século XVIII, é mais apropriado situar o início do Antropoceno entre o final da década de 1940 e o início dos anos 1950 (Angus, 2016).

[3] Incorporada ao discurso internacional, a partir da publicação do *Human Development Report* (HDR) de 1994, elaborado pelo Programa das Nações Unidas para o Desenvolvimento (UNDP, 1994). A segurança humana "possui dois aspectos principais. Em primeiro lugar, significa proteção contra ameaças crônicas, como a fome, a doença e a repressão. Em segundo lugar, refere-se à proteção contra perturbações súbitas e dolorosas na vida cotidiana, seja no lar, no trabalho ou na comunidade" (UNDP, 1994, p.26, tradução nossa). Essa concepção introduz uma abordagem multidimensional da segurança que passa a incorporar fatores sociais, econômicos, políticos e ambientais, destacando a centralidade do ser humano diante de contextos marcados por vulnerabilidade e risco. O HDR (PNUD, 1994) sistematiza a segurança humana em sete dimensões fundamentais, que compõem um quadro abrangente de proteção e bem-estar, a saber: segurança econômica, segurança alimentar, segurança sanitária, segurança ambiental, segurança pessoal, segurança comunitária e segurança política.

foi a Operação "Taquari II", conduzida pelo Estado brasileiro em resposta ao evento climático extremo que atingiu o Rio Grande do Sul, entre abril e maio de 2024 (Brasil, 2024a).

Adentrando a discussão sobre segurança, especialmente quanto à definição do termo lato sensu, observa-se que a recorrente utilização do argumento securitário como justificativa para diferentes ações estatais revela a amplitude e a polissemia do conceito, influenciando diretamente as formas como as dinâmicas de segurança são concebidas e interpretadas, tanto no campo teórico quanto na prática cotidiana (Klein, 2011).

Genericamente, a segurança é relacionada à sensação de proteção, estabilidade ou tranquilidade frente aos riscos e às ameaças, as quais podem afetar negativamente indivíduos, instituições ou ativos estratégicos (Medeiros Filho, 2018). Nessa perspectiva, ela se relaciona diretamente com a capacidade de diminuir os riscos e identificar as ameaças, além de contibuir para a manutenção da estabilidade e para o funcionamento de determinado sistema (Cepik, 2001).

Conforme apontam Buzan e Hansen (2012, p. 37), trata-se de um "conceito hifenizado", cuja compreensão integral depende da vinculação a um objeto de referência específico. No âmbito deste paper, o conceito de segurança será analisado em associação ao adjetivo "nacional". Nessa perspectiva, a Política Nacional de Defesa/Estratégia Nacional de Defesa (2024b, p. 79) define segurança nacional como:

> a condição que permite a preservação da soberania e da integridade territorial, a realização dos interesses nacionais, a despeito de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais.

De acordo com Fjäder (2014), a segurança nacional possui um caráter essencialmente preventivo e proativo, voltado à antecipação e neutralização de ameaças internas e externas antes que se concretizem, com o objetivo de preservar a integridade do território, das instituições e da população. Sua lógica fundamental é evitar falhas, uma vez que a destruição do objeto protegido representaria, em si, o fracasso da política de segurança.

Todavia, como reconhece o próprio Fjäder (2014), nem sempre é possível impedir a materialização das ameaças, o que evidencia a importância

do conceito de resiliência como componente da segurança nacional. Nessa perspectiva, a resiliência adquire um duplo caráter, proativo e reativo, voltando-se tanto para a mitigação dos impactos quanto para a manutenção de serviços essenciais e o fortalecimento da capacidade de adaptação e recuperação diante de choques, desastres ou crises inevitáveis.

Jatobá e Carvalho (2022) acrescentam que a resiliência trata da capacidade de adaptação dos sistemas para responder a demandas e eventos adversos ou disruptivos (como epidemias e desastres), ajustando seu funcionamento antes, durante e depois dessas perturbações, ao mesmo tempo em que mantém a continuidade e a qualidade da assistência, preservando suas atividades regulares.

Ela se manifesta de duas maneiras complementares: como propriedade emergente do funcionamento dos sistemas, derivada das quatro habilidades que orientam sua operação, ou seja, antecipar, monitorar, responder e aprender, e ainda, por meio de seus componentes e recursos, expressos em termos de resistência, robustez, estado de preparação e estratégias de adaptação, que sustentam o potencial do sistema para reagir a choques (Jatobá; Carvalho, 2022).

Desse modo, a diferença fundamental entre segurança nacional e resiliência reside no fato de que a primeira possui um caráter territorial e específico, voltado à proteção de pessoas, infraestruturas e fronteiras, enquanto a segunda apresenta um caráter sistêmico e difuso, orientado à preservação da continuidade das funções críticas da sociedade, mesmo diante de cenários de incerteza e disrupção (Fjäder, 2014).

No atual contexto de globalização e interdependência, em que os Estados se defrontam com ameaças cada vez mais transnacionais e imprevisíveis, como as mudanças climáticas, os ciberataques e as pandemias, parecem claras as limitações do paradigma tradicional da segurança nacional, o qual não contempla a resiliência como componente estruturante das estratégias de proteção e resposta.

Segundo Figueiredo e Mendes (2024), a segurança nacional contemporânea deve adotar uma abordagem mais ampla e integrada, que ultrapasse a simples reação a ameaças, incorporando desafios globais e vulnerabilidades emergentes. Essa concepção propõe uma estratégia voltada

ao enfrentamento de ameaças complexas e interconectadas, compreendendo a segurança como um esforço coordenado, multidimensional e intersetorial, que vai além do campo militar e envolve, de forma articulada, diversos setores e atores da sociedade.

Nesse contexto ampliado, a resiliência consolida-se como um componente relevante da segurança nacional, voltada sobretudo à proteção de infraestruturas críticas e à capacitação da sociedade para absorver, resistir e recuperar-se de crises (Fjäder, 2014), como exemplificado pela Operação "Taquari II", desencadeada em resposta ao evento climático extremo ocorrido no Rio Grande do Sul entre abril e maio de 2024 (Brasil, 2024a).

A Operação "Taquari II" como expressão da integração entre clima, segurança e resiliência

A Operação "Taquari II" constituiu um marco da atuação interagências brasileira diante de um evento climático extremo (Zucco, 2025) e exemplificou, de forma concreta, a interdependência entre os conceitos de mudanças climáticas, segurança nacional e resiliência.

Deflagrada em 1º de maio de 2024 (Brasil, 2024a), em resposta às severas enchentes que devastaram o Rio Grande do Sul entre abril e maio daquele ano (Escobar *et al*., 2024), a operação foi formalizada pela Portaria nº 2.309 do Ministério da Defesa, que ativou o Comando Conjunto "Taquari II" (Brasil, 2024c), órgão que aglutinou o trabalho interagências durante toda a operação (Brasil, 2024a).

Sua deflagração ocorreu logo após o reconhecimento oficial da limitação do governo estadual em enfrentar a crise e a declaração de estado de calamidade pública nas áreas atingidas, por meio do Decreto nº 57.596 (Rio Grande do Sul, 2024).

A operação interagências em questão insere-se no contexto de intensificação dos eventos climáticos extremos, resultantes do processo de transformação climática global impulsionado pela ação humana (Nelles; Serrer, 2020). Conforme alertam Shepherd (2023) e Giddens (2010), o agravamento do aquecimento global tende a modificar significativamente a frequência e

a intensidade de tais fenômenos, com implicações diretas sobre a segurança (Buzan; Wæver; De Wilde, 1998).

Assim, desastres como o ocorrido em território gaúcho deixam de ser meras anomalias ambientais para se tornarem questões de segurança (Góes; Couto, 2021), desafiando os Estados a desenvolver respostas adaptativas, rápidas e coordenadas.

Nesse sentido, a Operação "Taquari II" materializou, na prática, a necessidade de transformação da concepção tradicional de segurança nacional**,** centrada na defesa territorial e na neutralização de ameaças (Medeiros Filho, 2018)**,** para uma abordagem ampliada e integrada (Figueiredo; Mendes, 2024), em que a resiliência assume papel central.

Conforme Fjäder (2014), a resiliência amplia o escopo da segurança ao incorporar mecanismos de preparação, resposta e recuperação diante de crises inevitáveis. No caso da operação, um dos aspectos centrais da resiliência estatal foi a rapidez na mobilização das ações: as chuvas começaram em 27 de abril, e já em 30 de abril o Exército Brasileiro (EB) iniciou sua atuação por meio da Operação "Sempre Prontos!", sob coordenação do Comando Militar do Sul (Barros, 2024).

Apenas quatro dias após o início das chuvas, o governo federal, por meio do Ministério da Defesa, deflagrou oficialmente a Operação "Taquari II" (Brasil, 2024c), garantindo a continuidade e ampliação imediata da resposta nacional.

A magnitude do desastre evidenciou ainda o alto grau de complexidade da resposta estatal, exigindo coordenação simultânea nos níveis estratégico, operacional e tático, além da integração de diversas instituições civis e militares (Do Amor, 2024). A operação destacou-se pela gestão de uma extensa rede interagências, que mobilizou mais de 130 instituições públicas dos três níveis de governo, além de organizações privadas, entidades da sociedade civil e atores internacionais (Brasil, 2024a). No auge das ações, em 18 de maio, essa estrutura coordenou, de forma sincronizada, a atuação de 34.736 militares, policiais, bombeiros e demais agentes na área de operações (Brasil, 2024a).

Desse modo, a Operação "Taquari II" representa um exemplo concreto da necessidade de pensar a incorporação da resiliência às estratégias de segurança nacional, demonstrando que a capacidade de resposta do Estado

diante de eventos climáticos extremos depende não apenas da robustez de seus meios, mas da integração interinstitucional, da antecipação de riscos e da agilidade na coordenação.

Em um cenário de mudanças climáticas aceleradas e ameaças globais interconectadas, a experiência de 2024 reforça a necessidade de repensar a segurança nacional sob uma ótica multidimensional, em que defesa, clima e resiliência se entrelacem como pilares de uma nova arquitetura de segurança do século XXI.

A experiência da Operação Taquari II evidencia avanços relevantes no reconhecimento da centralidade das crises climáticas para a segurança nacional, mas também revela limitações analíticas e operacionais que merecem problematização. A ênfase na resiliência como eixo estratégico, embora normativamente atraente, carece de maior precisão conceitual e operacional. Trata-se de um conceito frequentemente utilizado de forma abrangente, o que pode resultar em ambiguidades quanto às responsabilidades institucionais e dificultar sua tradução em políticas públicas concretas. A valorização da capacidade adaptativa do Estado é pertinente, mas permanece pouco claro quais capacidades específicas devem ser priorizadas, como mensurá-las e de que forma integrá-las a estruturas já existentes sem gerar sobreposição ou ineficiência.

No campo da governança interagências, a análise aponta corretamente para a centralidade da coordenação entre atores civis, militares e privados, mas tende a subestimar os entraves estruturais que condicionam essa integração. A simples formalização de protocolos unificados e instâncias permanentes de coordenação não garante, por si só, maior efetividade. Disputas burocráticas, assimetrias de poder e diferenças de cultura organizacional constituem obstáculos recorrentes, amplamente discutidos na literatura sobre governança. Assim, a eficácia da atuação interagências depende não apenas de arranjos institucionais formais, mas também de incentivos adequados, liderança política e mecanismos de *accountability* capazes de sustentar a cooperação ao longo do tempo.

A ampliação do preparo das Forças Armadas e das agências civis para o enfrentamento de crises climáticas também exige uma abordagem mais matizada. Embora o desenvolvimento de capacidades operacionais, treinamentos conjuntos e simulações seja essencial diante da crescente

complexidade dos desastres, a centralidade atribuída às Forças Armadas pode suscitar o risco de uma militarização progressiva da gestão de crises. Tal dinâmica pode gerar ganhos imediatos em termos de eficiência logística, mas levanta questionamentos sobre a sustentabilidade institucional, a adequada distribuição de recursos e o equilíbrio nas relações civil-militares. Nesse sentido, torna-se fundamental considerar o fortalecimento paralelo das estruturas civis de proteção e defesa, evitando dependência excessiva de capacidades militares.

Por fim, a incorporação das mudanças climáticas à agenda de segurança e defesa representa um avanço importante ao reconhecer o caráter sistêmico dos riscos contemporâneos. Ainda assim, a securitização do tema pode produzir efeitos ambivalentes, como a priorização de respostas emergenciais em detrimento de políticas estruturais de mitigação e adaptação. A integração de dados meteorológicos, modelagens de vulnerabilidade e análises de impacto ao planejamento estratégico é um passo necessário, mas pressupõe capacidades técnicas, interoperabilidade de sistemas e governança de dados que nem sempre estão consolidadas. Ademais, a articulação entre políticas de defesa, gestão de desastres e adaptação climática envolve desafios de coordenação federativa e alinhamento intersetorial que permanecem como entraves significativos.

Dessa forma, a análise evidencia que, embora haja um reconhecimento crescente da relevância das crises climáticas no campo da segurança nacional, persistem lacunas importantes na tradução desse entendimento em capacidades estatais efetivas. O enfrentamento desses desafios depende menos da formulação de diretrizes gerais e mais da capacidade de lidar com constrangimentos institucionais, políticos e organizacionais que moldam a ação estatal em contextos de crise.

Considerações Finais

A análise desenvolvida ao longo deste artigo evidencia que as mudanças climáticas vêm produzindo impactos estruturais sobre a segurança nacional, exigindo uma revisão substantiva dos paradigmas tradicionais que orientam o campo da defesa e da segurança. A partir do diálogo com a Escola de Copenhague, com o conceito de segurança humana e com a abordagem da resiliência, demonstrou-se que a segurança contemporânea deve ser

compreendida como um fenômeno multidimensional, no qual ameaças ambientais assumem centralidade crescente.

Nesse contexto, a Operação "Taquari II" constitui um estudo empírico relevante ao evidenciar, na prática, a interdependência entre clima, segurança e resiliência. A resposta estatal ao desastre no Rio Grande do Sul revelou capacidades importantes de mobilização rápida, coordenação interagências e emprego de meios militares em apoio à população civil. Ao mesmo tempo, expôs limitações institucionais, desafios de coordenação e lacunas na integração entre políticas de defesa, gestão de desastres e adaptação climática.

A análise crítica da operação permite sustentar que a incorporação da resiliência à segurança nacional não pode se limitar a uma diretriz normativa ou discursiva. Trata-se de um processo que exige definição conceitual mais precisa, desenvolvimento de capacidades específicas, criação de mecanismos de coordenação efetivos e fortalecimento institucional, especialmente no âmbito civil. Do mesmo modo, a governança interagências, frequentemente apontada como solução para crises complexas, depende de condições políticas, organizacionais e culturais que vão além da formalização de estruturas.

Adicionalmente, a crescente participação das Forças Armadas em operações de resposta a desastres climáticos, embora funcional no curto prazo, levanta questões relevantes sobre o equilíbrio civil-militar, a alocação de recursos e a sustentabilidade dessas práticas no longo prazo. Esse aspecto reforça a necessidade de fortalecimento das capacidades civis de proteção e defesa, evitando a dependência excessiva de instrumentos militares para a gestão de crises essencialmente multidimensionais.

Por fim, a incorporação das mudanças climáticas à agenda de segurança e defesa representa um avanço analítico e estratégico, mas também demanda cautela quanto aos efeitos da securitização. Se, por um lado, esse enquadramento permite mobilizar recursos e priorizar o tema na agenda estatal, por outro pode deslocar o foco de políticas estruturais de mitigação e adaptação para respostas emergenciais.

Dessa forma, conclui-se que a construção de uma agenda de segurança nacional capaz de responder aos desafios do século XXI depende da consolidação de uma abordagem integrada, que articule defesa, desenvolvimento e sustentabilidade. A experiência da Operação

"Taquari II" demonstra que esse processo já está em curso, mas ainda requer avanços significativos em termos de coordenação institucional, planejamento estratégico e desenvolvimento de capacidades estatais orientadas à gestão de riscos climáticos.

Referências

ANGUS, I. *Facing the Anthropocene*: fossil capitalism and the crisis of the earth system. New York: NYU Press, 2016. 278 p. Disponível em: http://www.jstor.org/stable/j.ctt1bgz9vp. Acesso em: 31 maio 2025.

ANDRADE LIMA, J. R.; FIGUEIREDO, T. A. Mudanças climáticas e Forças Armadas: ampliando capacidades e desenvolvendo resiliência por meio das operações interagências. *Coleção Meira Mattos: revista de ciências militares,* v. 19, n. 64, p. 131–153, 26 ago. 2025. Disponível em: https://ebrevistas.eb.mil.br/RMM/article/view/13147. Acesso em: 15 set. 2025.

BARROS, M. Operação sempre prontos: Exército Brasileiro em ação no resgate às vítimas das chuvas no Rio Grande do Sul. *Defesa em Foco,* 1 maio 2024. Disponível em: https://www.defesaemfoco.com.br/de/operacao-sempre-prontos-exercito-brasileiro-em-acao-no-resgate-as-vitimas-das-chuvas-no-rio-grande. Acesso em: 18 set. 2025.

BRASIL. Ministério da Defesa. Comando Operacional Conjunto Taquari II. *Relatório final – Taquari II (abr. a dez. 2024)*. Porto Alegre: Comando Operacional Conjunto Taquari II, 16 dez. 2024a.

BRASIL. Ministério da Defesa. *Política Nacional de Defesa. Estratégia Nacional de Defesa.* Brasília, DF: Ministério da Defesa, 2024b. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf. Acesso em: 15 jul. 2025.

BRASIL. Ministério da Defesa. *Portaria GM-MD nº 2.309, de 1º de maio de 2024*. Aprova a diretriz ministerial que regula o emprego das Forças Armadas em apoio logístico à defesa civil (...). Brasília, DF: Ministério da Defesa, 2024c. Disponível em: https://static.poder360.com.br/2024/05/PORTARIA-GM-MD-No-2.309-DE-1o-DE-MAIO-DE-2024-PORTARIA-GM-MD-No-

2.309-DE-1o-DE-MAIO-DE-2024-DOU-Imprensa-Nacional.pdf. Acesso em: 4 jul. 2025.

BUZAN, B.; WÆVER, O.; DE WILDE, J. *Security:* a new framework for analysis. Boulder: Lynne Rienner, 1998.

BUZAN, B.; HANSEN, L. *A evolução dos estudos de segurança*. São Paulo: Ed. Unesp, 2012. 576 p.

CEPIK, M. Segurança nacional e segurança humana: problemas conceituais e consequências políticas. *Security and Defense Studies Review,* v. 1, 2001.

DO AMOR, F. *O trabalho interagências em desastres ambientais.* In: SEMINÁRIO OPERAÇÃO TAQUARI: O TRABALHO INTERAGÊNCIAS EM DESASTRES AMBIENTAIS, Rio de Janeiro, 26 jul. 2024. 1 vídeo. Disponível em: https://www.youtube.com/watch?v=PNzGbxRhUfk. Acesso em: 30 jun. 2025.

ESCOBAR, G. C. J.; ROCHA, F. P. da; ARSEGO, D. A.; NASCIMENTO, M. G. do; COSTA, I. C. da. *Evento extremo no Rio Grande do Sul entre final de abril e início de maio de 2024*. São José dos Campos: Instituto Nacional de Pesquisas Espaciais, 3 jul. 2024. Disponível em: https://www.gov.br/inpe/pt-br/assuntos/ultimas-noticias/relatorio-do-inpe-explica-evento-meteorologico-que-causou-a-tragedia-no-rs/chuvas-rio-grande-do-sul.pdf. Acesso em: 23 jul. 2025.

FIGUEIREDO, T. A.; MENDES, C. S. M. Impactos da ausência de uma estratégia nacional de segurança para a governança dos setores de segurança e defesa no Brasil. *Revista de Segurança, Desenvolvimento e Defesa*, v. 1, n. 1, jul./dez. 2024. Disponível em: https://rsdd.esd.gov.br/index.php/rsdd/article/view/19. Acesso em: 7 out. 2025.

FJÄDER, C. The nation-state, national security and resilience in the age of globalisation. *Resilience,* v. 2, n. 2, p. 114–129, 2014. Disponível em: http://dx.doi.org/10.1080/21693293.2014.914771. Acesso em: 16 set. 2025.

GIDDENS, A. *A política da mudança climática.* Rio de Janeiro: Zahar, 2010. 314 p.

GÓES, G. S.; COUTO, M. S. H. A segurança humana multidimensional e o Estado democrático de direito da era pós-pandemia. *Revista da Escola Superior de Guerra,* v. 36, n. 78, p. 11–39, set./dez. 2021. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/view/1226. Acesso em: 23 maio 2025.

JATOBÁ, A.; CARVALHO, P. V. R. Resiliência em saúde pública: preceitos, conceitos, desafios e perspectivas. *Saúde em Debate*, v. 46, n. esp. 8, p. 130–140, dez. 2022. Disponível em: https://www.scielosp.org/pdf/sdeb/2022.v46nspe8/130-139/pt. Acesso em: 16 set. 2025.

KEOHANE, R. O.; NYE JR., J. S. Power and interdependence. *Survival,* v. 15, n. 4, p. 158–165, 1973.

KLEIN, N. *Maritime security and the law of the sea.* New York: Oxford University Press, 2011.

MEDEIROS FILHO, O. *Segurança, defesa e uso da força:* desafios conceituais e políticos. Análise Estratégica, v. 7, n. 1, dez. 2017/fev. 2018. Disponível em: https://www.ceeex.eb.mil.br. Acesso em: 24 maio 2025.

NELLES, D.; SERRER, C. *Mudança climática: os fatos como você nunca viu antes.* Rio de Janeiro: Sextante, 2020. 132 p.

PALAZZO, A. Climate change & national security: implications for the military. Fort Leavenworth: Army University Press, 2022. 114 p. Disponível em: https://www.armyupress.army.mil. Acesso em: 25 maio 2025.

PRICE, S. F.; PITTS, T. R.; VAN ROEKEL, L. *Climate change and international responses increasing challenges to US national security through 2040*. Los Alamos: Los Alamos National Laboratory, 2021. Disponível em: https://www.dni.gov. Acesso em: 27 maio 2025.

RIO GRANDE DO SUL. Decreto nº 57.596, de 1º de maio de 2024. Declara estado de calamidade pública no território do Estado do Rio Grande do Sul afetado por eventos climáticos de chuvas intensas. *Diário Oficial do Estado do Rio Grande do Sul,* Porto Alegre, 1 maio 2024.

SHEPHERD, T. G. Extreme weather event. *McGraw Hill Access Science*, jul. 2023. Disponível em: https://www.accessscience.com/content/article/a249370. Acesso em: 30 jun. 2025.

WMO – WORLD METEOROLOGICAL ORGANIZATION. *Extreme weather*. Geneva: WMO, 2024. Disponível em: https://wmo.int/topics/extreme-weather. Acesso em: 30 jun. 2025.

UNDP – UNITED NATIONS DEVELOPMENT PROGRAM. *Human development report*: an agenda for social summit. Oxford: Oxford University Press, 1994. 243 p. Disponível em: https://digitallibrary.un.org/record/240220. Acesso em: 19 jul. 2025.

ZUCCO, M. L. D*esastres ambientais, emprego das Forças Armadas e resiliência*: Operação Taquari II. In: CURSO DE EXTENSÃO EM DEFESA NACIONAL, 30., 2025, Salvador. TV ESD, 22 maio 2025. 1 vídeo (65 min). Disponível em: https://www.youtube.com/watch?v=W3RvKbBpXIQ. Acesso em: 3 jun. 2025.

Sobre as organizadoras

VIVIANE MACHADO CAMINHA
Doutora em História das Ciências, das Técnicas e Epistemologia (UFRJ)
Escola Superior de Defesa (ESD)
E-mail: viviane.caminha@esd.gov.br

ÉRIKA RIGOTTI FURTADO
Doutora em Ciências Aeroespaciais (UNIFA)
Escola Superior de Defesa (ESD)/Academia da Força Aérea (AFA)
E-mail: erika.furtado@esd.gov.br

Sobre os autores e as autoras

ALINE BARBOSA XAVIER MUNIZ
Mestra em Ensino de Ciências (UERR). Doutoranda no Programa de Pós-Graduação em Educação (UCB)
Escola Superior de Defesa (ESD)/Universidade Federa de Roraima (UFRR)
E-mail: alinebxmuniz79@gmail.com

ANDRÉ BARROS DE OLIVEIRA
Mestre pelo Programa de Pós-graduação em Segurança Desenvolvimento e Defesa (PPGSDD/ESD)
Especialista em Estudos de Defesa (ESD). Advocacia-Geral da União (AGU)
E-mail: andrebarros1001@gmail.com

BRUNO CEZAR PEREIRA SOARES
Bacharel em Ciência Política (UDF). Mestrando no Programa de Pós-graduação em Segurança, Desenvolvimento e Defesa (PPGSDD ESD). Bolsista CAPES (Pró-Defesa V). Brasília, DF, Brasil
E-mail: bruno.soares@aluno.esd.gov.br

CAMILA ARAÚJO MACHADO
Doutora em Contabilidade (USP)
Escola Superior de Defesa (ESD)
E-mail: camila.machado@esd.gov.br

CARLOS EDUARDO GOMES
Doutor em Economia (UEM)
Escola Superior de Defesa (ESD)
E-mail: carlos.gomes@esd.gov.br

CINTENE SANDES MONFREDO MENDES
Doutora em História Comparada (UFRJ)
Escola Superior de Defesa (ESD)
E-mail: cintiene.mendes@esd.gov.br

CLAYTON MENDES DA SILVA
Graduado em Ciência Política (UDF). Mestrando no Programa de Pós-graduação em Segurança, Desenvolvimento e Defesa (PPGSDD/ESD). Bolsista CAPES (Pró-Defesa V). Brasília, DF, Brasil
E-mail: clayton.ms2020@gmail.com

GABRIEL CARLOS DOS REIS COSTA DIAS
Mestre pelo Programa de Pós-graduação em Segurança Desenvolvimento e Defesa (PPGSDD/ESD)
Pós-graduado em Direito Penal e Processual Penal (Centro Universitário Leonardo da Vinci), em Políticas e Gestão em Segurança Pública (Faculdade de Ciências de Wenceslau Braz), e Gestão Integrada de Inteligência (Escola de Inteligência)
Senado Federal
E-mail: gabrielcdias@gmail.com

IVAN FERNANDES FARIA
Mestre pelo Programa de Pós-graduação em Segurança, Desenvolvimento e Defesa (PPGSDD/ ESD)
Especialista em Relações Internacionais (UFRGS).
E-mail: ivanffaria@gmail.com/ivan.faira@defesa.gov.br

JAIME DE MELO GAMA DA SILVA
Mestre em Engenharia Elétrica (UnB).
Exército Brasileiro (EB)
E-mail: jaimemelo671@gmail.com

JOSÉ IRISMAR CABRAL JUNIOR
Mestre pelo Programa de Pós-graduação em Segurança, Desenvolvimento e Defesa (PPGSDD/ESD).
Bolsista CAPES (Pró-Defesa V). Brasília, DF, Brasil
E-mail: iriscabral@uol.com.br

JOSÉ ROBERTO DE ANDRADE PINHO E LIMA
Doutor em Saúde Pública (UFBA)
Escola Superior de Defesa (ESD)
E-mail: jose.roberto@esd.gov.br

JOSÉ SÉRGIO MARQUES DOS SANTOS
Mestre em economia (UNB)
Ministério da Gestão e da Inovação em Serviços Públicos (MGI)
E-mail: sergio.marques26@gmail.com

JULIO EDUARDO DA SILVA MENEZES
Doutor em Engenharia da Produção (COPPE/UFRJ)
Escola Superior de Defesa (ESD)
E-mail: julioesm@gmail.com

LEONARDO ULIAN DALL EVEDOVE
Doutor em Ciência Política (UFPE)
Escola Superior de Defesa (ESD)
E-mail: leonardo.evedove@esd.gov.br

LORENA HERMENEGILDO DE OLIVEIRA
Mestre em Instituições Sociais, Direito e Democracia (FUMEC)
Escola de Prerrogativas da OAB/MG
Email: lorena.advocacia.e@gmail.com

LUIZ GUSTAVO CELUPPI
Especialista em Ciências Policiais (ESMAFE/PR)
Secretaria Nacional de Políticas Penais (SENAPPEN)
E-mail: luiz.celuppi@mj.gov.br

MARCELO BATISTA SOARES BARROSO
Mestre pelo Programa de Pós-graduação em Segurança, Desenvolvimento e Defesa (PPGSDD/ ESD)
Exército Brasileiro (EB)
E-mail: mbatista84@gmail.com

MARCELO MARCEL FÉLIX
Mestre em Estudos Estratégicos pelo Colégio Interamericano de Defesa.
Marinha do Brasil (MB)
E-mail: marcelomarcelfelix@gmail.com

MATHEUS HENRIQUE DE SOUZA
Especialista em Direito Público (EBRADI)
Exército Brasileiro (EB)
E-mail: sgtmhenrique@gmail.com

MICHELE EDUARDA BRASIL DE SÁ
Doutora em Letras (UFRJ).
Mestra pelo Programa de Pós-graduação em Segurança, Desenvolvimento e Defesa (PPGSDD/ESD).
Bolsista CAPES (PRÓ-DEFESA V) Brasília, DF, Brasil
Escola Superior de Defesa (ESD)/Universidade Federal do Rio de Janeiro (UFRJ)
E-mail: michele.sa@esd.gov.br

NÁDIA XAVIER MOREIRA
Doutora em Antropologia Social (UnB); Doutora em Serviço Social (UFRJ)
Pós-doutorado em Antropologia Social (Museu Nacional/UFRJ)
Marinha do Brasil (MB)
E-mail: nadiaxmoreira@yahoo.com.br

PATRÍCIA PONTES BEZERRA
Doutora em Estudos Marítimos (EGN)
Marinha do Brasil (MB)/Escola Superior de Defesa (ESD)
E-mail: patypontes37@gmail.com

PETERSON FERREIRA SILVA
Doutor em Relações Internacionais (USP)
Escola Superior de Defesa (ESD)/Universidade da Força Aérea (UNIFA)
E-mail: peterson.silva@esd.gov.br

RÔMULO FERREIRA DOS SANTOS
Doutor em Computação (UNINI)
Exército Brasileiro (EB)
E-mail: romulo.ferreira@eb.mil.br

THIAGO ABREU DE FIGUEIREDO
Graduado em Ciências Navais (Escola Naval).
Mestre pelo Programa de Pós-graduação em Segurança, Desenvolvimento e Defesa (PPGSDD/ESD)
Bolsista CAPES (Pró-Defesa V). Brasília, DF, Brasil.
Escola Superior de Defesa (ESD)
E-mail: tafigueiredo@yahoo.com.br

WELLINGTON DANTAS DE AMORIM
PhD em Ciencia Política (UFF)
Escola Superior de Defesa (ESD)
E-mail: wellington.amorim@esd.gov.br

ISBN: 978-65-989042-1-0