ARTIGO DOI 10.52781/cmm.a194

O papel do big data e da inteligência artificial na segurança e defesa nacional

Harnessing big data and AI for national security and defense

Resumo: Este artigo analisa a integração estratégica de *big data* e inteligência artificial (IA) como vetores de modernização da defesa nacional. O objetivo é identificar como a transição para uma defesa orientada por dados (*data-driven defense*) pode reduzir assimetrias operacionais e elevar a soberania tecnológica brasileira. Utilizou-se como metodologia uma revisão de escopo (*scoping review*) e análise documental, confrontando o estado da arte internacional – com foco em doutrinas como *mosaic warfare* e o ciclo OODA acelerado – com a realidade institucional brasileira (Sisfron, CDCiber e Enia). Os resultados demonstram que, embora o Brasil possua iniciativas robustas de sensoriamento, persiste um hiato funcional caracterizado por silos informacionais entre as forças e a dependência de algoritmos estrangeiros ("caixas-pretas"). Conclui-se que a superação dessas barreiras exige a transição para arquiteturas de comando e controle unificadas (JADC2) e o fomento a tecnologias autóctones. O estudo propõe um *roadmap* estratégico fundamentado em IA Explicável (XAI) e *edge computing*, visando garantir a superioridade de decisão e a autonomia decisória do Estado em cenários de guerra centrada em dados (*data-centric warfare*).

Palavras-chave: *Big data*; Inteligência artificial; Defesa nacional; Segurança cibernética; Inteligência preditiva.

Abstract: This article analyzes the strategic integration of Big Data and Artificial Intelligence (AI) as drivers for the modernization of National Defense. The objective is to identify how the transition to a Data-Driven Defense model can reduce operational asymmetries and enhance Brazilian technological sovereignty. The methodology employed was a Scoping Review and documentary analysis, contrasting the international state-of-the-art focusing on doctrines such as Mosaic Warfare and the accelerated OODA loop with the Brazilian institutional reality (SISFRON, CDCiber, and ENIA). The results demonstrate that, although Brazil possesses robust sensing initiatives, a functional gap persists, characterized by information silos between the Armed Forces and a dependence on foreign "black-box" algorithms. It is concluded that overcoming these limitations requires a transition toward Joint All-Domain Command and Control (JADC2) architectures and the promotion of indigenous technologies. The study proposes a strategic roadmap based on Explainable AI (XAI) and Edge Computing, aiming to ensure decision superiority and the State's decision-making autonomy in Data-Centric Warfare scenarios.

Keywords: Big data; Artificial intelligence; National defense; Cybersecurity; Predictive intelligence.

Larissa Silva de Azevedo
Universidade de São Paulo (USP). Faculdade de Filosofia Ciências e Letras de Ribeirão Preto
Ribeirão Preto, SP, Brasil
lazevsil@gmail.com

Alex Soares Castro
Universidade de São Paulo (USP). Faculdade de Filosofia Ciências e Letras de Ribeirão Preto
Ribeirão Preto, SP, Brasil
alex.soares.castro@usp.br

João Paulo Mardegan Issa
Universidade de São Paulo (USP). Faculdade de Odontologia de Ribeirão Preto
Ribeirão Preto, SP, Brasil
jpmissa@forp.usp.br

Marcelo Firmino de Oliveira
Universidade de São Paulo (USP). Faculdade de Filosofia Ciências e Letras de Ribeirão Preto
Ribeirão Preto, SP, Brasil
marcelex@usp.br

Recebido: 01 ago. 2025
Aprovado: 09 abr. 2026

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1. INTRODUÇÃO

A digitalização tem exercido um impacto significativo nas estratégias de defesa e segurança nacional, modificando paradigmas convencionais de vigilância, salvaguarda e processos decisórios. O aumento exponencial de dados oriundos de sensores, satélites, dispositivos móveis e inteligência cibernética resulta em um ecossistema informacional de alta complexidade, frequentemente definido pelo conceito de *big data*[1] (Kitchin, 2021). Nesse cenário, a Inteligência Artificial (IA) – particularmente por meio de algoritmos de aprendizado de máquina e análise preditiva – atua como elemento central na conversão de dados massivos em inteligência estratégica, permitindo a identificação de padrões e a antecipação de ameaças com elevado grau de precisão (Scharre, 2023).

Nos conflitos contemporâneos, caracterizados por guerras híbridas e ameaças transnacionais, a celeridade no processamento da informação influencia diretamente a capacidade de resposta e a resiliência estatal (Scharre, 2023). Experiências globais evidenciam que nações como Estados Unidos, Israel e integrantes da Organização do Tratado do Atlântico Norte (Otan) já consolidaram arquiteturas integradas de dados capazes de sustentar sistemas de vigilância e suporte automatizado à decisão em ambientes de alta complexidade (Nato, 2021).

No contexto brasileiro, contudo, a incorporação dessas tecnologias ocorre de forma fragmentada, refletindo limitações estruturais que transcendem a mera disponibilidade tecnológica (Andrade; Lima, 2021). Embora a extensão territorial e a complexidade das fronteiras imponham demandas operacionais severas, os desafios nacionais decorrem, sobretudo, da ausência de uma estratégia integrada que articule infraestrutura, governança de dados e capacidades analíticas (Araujo; Mendes, 2025). Persistem, ainda, entraves relacionados à dependência tecnológica externa, à baixa maturidade em soberania digital e à escassez de recursos humanos especializados, fatores que limitam a internalização de IA em sistemas críticos (Bonanno, 2025).

Nesse sentido, o problema central não reside na adoção de ferramentas isoladas, mas na dificuldade de estruturar um ecossistema nacional robusto aplicado à defesa (Toni *et al*., 2025). Tal limitação compromete a autonomia estratégica do país e sua capacidade de resposta em cenários de crise. Diante desse panorama, este estudo é orientado pela seguinte questão de pesquisa: De que maneira a integração de *big data* e IA pode impactar as capacidades estratégicas da defesa nacional, considerando as dimensões de previsão de ameaças, segurança cibernética e suporte à tomada de decisões?

O objetivo principal deste trabalho é analisar o papel do *big data* e da IA no fortalecimento da defesa nacional, com ênfase em aplicações estratégicas e desafios de implementação no Brasil. Para além de uma análise descritiva, o estudo parte da hipótese de que o entrave à consolidação dessas capacidades no país não é estritamente tecnológico, mas estrutural. Argumenta-se que a ausência de uma arquitetura integrada, aliada a fragilidades na governança interinstitucional e à dependência externa, compromete a conversão de dados em inteligência operacional. Assim, a limitação brasileira deve ser compreendida como um problema de coordenação sistêmica e maturidade institucional.

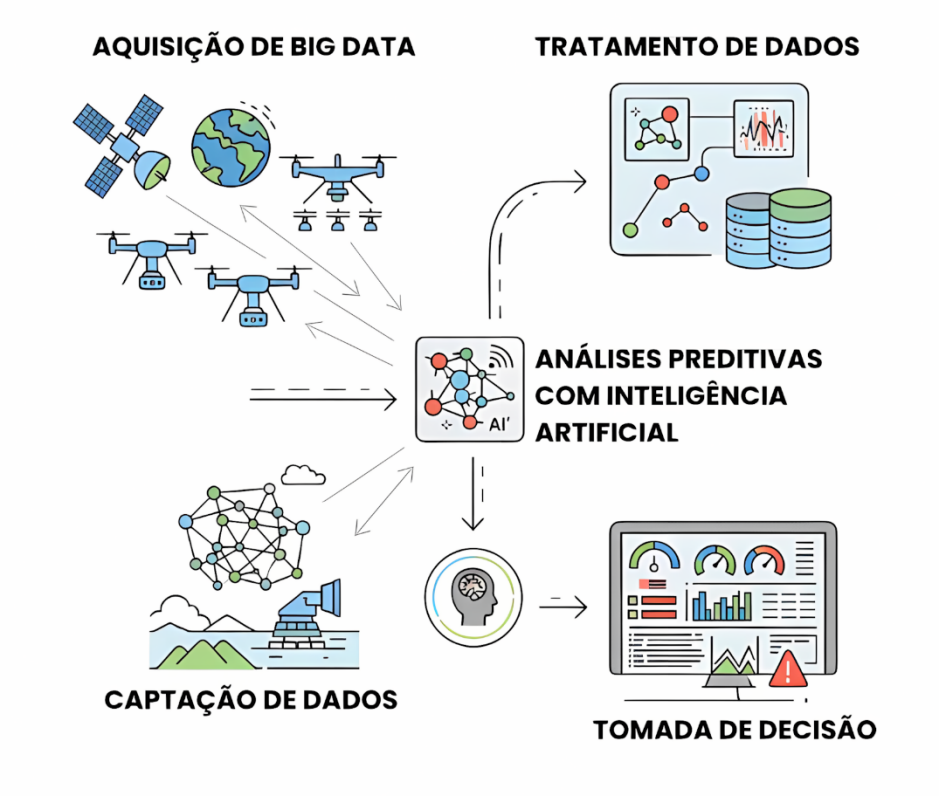
1 ***Big data***: ecossistema de infraestrutura computacional e algoritmos avançados (como processamento distribuído e *machine learning*) projetados para capturar, armazenar e analisar dados de alta escala que são grandes demais para serem gerenciados por sistemas de gestão de bancos de dados relacionais tradicionais.

Do ponto de vista metodológico, adota-se uma abordagem qualitativa e exploratória, baseada em revisão bibliográfica e documental estruturada, com foco no cenário nacional em comparação aos *benchmarks*[2] internacionais (Sousa, 2024). A análise busca contribuir para o debate sobre a modernização da defesa ao propor a integração entre infraestrutura de dados e sistemas inteligentes como eixo estruturante da capacidade estratégica contemporânea.

A principal contribuição deste estudo reside na proposição de um enquadramento analítico que interpreta a adoção de *big data* e IA na defesa nacional brasileira como um problema de coordenação sistêmica e maturidade institucional, e não meramente como uma limitação tecnológica.

A Figura 1 ilustra esse fluxo sistêmico, evidenciando a integração de fontes multimodais – como satélites, *Remotely Piloted Aircraft* (RPAs), sensores terrestres e redes digitais – e sua posterior assimilação por algoritmos preditivos. Esse encadeamento viabiliza não apenas a detecção precoce de hostilidades, mas também a adaptação dinâmica de respostas operacionais em cenários de fricção e incerteza.

Figura 1 – Fluxo de *big data* e inteligência artificial na defesa nacional



Fonte: Elaborada pelo autor.

2 ***Benchmarks***: refere-se a um padrão de referência ou parâmetro de excelência utilizado para fins de comparação sistemática. No contexto científico, serve como base normativa para avaliar o desempenho, a eficácia ou a qualidade de processos, sistemas ou resultados em relação às melhores práticas estabelecidas na literatura ou no mercado.

Conforme demonstrado no fluxo de *big data* e IA, a análise preditiva no domínio da defesa depende da articulação sinérgica entre infraestrutura de dados, capacidade computacional e modelos analíticos avançados. Tal integração permite o suporte a uma consciência situacional em tempo real, redefinindo a lógica decisória ao transitar de um modelo reativo para uma postura de antecipação contínua. Em última análise, essa arquitetura contribui diretamente para o fortalecimento da soberania nacional e a resiliência de infraestruturas críticas frente a ameaças multidimensionais.

2. METODOLOGIA

Este estudo adota uma abordagem qualitativa de natureza exploratória, estruturada por meio de uma revisão de escopo[3] (*scoping review*) e análise documental (Peterson *et al*., 2017). O desenho metodológico foi planejado para garantir a reprodutibilidade da coleta e o rigor na análise comparativa entre o cenário internacional e a realidade brasileira. O processo dividiu-se em três etapas, indicadas nos subtópicos a seguir.

2.1 Estratégia de busca de seleção

A prospecção de dados baseou-se em uma varredura sistemática em bases de dados científicas (como Google Scholar, Scopus e IEEE Xplore) e repositórios institucionais de defesa – incluindo documentos da Otan, da Defense Advanced Research Projects Agency (DARPA) e do Ministério da Defesa do Brasil. Foram incluídos documentos publicados entre 2015 e 2025, selecionados com base em sua relevância temática, aderência ao escopo do estudo e recorrência em bases científicas e institucionais. Foram excluídos documentos duplicados, não revisados por pares ou que não apresentassem relação direta com o objeto de análise. Para a recuperação das fontes, foram utilizados descritores combinados em português e inglês, tais como "*big data*", "*inteligência artificial*", "*defesa nacional*" e "*cybersecurity*". O recorte temporal priorizou publicações da última década, com o objetivo de capturar a aceleração das tecnologias orientadas por dados e suas implicações operacionais e soberanas.

2.2 Categorização analítica

Para evitar subjetividade na interpretação, o conteúdo selecionado foi filtrado por meio de três eixos temáticos fundamentais:

- **Inteligência preditiva e consciência situacional**: focado em aplicações de monitoramento e redução da incerteza operacional.
- **Resiliência e soberania cibernética**: voltado à proteção de infraestruturas críticas e autonomia tecnológica.

3 **Revisão de escopo**: método de síntese de conhecimento que visa mapear os principais conceitos, fontes e evidências disponíveis em uma determinada área de pesquisa, especialmente quando o tema é complexo ou ainda não foi revisado de forma abrangente.

- **Governança e integração sistêmica**: centrado nos desafios de interoperabilidade e políticas públicas de longo prazo.

2.3 Procedimento de análise comparativa

A pesquisa incorporou uma abordagem analítico-comparativa, utilizando como *benchmarks* as experiências de países com elevado grau de maturidade tecnológica (Estados Unidos, Israel e membros da Otan). Esse confronto de modelos permitiu identificar não apenas as ferramentas disponíveis, mas os hiatos estruturais, institucionais e de governança que condicionam a implementação dessas capacidades no contexto da defesa nacional brasileira.

3. DESENVOLVIMENTO

No domínio da defesa nacional, o conceito de *big data* transcende o mero armazenamento volumoso, referindo-se à capacidade estratégica de estruturar e explorar fluxos heterogêneos de dados em ambientes de alta volatilidade (Nie; Sun, 2016). A convergência de informações provenientes de múltiplos domínios – incluindo sensoriamento remoto, sistemas autônomos e inteligência cibernética – permite a construção de uma base informacional interconectada (Kitchin, 2021). Sob a perspectiva da defesa orientada por dados (*data-driven defense*), a superioridade estratégica é redefinida pela habilidade de converter esse volume massivo em inteligência acionável em tempo quase real, reduzindo a incerteza em cenários operacionais dinâmicos (Wu *et al.*, 2022).

A literatura contemporânea enfatiza que a transição para esse modelo exige mais do que a incorporação de tecnologias digitais; demanda a reconfiguração de estruturas organizacionais e mecanismos de governança (Nato, 2021). Nesse contexto, a eficácia militar deixa de depender exclusivamente de meios convencionais e passa a residir na construção de ecossistemas institucionais capazes de sustentar a interoperabilidade e a coordenação interagências (Morgan *et al.*, 2020). A IA atua como o motor dessa transformação, utilizando *machine learning*[4] e *deep learning*[5] para automatizar a triagem e a análise preditiva (Lecun; Bengio; Hinton, 2015).

A sofisticação dos modelos de *deep learning* introduziu uma mudança de paradigma na análise de Inteligência de Imagens (*Imagery Intelligence* [IMINT]) (Zhang; Zhou; Luo, 2022). Enquanto os algoritmos estatísticos tradicionais dependiam de parâmetros predefinidos manualmente para identificar objetos, as Redes Neurais Convolucionais[6] (CNN) operam por meio de múltiplas camadas de processamento que mimetizam a visão humana (Alzubaidi *et al.*, 2021). Essa

4 ***Machine learning*** **(aprendizado de máquina)**: subcampo da IA que se ocupa do desenvolvimento de algoritmos e modelos estatísticos capazes de identificar padrões e realizar inferências a partir de dados sem a necessidade de instruções de programação explícitas para cada tarefa. O desempenho do sistema é aprimorado de forma iterativa à medida que ele é exposto a novos conjuntos de dados.

5 ***Deep learning*** **(aprendizado profundo)**: subconjunto do *machine learning* baseado em redes neurais artificiais com múltiplas camadas de processamento (camadas ocultas). Essa arquitetura permite que o modelo aprenda representações de dados com múltiplos níveis de abstração, em que cada camada transforma a entrada em uma representação ligeiramente mais abstrata e complexa.

6 **Redes neurais convolucionais**: classe de algoritmos de *deep learning* projetada especificamente para o processamento de dados com topologia em grelha, como imagens. Sua arquitetura utiliza uma operação matemática denominada **convolução** em vez da multiplicação de matrizes convencional em pelo menos uma de suas camadas, permitindo a extração automática de características espaciais (bordas, texturas e formas) por meio de filtros aprendíveis.

arquitetura permite que o sistema aprenda e reconheça autonomamente padrões complexos em vídeos de drones e imagens de satélite, operando com latência mínima – essencial para o acompanhamento de alvos em movimento em tempo real (Kiranyaz *et al*., 2019).

Contudo, essa capacidade de processamento gera o que a literatura denomina como efeito "caixa-preta"[7], em que o caminho lógico percorrido pela máquina para chegar a uma conclusão é opaco ao operador humano. Surge, então, o desafio crítico da *Explainable AI* (XAI), ou IA Explicável, no teatro de operações, cujo objetivo é traduzir modelos matemáticos complexos em representações inteligíveis (Gunning; Aha, 2019). No campo de batalha, a confiança do comando depende da capacidade do algoritmo de fornecer uma justificativa interpretável para suas classificações (Scharre, 2023). Em suma, para que um comandante autorize o emprego de força, ele precisa compreender os critérios que levaram a IA a classificar um objeto como uma "ameaça" e não como um alvo civil, mitigando riscos de erros colaterais catastróficos em Sistemas de Armas Letais Autônomas (*Lethal Autonomous Weapons Systems*, LAWS) (Grand-Clément, 2023; Wille, 2016).

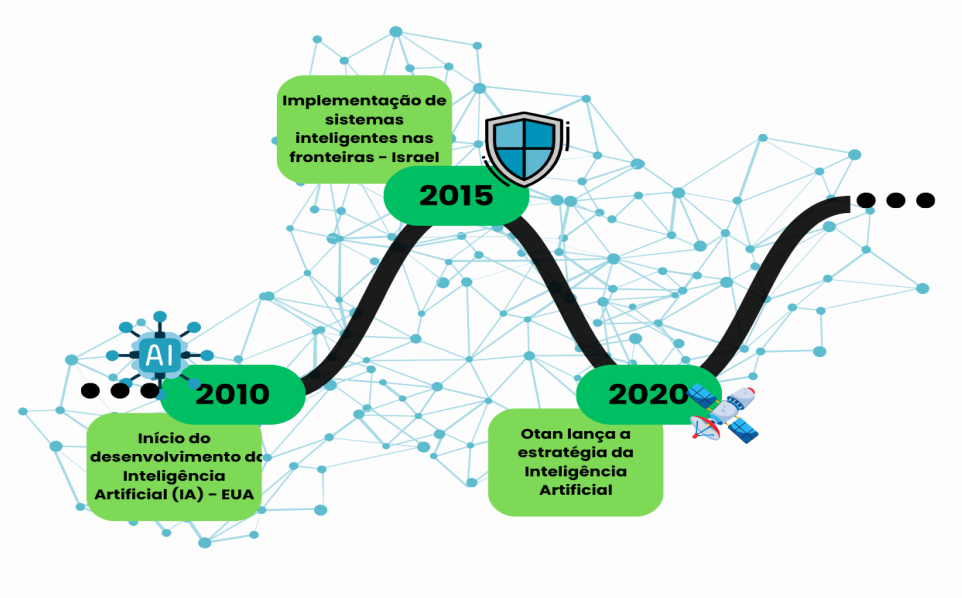
No cenário internacional, o programa Mosaic Warfare da DARPA exemplifica o emprego de sistemas distribuídos para amplificar a agilidade decisória (Rokvić, 2025). O conceito de Mosaic Warfare, embora citado como uma integração de sensores, representa uma evolução na doutrina de Comando e Controle (C2) (Magnuson, 2018). Ao contrário dos sistemas monolíticos e caros, o "mosaico" utiliza IA para coordenar centenas de pequenas unidades baratas e descartáveis (enxames de drones, sensores de baixo custo), criando um sistema de defesa resiliente e imprevisível (Scharre, 2023). Essa descentralização, suportada por uma arquitetura de *Big Data* distribuída, torna o esforço de guerra adversário ineficaz, pois não há um centro de gravidade único para ser atacado (Mcgarry; Saturno, 2020).

Paralelamente, a Otan tem liderado o movimento de institucionalização tecnológica com sua estratégia de IA (2021), focada em padronização ética e interoperabilidade multidomínio (Christie; Ertan, 2021). Israel, por sua vez, destaca-se pela integração de algoritmos proprietários em sistemas de vigilância, resultando em uma redução drástica no tempo de resposta em operações de contraterrorismo (Scharre, 2023). Para além da ciberdefesa, essas tecnologias redefinem a logística e o suporte à decisão tática, permitindo a otimização do emprego de recursos em ambientes de alta fricção (Ofili; Ezeadi; Jegede, 2024).

A Figura 2 ilustra os marcos dessa evolução global, evidenciando a transição de sistemas puramente reativos para arquiteturas de inteligência proativa (Kitchin, 2014). Observa-se que o divisor de águas tecnológico não foi apenas o aumento do poder de processamento, mas a capacidade de integrar fluxos de dados intensos em ambientes de combate contestados (Lowrey, 2021). Essa trajetória demonstra que a superioridade militar contemporânea não reside mais apenas na força cinética, mas na velocidade do ciclo de decisão (Nato, 2021).

7 **Caixa-preta**: refere-se a sistemas de *machine learning* ou *deep learning*, como as redes neurais profundas, que produzem resultados altamente precisos, mas cujos processos internos de decisão e ponderação de variáveis são complexos demais para serem interpretados por seres humanos.

Figura 2 – Marcos internacionais de adoção de *big data* e inteligência artificial na defesa



Fonte: Elaborada pelo autor.

Como demonstrado pelos marcos evolutivos, as nações que lideram o setor – como Estados Unidos, Israel e membros da Otan – deixaram de tratar o *big data* como um repositório estático para transformá-lo em um ativo dinâmico de consciência situacional (Nato, 2021). Essa mudança exigiu a consolidação de infraestruturas computacionais resilientes e, fundamentalmente, a formação de um capital humano capaz de operar na interseção entre a ciência de dados e a tática militar (Scharre, 2023).

A Tabela 1 sintetiza as principais estratégias dessas potências, oferecendo uma visão comparativa das abordagens que consolidaram os dados, como o novo centro de gravidade da defesa global.

Tabela 1 – Programas e estratégias internacionais de defesa com uso de *big data* e inteligência artificial

País/ organização (Ano)	Projeto/programa	Foco principal	Resultados operacionais	Ref.
Estados Unidos (DARPA) (2017)	Mosaic Warfare	Integração IA + sensores	Redução do tempo de decisão em campo	(Gunning; Aha, 2019)
Israel (2019)	Sistemas de fronteira inteligentes	Reconhecimento de padrões	Detecção precoce de ameaças terroristas	(Strat, 2023)
Otan (2021)	Estratégia de IA	Cibersegurança e operações multidomínio	Padrões éticos e interoperabilidade	(Nato, 2021)

Fonte: Elaborada pelo autor.

Atualmente, o estado da arte converge para a *data-centric warfare*[8], em que a superioridade militar não é mais medida apenas pelo poder de fogo cinético, mas pela superioridade de decisão (Amirolshah, 2024). O ciclo OODA (*Observe, Orient, Decide, Act*) é acelerado artificialmente, permitindo que o defensor neutralize ameaças antes mesmo que elas se materializem fisicamente (Priambodo *et al*., 2022). O desafio contemporâneo reside na proteção da integridade desses dados; ataques de envenenamento de dados (*data poisoning*), voltados a corromper o aprendizado da IA inimiga, emergem como a nova fronteira da contrainteligência digital (Schmidt, 2023).

Em contraste com a maturidade observada nos *benchmarks* globais, o Brasil ainda enfrenta desafios na articulação de suas capacidades e na continuidade dos investimentos (Medeiros; Gualberto, 2025). A análise comparativa sugere que o avanço nacional depende da transição de adoções pontuais para uma estratégia nacional integrada, compatível com as especificidades geopolíticas do país.

3.2 O cenário brasileiro

No Brasil, a incorporação de tecnologias orientadas por dados na defesa nacional reflete um esforço de modernização estrutural, embora ainda marcado por uma implementação fragmentada (Soares, 2015). O principal expoente dessa transição é o Sistema Integrado de Monitoramento de Fronteiras (Sisfron) (Andrade; Lima, 2018). Concebido como uma arquitetura de sensores e comunicações estratégicas, o Sisfron representa o maior desafio nacional de *big data*: a necessidade de integrar fluxos heterogêneos de dados terrestres e orbitais para gerar consciência situacional em tempo real ao longo de 16 mil quilômetros de fronteira (Andrade, 2025).

No campo da ciberdefesa, a atuação do Centro de Defesa Cibernética (CDCiber) e a formulação da Estratégia Brasileira de Inteligência Artificial (Ebia) sinalizam o reconhecimento da IA como tecnologia de dupla finalidade (*dual-use*) (Barboza; Ferneda; Cristóvam, 2023). O Exército Brasileiro, por meio de diretrizes estratégicas, busca aplicar o aprendizado de máquina na proteção de infraestruturas críticas e na antecipação de ameaças híbridas (Bonanno, 2025). Entretanto, a maturidade desses sistemas no Brasil ainda é considerada intermediária quando comparada aos *benchmarks* internacionais (Estados Unidos e Israel), devido a três hiatos fundamentais (Scharre, 2023):

- **Fragmentação de silos**: a ausência de uma interoperabilidade plena entre as bases de dados da Marinha, do Exército e da Aeronáutica dificulta a criação de um ecossistema de inteligência conjunta (Brasil, 2025b).
- **Dependência tecnológica**: a predominância de componentes e algoritmos estrangeiros – muitas vezes operando como "caixas-pretas" (*black boxes*) – impõe riscos à soberania digital e limita a auditoria nacional sobre os processos decisórios (Polido, 2024).
- **Continuidade orçamentária**: a natureza plurianual dos projetos de IA e *big data* colide com contingenciamentos financeiros, gerando hiatos de atualização que favorecem a obsolescência tecnológica (Azevedo; Borba; Araújo, 2021).

8 ***Data-centric warfare***: paradigma militar contemporâneo que estabelece o dado como elemento central da superioridade operacional.

Portanto, o cenário brasileiro caracteriza-se por uma robusta fundamentação doutrinária, expressa na Estratégia Nacional de Defesa, mas que ainda carece de uma execução sistêmica (Dalbosco; Cortinhas, 2024). O fortalecimento das capacidades nacionais depende da transição para o desenvolvimento de tecnologias autóctones[9], capazes de garantir que a autonomia decisória do Estado brasileiro não seja comprometida pela dependência de infraestruturas externas em momentos de crise (Brasil, 2024; Gomes, 2024).

A partir do confronto entre os *benchmarks* internacionais e a realidade brasileira descrita anteriormente, observa-se um hiato funcional que transcende a tecnologia. Enquanto potências globais operam sob o paradigma da superioridade de decisão, o Brasil ainda consolida sua consciência situacional (Nato, 2021). Para transpor essa barreira, a análise documental sugere que o país deve evoluir de sistemas de prateleira para arquiteturas de dados integradas (Scharre, 2023). A Tabela 3 sintetiza os principais óbices identificados e as respectivas recomendações estratégicas para a defesa nacional.

4. RESULTADOS E DISCUSSÕES

4.1 Aplicações estratégicas na defesa nacional brasileira

A incorporação de tecnologias orientadas por dados e IA na defesa nacional representa uma mudança paradigmática na forma como ameaças multidimensionais são monitoradas e neutralizadas (Cummings, 2017; Stiles; Netessine, 2025). No contexto brasileiro, marcado por uma vasta extensão territorial e complexidade geoestratégica, tais ferramentas reduzem assimetrias operacionais em cenários de difícil monitoramento, como a Amazônia Legal e a "Amazônia Azul" (Figueiredo, 2025).

Embora iniciativas como o Sisfron (Oliveira; Farias, 2023), o CDCiber (Brasil, 2023) e a Enia (Brasil, 2025a) demonstrem o vigor institucional, os dados revelam que estas ainda operam em estágios intermediários de integração. A análise indica a persistência de lacunas em interoperabilidade e escalabilidade, essenciais para transitar de uma vigilância passiva para uma defesa proativa.

4.1.1 Vigilância e sensoriamento de fronteiras

No âmbito do Sisfron, a análise aponta que o sistema evoluiu na capacidade de "enxergar" a fronteira, mas ainda tateia na capacidade de "antecipar" eventos (Oliveira; Farias, 2023). A expansão sugerida por este estudo envolve a implementação de modelos de visão computacional[10] e *deep*

9 **Tecnologias autóctones**: referem-se ao conjunto de conhecimentos, processos e ferramentas desenvolvidos integralmente dentro das fronteiras nacionais, utilizando capacidades científicas e industriais próprias. No setor de defesa, a autonomia tecnológica é considerada um ativo estratégico, pois reduz a dependência de fornecedores estrangeiros e mitiga vulnerabilidades relacionadas a embargos, tecnológicas ou restrições de uso impostas por terceiros.

10 **Visão computacional**: campo interdisciplinar da inteligência artificial que desenvolve técnicas algorítmicas para permitir que computadores e sistemas extraiam informações significativas, identifiquem padrões e compreendam o conteúdo de imagens digitais, vídeos ou outras entradas visuais. Diferentemente do simples processamento de imagens, a visão computacional busca a interpretação semântica da cena para a tomada de decisões automatizada.

learning diretamente na "ponta" (*edge* AI[11]) (Zhou *et al.*, 2019). Ao dotar drones e sensores terrestres com capacidade de processamento autônomo, reduz-se a sobrecarga dos centros de C2, permitindo que apenas anomalias críticas sejam reportadas (Silva, 2024). Isso é vital para o combate a crimes transnacionais, em que a janela de oportunidade para interceptação é extremamente reduzida.

4.1.2 Ciberdefesa e a resiliência de infraestruturas

A discussão sobre ciberdefesa revela que o CDCiber atua em um cenário de guerra assimétrica constante (Brasil, 2023). A expansão dessa capacidade exige o uso de IA para a detecção de Ameaças Persistentes Avançadas (APT), que mimetizam comportamentos legítimos de usuários (Mohamed, 2024). A análise documental sugere que a proteção de redes governamentais brasileiras depende da criação de um "escudo inteligente" capaz de realizar a correlação de eventos em milissegundos – uma tarefa impossível para operadores humanos sem o auxílio de *big data* analítico (Wang; Jones, 2017).

4.2 O dilema da soberania digital e das tecnologias autóctones

Um ponto crítico que emerge da discussão é a vulnerabilidade de dependência. Ao utilizar soluções de prateleira (*off-the-shelf*) de potências estrangeiras, o Brasil incorre no risco de "caixas-pretas" algorítmicas (Gonzalez; Ferreira, 2020). Em um cenário de conflito, o acesso a esses sistemas ou a atualizações de segurança pode ser revogado, paralisando as capacidades de defesa nacional. Portanto, a soberania digital não é apenas um conceito retórico, mas uma necessidade operacional.

O fomento à Base Industrial de Defesa (BID) para a criação de algoritmos nacionais configura-se como uma via estratégica para garantir a *accountability*[12] e a XAI das decisões militares (Gunning; Aha, 2019). Sem o domínio do código-fonte, o Estado brasileiro não possui total controle sobre os critérios que levam uma IA a classificar um alvo ou uma ameaça, o que levanta sérias implicações éticas e jurídicas sob a égide do direito internacional dos conflitos armados (Medeiros; Alvarez, 2026).

4.2.1 A ética do "human-in-the-loop"

A expansão da discussão ética é mandatória. Este estudo reforça que a IA na defesa brasileira deve seguir o princípio do humano no ciclo de decisão (Batista *et al.*, 2025). Embora a máquina possa processar bilhões de dados para identificar um padrão de ataque, a decisão final de engajamento deve ser humana. Isso mitiga o risco de erros algorítmicos derivados de *datasets*[13]

11 ***Edge* AI (IA de borda)**: paradigma computacional que consiste na implementação de algoritmos de IA diretamente em dispositivos locais (sensores, câmeras, drones), situados na "borda" da rede.

12 ***Accountability***: refere-se à capacidade de atribuir responsabilidade pelos resultados produzidos por sistemas automatizados. Em cenários de *machine learning* caixa-preta, a *accountability* exige que os desenvolvedores e operadores possam auditar e explicar o comportamento do sistema, garantindo que as decisões da IA estejam em conformidade com normas éticas e legais.

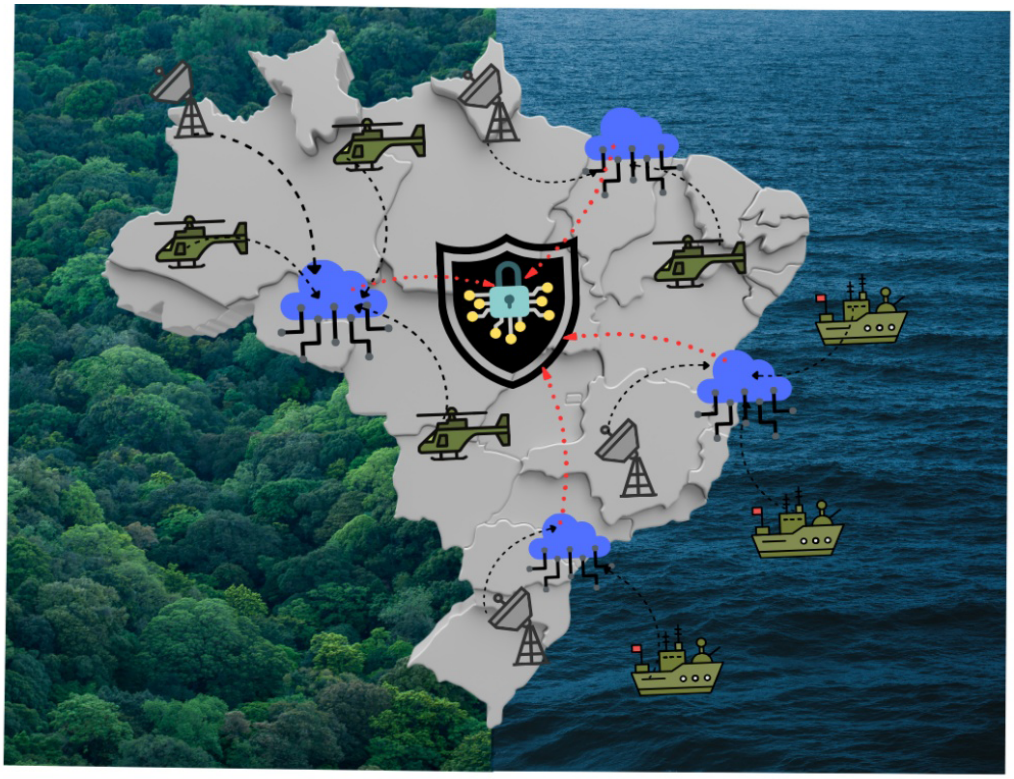
13 ***Datasets* (conjuntos de dados)**: coleções estruturadas de informações relacionadas que servem como base para o treinamento, validação e teste de algoritmos de *machine learning*.

enviesados e garante a responsabilidade jurídica por atos de força (Rojas-Contreras; Orjuela Duarte; Santos Jaimes, 2025).

4.2.2 Síntese das recomendações estratégicas

De forma geral, a aplicação de *big data* e IA no contexto brasileiro revela um elevado potencial para o adensamento das capacidades da defesa nacional. Contudo, o impacto estratégico dessas tecnologias é condicionado pela capacidade de integração interforças, pela continuidade orçamentária dos projetos e pela consolidação de uma doutrina de dados soberana (Brasil, 2024). A Figura 3 sintetiza espacialmente as principais áreas de aplicação, destacando regiões estratégicas e os vetores tecnológicos associados.

Figura 3 – Vetores de *big data* e inteligência artificial na defesa nacional brasileira



Legenda: ícones de helicópteros representam vigilância aérea; embarcações indicam monitoramento marítimo; antenas simbolizam sistemas de comunicação e radar; nuvens conectadas representam processamento de dados em ambientes de *big data* e IA; e o escudo central indica a integração das informações com foco em segurança cibernética e defesa estratégica.
Fonte: Elaborada pelo autor.

Mais do que uma representação descritiva, a Figura 3 evidencia a distribuição espacial dos desafios e das capacidades necessárias para sua mitigação.

A distribuição dos elementos visuais no mapa foi definida com base em critérios estratégicos, incluindo: (i) áreas de maior extensão territorial e dificuldade de monitoramento, como a Amazônia Legal; (ii) regiões com elevada incidência de ilícitos transnacionais, como tráfico de drogas e contrabando em zonas de fronteira; (iii) áreas marítimas de interesse econômico e geopolítico, especialmente relacionadas à exploração de recursos naturais; e (iv) pontos críticos de infraestrutura sensível, sujeitos a riscos cibernéticos e operacionais.

Nesse contexto, a presença de sensores, plataformas aéreas e sistemas navais nessas regiões não representa posicionamentos reais específicos, mas uma abstração conceitual baseada em parâmetros estratégicos de vigilância, risco e relevância operacional.

A inclusão de helicópteros, embarcações de origem militar e sensores remotos representa a articulação entre os mecanismos de fiscalização aérea, terrestre e marítima, ao passo que o emblema central, adornado com um cadeado digital, simboliza a segurança cibernética e a concentração de informações estratégicas. As interações entre nuvens e sensores evidenciam o fluxo ininterrupto de dados analisados por sistemas preditivos, destacando a capacidade dessas tecnologias de prever ameaças, aprimorar a alocação de recursos e fortalecer a soberania nacional.

A Tabela 2 complementa essa análise ao sistematizar, de forma estruturada, as principais áreas de aplicação dessas tecnologias no Brasil, detalhando os recursos tecnológicos empregados e os benefícios estratégicos associados.

Tabela 2 – Aplicações potenciais de *big data* e inteligência artificial na defesa nacional brasileira

Área	Tecnologias envolvidas	Benefícios esperados
Monitoramento de fronteiras	Sensores remotos (satélites, drones, radares) + IA (visão computacional, *machine learning*)	Detecção precoce de ilícitos transnacionais e aumento da vigilância em áreas de difícil acesso
Cibersegurança	*Big data* + algoritmos preditivos (*machine learning /deep learning*) + sistemas de detecção de intrusão	Prevenção e mitigação de ataques a infraestruturas críticas e redes governamentais
Operações militares em campo	IA embarcada + integração multiplataforma + análise em tempo real	Apoio à tomada de decisão tática, aumento da proteção de tropas e otimização do uso de recursos

Fonte: Elaborada pelo autor.

A incorporação de tecnologias orientadas por dados e IA na defesa nacional não apenas amplia a capacidade de resposta, mas redefine a lógica de atuação das Forças Armadas, ao permitir decisões baseadas em inteligência contínua e integrada (Brasil, 2024). Nesse sentido, o avanço brasileiro nessa área depende da construção de um ecossistema tecnológico robusto, capaz de sustentar análise em larga escala, interoperabilidade entre sistemas e autonomia estratégica (Brasil, 2025a).

4.3 Desafios e barreiras estruturais

A implementação de tecnologias orientadas por dados e IA na defesa nacional brasileira enfrenta desafios que transcendem a dimensão técnica, envolvendo limitações institucionais, dependência externa e lacunas regulatórias. Esses obstáculos formam um complexo gargalo que impede a transição plena para uma defesa baseada em inteligência preditiva (Brasil, 2025a).

4.3.1 Infraestrutura e fragmentação sistêmica

Um dos principais entraves reside na infraestrutura tecnológica. A adoção de sistemas analíticos avançados exige capacidade computacional escalável e integração contínua entre plataformas heterogêneas. Atualmente, a fragmentação dos sistemas existentes e a limitação de investimentos comprometem o processamento em larga escala, reduzindo a efetividade das soluções no suporte à decisão estratégica (Brasil, 2025a).

4.3.2 O dilema da soberania digital

A dependência de tecnologias estrangeiras expõe o país a vulnerabilidades críticas, como o risco de acesso indevido a dados sensíveis ou a interrupção de serviços essenciais em cenários de crise geopolítica. O desenvolvimento de capacidades autóctones – abrangendo software, hardware e modelos analíticos proprietários – é imperativo para a autonomia estratégica. Sem o domínio de tecnologias nacionais, o Estado permanece sujeito a decisões de fornecedores externos que podem não se alinhar aos interesses de soberania nacional (Polido, 2024).

4.3.3 Ética, governança e capital humano

O processamento de grandes volumes de dados no setor de defesa impõe uma conformidade rigorosa à Lei Geral de Proteção de Dados (LGPD), exigindo transparência e responsabilidade algorítmica. Paralelamente, o emprego de sistemas autônomos impõe dilemas de *accountability* e redefine os limites operacionais das decisões automatizadas, exigindo supervisão humana clara (Brasil, 2018).

Complementarmente, a escassez de profissionais qualificados representa um fator limitante crítico. A formação de especialistas que dominem simultaneamente a ciência de dados e a doutrina de defesa exige uma articulação profunda entre universidades, centros de pesquisa e instituições militares para o desenvolvimento de capital humano especializado (Araujo; Mendes, 2025). A Tabela 3 sintetiza a matriz de riscos identificada e as respectivas recomendações para a mitigação desses hiatos.

Tabela 3 – Desafios *versus* possíveis soluções no Brasil

Categoria analítica	Desafio identificado (hiatos)	Recomendação estratégica (soluções técnicas)
Inteligência e consciência situacional	**Silos de dados**: fragmentação de informações entre Marinha, Exército e Aeronáutica, impedindo a visão holística	Implementação de Arquiteturas *Joint All-Domain* (JADC2) para garantir a interoperabilidade nativa e o fluxo de dados em tempo real entre forças
	Latência decisional: excesso de dados brutos sem processamento na "ponta" (*edge*), sobrecarregando os centros de comando	Adoção de *edge computing* e AI *on the edge* para processamento local em drones e sensores, enviando apenas inteligência refinada para o comando
Resiliência e soberania	**Dependência tecnológica (*black box*)**: uso de algoritmos proprietários estrangeiros que limitam a autonomia e criam vulnerabilidades	Fomento à BID com foco em *Open Source Intelligence* (OSINT) e algoritmos de auditoria nacional para garantir soberania digital
	Vulnerabilidade de modelos: riscos de ataques adversários que podem "enganar" a IA de reconhecimento de alvos	Desenvolvimento de protocolos de *robustness testing* e *red teaming* específicos para sistemas de IA militar
Governança e integração	**Déficit de talentos híbridos**: escassez de militares com formação em ciência de dados e civis com compreensão de doutrina de defesa.	Criação de carreiras tecnológicas de Estado e parcerias público-privadas para o desenvolvimento de centros de excelência em IA e defesa
	Descontinuidade orçamentária: projetos de longo prazo (como Sisfron) sujeitos a contingenciamentos que geram obsolescência técnica	Estabelecimento de fundos setoriais de defesa blindados e alinhamento com a Estratégia Nacional de Inteligência Artificial (EB)

Fonte: Elaborada pelo autor.

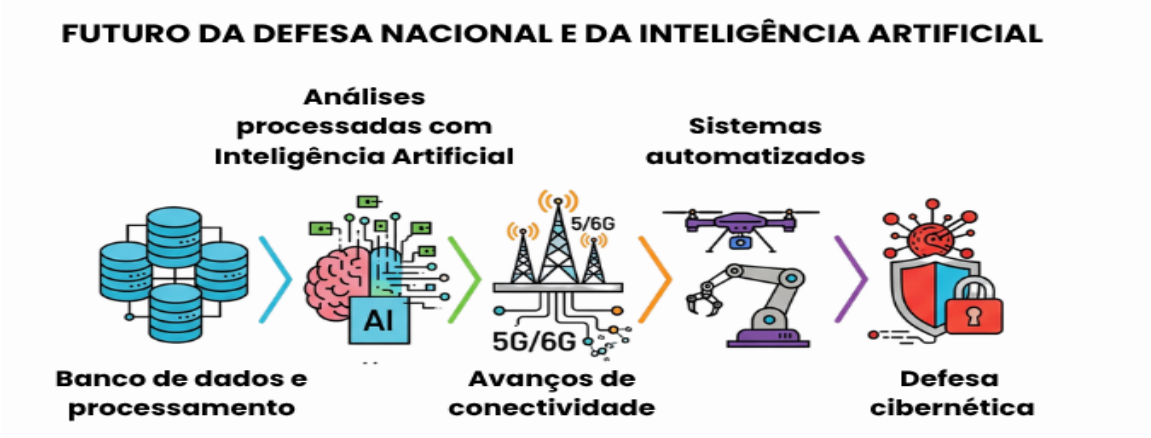
A mitigação desses hiatos exige uma coordenação sistêmica que vá além da simples aquisição de ferramentas prontas, demandando o fomento a tecnologias desenvolvidas internamente. Em última análise, a integração de *big data* e IA no teatro de operações brasileiro deixa de ser uma opção de modernização e torna-se um imperativo de sobrevivência estratégica em um cenário de guerra centrada em dados (*data-centric warfare*) (Magnuson, 2018).

4.4. Perspectivas futuras

A consolidação de uma defesa nacional orientada por dados depende da formulação de estratégias de longo prazo que articulem inovação disruptiva, autonomia soberana e robustez institucional. Nesse contexto, a criação de centros nacionais de análise preditiva surge como uma iniciativa estruturante (Silva, 2025). Concebidos como núcleos de excelência, esses centros devem operar em regime de hélice tríplice (universidades, instituições militares e setor privado), favorecendo a convergência entre a pesquisa aplicada e as demandas operacionais imediatas do teatro de operações (Brasil, 2025a).

As tendências globais indicam uma integração profunda entre a IA e tecnologias emergentes de conectividade. A Figura 4 apresenta o *roadmap* estratégico necessário para essa evolução, fundamentado na transição de sistemas isolados para uma arquitetura multiplataforma altamente conectada.

Figura 4 – *Roadmap* futuro da defesa nacional com integração de *big data*, inteligência artificial e tecnologias emergentes



Fonte: Elaborada pelo autor.

Conforme ilustrado, o avanço nesse domínio está diretamente associado ao fortalecimento das capacidades nacionais em análise de dados, IA e infraestrutura digital, aliado a investimentos contínuos em pesquisa aplicada e inovação. Essa trajetória aponta para a transição de um modelo reativo para uma lógica de atuação preditiva e integrada.

Outra tendência relevante refere-se ao avanço da IA explicável (XAI), que permite maior transparência nos processos decisórios automatizados (Gunning; Aha, 2019). A adoção de modelos interpretáveis torna-se especialmente crítica em contextos militares, nos quais a confiabilidade e a auditabilidade das decisões são requisitos fundamentais (Wang; Jones, 2017).

Além disso, a convergência com tecnologias como 5G/6G, internet das coisas e computação quântica tende a ampliar significativamente a capacidade de processamento, conectividade e segurança dos sistemas de defesa, viabilizando operações mais ágeis, distribuídas e resilientes (Goodfellow *et al.*, 2016)

4.4.1 Inovação aberta e soberania tecnológica

O fortalecimento de parcerias internacionais estratégicas pode acelerar o desenvolvimento dessas capacidades, desde que acompanhado de políticas voltadas à proteção da soberania tecnológica. Nesse sentido, a articulação entre cooperação internacional e desenvolvimento interno configura um eixo central para a consolidação de um ecossistema nacional robusto e sustentável em defesa (Brasil, 2025a; Dalbosco; Cortinhas, 2024).

A inovação tecnológica constitui um vetor central para a consolidação dessas perspectivas futuras, exigindo não apenas a adoção de tecnologias emergentes, mas o desenvolvimento de soluções adaptadas às especificidades operacionais da defesa nacional (Assur, 2024). Nesse contexto, iniciativas voltadas à inovação aberta, ao incentivo a *startups*[14] de base tecnológica e à criação de ambientes de experimentação, como *sandboxes*[15] regulatórios e laboratórios de prototipagem, podem acelerar a transição entre pesquisa e aplicação prática (Assur, 2024). Adicionalmente, o estímulo à pesquisa interdisciplinar e à transferência de tecnologia entre academia, setor produtivo e instituições militares é fundamental para reduzir o hiato entre desenvolvimento científico e implementação operacional, fortalecendo a capacidade do país de gerar soluções inovadoras com impacto direto na segurança e na soberania nacional.

5. CONCLUSÃO

A aplicação estratégica de tecnologias orientadas por dados e IA representa uma transformação estrutural na lógica de atuação da defesa nacional, ao possibilitar não apenas a identificação antecipada de ameaças, mas a construção de capacidades preditivas e adaptativas em cenários operacionais complexos.

Sob a perspectiva teórico-conceitual, a integração dessas tecnologias insere-se no paradigma contemporâneo da guerra informacional e da defesa orientada por dados (*data-driven defense*), no qual a vantagem estratégica decorre da capacidade de transformar fluxos massivos de dados em inteligência acionável em tempo real.

A experiência internacional demonstra que essas capacidades já se consolidaram como elementos centrais nos sistemas de defesa contemporâneos, reforçando a necessidade do Brasil de avançar na construção de estruturas integradas e autônomas. No entanto, a análise do contexto nacional evidencia que o país ainda se encontra em um estágio intermediário, marcado por iniciativas fragmentadas, limitações de integração sistêmica e dependência tecnológica externa em áreas críticas, especialmente no domínio cibernético e na infraestrutura de dados estratégicos.

Para superar essas limitações, torna-se necessário enfrentar desafios relacionados à infraestrutura tecnológica, à soberania digital, à governança ética e à formação de recursos humanos especializados. Nesse sentido, a criação de centros nacionais de análise preditiva, o avanço em inteligência artificial explicável e a consolidação de políticas integradas de ciberdefesa configuram caminhos estratégicos para o fortalecimento da capacidade nacional. Adicionalmente, a articulação entre inovação tecnológica, cooperação institucional e desenvolvimento de capacidades internas será determinante para a construção de um ecossistema de defesa orientado por dados.

Diante desse cenário, conclui-se que a implementação coordenada dessas tecnologias deve ser tratada como prioridade estratégica, não apenas para ampliar a capacidade de resposta,

14 ***Startups***: são empresas emergentes, geralmente de base tecnológica, caracterizadas pelo desenvolvimento de soluções inovadoras sob condições de alta incerteza, com potencial de crescimento acelerado e foco na criação de novos produtos, serviços ou modelos de negócio escaláveis.

15 ***Sandboxes***: são ambientes controlados de teste nos quais novas tecnologias, produtos ou serviços podem ser desenvolvidos e avaliados sob supervisão de autoridades reguladoras, com flexibilização temporária de regras, permitindo experimentação segura antes da implementação em larga escala.

mas para assegurar autonomia decisória e competitividade no cenário internacional. Esse avanço, contudo, depende da consolidação de uma estratégia nacional integrada, capaz de alinhar dimensões tecnológicas, operacionais e institucionais de forma coerente e sustentável.

Por fim, a ausência desse movimento tende a ampliar a vulnerabilidade estratégica do país frente a ameaças emergentes, evidenciando que o investimento estruturado em tecnologias orientadas por dados deixou de ser uma opção e passou a constituir uma necessidade estratégica para a defesa nacional. Mais do que um desafio tecnológico, trata-se de um problema estrutural de coordenação, integração e governança de dados no âmbito da defesa nacional.

Agradecimentos

Conselho Nacional de Desenvolvimento Científico e Tecnológico. Processo: 302742/2022-0.

Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. Processo: 88887.613955/2021-00

Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. Processo: PROCAD 16/2020

Fundação de Amparo à Pesquisa do Estado de São Paulo. Processo: 2025/04394-0

REFERÊNCIAS

ALZUBAIDI, L. *et al.* Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. **Journal of Big Data**, New York, v. 8, n. 1, p. 53, 2021.

AMIROLSHAH, A. Advanced data analytics techniques for enhancing national security strategies. **The Journal of Defence and Security**, v. 20, n. 1, p. 36-42, 2024.

ANDRADE, D. L. O. D. **Inteligência artificial**: como incorporar a inteligência artificial na "Força Terrestre Brasileira de Próxima Geração". 2025. Monografia (Trabalho de Investigação Individual) – Instituto Universitário Militar, Maia. Disponível em: https://comum.rcaap.pt/bitstreams/d037aae5-80a2-4721-a214-32194903b510/download. Acesso em: 21 abr. 2026.

ANDRADE, I. D. O.; LIMA, R. C. Segurança e defesa nacional nas fronteiras brasileiras. *In*: MOURA, R. (org.). **Fronteiras do Brasil**: uma avaliação de política pública. Brasil: Ipea, 2018. v. 1, p. 111-150.

ANDRADE, M. B.; LIMA, C. R. P. D. Medidas de enforcement na estratégia brasileira de inteligência artificial: lacunas e perspectivas. **Revista Brasileira de Inteligência Artificial e Direito**, Brasília, DF, v. 1, 2021.

ARAUJO, M.; MENDES, A. Cibersegurança como soberania nacional? Perspectivas do Brasil e da China. **Liinc em Revista**, Rio de Janeiro, v. 21, n. 1, 2025.

ASSUR, J. R. **Inovação e desendolvimente tecnológico da defesa**: um estudo de caso no Centro de Inovação Estratégico na Marinha do Brasil. 2024. Monografia (Curso de Estado-Maior para Oficiais Superiores) – Escola de Guerra Naval, Rio de Janeiro, 2024. Disponível em: https://repositorio.marinha.mil.br/bitstream/ripcmb/847402/1/C-EMOS2024_CC_ASSUR.pdf. Acesso em: 21 abr. 2026.

AZEVEDO, C. E. F.; BORBA, G. A.; ARAÚJO, L. E. Desafios para a política de inovação no setor de defesa brasileiro: óbices e barreiras culturais e estruturais. **Revista da Escola de Guerra Naval**, 27, n. 1, p. 121-160, 2021.

BARBOZA, H. L.; FERNEDA, A. S.; CRISTÓVAM, J. S. D. S. A Estratégia brasileira de inteligência artificial no paradigma do governo digital. **Revista do Direito**, Santa Cruz do Sul, n. 67, p. 1-18, 2023.

BATISTA, E. D. S. S. L. *et al.* Human-In-The-Loop (HITL): uma abordagem que integra a participação humana em sistemas de inteligência artificial e automação. **Revista para Graduandos**, São Paulo, v. 10, n. 4, p. 84-90, 2025.

BONANNO, B. D. M. **Desafios à consolidação de uma rede nacional de gestão cibernética**: impactos da inclusão digital na defesa e soberania do Brasil. 2025. Monografia (Curso Superior de Segurança e Defesa Cibernética) – Escola Superior de Guerra, Rio de Janeiro, 2025. Disponível em: https://repositorio.esg.br/bitstream/123456789/2134/1/EA_CSSDC_2025_-_Beatriz_da_Mota_Bonanno.pdf. Acesso em: 21 abr. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 abr. 2026.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Estratégia brasileira de inteligência artificial – Ebia**. Brasília, DF: MCTI, 2025. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/ebia.pdf. Acesso em: 21 abr. 2026.

BRASIL. Ministério da Defesa. **Curso de governança em defesa**: 2025: trabalhos finais. Rio de Janeiro: ESG, 2025b. Disponível em: https://www.gov.br/esg/pt-br/composicao/editora/coletanea-cged-2025-capa-2.pdf/@@display-file/file. Acesso em: 21 abr. 2026.

BRASIL. Ministério da Defesa. **Doutrina militar de defesa cibernética**: MD31-M-07. Brasília, DF: Ministério da Defesa, 2023. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 21 abr. 2026.

BRASIL. Ministério da Defesa. **Política nacional de defesa e a 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_.pdf. Acesso em: 21 abr. 2026.

CHRISTIE, E.; ERTAN, A. Nato and artificial intelligence. *In*: ROMANIUK, S.; MANJIKIAN, M. (ed.). **Routledge companion to artificial intelligence and national security policy**. Abingdon-on-Thames: Routledge, 2021.

CUMMINGS, M. **Artificial intelligence and the future of warfare**. London: Chatam House, 2017.

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.

FIGUEIREDO, W. B. Política nacional de defesa e estratégia nacional de defesa: desigualdade regional e desenvolvimento. **Revista Faz Ciência**, Francisco Beltrão, v. 27, n. 46, p. 6-30, 2025.

GOMES, N. L. D. S. **A segurança e a defesa cibernética no Brasil**: análise dos discursos das Forças Armadas brasileiras (2016-2021). 2024. Dissertação (Mestrado em Segurança Internacional e Defesa) – Escola Superior de Guerra, Rio de Janeiro, 2024. Disponível em: https://repositorio.esg.br/handle/123456789/1951. Acesso em: 21 abr. 2026.

GONZALEZ, C. D. O.; FERREIRA, P. P. Anatomia de um sistema de inteligência artificial. **ComCiência**, Campinas, 20 set. 2020. Disponível em: https://www.comciencia.br/anatomia-de-um-sistema-de-inteligencia-artificial/. Acesso em: 21 abr. 2026.

GOODFELLOW, I. *et al*. **Deep learning**. Cambridge: The MIT Press, 2016.

GRAND-CLÉMENT, S. **Artificial intelligence beyond weapons**: application and impact of AI in the military domain. Geneva: Unidir, 2023.

GUNNING, D.; AHA, D. W. DARPA's explainable artificial intelligence (XAI) program. **AI Magazine**, Hoboken, v. 40, n. 2, p. 44-58, 2019.

KIRANYAZ, S. *et al*. Real-time fault detection and identification for MMC using 1-D convolutional neural networks. **IEEE Transactions on Industrial Electronics**, v. 66, n. 11, p. 8760-8771, 2019.

KITCHIN, R. The real-time city? Big data and smart urbanism. **GeoJournal**, New York, v. 79, n. 1, p. 1-14, 2014.

KITCHIN, R. **Data lives**: How data are made and shape our world. Bristol: Bristol University Press, 2021.

LECUN, Y.; BENGIO, Y.; HINTON, G. Deep learning. **Nature**, New York, v. 521, n. 7553, p. 436-444, 2015.

LOWREY, N. S. **Repealing don't ask, don't tell**: a historical perspective from the joint chiefs of staff. Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 2021.

MAGNUSON, S. Darpa pushes "Mosaic Warfare" concept. **National Defense**, Arlington, v. 103, n. 780, p. 18-19, 2018.

MCGARRY, B. W.; SATURNO, J. V. **Defense primer**: defense appropriations process. Washington, DC: Congressional Research Service, 2020.

MEDEIROS, C. D. D. S.; GUALBERTO, É. S. **Impacto das novas tecnologias na proteção de dados e segurança cibernética na administração pública**: o uso de inteligência artificial e computação em nuvem. Brasília, DF: UnB, 2025.

MEDEIROS, S.; ALVAREZ, L. I. Drones, inteligência artificial e direito internacional: desafios regulatórios e responsabilidade estatal no emprego da força. **Revista de Doutrina e Jurisprudência do Superior Tribunal Militar**, Lisboa, v. 34, n. 2, 2026.

MOHAMED, N. A review of AI approaches in combating advanced persistent threats (APTs) in cybersecurity. **IEEE**, 2024.

MORGAN, F. E. *et al.* **Military applications of artificial intelligence**: ethical concerns in an uncertain world. Santa Monica: Rand Corporation, 2020.

NATO. **Summary of the NATO artificial intelligence strategy**. Brussels: Nato, 2021. Disponível em: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy. Acesso em: 21 abr. 2026.

NIE, S.; SUN, D. Research on counter-terrorism based on big data. **IEEE**, 2016.

OFILI, B. T.; EZEADI, S. C.; JEGEDE, T. B. Securing US national interests with cloud innovation: data sovereignty, threat intelligence and digital warfare preparedness. **International Journal of Science and Research Archive**, Jalgaon, v. 12, n. 1, p. 3160-3179, 2024.

OLIVEIRA, A. L. F. T. D.; FARIAS, H. C. O Sisfron como ferramenta da estratégia da presença em meio ao desafio orçamentário entre 2012 e 2022. **Revista Brasileira de Estudos de Defesa**, v. 10, n. 2, 2023.

PETERSON, J. *et al*. Understanding scoping reviews: definition, purpose, and process. **Journal of the American Association of Nurse Practitioners**, v. 29, n. 1, p. 12-16, 2017.

POLIDO, F. B. P. Estado, soberania digital e tecnologias emergentes: interações entre direito internacional, segurança cibernética e inteligência artificial. **Revista de Ciências do Estado**, Belo Horizonte, v. 9, n. 1, p. 1-30, 2024.

PRIAMBODO, D. F. *et al*. Observe-orient-decide-act (ooda) for cyber security education. **International Journal of Advanced Computer Science and Applications**, Cleckheaton, v. 13, n. 10, p. 246-255, 2022.

ROJAS-CONTRERAS, M.; ORJUELA DUARTE, A.; SANTOS JAIMES, L. **Human-in-the-loop (HITL) as a verification and validation strategy for knowledge generated by generative artificial intelligence**. Mexico City: LACCEI, 2025.

ROKVIĆ, V. Mosaic warfare as a new art of war? **The Review of International Affairs**, Frankfurt am Main, v. 76, n. 1195, p. 421-448, 2025.

SCHARRE, P. **Four battlegrounds**: power in the age of artificial intelligence. New York: WW Norton & Company, 2023.

SCHMIDT, E. US National Security Commission on Artificial Intelligence. *In*: ARAYA, D.; MARBER, P. (ed.). **Augmented education in the global age**. Abingdon-on-Thames: Routledge, 2023. p. 234-244.

SILVA, M. A. A. D. **O impacto do uso da inteligência artificial na cibernética envolvendo sistemas de comando e controle:** a importância do alinhamento das estratégias à política e aos objetivos nacionais. 2024. Monografia (Bacharelado em Segurança e Defesa Cibernética) – Escola Superior de Guerra, Rio de Janeiro, 2024. Disponível em: https://repositorio.esg.br/bitstream/123456789/1972/1/MARCUS%20ALBERT%20ALVES%20DA%20SILVA.pdf. Acesso em: 21 abr. 2026.

SILVA, W. L. P. D. Análise preditiva de ataques cibernéticos usando redes neurais. **Anais da Semana da Computação**, Jataí, v. 1, p. 1-6, 2025.

SOARES, R. D. L. B. Base industrial de defesa brasileira ea política externa. **Cadernos de Política Exterior**, Brasília, DF, v. 1, p. 47-62, 2015.

SOUSA, D. P. D. Metodologia de investigação científica. **De Legibus**: Revista de Direito da Universidade Lusófona Lisboa, Lisboa, n. 7, p. 1-27, 2024.

STILES, A.; NETESSINE, S. **Generative AI adoption in the US Military:** a framework for assessment, and what the private sector can learn. Philadelphia: The Wharton School, 2025.

STRAT, F. E. **Insecurity unveiled? China and Israel's use of AI and mass surveillance for national security and identity**. 2023. Thesis (Master in Security, Intelligence and Strategic Studies) – Charles University, Prague, 2023. Disponível em: http://hdl.handle.net/20.500.11956/187326. Acesso em: 21 abr. 2026.

TONI, J. D. *et al*. **Uma análise do ecossistema organizacional da administração pública federal brasileira a partir da perspectiva de estabilidade ágil**: diagnóstico e propostas. Brasil: Enap, 2025.

WANG, L.; JONES, R. Big data analytics for network intrusion detection: a survey. **International Journal of Networks and Communications**, Thousand Oaks, v. 7, n. 1, p. 24-31, 2017.

WILLE, C. The Implications of the reverberating effects of explosive weapons use in populated areas for implementing the sustainable development goals. **Unidir Resources**, Geneva, 2016.

WU, S. *et al.* An integrated data-driven scheme for the defense of typical cyber-physical attacks. **Reliability Engineering & System Safety**, Amsterdam, v. 220, 2022.

ZHANG, X.; ZHOU, Y. N.; LUO, J. Deep learning for processing and analysis of remote sensing big data: a technical review. **Big Earth Data**, Abingdon-on-Thames, v. 6, n. 4, p. 527-560, 2022.

ZHOU, Z. *et al.* Edge intelligence: paving the last mile of artificial intelligence with edge computing. **Proceedings of the IEEE**, v. 107, n. 8, p. 1738-1762, 2019.