ARTÍCULO DOI 10. 52781/cmm.a194

# El papel del *big data* y la inteligencia artificial en la seguridad y en la defensa nacional

*The role of big data and AI for Brazil's national security and defense*

**Resumen:** Este artículo analiza la integración estratégica del *big data* y la inteligencia artificial (IA) como vectores para la modernización de la defensa nacional. El objetivo es identificar cómo la transición a la defensa basada en datos (*data-driven defense*) puede reducir las asimetrías operativas y elevar la soberanía tecnológica brasileña. Se utilizó como metodología una revisión de alcance (*scoping review*) y un análisis documental con el fin de confrontar el estado del arte internacional, centrándose en doctrinas como *mosaic warfare* y el ciclo OODA acelerado, con la realidad institucional brasileña (Sisfron, CDCiber y Enia). Los resultados demuestran que, aunque Brasil tiene sólidas iniciativas de detección, todavía persiste una brecha funcional caracterizada por silos informativos entre las fuerzas y la dependencia de algoritmos extranjeros ("cajas negras"). Se concluye que la superación de estas barreras requiere la transición a arquitecturas unificadas de mando y control (JADC2) y la promoción de tecnologías autóctonas. El estudio propone un *roadmap* estratégico basado en IA explicable (XAI) y *edge computing* para garantizar la superioridad en la decisión y la autonomía de la toma de decisiones del Estado en escenarios de guerra centrada en datos (*data-centric warfare*).

**Palabras clave:** *Big data*; Inteligencia artificial; Defensa nacional; Ciberseguridad; Inteligencia predictiva.

**Abstract:** This study analyzes the strategic integration of big data and artificial intelligence (AI) as drivers for the modernization of Brazil's national defense. It aims to find how the transition to a data-driven defense model can reduce operational asymmetries and enhance Brazilian technological sovereignty. The methodology included a scoping review and documentary analysis, contrasting the international state-of-the-art (doctrines such as Mosaic Warfare and the accelerated OODA loop) with the Brazilian institutional reality (SISFRON, CDCiber, and ENIA). The results show that, although Brazil possesses robust sensing initiatives, a functional gap persists, consisting of information silos between the Armed Forces and a dependence on foreign "black-box" algorithms. Overcoming these limitations requires a transition toward joint all-domain command and control architectures and the promotion of national technologies. This study proposes a strategic roadmap based on explainable AI and edge computing that aims to ensure decision superiority and State 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

**Recibido: 01 ago. 2025**
**Aprobado: 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. INTRODUCCIÓN

La digitalización ejerce un impacto significativo en las estrategias nacionales de defensa y seguridad al modificar los paradigmas convencionales de vigilancia, salvaguarda y toma de decisiones. El creciente aumento de datos provenientes de sensores, satélites, dispositivos móviles y ciberinteligencia da como resultado un ecosistema de información altamente complejo, muchas veces definido por el concepto de *big data*[1] (Kitchin, 2021). En este escenario, la inteligencia artificial (IA), particularmente mediante algoritmos de aprendizaje automático y análisis predictivo, actúa como un elemento central en la conversión de datos masivos en inteligencia estratégica al permitir la identificación de patrones y la anticipación de amenazas con un alto grado de precisión (Scharre, 2023).

En los conflictos contemporáneos caracterizados por guerras híbridas y amenazas transnacionales, la rapidez en el procesamiento de la información influye directamente en la capacidad de respuesta y resiliencia del Estado (Scharre, 2023). Las experiencias globales muestran que naciones como Estados Unidos, Israel y los miembros de la Organización del Tratado del Atlántico Norte (OTAN) ya han consolidado arquitecturas de datos integradas capaces de soportar sistemas de vigilancia y soporte automatizado a las decisiones en entornos altamente complejos (Nato, 2021).

En el contexto brasileño, la incorporación de estas tecnologías ocurre todavía de manera fragmentada, lo cual refleja limitaciones estructurales que trascienden la mera disponibilidad tecnológica (Andrade; Lima, 2021). Si bien la extensión territorial y la complejidad de las fronteras imponen severas demandas operativas, los desafíos nacionales surgen, sobre todo, de la ausencia de una estrategia integrada que articule infraestructura, gobernanza de datos y capacidades analíticas (Araujo; Mendes, 2025). También persisten obstáculos relacionados con la dependencia tecnológica externa, con la baja madurez en la soberanía digital y con la escasez de recursos humanos especializados, factores que limitan la internalización de la IA en los sistemas críticos (Bonanno, 2025).

En esta dirección, el problema central no radica en la adopción de herramientas aisladas, sino en la dificultad de estructurar un ecosistema nacional robusto aplicado a la defensa (Toni *et al*., 2025). Esta limitación compromete la autonomía estratégica del país y su capacidad de respuesta en escenarios de crisis. Ante el contexto, este estudio parte de la siguiente pregunta de investigación: ¿Cómo puede impactar la integración de *big data* e IA en las capacidades estratégicas de la defensa nacional al tener en cuenta las dimensiones de predicción de amenazas, ciberseguridad y apoyo a la toma de decisiones?

El objetivo principal de este trabajo es analizar el papel del *big data* y de la IA en el fortalecimiento de la defensa nacional, con énfasis en las aplicaciones estratégicas y los desafíos de implementación en Brasil. Además de un análisis descriptivo, este estudio parte de la hipótesis de que el obstáculo para la consolidación de estas capacidades en el país no es solo tecnológico, sino que estructural. Se argumenta que la ausencia de una arquitectura integrada, combinada con debilidades en la gobernanza interinstitucional y con la dependencia externa, compromete la conversión de datos en inteligencia operativa. Por lo tanto, la limitación brasileña debe entenderse como un problema de coordinación sistémica y madurez institucional.

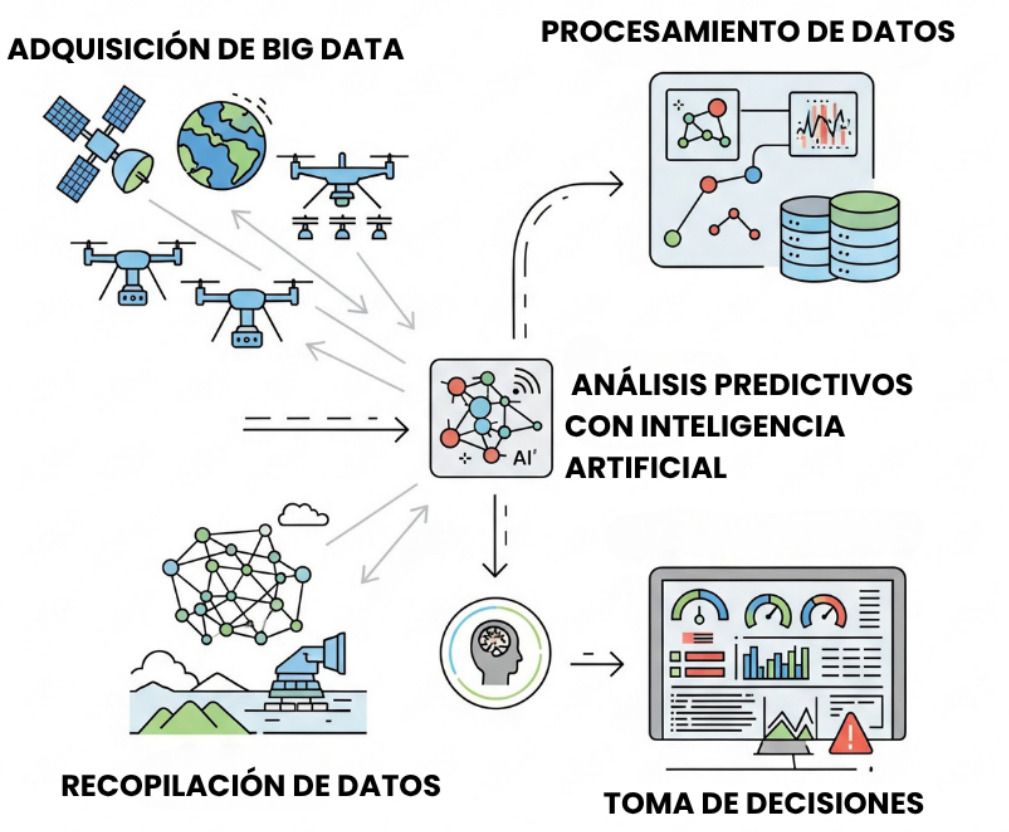
1 **Big data**: ecosistema de infraestructura informática y algoritmos avanzados (como el procesamiento distribuido y machine learning) diseñado para capturar, almacenar y analizar datos a gran escala que son demasiado grandes para ser administrados por los sistemas tradicionales de gestión de bases de datos relacionales.

Como metodología se adopta un enfoque cualitativo y exploratorio, basado en una revisión bibliográfica y documental estructurada al centrarse en el escenario nacional en comparación con los puntos de *benchmarks*[2] internacionales (Sousa, 2024). El análisis busca contribuir al debate sobre la modernización de la defensa al proponer la integración de la infraestructura de datos y de los sistemas inteligentes como eje estructurador de la capacidad estratégica contemporánea.

La principal contribución de este estudio radica en la propuesta de un marco analítico que interpreta la adopción de *big data* e IA en la defensa nacional brasileña como un problema de coordinación sistémica y madurez institucional, y no simplemente como una limitación tecnológica.

La Figura 1 ilustra este flujo sistémico al mostrar la integración de fuentes multimodales –como satélites, *Remotely Piloted Aircraft* (RPA), sensores terrestres y redes digitales– y su posterior asimilación mediante algoritmos predictivos. Esta secuencia permite no solo la detección temprana de actos hostiles, sino también la adaptación dinámica de las respuestas operativas en escenarios de fricción e incertidumbre.

**Figura 1 – Flujo de *big data* e inteligencia artificial en defensa nacional**




Fuente: Elaborada por el autor.

2 ***Benchmarks***: se refiere a un punto de referencia o parámetro de excelencia utilizado con el propósito de hacer una comparación sistemática. En el contexto científico, sirve como base normativa para evaluar el desempeño, la efectividad o la calidad de los procesos, sistemas o resultados en relación con las mejores prácticas establecidas en la literatura o en el mercado.

De acuerdo con lo que se demostró en el flujo de *big data* e IA, el análisis predictivo en el dominio de la defensa depende de la articulación sinérgica entre la infraestructura de datos, la capacidad computacional y los modelos analíticos avanzados. Esta integración permite apoyar la conciencia situacional en tiempo real al redefinir la lógica de decisión al pasar de un modelo reactivo a una postura de anticipación continua. En definitiva, esta arquitectura contribuye directamente al fortalecimiento de la soberanía nacional y a la resiliencia de las infraestructuras críticas ante amenazas multidimensionales.

## 2. METODOLOGÍA

Este estudio utiliza un enfoque cualitativo de carácter exploratorio, estructurado mediante una revisión de alcance[3] (*scoping review*) y análisis documental (Peterson *et al*., 2017). El diseño metodológico se planificó para asegurar la reproducibilidad de la colección y el rigor en el análisis comparativo entre el escenario internacional y la realidad brasileña. El proceso se dividió en tres etapas indicadas en los siguientes subtemas.

### 2.1 Estrategia de búsqueda de selección

La búsqueda de datos se basó en un análisis sistemático en bases de datos científicas (como Google Scholar, Scopus e IEEE Xplore) y repositorios institucionales de defensa, incluidos documentos de la OTAN, de la *Defense Advanced Research Projects Agency* (DARPA) y del Ministerio de Defensa de Brasil. Se incluyeron documentos publicados entre 2015 y 2025, seleccionados en función de su relevancia temática, adherencia al alcance del estudio y recurrencia en bases científicas e institucionales. Se excluyeron los documentos duplicados, no revisados por pares o que no estuvieron directamente relacionados con el objeto de análisis. Para recuperar las fuentes, se utilizaron descriptores combinados en portugués e inglés, como "*big data*", "*inteligência artificial*", "*defesa nacional*" y "*cybersecurity*". El marco temporal priorizó las publicaciones de la última década, con el objetivo de capturar la aceleración de las tecnologías basadas en datos y sus implicaciones operativas y soberanas.

### 2.2 Categorización de análisis

Para evitar la subjetividad en la interpretación, el contenido seleccionado se estructuró en tres ejes temáticos fundamentales:

- Inteligencia predictiva y conciencia situacional: centrada en el seguimiento y la reducción de la incertidumbre operativa.
- Resiliencia y **soberanía cibernética**: orientado a proteger las infraestructuras críticas y la autonomía tecnológica.

3 **Revisión de alcance**: método de síntesis del conocimiento que tiene como objetivo mapear los principales conceptos, fuentes y evidencia disponibles en un área de investigación determinada, especialmente cuando el tema es complejo o aún no ha sido revisado de manera integral.

- Gobernanza e integración sistémica: centrado en los desafíos de la interoperabilidad y las políticas públicas a largo plazo.

### 2.3 Procedimiento de análisis comparativo

Este estudio adoptó un enfoque analítico-comparativo y utilizó como *benchmarks* las experiencias de países con un alto grado de madurez tecnológica (Estados Unidos, Israel y miembros de la OTAN). Esta confrontación de modelos permitió identificar no solo las herramientas disponibles, sino que también las brechas estructurales, institucionales y de gobernanza que condicionan la implementación de estas capacidades en el contexto de la defensa nacional brasileña.

## 3. DESARROLLO

En el ámbito de la defensa nacional, el concepto de *big data* trasciende el mero almacenamiento abundante para referirse a la capacidad estratégica de estructurar y explorar flujos de datos heterogéneos en entornos de alta volatilidad (Nie; Sun, 2016). La convergencia de información provenientes de múltiples dominios, incluida la teledetección, los sistemas autónomos y la ciberinteligencia, permite construir una base de información interconectada (Kitchin, 2021). Desde la perspectiva de la defensa basada en datos (*data-driven defense*), la superioridad estratégica se redefine por la capacidad de convertir este volumen masivo en inteligencia procesable casi en tiempo real, lo cual reduce la incertidumbre en escenarios operativos dinámicos (Wu *et al.*, 2022).

La literatura contemporánea destaca que la transición a este modelo requiere más que la incorporación de tecnologías digitales, exige la reconfiguración de estructuras organizativas y mecanismos de gobernanza (Nato, 2021). En este contexto, la efectividad militar deja de depender exclusivamente de los medios convencionales y comienza a residir en la construcción de ecosistemas institucionales capaces de sostener la interoperabilidad y la coordinación interagencia (Morgan *et al.*, 2020). La IA actúa como el motor de esta transformación, mediante el uso de *machine learning*[4] y *deep learning*[5] para automatizar el cribado y el análisis predictivo (Lecun; Bengio; Hinton, 2015).

La sofisticación de los modelos de deep learning marcó un cambio de paradigma en el análisis de la Inteligencia de Imágenes (Imagery Intelligence [IMINT]) (Zhang; Zhou; Luo, 2022). Mientras que los algoritmos estadísticos tradicionales se basaban en parámetros predefinidos manualmente para identificar objetos, las redes neuronales convolucionales6 (CNN) operan mediante múltiples capas de procesamiento que imitan la visión humana (Alzubaidi et al., 2021).

4 ***Machine learning*** (aprendizaje automático): subcampo de la IA que se ocupa del desarrollo de algoritmos y modelos estadísticos capaces de identificar patrones y hacer inferencias a partir de datos sin necesidad de instrucciones explícitas de programación para cada tarea. El rendimiento del sistema se mejora iterativamente a medida que se expone a nuevos conjuntos de datos.

5 **Deep learning** (aprendizaje profundo): subconjunto del machine learning basado en redes neuronales artificiales con múltiples capas de procesamiento (capas ocultas). Esta arquitectura permite que el modelo aprenda representaciones de datos con múltiples niveles de abstracción, en que cada capa transforma la entrada en una representación un poco más abstracta y compleja.

6 **Redes neuronales convolucionales**: una clase de algoritmos de deep learning diseñados específicamente para procesar datos de topología de cuadrícula como imágenes. Su arquitectura utiliza una operación matemática llamada convolución en lugar de la multiplicación convencional de matrices en al menos una de sus capas, lo que permite la extracción automática de características espaciales (bordes, texturas y formas) mediante filtros que se pueden aprender.

Esta arquitectura permite que el sistema aprenda y reconozca de forma autónoma patrones complejos en videos de drones e imágenes satelitales al operar con una latencia mínima, esencial para rastrear objetivos en movimiento en tiempo real (Kiranyaz et al., 2019).

Sin embargo, esta capacidad de procesamiento genera lo que la literatura denomina efecto de "caja negra"[7], en el cual el camino lógico que utiliza la máquina para llegar a una conclusión es opaco para el operador humano. Luego, surge el desafío crítico de la *Explainable AI* (XAI) o IA Explicable en el teatro de operaciones, cuyo objetivo es traducir modelos matemáticos complejos en representaciones inteligibles (Gunning; AHA, 2019). En el campo de batalla, la confianza en el mando depende de la capacidad del algoritmo para proporcionar una justificación interpretable para sus clasificaciones (Scharre, 2023). En resumen, para autorizar el uso de la fuerza, el comandante necesita comprender los criterios que llevaron a la IA a clasificar un objeto como "amenaza" en lugar de un objetivo civil, con el fin de mitigar los riesgos de errores colaterales catastróficos en los Sistemas de Armas Letales Autónomas (*Lethal Autonomous Weapons Systems*, LAWS) (Grand-Clément, 2023; Wille, 2016).

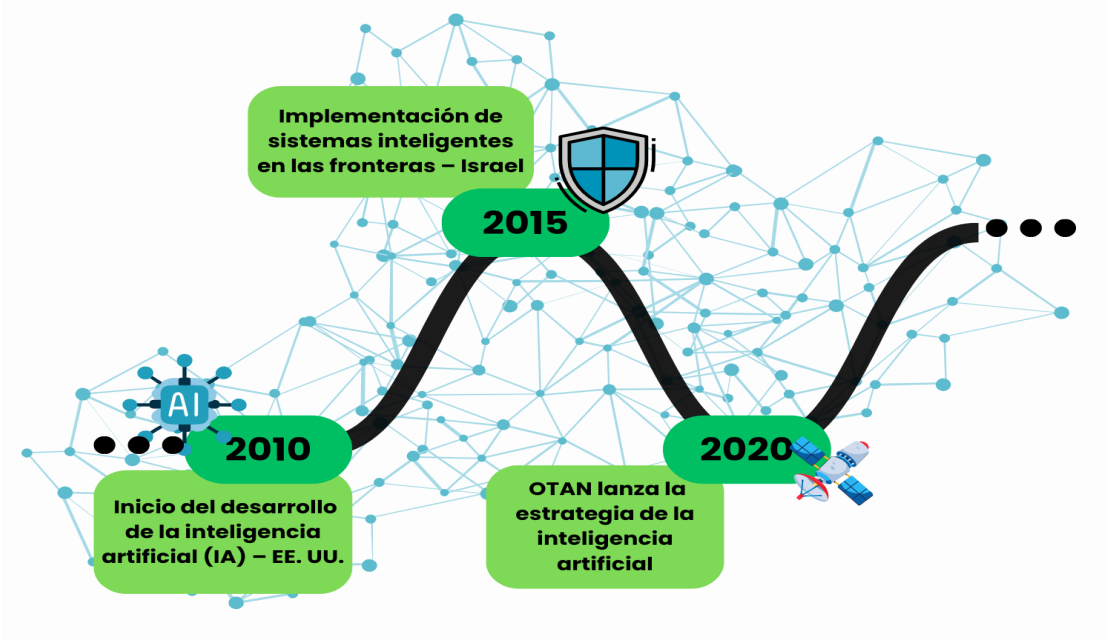
En el escenario internacional, el programa Mosaic Warfare de DARPA ilustra el uso de sistemas distribuidos para ampliar la agilidad de la toma de decisiones (Rokvić, 2025). El concepto de Mosaic Warfare, aunque citado como una integración de sensores, representa una evolución en la doctrina de Mando y Control (C2) (Magnuson, 2018). A diferencia de los sistemas monolíticos y caros, el "mosaico" utiliza la IA para coordinar cientos de pequeñas unidades baratas y desechables (enjambres de drones, sensores de bajo costo), creando un sistema de defensa resistente e impredecible (Scharre, 2023). Esta descentralización, respaldada por una arquitectura distribuida de *Big Data*, hace que el esfuerzo de guerra del adversario sea ineficaz, ya que no hay un solo centro de gravedad para atacar (McGarry; Saturno, 2020).

Al mismo tiempo, la OTAN ha liderado el movimiento de institucionalización tecnológica con su estrategia de IA (2021), centrada en la estandarización ética y la interoperabilidad multidominio (Christie; Ertan, 2021). Israel, a su vez, se destaca por integrar algoritmos propietarios en los sistemas de vigilancia, lo que resulta en una reducción drástica del tiempo de respuesta en las operaciones antiterroristas (Scharre, 2023). Además de la defensa cibernética, estas tecnologías redefinen la logística y el apoyo a la toma de decisiones tácticas al permitir la optimización del uso de recursos en entornos de alta fricción (Ofili; Ezeadi; Jegede, 2024).

La Figura 2 ilustra los hitos de esta evolución global y muestra la transición de los sistemas puramente reactivos a arquitecturas de inteligencia proactiva (Kitchin, 2014). Se observa que el punto de inflexión tecnológico no fue solo el aumento de la potencia de procesamiento, sino la capacidad de integrar flujos de datos intensos en entornos de combate disputados (Lowrey, 2021). Esta trayectoria demuestra que la superioridad militar contemporánea ya no reside solo en la fuerza cinética, sino en la velocidad del ciclo de decisión (Nato, 2021).

7 **Caja negra:** se refiere a los sistemas de machine learning o deep learning como las redes neuronales profundas que producen resultados altamente precisos, pero cuyos procesos internos para decidir y sopesar variables son demasiado complejos para la interpretación humana.

**Figura 2 – Hitos internacionales para la adopción de *big data* e inteligencia artificial en defensa**




**Fuente:** Elaborada por el autor.

Como demuestran los hitos evolutivos, las naciones que lideran el sector, como Estados Unidos, Israel y los miembros de la OTAN, pasaron a tratar el *big data* como un repositorio estático a transformarlo en un activo dinámico de conciencia situacional (Nato, 2021). Este cambio requirió consolidar infraestructuras informáticas resilientes y, fundamentalmente, formar un capital humano capaz de operar en la intersección de la ciencia de datos y la táctica militar (Scharre, 2023).

La Tabla 1 resume las principales estrategias de estas potencias y ofrece una visión comparativa de los enfoques que consolidaron los datos, como el nuevo centro de gravedad de la defensa global.

**Tabla 1 – Programas y estrategias de defensa internacional con el uso de *big data* e inteligencia artificial**

| País/ organización (Año) | Proyecto/programa | Foco principal | Resultados operacionales | Ref. |
|---|---|---|---|---|
| Estados Unidos (DARPA) (2017) | Mosaic Warfare | Integración IA + sensores | Reducción del tiempo de decisión en el campo | (Gunning; Aha, 2019) |
| Israel (2019) | Sistemas de frontera inteligentes | Reconocimiento de patrones | Detección temprana de amenazas terroristas | (Strat, 2023) |
| Otan (2021) | Estrategia de IA | Ciberseguridad y operaciones multidominio | Estándares éticos e interoperabilidad | (Nato, 2021) |

**Fuente:** Elaborada por el autor.

Actualmente, el estado del arte converge en la data-centric warfare8, en que la superioridad militar ya no se mide solo por la potencia de fuego cinética, sino por la superioridad de decisión (Amirolshah, 2024). El ciclo OODA (Observar, Orientar, Decidir, Actuar) se acelera artificialmente al permitir al defensor neutralizar las amenazas incluso antes de materializarlas físicamente (Priambodo et al., 2022). El desafío contemporáneo radica en proteger la integridad de estos datos; los ataques de envenenamiento de datos (data poisoning), destinados a corromper el aprendizaje de la IA enemiga, emergen como la nueva frontera de la contrainteligencia digital (Schmidt, 2023).

En contraste con la madurez observada en los *benchmarks* globales, Brasil aún enfrenta desafíos en la articulación de sus capacidades y en la continuidad de las inversiones (Medeiros; Gualberto, 2025). El análisis comparativo sugiere que el progreso nacional depende de la transición de las adopciones puntuales a una estrategia nacional integrada, compatible con las especificidades geopolíticas del país.

### 3.2 El escenario brasileño

En Brasil, la incorporación de tecnologías basadas en datos en la defensa nacional refleja un esfuerzo de modernización estructural, aunque todavía marcado por una implementación fragmentada (Soares, 2015). El principal exponente de esta transición es el Sistema Integrado de Monitoreo de Fronteras (Sisfron) (Andrade; Lima, 2018). Concebido como una arquitectura de sensores y comunicaciones estratégicas, Sisfron representa el mayor desafío nacional de *big data*: la necesidad de integrar flujos heterogéneos de datos terrestres y orbitales para generar conciencia situacional en tiempo real a lo largo de 16.000 kilómetros de frontera (Andrade, 2025).

En el campo de la ciberdefensa, el trabajo del Centro de Ciberdefensa (CDCiber) y la formulación de la Estrategia Brasileña de Inteligencia Artificial (Ebia) señalan el reconocimiento de la IA como una tecnología con doble propósito (*dual-use*) (Barboza; Ferneda; Cristóvam, 2023). El Ejército Brasileño, mediante directrices estratégicas, busca aplicar el aprendizaje automático en la protección de las infraestructuras críticas y en la anticipación a las amenazas híbridas (Bonanno, 2025). Sin embargo, la madurez de estos sistemas en Brasil todavía se considera intermedia en comparación con *benchamarks* internacionales (Estados Unidos e Israel), debido a tres marcos fundamentales (Scharre, 2023):

- Fragmentación de silos: la ausencia de interoperabilidad total entre las bases de datos de la Armada, del Ejército y de la Fuerza Aérea dificulta la creación de un ecosistema de inteligencia conjunto (Brasil, 2025b).
- Dependencia tecnológica: el predominio de componentes y algoritmos extranjeros, que muchas veces operan como "cajas negras" (black boxes), impone riesgos para la soberanía digital y limita la auditoría nacional de los procesos de toma de decisiones (Polido, 2024).
- Continuidad presupuestaria: el carácter plurianual de los proyectos de IA y big data colisiona con las restricciones financieras y genera brechas de actualización que favorecen la obsolescencia tecnológica (Azevedo; Borba; Araújo, 2021).

8 ***Data-centric warfare***: paradigma militar contemporáneo que establece los datos como un elemento central de la superioridad operativa.

Por lo tanto, el escenario brasileño se caracteriza por una base doctrinal robusta, expresada en la Estrategia Nacional de Defensa aunque carece de una ejecución sistémica (Dalbosco; Cortinhas, 2024). El fortalecimiento de las capacidades nacionales depende de la transición al desarrollo de tecnologías autóctonas[9], capaces de garantizar que la autonomía de toma de decisiones del Estado brasileño no se vea comprometida por la dependencia de infraestructuras externas en tiempos de crisis (Brasil, 2024; Gomes, 2024).

A partir de la confrontación entre los *benchmarks* internacionales y la realidad brasileña descrita anteriormente, existe una brecha funcional que trasciende la tecnología. Si bien las potencias globales operan bajo el paradigma de la superioridad de decisión, Brasil aún consolida su conciencia situacional (Nato, 2021). Para superar esta barrera, el análisis documental sugiere que el país debe evolucionar de sistemas de estantería a arquitecturas de datos integradas (Scharre, 2023). La Tabla 3 resume los principales obstáculos identificados y las respectivas recomendaciones estratégicas para la defensa nacional.

## 4. RESULTADOS Y DISCUSIONES

### 4.1 Aplicaciones estratégicas en la defensa nacional brasileña

La incorporación de tecnologías basadas en datos e IA en la defensa nacional representa un cambio de paradigma en la forma en que se monitorean y neutralizan las amenazas multidimensionales (Cummings, 2017; Stiles; Netessine, 2025). En el contexto brasileño marcado por una gran extensión territorial y complejidad geoestratégica, estas herramientas reducen las asimetrías operativas en escenarios difíciles de monitorear, como la Amazonía Legal y la "Amazonía Azul" (Figueiredo, 2025).

Aunque iniciativas como Sisfron (Oliveira; Farias, 2023), CDCiber (Brasil, 2023) y Enia (Brasil, 2025a) demuestran vigor institucional, los datos revelan que estas aún operan en etapas intermedias de integración. El análisis revela la persistencia de brechas en la interoperabilidad y escalabilidad, esenciales para la transición de la vigilancia pasiva a la defensa proactiva.

#### *4.1.1 Vigilancia y detección de fronteras*

En el ámbito de Sisfron, el análisis señala que el sistema ha evolucionado en la capacidad de "ver" la frontera, pero aún anda a tientas en la capacidad de "anticipar" eventos (Oliveira; Farias, 2023). La expansión que sugiere este estudio implica la implementación de modelos de visión por computadora10

9 **Tecnologías autóctonas**: se refieren al conjunto de conocimientos, procesos y herramientas plenamente desarrollados dentro de las fronteras nacionales mediante el uso de sus propias capacidades científicas e industriales. En el sector de la defensa, la autonomía tecnológica se considera un activo estratégico, ya que reduce la dependencia de proveedores extranjeros y mitiga las vulnerabilidades relacionadas con embargos, tecnologías o restricciones de uso impuestas por terceros.

10 **Visión por computadora**: un campo interdisciplinario de la inteligencia artificial que desarrolla técnicas algorítmicas para permitir que las computadoras y los sistemas extraigan información significativa, identifiquen patrones y comprendan el contenido de imágenes digitales, videos u otras entradas visuales. A diferencia del procesamiento simple de imágenes, la visión por computadora busca la interpretación semántica de la escena para la toma de decisiones automatizada.

y deep learning directamente en la "punta" (edge AI11) (Zhou et al., 2019). Al proporcionar drones y sensores de tierra con capacidad de procesamiento autónomo, se reduce la sobrecarga de los centros C2 y permite solo reportar anomalías críticas (Silva, 2024). Esto es vital para combatir la delincuencia transnacional, en que la ventana de oportunidad para la interceptación es extremadamente pequeña.

#### *4.1.2 Ciberdefensa y la resiliencia de las infraestructuras*

La discusión sobre la defensa cibernética revela que CDCiber opera en un escenario de guerra asimétrica constante (Brasil, 2023). La expansión de esta capacidad requiere el uso de IA para detectar Amenazas Persistentes Avanzadas (APT), que imitan los comportamientos legítimos de los usuarios (Mohamed, 2024). El análisis documental sugiere que la protección de las redes gubernamentales brasileñas depende de la creación de un "escudo inteligente" capaz de correlacionar eventos en milisegundos, una tarea imposible para los operadores humanos sin la ayuda de *big data* analítico (Wang; Jones, 2017).

### 4.2 El dilema de la soberanía digital y las tecnologías autóctonas

Un punto crítico que surge de la discusión es la vulnerabilidad de la dependencia. Al utilizar soluciones de estantería (*off-the-shelf*) de potencias extranjeras, Brasil incurre en el riesgo de "cajas negras" algorítmicas (González; Ferreira, 2020). En un escenario de conflicto, el acceso a estos sistemas o actualizaciones de seguridad puede revocarse, lo cual paraliza las capacidades de defensa nacional. Por lo tanto, la soberanía digital no es solo un concepto retórico, sino una necesidad operativa.

La promoción de la Base Industrial de Defensa (BID) para la creación de algoritmos nacionales se configura como una vía estratégica para asegurar la *accountability*[12] y la XAI de las decisiones militares (Gunning; AHA, 2019). Sin dominar el código fuente, el Estado brasileño no tiene pleno control sobre los criterios que llevan a una IA a clasificar un objetivo o una amenaza, lo que plantea graves implicaciones éticas y legales bajo la égida del derecho internacional de los conflictos armados (Medeiros; Álvarez, 2026).

#### *4.2.1 La ética del "human-in-the-loop"*

La expansión de la discusión ética es obligatoria. Este estudio refuerza que la IA en la defensa brasileña debe seguir el principio del ser humano en el ciclo de decisión (Batista *et al.*, 2025). Si bien la máquina puede procesar miles de millones de datos para identificar un patrón de ataque, la decisión final de participación debe ser humana. Esto mitiga el riesgo de errores algorítmicos derivados de *datasets*[13]

11 ***Edge AI*** (IA en el borde): paradigma computacional que consiste en implementar algoritmos de IA directamente en dispositivos locales (sensores, cámaras, drones), ubicados en el "borde" de la red.

12 ***Accountability***: se refiere a la capacidad de asignar responsabilidad por los resultados producidos por los sistemas automatizados. En los escenarios de machine learning caja negra, la accountability requiere que los desarrolladores y operadores puedan auditar y explicar el comportamiento del sistema, lo cual asegura que las decisiones de IA cumplan con los estándares éticos y legales.

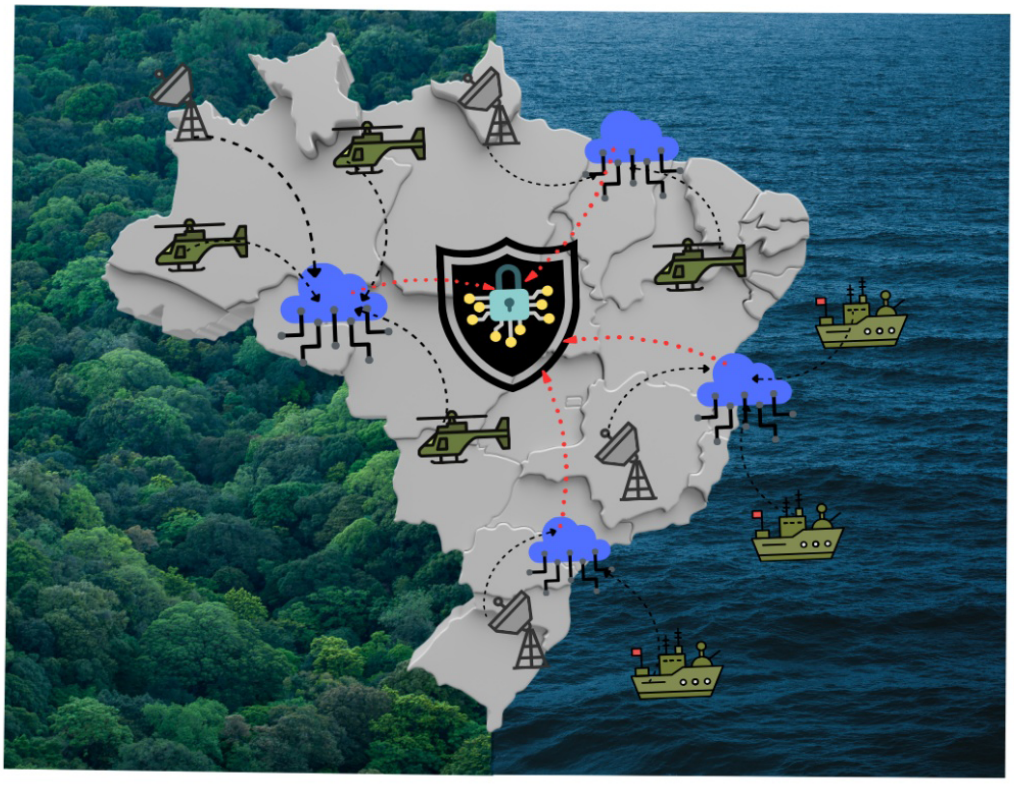
13 ***Datasets*** (conjuntos de datos): colecciones estructuradas de información relacionada que sirven como base para capacitar, validar y probar algoritmos de machine learning.

sesgados y garantiza la responsabilidad legal por actos de fuerza (Rojas-Contreras; Orjuela Duarte; Santos Jaimes, 2025).

### *4.2.2 Síntesis de recomendaciones estratégicas*

En general, la aplicación de *big data* e IA en el contexto brasileño revela un alto potencial para la consolidación de las capacidades de defensa nacional. Sin embargo, el impacto estratégico de estas tecnologías está condicionado por la capacidad de integración interfuerzas, por la continuidad presupuestaria de los proyectos y por la consolidación de una doctrina de datos soberanos (Brasil, 2024). La Figura 3 resume espacialmente las principales áreas de aplicación y destaca las regiones estratégicas y los vectores tecnológicos asociados.

**Figura 3 – Vectores de *big data* e inteligencia artificial en la defensa nacional brasileña**



**Leyenda:** los iconos de helicópteros representan la vigilancia aérea; los buques indican el monitoreo marítimo; las antenas simbolizan los sistemas de comunicación y radar; las nubes conectadas representan el procesamiento de datos en entornos de big data e IA; y el escudo central indica la integración de la información con un enfoque en la ciberseguridad y la defensa estratégica.
**Fuente:** Elaborada por el autor.

Más que una representación descriptiva, la Figura 3 muestra la distribución espacial de los desafíos y de las capacidades necesarias para su mitigación.

La distribución de los elementos visuales en el mapa se definió en función de criterios estratégicos, que incluyen: (a) áreas de mayor extensión territorial y dificultad de monitoreo, como la Amazonía Legal; (b) regiones con una alta incidencia de actos ilícitos transnacionales, como el tráfico de drogas y el contrabando en zonas fronterizas; (c) áreas marítimas de interés económico y geopolítico, especialmente relacionadas con la explotación de recursos naturales; y (d) puntos críticos de infraestructura sensible, sujetos a riesgos cibernéticos y operativos.

En este contexto, la presencia de sensores, plataformas aéreas y sistemas navales en estas regiones no representa posiciones reales específicas, sino una abstracción conceptual basada en parámetros estratégicos de vigilancia, riesgo y relevancia operativa.

La inclusión de helicópteros, buques militares y sensores remotos representa la articulación entre los mecanismos de vigilancia aérea, terrestre y marítima, mientras que el emblema central, adornado con un candado digital, simboliza la ciberseguridad y la concentración de información estratégica. Las interacciones entre nubes y sensores resaltan el flujo ininterrumpido de datos analizados por los sistemas predictivos, lo cual destaca la capacidad de estas tecnologías para predecir amenazas, mejorar la asignación de recursos y fortalecer la soberanía nacional.

La Tabla 2 complementa este análisis al sistematizar, de manera estructurada, las principales áreas de aplicación de estas tecnologías en Brasil y detalla los recursos tecnológicos utilizados y los beneficios estratégicos asociados.

**Tabla 2 – Aplicaciones potenciales de *big data* e inteligencia artificial en la defensa nacional brasileña**

| Área | Tecnologías involucradas | Beneficios esperados |
|---|---|---|
| Monitoreo fronterizo | Sensores remotos (satélites, drones, radares) + IA (visión artificial, machine learning) | Detección temprana de actos ilícitos transnacionales y aumento de la vigilancia en zonas de difícil acceso |
| Ciberseguridad | Big data + algoritmos predictivos (machine learning /deep learning) + sistemas de detección de intrusiones | Prevención y mitigación de ataques a infraestructuras críticas y redes gubernamentales |
| Operaciones militares de campo | IA integrada + integración multiplataforma + análisis en tiempo real | Apoyar la toma de decisiones tácticas, aumentar la protección de las tropas y optimizar el uso de los recursos |

**Fuente:** Elaborada por el autor.

La incorporación de tecnologías basadas en datos e IA en la defensa nacional no solo amplía la capacidad de respuesta, sino que redefine la lógica de acción de las Fuerzas Armadas al permitir decisiones basadas en una inteligencia continua e integrada (Brasil, 2024). En este sentido, el progreso brasileño en esta área depende de la construcción de un ecosistema tecnológico robusto, capaz de sostener análisis a gran escala, interoperabilidad entre sistemas y autonomía estratégica (Brasil, 2025a).

### 4.3 Desafíos y barreras estructurales

La implementación de tecnologías basadas en datos e IA en la defensa nacional brasileña enfrenta desafíos que trascienden la dimensión técnica al involucrar limitaciones institucionales, dependencia externa y brechas regulatorias. Estos obstáculos forman un cuello de botella complejo que impide la transición completa a una defensa basada en la inteligencia predictiva (Brasil, 2025a).

#### *4.3.1 Infraestructura y fragmentación sistémica*

Uno de los principales obstáculos radica en la infraestructura tecnológica. La adopción de sistemas analíticos avanzados requiere una potencia computacional escalable y una continua integración en plataformas heterogéneas. Actualmente, la fragmentación de los sistemas existentes y la limitación de las inversiones comprometen el procesamiento a gran escala y reduce la efectividad de las soluciones para apoyar la toma de decisiones estratégicas (Brasil, 2025a).

#### *4.3.2 El dilema de la soberanía digital*

La dependencia de tecnologías extranjeras expone al país a vulnerabilidades críticas, como el riesgo de acceso indebido a datos confidenciales o la interrupción de servicios esenciales ante escenarios de crisis geopolítica. El desarrollo de capacidades autóctonas, que abarcan *software*, *hardware* y modelos analíticos propietarios, es imperativo para la autonomía estratégica. Sin el dominio de las tecnologías nacionales, el Estado sigue sujeto a decisiones de proveedores externos que pueden no alinearse con los intereses de la soberanía nacional (Polido, 2024).

#### *4.3.3 Ética, gobernanza y capital humano*

El tratamiento de grandes volúmenes de datos en el sector de la defensa cumple la estricta Ley General de Protección de Datos (LGPD) y exige transparencia y responsabilidad algorítmica. Al mismo tiempo, el uso de sistemas autónomos impone dilemas de *accountability* y redefine los límites operativos de las decisiones automatizadas, lo cual requiere una clara supervisión humana (Brasil, 2018).

Además, la escasez de profesionales cualificados representa un factor limitante crítico. La formación de especialistas que dominen simultáneamente la ciencia de datos y la doctrina de defensa requiere una profunda articulación entre las universidades, los centros de investigación y las instituciones militares para el desarrollo del capital humano especializado (Araujo; Mendes, 2025). La Tabla 3 resume la matriz de riesgos identificada y las respectivas recomendaciones para mitigar estas brechas.

**Tabla 3 – Desafíos versus posibles soluciones en Brasil**

| Categoría analítica | Desafío identificado (hiatos) | Recomendación estratégica (soluciones técnicas) |
|---|---|---|
| Inteligencia y conciencia situacional | Silos de datos: fragmentación de la información entre Armada, Ejército y Aeronáutica impidiendo una visión holística | Implementación de Arquitecturas Joint All-Domain (JADC2) para garantizar la interoperabilidad nativa y el flujo de datos en tiempo real entre las fuerzas |
| | Latencia decisional: exceso de datos brutos sin procesar en la "punta"(edge) sobrecargando los centros de mando | Adopción de edge computing e IA on the edge para el procesamiento local en drones y sensores, enviando solo inteligencia refinada para el mando |
| Resiliencia y soberanía | Dependencia tecnológica (black box): uso de algoritmos propietarios extranjeros que limitan la autonomía y crean vulnerabilidades | Promoción de la BID con un enfoque en Open Source Intelligence (OSINT) y algoritmos de auditoría nacional para garantizar la soberanía digital |
| | Vulnerabilidad de modelos: riesgos de ataques adversarios que pueden "engañar" a la IA de reconocimiento de objetivos | Desarrollo de protocolos de robustness testing y red teaming específicos para sistemas de IA militar |
| Gobernanza e integración | Falta de talento híbrido: escasez de personal militar con experiencia en ciencia de datos y civiles con una comprensión de la doctrina de defensa. | Creación de carreras tecnológicas estatales y alianzas público-privadas para el desarrollo de centros de excelencia en IA y defensa |
| | Discontinuidad presupuestaria: proyectos a largo plazo (como Sisfron) sujetos a restricciones que generan obsolescencia técnica | Establecimiento de fondos del sector de defensa blindada y alineación con la Estrategia Nacional de Inteligencia Artificial (EB) |

**Fuente:** Elaborada por el autor.

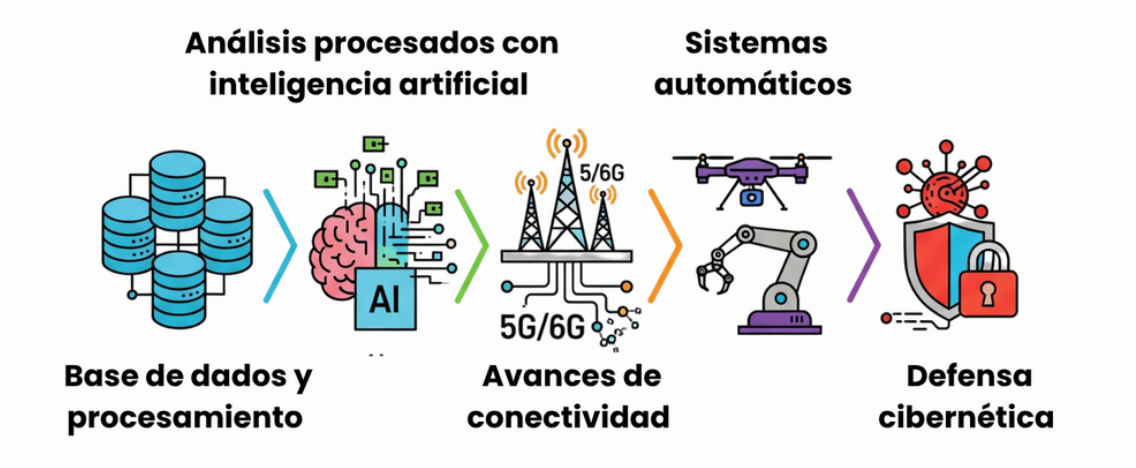
Mitigar estas brechas requiere una coordinación sistémica que vaya más allá de la simple adquisición de herramientas ya disponibles, lo cual exige la promoción de tecnologías desarrolladas internamente. En última instancia, la integración de *big data* e IA en el teatro de operaciones brasileño deja de ser una opción para la modernización y se convierte en un imperativo estratégico de supervivencia en un escenario de guerra centrada en los datos (*data-centric warfare*) (Magnuson, 2018).

### *4.4. Perspectivas de futuro*

La consolidación de una defensa nacional basada en datos depende de la formulación de estrategias a largo plazo que articulen la innovación disruptiva, la autonomía soberana y la solidez institucional. En este contexto, la creación de centros nacionales de análisis predictivo surge como una iniciativa estructuradora (Silva, 2025). Diseñados como centros de excelencia, estos centros deben operar en un régimen de triple hélice (universidades, instituciones militares y sector privado), los cuales favorecen la convergencia entre la investigación aplicada y las demandas operativas inmediatas del teatro de operaciones (Brasil, 2025a).

Las tendencias mundiales muestran una profunda integración entre la IA y las tecnologías de conectividad emergentes. La Figura 4 presenta *roadmap* estratégica necesaria para esta evolución, basada en la transición de sistemas aislados a una arquitectura multiplataforma altamente conectada.

**Figura 4 – *Roadmap* futura de la defensa nacional con integración de *big data*, inteligencia artificial y tecnologías emergentes**




**Fuente:** Elaborada por el autor.

Como se ilustra anteriormente, el avance en este ámbito está directamente asociado con el fortalecimiento de las capacidades nacionales en análisis de datos, IA e infraestructura digital, combinado con inversiones continuas en investigación aplicada e innovación. Esta trayectoria apunta a la transición de un modelo reactivo a una lógica de acción predictiva e integrada.

Otra tendencia relevante se refiere al avance de la IA explicable (XAI), que permite una mayor transparencia en los procesos de toma de decisiones automáticas (Gunning; Aha, 2019). La adopción de modelos interpretables se vuelve especialmente crítica en contextos militares, en los que la fiabilidad y la auditabilidad de las decisiones son requisitos fundamentales (Wang; Jones, 2017).

Además, la convergencia con tecnologías como 5G/6G, internet de las cosas y computación cuántica tiende a aumentar significativamente la capacidad de procesamiento, conectividad y seguridad de los sistemas de defensa, lo cual permite operaciones más ágiles, distribuidas y resilientes (Goodfellow *et al.*, 2016).

### *4.4.1 Innovación abierta y soberanía tecnológica*

El fortalecimiento de las alianzas estratégicas internacionales puede acelerar el desarrollo de estas capacidades, siempre que vaya acompañado de políticas orientadas a proteger la soberanía tecnológica. En esta dirección, la articulación entre la cooperación internacional y el desarrollo interno constituye un eje central para consolidar un ecosistema nacional robusto y sostenible en defensa (Brasil, 2025a; Dalbosco; Cortinhas, 2024).

La innovación tecnológica es un vector central para consolidar estas perspectivas de futuro, lo cual requiere no solo la adopción de tecnologías emergentes, sino el desarrollo de soluciones adaptadas a las especificidades operativas de la defensa nacional (Assur, 2024). En esa dirección, las iniciativas dirigidas a la innovación abierta, al fomento de *startups*[14] de base tecnológica y a la creación de entornos de experimentación, como *sandboxes*[15] regulatorios y laboratorios de prototipado, pueden acelerar la transición entre la investigación y la aplicación práctica (Assur, 2024). Además, la promoción de estudios interdisciplinarios y la transferencia de tecnología entre la academia, el sector productivo y las instituciones militares son esenciales para reducir la brecha entre el desarrollo científico y la implementación operativa, lo cual fortalece la capacidad del país para generar soluciones innovadoras con un impacto directo en la seguridad y la soberanía nacional.

## 5. CONCLUSIÓN

La aplicación estratégica de tecnologías basadas en datos e IA representa una transformación estructural en la lógica de acción de la defensa nacional al permitir no solo la identificación temprana de amenazas, sino la construcción de capacidades predictivas y adaptativas ante escenarios operativos complejos.

Desde una perspectiva teórico-conceptual, la integración de estas tecnologías forma parte del paradigma contemporáneo de la guerra de la información y la defensa basada en datos (*data-driven defense*), en el que la ventaja estratégica se deriva de la capacidad de transformar flujos masivos de datos en inteligencia procesable en tiempo real.

La experiencia internacional muestra que estas capacidades ya se consolidaron como elementos centrales en los sistemas de defensa contemporáneos al reforzar la necesidad de Brasil de avanzar en la construcción de estructuras integradas y autónomas. Sin embargo, el análisis del contexto nacional muestra que el país aún se encuentra en una etapa intermedia, marcada por iniciativas fragmentadas, limitaciones de integración sistémica y dependencia tecnológica externa en áreas críticas, especialmente en el dominio cibernético y en la infraestructura estratégica de datos.

Para superar estas limitaciones, es necesario enfrentar desafíos relacionados con la infraestructura tecnológica, la soberanía digital, la gobernanza ética y la formación de recursos humanos especializados. En esta dirección, la creación de centros nacionales de análisis predictivo, el avance en inteligencia artificial explicable y la consolidación de políticas integradas de ciberdefensa son caminos estratégicos para fortalecer la capacidad nacional. Además, la articulación entre la innovación tecnológica, la cooperación institucional y el desarrollo de capacidades internas será decisiva para la construcción de un ecosistema de defensa basado en datos.

Ante este escenario, se concluye que la implementación coordinada de estas tecnologías debe tratarse como una prioridad estratégica no solo para aumentar la capacidad de respuesta, sino

14 ***Startups***: son empresas emergentes, generalmente de base tecnológica, caracterizadas por el desarrollo de soluciones innovadoras en condiciones de alta incertidumbre, con potencial de crecimiento acelerado y con foco en la creación de nuevos productos, servicios o modelos de negocio escalables.

15 ***Sandboxes***: son entornos de prueba controlados en los que se pueden desarrollar y evaluar nuevas tecnologías, productos o servicios bajo la supervisión de las autoridades reguladoras, con flexibilización temporal de las normas, lo cual permite una experimentación segura antes de su implementación a gran escala.

para asegurar la autonomía de la toma de decisiones y la competitividad en el escenario internacional. Este avance, sin embargo, depende de la consolidación de una estrategia nacional integrada, capaz de alinear las dimensiones tecnológicas, operativas e institucionales de manera coherente y sostenible.

Finalmente, la ausencia de este movimiento tiende a aumentar la vulnerabilidad estratégica del país a las amenazas emergentes, lo cual demuestra que la inversión estructurada en tecnologías basadas en datos ya no es una opción y se volvió una necesidad estratégica para la defensa nacional. Más que un desafío tecnológico, es un problema estructural de coordinación, integración y gobernanza de datos en el ámbito de la defensa nacional.

## Agradecimientos

Consejo Nacional de Desarrollo Científico y Tecnológico. Proceso: 302742/2022-0.

Coordinación del Perfeccionamiento de Personal de Nivel Superior. Proceso: 88887.613955/2021-00

Coordinación del Perfeccionamiento de Personal de Nivel Superior. Proceso: PROCAD 16/2020

Fundación de Apoyo a la Investigación del Estado de São Paulo. Proceso: 2025/04394-0

## REFERENCIAS

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. Disponible en: https://comum.rcaap.pt/bitstreams/d037aae5-80a2-4721-a214-32194903b510/download. Acceso el: 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. Disponible en: https://repositorio.marinha.mil.br/bitstream/ripcmb/847402/1/C-EMOS2024_CC_ASSUR.pdf. Acceso el: 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. Disponible en: https://repositorio.esg.br/bitstream/123456789/2134/1/EA_CSSDC_2025_-_Beatriz_da_Mota_Bonanno.pdf. Acceso el: 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. Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acceso el: 21 abr. 2026.

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

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

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

BRASIL. Ministério da Defesa. **Política nacional de defesa e a estratégia nacional de defesa**. Brasília, DF: Ministério da Defesa, 2024. Disponible en: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acceso el: 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. Disponible en: https://repositorio.esg.br/handle/123456789/1951. Acceso el: 21 abr. 2026.

GONZALEZ, C. D. O.; FERREIRA, P. P. Anatomia de um sistema de inteligência artificial. **ComCiência**, Campinas, 20 set. 2020. Disponible en: https://www.comciencia.br/anatomia-de-um-sistema-de-inteligencia-artificial/. Acceso el: 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. ¿La ciudad en tiempo real? 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: e**thical concerns in an uncertain world. Santa Monica: Rand Corporation, 2020.

NATO. **Summary of the NATO artificial intelligence strategy.** Brussels: Nato, 2021. Disponible en: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy. Acceso el: 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. F**our 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. Disponible en: https://repositorio.esg.br/bitstream/123456789/1972/1/MARCUS%20ALBERT%20ALVES%20DA%20SILVA.pdf. Acceso el: 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. Disponible en: http://hdl.handle.net/20.500.11956/187326. Acceso el: 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.