ARTICLE DOI 10. 52781/cmm.a194

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

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

**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.

**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.

**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

**Received: Aug. 01, 2025**
**Approved: Apr. 09, 2026**

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

## 1. INTRODUCTION

Digitalization has significantly impacted defense and national security strategies, modifying conventional surveillance, safeguarding, and decision-making paradigms. The exponential increase in data from sensors, satellites, mobile devices, and cyber intelligence results in a highly complex informational ecosystem—often defined as big data[1] (Kitchin, 2021). In this scenario, artificial intelligence (AI)—particularly via machine learning algorithms and predictive analysis—acts as a central element in the conversion of massive data into strategic intelligence, finding patterns and the anticipating threats with great accuracy (Scharre, 2023).

In contemporary conflicts characterized by hybrid wars and transnational threats, the speed of information processing directly influences the response capacity and resilience of states (Scharre, 2023). Nations such as the United States, Israel, and members of the North Atlantic Treaty Organization (NATO) have consolidated integrated data architectures that can sustain surveillance systems and automated decision support in highly complex environments (NATO, 2021).

However, Brazil incorporates these technologies in a fragmented way, reflecting structural limitations beyond mere technological availability (Andrade; Lima, 2021). Although its territorial extension and border complexity impose severe operational demands, its challenges mainly stem from the absence of an integrated strategy that articulates infrastructure, data governance, and analytical capabilities (Araujo; Mendes, 2025). Obstacles related to external technological dependence, low digital sovereignty maturity, and scarce specialized human resources persist, factors that limit the internalization of AI in critical systems (Bonanno, 2025).

Thus, the central problem lies in its difficulty of structuring a robust national defense-applied ecosystem rather than in the adoption of isolated tools (Toni *et al*., 2025). Such limitation compromises Brazil's strategic autonomy and capacity to respond to crises. Thus, this study posits the following guiding question: How can the integration of big data and AI enhance Brazil's strategic national defense capabilities in threat prediction, cybersecurity, and decision-making support?

This study aims to analyze the role of big data and AI in strengthening national defense, especially regarding strategic applications and implementation challenges in Brazil. In addition to its descriptive analysis, this study hypothesized that Brazil faces a structural (rather than a strictly technological) obstacle to the consolidation of these capacities. It argues that the absence of an integrated architecture, weak interinstitutional governance, and external dependence compromise the conversion of data into operational intelligence. Thus, the problem Brazil faces involves systemic coordination and institutional maturity.

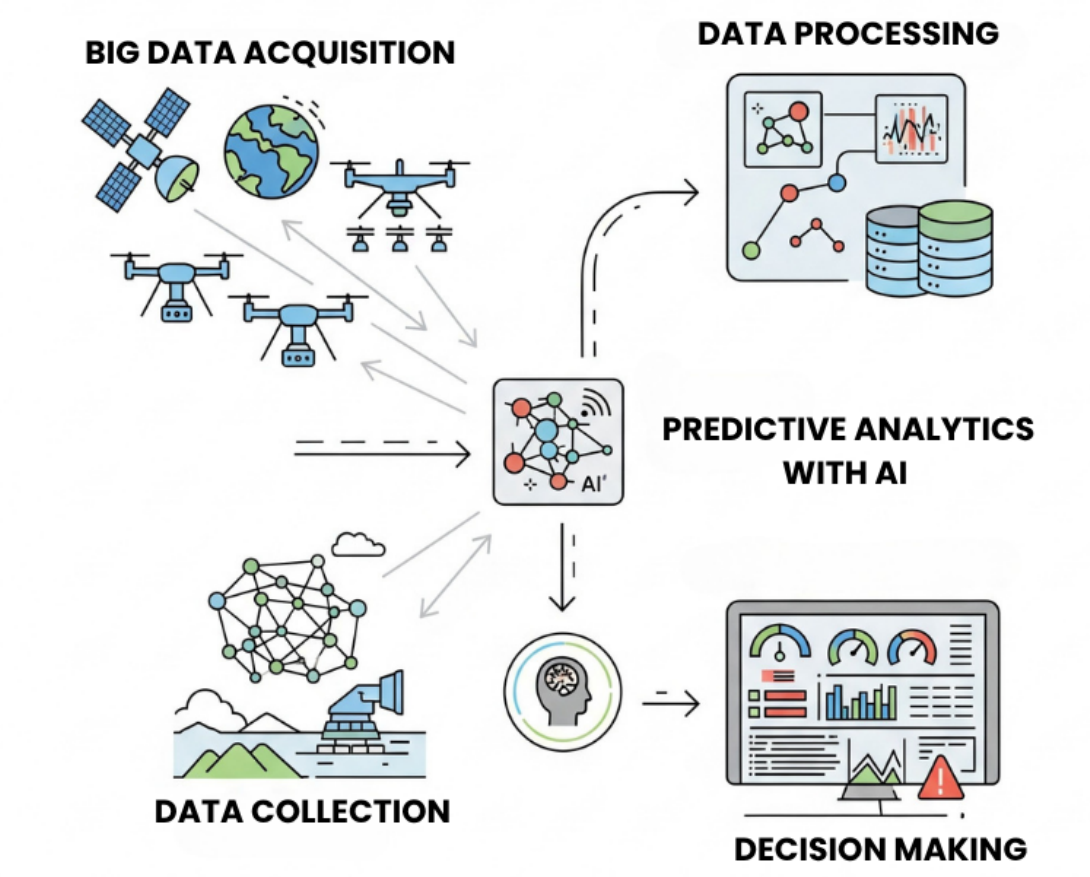
1 **Big data**: an ecosystem of computational infrastructure and advanced algorithms (such as distributed processing and machine learning) designed to capture, store, and analyze high-scale data that are too large for traditional relational database management systems.

This qualitative and exploratory study based itself on a structured bibliographic and documentary review that focused on the Brazilian scenario in relation to international benchmarks[2] (Sousa, 2024). Its analysis seeks to contribute to the debate on the modernization of defense by proposing the integration between data infrastructure and intelligent systems as a structuring axis of its contemporary strategic capacity.

The main contribution of this study lies in its proposition of an analytical framework that interprets the adoption of big data and AI in Brazil's national defense as a problem of systemic coordination and institutional maturity rather than merely as a technological limitation.

Figure 1 illustrates this systemic flow, evincing the integration of multimodal sources—such as satellites, remotely piloted aircraft, terrestrial sensors, and digital networks—and their subsequent assimilation by predictive algorithms. This chain enables the early detection of hostilities and the dynamic adaptation of operational responses under friction and uncertainty.

**Figure 1 — Flow of big data and artificial intelligence in national defense**




**Source:** Prepared by the author.

2 ***Benchmarks***: those used for systematic comparisons. In science, it serves as a normative basis for evaluating the performance, effectiveness, or quality of processes, systems, or results in relation to the best practices in the literature or in the market.

As in the flowchart above, predictive analyses in defense rely on the synergistic articulation between data infrastructure, computing capacity, and advanced analytical models. Such integration can support situational awareness in real time, redefining the decision-making logic by moving from a reactive model toward continuous prediction. This architecture directly contributes to the strengthening of Brazil's national sovereignty and the resilience of its critical infrastructures in the face of multidimensional threats.

## 2. METHODOLOGY

This qualitative and exploratory study was structured by a scoping review[3] and document analysis (Peterson *et al*., 2017). Its methodological design was planned to ensure the reproducibility of its collection and the rigor of its comparative analysis between the international scenario and the Brazilian reality. Its process was divided into three stages, indicated in the following subtopics.

### 2.1 Search strategy

Data mining was based on a systematic scan of scientific databases (such as Google Scholar, Scopus, and IEEE Xplore) and institutional defense repositories— including documents from NATO, the Defense Advanced Research Projects Agency, and the Brazilian Ministry of Defense. Documents published from 2015 to 2025 were chosen based on their thematic relevance, adherence to the scope of this study, and recurrence in scientific and institutional databases. Duplicates, non-peer-reviewed documents, or those that lacked a direct relationship with the object of analysis were excluded from this study. To retrieve the sources, combined descriptors in Portuguese and English were used, such as "*big data*," "*inteligência artificial*," "*defesa nacional*," and "*cybersecurity*." Publications from the last decade were prioritized in the chosen time frame to capture the acceleration of data-driven technologies and their operational and sovereign implications.

### 2.2 Analytical categorization

To avoid subjectivity in the interpretation, the selected content was filtered by three fundamental thematic axes:

- **Predictive intelligence and situational awareness**: monitoring applications and the reduction of operational uncertainty.
- **Cyber resilience and sovereignty**: protection of critical infrastructures and technological autonomy.

3 **Scoping review**: a synthesis of knowledge that aims to map the main concepts, sources, and evidence in a research area, especially when the topic is complex or yet to be comprehensively reviewed.

- **Governance and systemic integration**: interoperability challenges and long--term public policies.

### 2.3 Comparative analysis

The experiences of countries with a high degree of technological maturity (the United States, Israel, and NATO members) were used as benchmarks in the analytical-comparative approach of this research. This comparison of models found the available tools and the structural, institutional, and governance gaps that condition the implementation of these capabilities in Brazil's national defense.

## 3. DEVELOPMENT

In national defense, big data goes beyond mere bulk storage, referring to the strategic ability to structure and exploit heterogeneous data flows in high-volatility environments (Nie; Sun, 2016). The convergence of information from multiple domains—including remote sensing, autonomous systems, and cyber intelligence—can build an interconnected informational base (Kitchin, 2021). Data-driven defense redefines strategic superiority as the ability to convert this massive volume into actionable intelligence in near real-time, reducing uncertainty in dynamic operational scenarios (Wu *et al.*, 2022).

The contemporary literature emphasizes that transitioning to this model requires more than incorporating digital technologies; it demands the reconfiguration of organizational structures and governance mechanisms (NATO, 2021). In this context, military effectiveness no longer solely depends on conventional means, residing in the construction of institutional ecosystems that can sustain interoperability and interagency coordination (Morgan *et al.*, 2020). AI acts as the engine of this transformation, using machine[4] and deep learning[5] to automate screening and predictive analyses (Lecun; Bengio; Hinton, 2015).

The sophistication of deep learning introduced a paradigm shift in imagery intelligence (Zhang; Zhou; Luo, 2022). While traditional statistical algorithms relied on manually predefined parameters to find objects, convolutional neural networks[6] operate by multiple layers of processing that mimic human vision (Alzubaidi *et al.*, 2021). This architecture enables systems to autonomously learn and recognize complex patterns in drone videos and satellite

4 **Machine learning**: a subfield of AI that develops algorithms and statistical models that can find patterns and make inferences from data without the need for explicit programming instructions for each task. System performance is improved iteratively as it is exposed to new datasets.

5 **Deep learning**: subset of the machine learning based on artificial neural networks with multiple hidden processing layers. This architecture enables models to learn data representations with multiple levels of abstraction (in it, each layer transforms the input into a slightly more abstract and complex representation).

6 **Convolutional neural networks**: a class of deep learning algorithms designed to process data with a grid topology, such as images. Their architecture uses a mathematical operation called **convolution** instead of the conventional matrix multiplication in at least one of its layers, enabling the automatic extraction of spatial features (edges, textures, and shapes) via learning filters.

imagery, operating with minimal latency—essential for tracking moving targets in real time (Kiranyaz *et al*., 2019).

However, such processing capacity generates what the literature calls the "black box" effect[7], in which the logical path the machine took to reach a conclusion is opaque to human operators; hence the critical challenge of explainable AI in the theater of operations—which aims to translate complex mathematical models into intelligible representations (Gunning; Aha, 2019). On the battlefield, command confidence depends on the ability of an algorithm to provide an interpretable justification for its ratings (Scharre, 2023). In short, commanders authorizing the use of force requires that they understand the criteria that led AI to classify an object as a "threat" rather than as a civilian target, mitigating the risks of catastrophic collateral errors in lethal autonomous weapons systems (Grand-Clément, 2023; Wille, 2016).

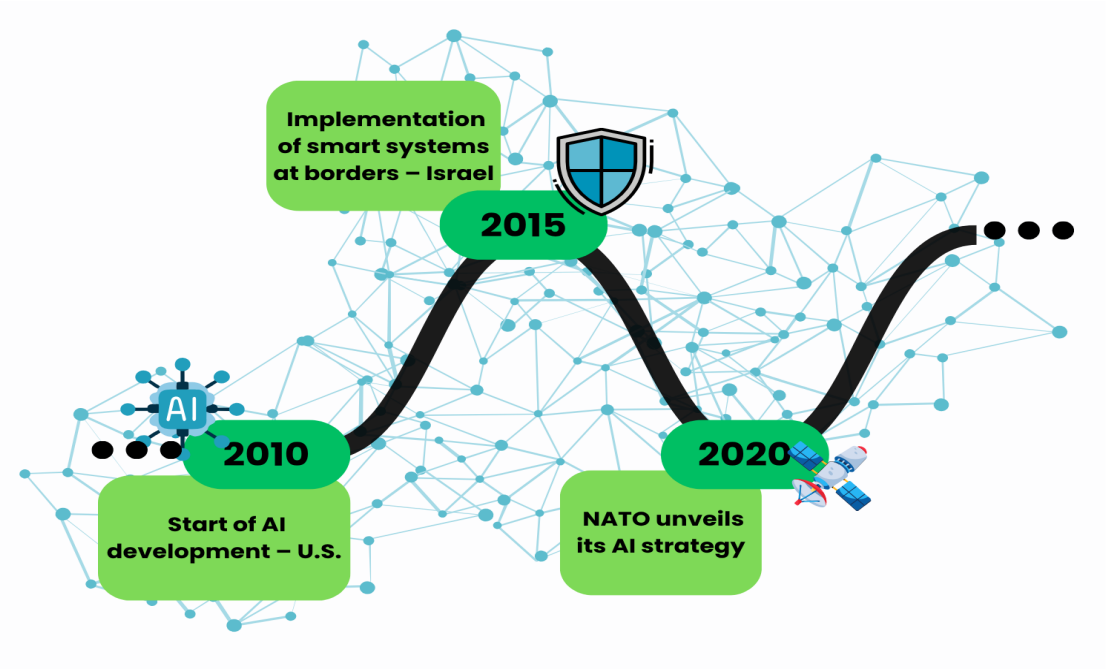
Abroad, the Defense Advanced Research Projects Agency Mosaic Warfare program exemplifies the use of distributed systems to amplify decision-making agility (Rokvić, 2025). The concept of Mosaic Warfare, although mentioned as an integration of sensors, represents an evolution in the command and control (Magnuson, 2018). Unlike monolithic and expensive systems, the "mosaic" uses AI to coordinate hundreds of small, inexpensive, disposable units (swarms of drones, low-cost sensors), creating a resilient and unpredictable defense system (Scharre, 2023). Such decentralization, supported by a distributed big data architecture, makes adversary war efforts ineffective due to the absence of single center of gravity to be attacked (Mcgarry; Saturno, 2020).

At the same time, NATO has led the movement for technological institutionalization with its AI strategy (2021), which focuses on ethical standardization and multi-domain interoperability (Christie; Ertan, 2021). Israel, in turn, stands out for its integration of proprietary algorithms into surveillance systems, which drastically reduced response time in counterterrorism operations (Scharre, 2023). In addition to cyberdefense, these technologies redefine logistics and tactical decision support, optimizing the use of resources in high-friction environments (Ofili; Ezeadi; Jegede, 2024).

Figure 2 illustrates the milestones of this global evolution, evincing the transition from purely reactive systems to proactive intelligence architectures (Kitchin, 2014). The technological game-changer included the increase in processing power and the ability to integrate intense data streams into contested combat environments (Lowrey, 2021). This trajectory shows that contemporary military superiority resides in kinetic force and in the speed of the decision cycle (NATO, 2021).

7 **Black box**: machine or deep learning systems (such as deep neural networks) that produce highly accurate results but the internal processes of decision and weighting of variables of which are too complex to be interpreted by humans.

**Figure 2 – International milestones for the adoption of big data and artificial intelligence in defense**




**Source:** Prepared by the author.

As per the evolutionary milestones, the nations that lead the sector—such as the United States, Israel, and NATO members—have stopped dealing with big data as a static repository, transforming it into a dynamic situational awareness asset (NATO, 2021). This shift required the consolidation of resilient computing infrastructures and, crucially, the formation of human capital who can operate at the intersection of data science and military tactics (Scharre, 2023).

Table 1 summarizes the main strategies of these powers, comparing the approaches that consolidated the data and the new center of gravity of global defense.

**Table 1 – International defense programs and strategies that use big data and artificial intelligence**

| Country/ Organization: (Year) | Project/program | Main focus | Operational results | Ref. |
|---|---|---|---|---|
| United States (Defense Advanced Research Projects Agency) (2017) | Mosaic Warfare | AI + sensor integration | Shorter decisions on the field | (Gunning; Aha, 2019) |
| Israel (2019) | Intelligent border systems | Pattern recognition | Early detection of terrorist threats | (Strat, 2023) |
| NATO (2021) | AI strategy | Cybersecurity and multi-domain operations | Ethical standards and interoperability | (NATO, 2021) |

**Source:** Prepared by the author.

Currently, the state of the art converges on data-centric warfare[8], which measures military superiority by kinetic firepower and decision superiority (Amirolshah, 2024). The observe, orient, decide, act loop is artificially accelerated, enabling defenders to neutralize threats before they even physically materialize (Priambodo *et al*., 2022). The contemporary challenge lies in protecting the integrity of this data. Data poisoning attacks aimed at corrupting enemy AI learning emerge as the new frontier of digital counterintelligence (Schmidt, 2023).

In contrast to the maturity in the global benchmarks, Brazil still faces challenges in articulating its capacities and continuing investments (Medeiros; Gualberto, 2025). The comparative analysis in this study suggests that the national progress depends on the transition from one-off adoptions to an integrated national strategy compatible with the geopolitical specificities of Brazil.

### 3.2 The Brazilian scenario

In Brazil, the incorporation of data-driven technologies into its national defense reflects an effort at structural modernization, although still marked by fragmented implementation (Soares, 2015). Its Integrated Border Monitoring System (SISFRON) configures the main exponent of this transition (Andrade; Lima, 2018). Conceived as a strategic sensor and communications architecture, SISFRON represents Brazil's greatest challenge in big data: the need to integrate heterogeneous terrestrial and orbital data flows to generate real-time situational awareness across 16,000 kilometers of border (Andrade, 2025).

In cyberdefense, the activities of the Center for Cyber Defense and the formulation of the Strategy for Artificial Intelligence signal the acknowledgement of AI as a dual-use technology (Barboza; Ferneda; Cristóvam, 2023). The Army strategic guidelines seek to apply machine learning to protect critical infrastructures and anticipate hybrid threats (Bonanno, 2025). However, the maturity of these systems in Brazil is still considered intermediate when compared to the benchmarks (United States and Israel) due to three fundamental gaps (Scharre, 2023):

- **Silo fragmentation**: the absence of full interoperability between the Navy, Army, and Air Force databases makes it difficult to create a joint intelligence ecosystem (Brasil, 2025b).
- **Technological dependence**: the predominance of foreign components and algorithms—often operating as "black boxes"—offers risks to digital sovereignty and limits the local auditing of decision-making processes (Polido, 2024).
- **Budget continuity**: the multiannual nature of AI and big data projects collides with financial contingencies, generating updating gaps that favor technological obsolescence (Azevedo; Borba; Araújo, 2021).

8 **Data-centric warfare**: a contemporary military paradigm that establishes the datum as a central element of operational superiority.

Thus, the Brazilian scenario shows a robust doctrinal foundation (expressed in its National Defense Strategy) that still lacks systemic implementation (Dalbosco; Cortinhas, 2024). Strengthening national capacities depends on the transition to the development of national technologies[9] that can ensure that the decision-making autonomy of the Brazilian State has no dependence on external infrastructures during crises (Brasil, 2024; Gomes, 2024).

Comparing the benchmarks and the Brazilian reality shows a functional gap that goes beyond technology. While global powers operate under the paradigm of decision-making superiority, Brazil is still consolidating its situational awareness (NATO, 2021). To overcome this barrier, the documentary analysis in this research suggests that it must evolve from rack systems to integrated data architectures (Scharre, 2023). Table 3 summarizes the main found obstacles and strategic recommendations for national defense.

## 4. RESULTS AND DISCUSSIONS

### 4.1 Strategic applications in Brazil's national defense

The incorporation of data-driven technologies and AI into national defense represents a paradigmatic shift in the way multidimensional threats are monitored and neutralized (Cummings, 2017; Stiles; Netessine, 2025). In Brazil (due to its vast territorial extension and geostrategic complexity), such tools reduce operational asymmetries in scenarios that are difficult to monitor, such as the Legal and "Blue" Amazons (Figueiredo, 2025).

Although initiatives such as SISFRON (Oliveira; Farias, 2023), the Center for Cyber Defense (Brasil, 2023), and the National Meeting on Artificial Intelligence (Brasil, 2025a) show institutional vigor, the data show that they still operate in intermediate stages of integration. The analysis indicates persistent gaps in interoperability and scalability, which are essential to transition from passive surveillance to proactive defense.

#### *4.1.1 Border surveillance and sensing*

The analysis in this study points out that SISFRON has evolved its ability to "watch" the border. However, it still has a tentative ability to "anticipate" events (Oliveira; Farias, 2023). The expansion suggested by this study involves implementing computer vision models[10] and deep

9 **National technologies**: the set of knowledge, processes, and tools developed entirely within national borders using its own scientific and industrial capacities. Defense considers technological autonomy a strategic asset as it reduces dependence on foreign suppliers and mitigates vulnerabilities related to embargoes, technologies, or restrictions on use from third parties.

10 **Computer vision**: an interdisciplinary field of AI that develops algorithmic techniques to enable computers and systems to extract meaningful information, find patterns, and understand the content of digital images, videos, or other visual inputs. Unlike simple image processing, computer vision seeks the semantic interpretation of scenes for automated decision-making.

learning directly at edge AI[11] (Zhou *et al.*, 2019). Providing drones and ground sensors with autonomous processing capabilities will reduce the overload of command and control centers as they will only report critical anomalies (Silva, 2024). This is vital for combating transnational crime due to its extremely small window of opportunity for interception.

*4.1.2 Cyber defense and infrastructure resilience*

The discussion on cyberdefense shows that the Center for Cyber Defense operates in a scenario of constant asymmetric warfare (Brasil, 2023). Expanding this capability requires AI for detecting advanced persistent threats that mimic legitimate user behaviors (Mohamed, 2024). The documentary analysis above suggests that the protection of Brazilian government networks depends on the creation of an "intelligent shield" that can correlate events in milliseconds—an impossible task for human operators without the aid of analytical big data (Wang; Jones, 2017).

## 4.2 The dilemma of digital sovereignty and indigenous technologies

A critical point that emerges from this discussion refers to dependency vulnerability since Brazil runs the risk of algorithmic "black boxes" when using rack solutions from foreign powers (Gonzalez; Ferreira, 2020). In conflicts, access to these systems or security updates can be revoked, crippling national defense capabilities. Thus, digital sovereignty constitutes an operational necessity rather than a rhetorical concept.

Promoting the Brazilian defense industrial base toward the creation of national algorithms configures a strategic way to ensure accountability[12] and the explainable AI of military decisions (Gunning; Aha, 2019). Without control of the source code, Brazil will lack full control over the criteria that lead AI to classify a target or a threat, raising serious ethical and legal implications under the aegis of the international law of armed conflict (Medeiros; Alvarez, 2026).

*4.2.1 "Human-in-the-loop" ethics*

The expansion of the ethical discussion is mandatory. This study reinforces that AI in Brazil's defense must follow the principle of humans in the decision cycle (Batista *et al.*, 2025). While the machine can process billions of data points to find an attack pattern, the final engagement decision must be human. This mitigates the risk of algorithmic errors from biased datasets[13]

11 **Edge AI**: computational paradigm that directly implements AI algorithms in local devices (sensors, cameras, drones) at the "edge" of a network.

12 **Accountability**: the ability to assign responsibility for the results from automated systems. In machine learning black boxes, accountability requires developers and operators to be able to audit and explain the behavior of a system, ensuring that AI decisions comply with ethical and legal standards.

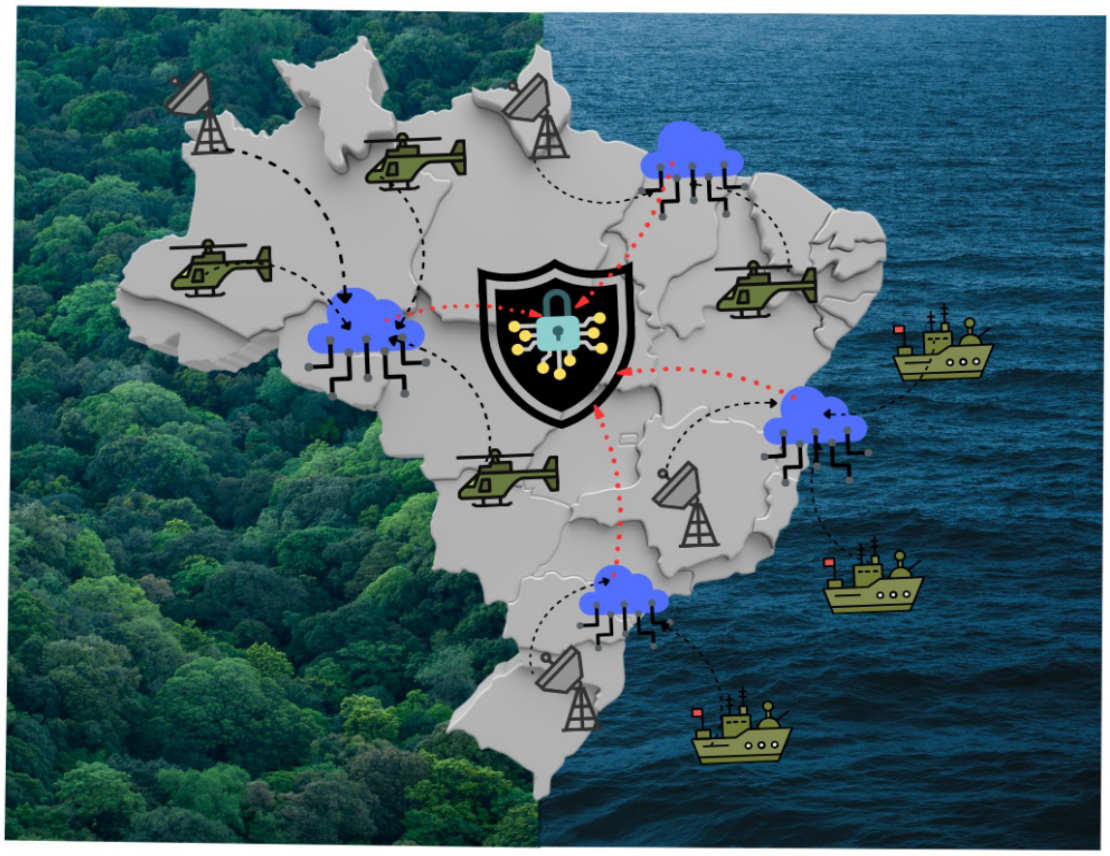
13 **Datasets**: structured sets of related information that serve as the basis to train, validate, and test machine learning algorithms.

and guarantees legal liability for acts of force (Rojas-Contreras; Orjuela Duarte; Santos Jaimes, 2025).

*4.2.2 Summary of policy recommendations*

In general, the application of big data and AI in Brazil shows a high potential for the densification of national defense capabilities. However, the strategic impact of these technologies follows the capacity for inter-force integration, the budgetary continuity of projects, and the consolidation of a sovereign data doctrine (Brasil, 2024). Figure 3 spatially summarizes the main application areas, highlighting strategic regions and the associated technological vectors.

**Figure 3 – Vectors of big data and artificial intelligence in Brazil's national defense**



**Legend:** Helicopter icons represent aerial surveillance, vessels indicate maritime monitoring, antennas symbolize communication and radar systems, connected clouds represent data processing in big data and AI environments, and the central shield indicates the integration of information with a focus on cybersecurity and strategic defense.
**Source:** Prepared by the author.

More than a descriptive representation, Figure 3 shows the spatial distribution of the challenges and the capacities necessary for their mitigation.

The distribution of the visual elements above followed strategic criteria, including (i) areas of greater territorial extension and monitoring difficulty (such as the Legal Amazon), (ii) regions with a high incidence of transnational crimes (such as drug trafficking and smuggling in border areas), (iii) maritime areas of economic and geopolitical interest (especially related to the exploitation of natural resources), and (iv) critical points of sensitive infrastructure (subject to cyber and operational risks).

The presence of sensors, aerial platforms, and naval systems in these regions represents no specific real placements but a conceptual abstraction based on strategic surveillance, risk, and operational relevance parameters.

The inclusion of helicopters, military vessels, and remote sensors represents the articulation between air, land, and maritime surveillance mechanisms, whereas the central emblem (adorned with a digital padlock) symbolizes cybersecurity and the concentration of strategic information. The interactions between clouds and sensors highlight the uninterrupted flow of data analyzed by predictive systems, highlighting the ability of these technologies to predict threats, improve resource allocation, and strengthen national sovereignty.

Table 2 complements this analysis by structurally systematizing the main application areas of these technologies in Brazil, detailing its technological resources and associated strategic benefits.

**Table 2 – Potential applications of big data and artificial intelligence in Brazil's national defense**

| Area | Involved technologies | Expected benefits |
|---|---|---|
| Border monitoring | Remote sensors (satellites, drones, radars) + AI (computer vision, machine learning) | Early detection of transnational crimes and increased surveillance in hard-to--reach areas |
| Cybersecurity | Big data + predictive algorithms (machine/deep learning) + intrusion detection systems | Preventing and mitigating attacks on critical infrastructure and government networks |
| Military field operations | Embedded AI + cross-platform integration + real-time analyses | Supporting tactical decision-making, increasing troop protection, and optimizing resource use |

**Source:** Prepared by the author.

The incorporation of data-driven technologies and AI in national defense expands response capacity and redefines the Armed Forces action logic by enabling decisions based on continuous and integrated intelligence (Brasil, 2024). Thus, Brazilian progress in this area depends on the construction of a robust technological ecosystem that can sustain large-scale analysis, interoperability between systems, and strategic autonomy (Brasil, 2025a).

### 4.3 Structural challenges and barriers

Implementing data- and AI-driven technologies in Brazil's national defense faces challenges that go beyond the technical dimension, involving institutional limitations, external dependence, and regulatory gaps. These obstacles form a complex bottleneck that prevents Brazil's full transition to a defense based on predictive intelligence (Brasil, 2025a).

#### *4.3.1 Infrastructure and systemic fragmentation*

One of the main obstacles lies in technological infrastructure. Adopting advanced analytical systems requires scalable computing capacity and seamless integration across heterogeneous platforms. Fragmented systems and limited investments compromise large-scale processing, reducing the effectiveness of solutions to support strategic decision making (Brasil, 2025a).

#### *4.3.2 The digital sovereignty dilemma*

Reliance on foreign technologies exposes Brazil to critical vulnerabilities, such as the risk of improper access to sensitive data or the disruption of essential services in geopolitical crises. Strategic autonomy requires the development of national capabilities (proprietary software, hardware, and analytical models). Without local technologies, Brazil remains subject to decisions by external suppliers, which may show no alignment with the interests of national sovereignty (Polido, 2024).

#### *4.3.3 Ethics, governance, and human capital*

The processing of large data volumes in defense enforces strict compliance with the Brazilian General Data Protection Law, which requires transparency and algorithmic accountability. The use of autonomous systems also imposes accountability dilemmas and redefines the operational limits of automated decisions, requiring clear human oversight (Brasil, 2018).

The shortage of trained professionals also represents a critical limiting factor. Training specialists who excel in data science and defense doctrine requires a deep articulation between universities, research centers, and military institutions for the development of specialized human capital (Araujo; Mendes, 2025). Table 3 summarizes the found risk matrix and recommendations for mitigating these gaps.

**Table 3 – Challenges *versus* possible solutions in Brazil**

| Analytical category | Found challenge (hiatuses) | Strategic recommendation (technical solutions) |
|---|---|---|
| Intelligence and situational awareness | **Data silos**: the fragmentation of information between the Navy, Army, and Air Force prevents a holistic view | Implementation of Joint All-Domain Command and Control Architectures to ensure native interoperability and real-time data flow between forces |
| | **Decisional latency**: excess raw data without edge processing overloads command centers | Adoption of edge computing and AI for local processing on drones and sensors, sending only fine-grained intelligence to the command |
| Resilience and sovereignty | **Technological dependence (black box)**: use of foreign proprietary algorithms limits autonomy and create vulnerabilities | Promotion of the defense industrial base, focusing on open-source intelligence and national audit algorithms to ensure digital sovereignty |
| | **Template vulnerability**: risks of adversarial attacks that can "fool" target recognition AI | Development of robustness testing and red teaming that are specific to military AI systems |
| Governance and integration | **Hybrid talent deficit**: Shortage of military personnel with a background in data science and civilians with an understanding of defense doctrine. | Creation of State technological careers and public-private partnerships for the development of AI and defense centers of excellence |
| | **Budget discontinuity**: long-term projects (such as SISFRON) suffer from contingencies that generate technical obsolescence | Establishment of armored defense sector funds and alignment with the National Artificial Intelligence Strategy |

**Source:** Prepared by the author.

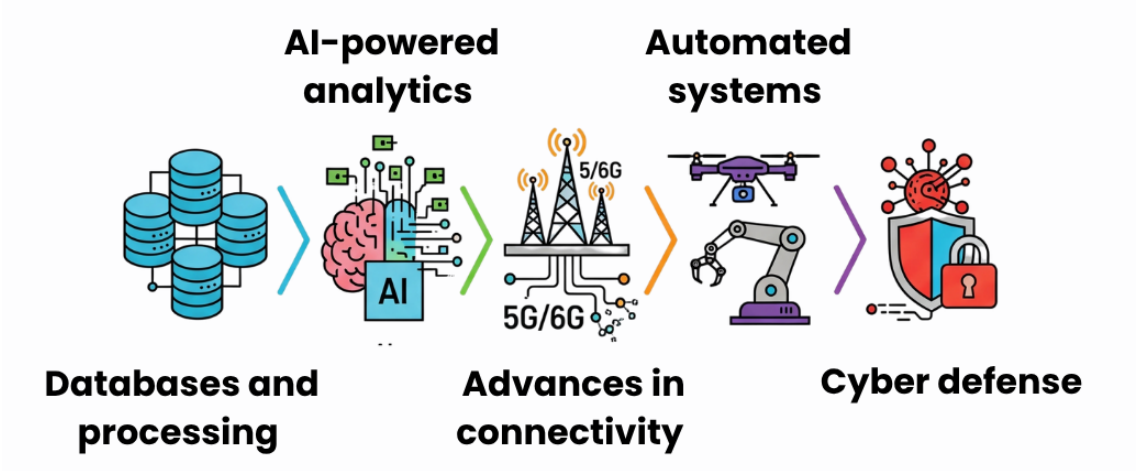
Mitigating these gaps requires systemic coordination that goes beyond acquiring ready-made tools, demanding the promotion of internally developed technologies. Ultimately, the integration of big data and AI in the Brazilian theater of operations no longer constitutes an option for modernization, becoming an imperative for its strategic survival in data-centric warfare (Magnuson, 2018).

### 4.4. Future perspectives

The consolidation of a data-driven national defense depends on Brazil formulating long-term strategies that articulate disruptive innovation, sovereign autonomy, and institutional robustness. The creation of national predictive analysis centers emerges as a structuring initiative in this context (Silva, 2025). These centers of excellence should operate in a triple helix regime (universities, military institutions, and the private sector), favoring the convergence between applied research and the immediate operational demands of the theater of operations (Brasil, 2025a).

Global trends indicate a deep integration between AI and emerging connectivity technologies. Figure 4 shows the strategic roadmap necessary for this evolution based on the transition from siloed systems to a highly connected multiplatform architecture.

**Figure 4 – Future roadmap of national defense with the integration of big data, artificial intelligence, and emerging technologies**




**Source:** Prepared by the author.

As illustrated, progress in this domain is directly associated with strengthening national capacities in data analysis, AI, and digital infrastructure and with continued investments in applied research and innovation. This trajectory points to the transition from a reactive model to a logic of predictive and integrated action.

Another relevant trend refers to furthering explainable AI, which enables greater transparency in automated decision-making processes (Gunning; Aha, 2019). The adoption of interpretable models becomes especially critical in military contexts, in which the reliability and auditability of decisions are fundamental requirements (Wang; Jones, 2017).

Moreover, convergence with technologies such as 5G/6G, the internet of things, and quantum computing tends to significantly expand the processing capacity, connectivity, and security of defense systems, enabling more agile, distributed, and resilient operations (Goodfellow *et al.*, 2016)

*4.4.1 Open innovation and technological sovereignty*

Strengthening strategic international partnerships can accelerate the development of these capabilities, as long as they are followed by policies to protect technological sovereignty. Thus, the articulation between international cooperation and internal development configures a central axis for the consolidation of a robust and sustainable national defense ecosystem (Brasil, 2025a; Dalbosco; Cortinhas, 2024).

Technological innovation constitutes a central vector to consolidate these future perspectives, requiring the adoption of emerging technologies and the development of solutions adapted to the operational specificities of Brazil's national defense (Assur, 2024). In this context, initiatives that target open innovation, encourage startups[14], and create environments for experimentation (such as regulatory sandboxes[15] and prototyping laboratories) can accelerate the transition between research and practical application (Assur, 2024). Moreover, stimulating interdisciplinary research and technology transfer between academia, the productive sector, and military institutions is essential to reduce the gap between scientific development and operational implementation, strengthening Brazil's capacity to generate innovative solutions that directly impact national security and sovereignty.

## 5. CONCLUSION

The strategic application of data- and AI-driven technologies represents a structural transformation in the Brazilian national defense logic as it can find threats early and construct predictive and adaptive capabilities in complex operational scenarios.

From a theoretical-conceptual perspective, the integration of these technologies belongs to the contemporary paradigm of information warfare and data-driven defense, in which strategic advantages stem from the ability to transform massive streams of data into real-time actionable intelligence.

International experiences show that these capabilities configure central elements in contemporary defense systems, reinforcing the need for Brazil to further the construction of integrated and autonomous structures. However, analyzing its national context shows that it remains at an intermediate stage that includes fragmented initiatives, limited systemic integration, and external technological dependence in critical areas, especially in the cyber domain and strategic data infrastructure.

Overcoming these limitations requires facing challenges in technological infrastructure, digital sovereignty, ethical governance, and specialized human resource training. Thus, creating national predictive analysis centers, advancing explainable artificial intelligence, and consolidating integrated cyberdefense policies constitute strategic paths to strengthen the Brazilian capacity. Moreover, the articulation between technological innovation, institutional cooperation, and internal capacity development will be decisive for the construction of a data-driven defense ecosystem.

The coordinated implementation of these technologies constitutes a strategic priority to expand response capacity and ensure decision-making autonomy and competitiveness in the

14 **Startups**: emerging (usually technology-based) companies that develop innovative solutions under great uncertainty that can accelerate growth and that focus on creating new products, services, or scalable business models.

15 **Sandboxes**: controlled test environments to develop and evaluate new technologies, products, or services under the supervision of regulatory authorities. Their temporary relaxation of rules enable safe experimentation before large-scale implementation.

international scenario. However, such advance depends on the consolidation of an integrated national strategy that can coherently and sustainably coordinate technological, operational, and institutional dimensions.

Finally, the absence of this movement tends to increase the Brazilian strategic vulnerability in the face of emerging threats, showing that structured investment in data-driven technologies has become a strategic necessity for national defense rather than an option. Beyond a technological challenge, this is a structural problem of coordination, integration, and data governance in national defense.

## Acknowledgments

National Council for Scientific and Technological Development. Opinion: 302742/2022-0.

Brazilian Federal Agency for Support and Evaluation of Graduate Education. Opinion: 88887.613955/2021-00

Brazilian Federal Agency for Support and Evaluation of Graduate Education. Opinion: PROCAD 16/2020

São Paulo Research Foundation. Opinion: 2025/04394-0

## REFERENCES

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

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

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

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

BRASIL. Ministério da Defesa. **Política nacional de defesa e a estratégia nacional de defesa**. Brasília, DF: Ministério da Defesa, 2024. Available at: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Access on: April 21, 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. Available at: https://repositorio.esg.br/handle/123456789/1951. Access on: April 21, 2026.

GONZALEZ, C. D. O.; FERREIRA, P. P. Anatomia de um sistema de inteligência artificial. **ComCiência**, Campinas, 20 set. 2020. Available at: https://www.comciencia.br/anatomia-de-um-sistema-de-inteligencia-artificial/. Access on: April 21, 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. Available at: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy. Access on: April 21, 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. Available at: https://repositorio.esg.br/bitstream/123456789/1972/1/MARCUS%20ALBERT%20ALVES%20DA%20SILVA.pdf. Access on: April 21, 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. Available at: http://hdl.handle.net/20.500.11956/187326. Access on: April 21, 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.