

BRAZIL AT RISK? THE OMISSION OF THE DEFENSE SECTOR IN THE BRAZILIAN ARTIFICIAL INTELLIGENCE STRATEGY

Carlos Eduardo Franco Azevedo¹

Rachel Camilly Soares de Souza²

Introduction

The revolution provoked by Artificial Intelligence (AI) has reshaped the strategic perceptions of states in the 21st century and may influence the balance of power and international conflicts (Horowitz 2018). The capacity for large-scale data processing, machine learning, and real-time decision-making confers upon AI a determinant role in contemporary defense doctrines (Scharre 2018). Global military powers have systemically incorporated these technologies into their national defense strategies, recognizing their transformative potential for maintaining sovereignty and protecting national interests (Payne 2018).

The development of autonomous weapon systems, threat detection algorithms, and intelligence mechanisms grounded in AI currently constitute essential elements for any power that intends to ensure its autonomy in the international scenario (Ayoub and Payne 2015). In Brazil, however, a serious institutional gap is observed. The Brazilian Strategy for Artificial Intelligence (EBIA), published in 2021, although comprehensive across various sectors, neglects fundamental aspects related to the application of AI for National Defense purposes (Brasil 2021). This omission, far from representing a mere documentary lapse, configures itself as a strategic vulnerability, especially considering the growing use of AI technologies.

In this context, follows the research question of this article: What

¹ Escola de Comando e Estado Maior do Exército (ECEME), Rio de Janeiro, Brazil. E-mail: francoazevedo@francazevedo.com. ORCID: 0000-0002-8021-0723.

² Escola de Comando e Estado Maior do Exército (ECEME), Rio de Janeiro, Brasil. E-mail: rachelcamillyss@gmail.com. ORCID: 0009-0004-1888-0218.

are the implications of the absence of National Defense in the Brazilian Strategy for Artificial Intelligence? This article proposes a critical analysis of the Brazilian strategic gap, comparing international models of AI integration into Defense doctrines, and evaluates the resulting vulnerabilities for National Defense. It further suggests guidelines for the formulation of a specific public policy for AI in the Defense sector or its complementation within a pre-existing policy. The central hypothesis is that the absence of a strategy for the incorporation of AI into National Defense constitutes a critical failure that compromises Brazilian sovereignty in multiple dimensions: technological, military, economic, and geopolitical.

To this end, the study adopts a multidisciplinary theoretical approach, incorporating contributions from international security, contemporary strategic studies, and the technical literature on AI applied to defense. The relevance of this study lies in the need to foster academic and political debate on the insertion of AI into Brazil's Defense, to mitigate vulnerabilities and consolidate a digital protection strategy compatible with contemporary geopolitical challenges. Therefore, it seeks to contribute to filling this critical gap in contemporary Brazilian strategic thought.

Methodology

This study sought to critically analyze the absence of the Defense sector in the EBIA and its implications for national sovereignty. To this end, a qualitative approach was adopted (Gil 1999; Godoy 1995), based on a multidisciplinary analysis that incorporated contributions from international security theory, contemporary strategic studies, and the technical literature on AI applied to defense. The choice of this approach is justified by the need to understand in depth the nuances and interconnections between public AI policies and the Defense sector, as well as the complex relations of power and technological dependency in the international scenario.

The research was developed through the collection and analysis of documentary data (Gil 1999), with the systematic review of official documents and reports as its primary source. At the national level, the EBIA, published in 2021, and the Brazilian Artificial Intelligence Plan (PBIA), from 2024, were examined. These documents were central to identifying Brazil's official approach regarding AI and, more specifically, the presence or absence of guidelines aimed at the Defense sector.

Complementarily, national AI strategies and defense documents from globally prominent countries were consulted. The selection of these

countries, the United States, China, the United Kingdom, France, Russia, and Israel, was based on three explicit criteria: (i) international leadership in AI research and development, according to indicators such as the Stanford AI Index (AI index report 2025) and OCDE.AI; (ii) geopolitical and military relevance, particularly regarding the use of dual or strictly military AI; and (iii) the existence of formalized national strategies that allow for a structural comparison with the EBIA. These criteria ensured institutional diversity while maintaining a minimum level of methodological comparability across the cases.

To ensure consistency in the comparison, a textual analysis protocol was applied to the selected strategies. This protocol involved identifying and quantifying key defense-related terms – such as “national defense”, “military”, “armed forces”, “national security”, and “sovereignty” – as well as equivalent expressions used across different political-strategic traditions. In instances where literal translations failed to adequately capture the strategic meaning, a criterion of conceptual equivalence was adopted, taking into account terms such as *souveraineté*, *autonomie stratégique*, *technological sovereignty*, or *resilience* when used with the same analytical function. This approach minimized linguistic asymmetries and strengthened the validity of the comparison.

The collected data were subjected to a comparative and textual analysis (Schneider and Schmitt 1998). Initially, a systematic textual analysis of the EBIA and the selected international strategies was conducted. This technique allowed for the quantification of the frequency of key terms related to defense and security (such as “military,” “armed forces,” “national defense,” “national security,” and “sovereignty”) in the documents, evidencing the gap in the defense dimension of the Brazilian strategy compared to the approaches of other nations. Therewith, structural differences between the documents were observed, examining how each country articulates AI with its military doctrines, innovation policies and institutional mechanisms of civil-military integration. This phase sought to identify the presence of terms, as well as the way they fit into institutional arrangements, strategic priorities and conceptions of technological autonomy.

Subsequently, an in-depth comparative study was carried out (Schneider and Schmitt 1998), in which Brazil’s approaches and priorities were contrasted with international trends. This comparison highlighted Brazil’s misalignment with global powers and the strategic vulnerabilities resulting from the omission of the Defense sector in the national AI policy.

However, limitations inherent to the adopted method are acknowledged: national strategies vary in depth, terminology, and degree of transparency; some military capabilities remain classified; and linguistic differences may

introduce nuances of interpretation. Nevertheless, by explicitly stating criteria, procedures, and limitations, the aim was to reinforce the study's reliability, consistency, and reproducibility. Finally, based on the identified gap and the international comparative analysis, the implications for Brazil's sovereignty and security were discussed, considering the context of hybrid threats and persistent technological dependency, elements crucial for understanding the contemporary strategic scenario.

Artificial Intelligence and National Defense: Global Overview

Coined in the 1950s, the term artificial intelligence refers to computer programs that simulate intelligence. According to Russell and Norvig (2016), AI can be defined as the ability of computer systems to perform tasks that would normally require human intelligence, such as speech recognition, decision-making, and problem-solving. From a Brazilian perspective, AI is defined as computational systems that, by processing large volumes of data for specific objectives and autonomies, can predict, classify, recommend, or decide, impacting physical and virtual environments (Brasil 2024a; Brasil 2024b).

The integration of Artificial Intelligence into defense systems represents a significant transformation in military paradigms. According to Allen and Chan (2017), the development of AI can be as transformative as nuclear weapons, aviation, and cyberspace. Unlike incremental innovations, AI has fundamentally reconfigured the operational, tactical, and strategic capabilities of global armed forces. This disruptive technology not only enhances systems but also enables new operational models, generating new military capabilities (Horowitz 2018).

Military applications of AI encompass various functions, increasing the military power of states. In the domain of autonomous systems, AI has enabled the development of unmanned platforms with greater operational independence. According to Scharre (2018), "The rise of artificial intelligence will transform warfare," making autonomous aerial, land, and naval vehicles an inevitable trend in military doctrines. The use of AI in defense revolutionizes different fronts, including logistics automation, decision optimization, and the development of autonomous weapons. In military logistics, for example, the US Department of Logistics uses AI tools, such as the Logistics Federation (LOGFED), to train commanders and staff in sustainment (Matos 2024).

As these applications multiply across various operational contexts, three technological trends that frequently appear in the defense strategies of

numerous countries and help to shed light on the general direction taken by this transformation are observed. They emerge as trends that interconnect in practice: the growing use of AI to support command and control processes, the expansion of autonomous systems across multiple domains, and the increasingly deep integration of AI techniques into cyber operations.

First, AI has been incorporated into command and control activities, enhancing the capacity to integrate information, anticipate scenarios, and support decision-making in environments characterized by complexity and a growing volume of data. The examples discussed, such as the use of advanced decision-support tools and the optimization of logistics processes, illustrate how AI contributes to making military decision-making more responsive and less vulnerable to information overload.

A second set of applications appears in autonomous and semi-autonomous systems, whether aerial, ground-based, or naval, which have become central to how armed forces conduct reconnaissance, surveillance, and, in some cases, even offensive operations. Technologies described in the text, such as intelligent drones, autonomous navigation algorithms, and target identification systems, demonstrate that the autonomization of platforms is a structural transformation in battlefield operations.

Finally, AI also plays a role in the cyber domain, where it is used for threat detection, response automation, and the protection of critical infrastructure. Ongoing discussions regarding AI-driven cyberattacks highlight how adaptive models and automated intrusion techniques are altering the information environment, presenting unprecedented challenges for national defense.

Furthermore, the rapid digitization driven by AI has transformed cyber defense and modern conflicts. AI is essential for strengthening the security of critical infrastructures and command and control systems, both military and civilian, given that cyber attacks can compromise a country's sovereignty (Faria 2014). AI in Information Security is increasingly sought to prevent and combat hacker attacks, a challenge that transcends the private sector and directly impacts national security (Zequim and Ribeiro 2022).

Despite its transformative potential, AI presents unprecedented risks to international security. The technological competition between the US and China could generate new hybrid wars, with autonomous weapons and cyber attacks shaping the future of conflicts (Johnson 2019). The absence of an effective debate and regulation could lead to the uncontrolled proliferation of autonomous weapons, threatening international stability (Haner and Garcia 2019). The introduction of AI into autonomous systems in conflicts is a controversial topic, requiring international ethical and legal monitoring.

The practical use of AI on the battlefield is already a reality, demonstrated by drones and swarms in the Russian-Ukrainian conflict (Rosa, Silva and Ribeiro 2024). The Israel Defense Forces have deployed AI-based systems in their operations, including autonomous armored vehicles and target suggestion systems like “The Gospel” and “Lavender” (Serhan 2024).

In Brazil, however, initiatives for incorporating AI into Defense remain incipient and fragmented. Although there are isolated efforts – such as the Brazilian Air Force’s (FAB) AI Laboratory (Brazilian Air Force 2024), the Military Institute of Engineering’s (IME) LIARC and the Pró-Defesa V Program-IATQ – these actions lack systemic coordination and a national strategic framework, as will be detailed in the following comparative analysis.

Comparison with the international scenario highlights Brazil’s distance from other nations. According to the report “The Global AI Vibrancy Ranking” (2024) from Stanford University, countries like the US, China, the UK, and India lead in AI development, while Brazil appears in 34th place out of 36 states (Fattorini et al. 2024). This technological misalignment compromises Brazil’s ability to respond autonomously to contemporary conflicts. To understand this gap and successful approaches, it is essential to analyze international models of AI in Defense, which are detailed in the next section.

Although the United States and China naturally stand out due to the sheer volume of documentation and the scale of their defense programs, the other countries analyzed share similar trajectories and, in some instances, are even further along in integrating AI into Defense. France and the United Kingdom, for example, link AI to clear operational concepts, such as “information advantage” and “AI-ready” in the British case, and “*autonomie stratégique*” in French doctrine, translating these guidelines into sustained investment in autonomous systems, cyber defense, and AI applications for command and control. Despite having fewer resources, these nations possess established institutional frameworks that bridge civil and military innovation, demonstrating a high degree of internal coherence in their strategies.

Russia and Israel, in turn, reinforce trends already discussed regarding the United States and China, particularly the use of AI to support large-scale operations, automate target selection processes, and sustain offensive and defensive actions in the cyber domain. Russia prioritizes automation-based capabilities to offset industrial constraints while also integrating AI into surveillance and electronic warfare systems; Israel, as previously discussed, combines autonomous technologies, rapid data analysis, and operational integration within highly volatile urban environments. Thus, even if the level of documentary detail is lower, the strategic direction is comparable: all of the

countries are incorporating AI into three core areas, command and control, autonomous systems, and cyber capabilities, reflecting an international convergence in the militarization of AI.

Aspects Related to International Models of AI Applied to Defense

The technological revolution driven by AI has redefined strategic and operational paradigms in global defense and security. AI's capacity to process data, learn patterns, and automate processes transforms the operation and protection of nations by military organizations. This disruptive technology enhances existing systems and enables new operational models and defense strategies. Prominent research areas in the sector over the last five years include cybersecurity, machine learning, robotics, sensing, data analysis, decision support, simulation, and neural language processing (Sá et al. 2025).

The growing importance of AI is reflected in market data. According to Fortune Business Insights, the global AI market was valued at US\$ 233.46 billion in 2024, projecting growth of 29.2% to US\$ 1,771.62 billion by 2033 (Fortune Business Insights 2025). In this ecosystem, AI applied to Defense, although smaller, demonstrates notable dynamism, valued at US\$ 7.15 billion in 2024 and projected to reach US\$ 23.06 billion by 2033 (Global Growth Insights 2025). This growth is driven by defense budgets, global security concerns, and advances in AI, which enhance capabilities in surveillance, threat detection, and autonomous systems. Thus, AI is not only a tool for efficiency but an asset that confers strategic superiority and enhances defenses, becoming a competitive and evolving sector. Governments and private entities invest heavily to obtain this advantage, resulting in continuous innovations.

This landscape of investments and technological advances serves as a basis for understanding the approaches of different nations. International models reveal diverse approaches, but with a common denominator: AI is a pillar of national security and sovereignty. The main initiatives of key countries are detailed below.

The US maintains global leadership in AI (1st in Stanford's The Global AI Vibrancy Ranking 2024) and demonstrates a strong commitment to integrating the technology into its defense. Its national strategy, "Maintaining American Leadership in AI-2025" (2025), aims to consolidate leadership in R&D, autonomous systems, logistics, data infrastructure, and open-source AI (Fattorini et al. 2024). One pillar is the "Project StarGate" (2025),

a public-private partnership estimating US\$ 500 billion in investments for infrastructure and data centers (Open AI 2025). The US also has an exclusive AI strategy for Defense, materialized by the creation of the Joint Artificial Intelligence Center (JAIC) in 2018 and, subsequently, the Chief Data and Analytics Officers (CDAOs) in 2022, which absorbed the JAIC, centralizing the integration of AI into military operations (Barreiros e Poty 2021). The DoD plans to invest US\$ 1.8 billion in AI in 2025 (up from US\$ 874 million in 2022) (Vincent 2024). Important projects include Maven, JADC2, and Loyal Wingman Drones.

China (2nd in The Global AI Vibrancy Ranking 2024) intends to become the main global center for AI innovation by 2030, challenging US leadership (Fattorini et al. 2024). Its AI strategy in Defense includes the “Military Intelligence 2030” program, integrated into “Made in China 2025,” which transfers civil innovations to military applications (Kania, 2017). China’s AI strategy, as observed by Kania (2020), stands out for its military-civil fusion, which integrates universities, industries, and the military in technological development. This approach aims to eliminate barriers between sectors, promoting innovation in dual-use technologies for civilian and military applications. It allows the same technologies and teams to act simultaneously, accelerating the incorporation of AI advances in Defense. Although R&D spending is comprehensive (US\$ 500 billion in 2024), investment in AI-equipped hardware for military purposes ranged between US\$ 1.6 billion and US\$ 2.7 billion annually (2018-2020). China focuses on “AI Warfare,” surveillance, autonomous drones, and decision support, consolidating itself as an emerging power in AI applied to Defense (Fedasiuk, Melot and Murphy 2021; Fattorini et al. 2024).

The United Kingdom (3rd in The Global AI Vibrancy Ranking 2024) adopts a dual approach, with national AI strategies and a specific one for Defense (Fattorini et al. 2024). Its AI National Strategy (2021) and AI Opportunities Action Plan (2025) aim for US\$ 500 billion in the British economy by 2030 (United Kingdom 2021; United Kingdom 2025). The country invests in AI Doctoral Training Centres (US\$ 127 million) and “AI Growth Zones” (AIGZs), fostering innovation in strategic regions (United Kingdom 2025). In Defense, the Defence AI Strategy (2022) seeks to make the UK an effective and influential organization in AI, promoting safe and responsible military development (United Kingdom 2022). The UK and France collaborated on the Maritime Mine Countermeasures System (MMCM), an innovative AI solution to detect and neutralize mines without risk to sailors. The system, delivered in 2025, employs sonar on a drone boat to map mines, which are neutralized by a remote vehicle. AI speeds up the process and reduces the

need for manned ships, offering advantages in efficiency and safety (Padilha, 2025). Combining innovation and national security, the UK demonstrates a robust commitment to AI, reinforcing its position as a global actor in artificial intelligence.

France (6th in The Global AI Vibrancy Ranking 2024) seeks sovereignty in AI for Defense, with investments in infrastructure and innovation (Fattorini et al. 2024). In March 2024, it launched the “*Stratégie ministérielle sur l’intelligence artificielle*”, aiming to guide and accelerate the use of a credible and effective “defense AI”. A main initiative is the creation of the Ministerial Agency for Defense AI (AMIAD), which centralizes resources and seeks to guarantee French mastery of these technologies, avoiding dependency (France 2024). The strategy also highlights the importance of a supercomputer dedicated to AI by 2025, the largest in Europe, capable of processing classified data (France 2024). As part of the effort, France announced US\$ 126 billion for infrastructure and data centers, reinforcing its technological and strategic capacity. The “France 2030” plan dedicates 2.5 billion euros (US\$ 2.7 billion) to AI in Defense, consolidating the strategic role of the technology (Rondepierre 2024). With robust investments, advanced infrastructure, and international collaboration, France reinforces its position as a global actor in AI for Defense.

Israel (16th in The Global AI Vibrancy Ranking 2024) is recognized for tactical-operational innovation and the systemic integration of AI, focusing on military and security applications (Fattorini et al. 2024). The country invested US\$ 300 million in the National AI Program, including a national supercomputer and an “AI Factory” to integrate algorithms into military strategy. This approach encompasses military operations, target identification, logistics, and autonomous systems, consolidating AI as central to the doctrines of the Israel Defense Forces (IDF) (Mimran and Dahan 2024). IDF officials highlighted the growing use of AI, especially in the Israel-Hamas conflict (2023). Systems like Alchemist, Fire Factory, and Depth of Wisdom collect and analyze vast volumes of intelligence (signal, geographic, human, and surveillance), allowing efficient dissemination of information among units and precise military attacks with unmanned vehicles and other autonomous technologies (Renic and Schwarz 2023). Additionally, Israel uses Gospel and Lavender for target suggestion and monitoring, and autonomous armored vehicles for bomb disposal. The integration of AI offers a continuous technological advantage, allowing it to assimilate and apply intelligence from various war domains efficiently and precisely.

Russia (29th in The Global AI Vibrancy Ranking 2024) launched its National AI Strategy until 2030 in 2019, prioritizing Defense, health,

education, and business automation. The strategy seeks to reduce foreign dependency and modernize technological capabilities. Since 2017, Russia has emphasized that leadership in AI is essential for sovereignty and global position (Russia 2019; Fattorini et al. 2024). Militarily, Russia developed the Concept for the Use of Robotic Systems for Military Purposes until 2030, aiming to robotize 30% of combat power by 2025, with a budget of US\$ 346 billion until 2021. It also created an AI department within the Ministry of Defense, reinforcing its commitment to automation (Nadibaidze 2022). The practical application of AI was announced by Putin during the invasion of Ukraine (2022), with hypersonic missiles like the Kinzhal, demonstrating the integration of advanced technologies (Ayres and Medeiros 2022). These advances reflect the Russian effort to modernize its armed forces and compete, consolidating its geopolitical position.

Finally, Brazil (34th in The Global AI Vibrancy Ranking 2024) presents incipient and fragmented initiatives in AI for defense (Fattorini et al. 2024). The EBIA does not explicitly focus on Defense, and the PBIA plans to invest R\$ 23 billion (US\$ 4.6 billion) in AI by 2028, with no specific budget for military AI. In the Brazilian context, defense initiatives include: the FAB AI Laboratory (R\$ 6.5 million/US\$ 1.3 million), LIARC at the IME, the development of AI models for aircraft wreckage detection by the ITA, the inclusion of AI disciplines in Military Schools, the leadership in the Pró-Defesa V Program-IATQ, the promotion of the symposium “Artificial Intelligence in the Military Expression of National Power,” and the publication of the Brazilian Army’s Strategic Directive on AI (2024). However, these initiatives lack systemic coordination and a consolidated doctrinal foundation, reflecting the absence of a specific national policy for AI in Defense.

The Brazilian Artificial Intelligence Strategy and the Gap in Defense

The Brazilian Artificial Intelligence Strategy (EBIA), established by Ordinance MCTI No. 4,617 of April 6, 2021, represents the first systematic effort to formulate a national public policy for this emerging technological field (Brasil 2021). The document establishes a vision, objectives, and thematic axes to guide the development and application of AI in the country, seeking to position Brazil as a protagonist in the so-called “Fourth Industrial Revolution” (Brasil 2021).

The EBIA is structured around nine thematic axes: Legislation, Regulation, and Ethical Use; AI Governance; International Aspects;

Education; Workforce and Capacity Building; Research, Development, Innovation (R&D&I) and Entrepreneurship; Application in Productive Sectors; Application in Public Power; and Public Security (Brasil 2021). For each axis, the document establishes strategic objectives and indicative actions, outlining institutional responsibilities and estimated implementation deadlines.

In a critical analysis of the EBIA's structure and content, an emphasis on regulatory, educational, and basic research aspects is observed, without adequate depth in specific sectoral applications. Thereby, we point out that although the EBIA presents a comprehensive conceptual structure, it demonstrates an imbalance between generalist formulations and concrete operational guidelines, resulting in a document that, although meritorious as a first initiative, lacks implementable specificity.

The International Aspects axis highlights global cooperation in AI but does not mention strategic partnerships for the development of defense technologies. In a competitive global scenario, where countries invest heavily in military AI, Brazil demonstrates that it ignores this essential dimension. Although the document encourages AI research and development, it does not direct efforts toward defense-oriented technologies. Leading AI countries often prioritize projects with dual (civilian and military) applications, an aspect not considered in the Brazilian strategy (Brasil 2021).

Although there is an axis dedicated to "Public Security," it is limited to aspects such as predictive policing and combating organized crime. There is, however, no mention of the role of AI in Defense against external threats or in strengthening Brazil's cyber defense or even in the defense of critical infrastructures. In a world where cyber attacks can compromise a country's sovereignty, the lack of this approach is worrying (Brasil 2021).

Even though the EBIA does not mention Defense, the Brazilian Army, in turn, formalized the Strategic Directive for Artificial Intelligence (Ordinance EME/C Ex No. 1,318 of May 14, 2024), establishing institutional guidelines for the integration of AI within the organization. Its central objective is to promote the modernization and operational efficiency of the Army, through the responsible employment of AI systems in different areas, such as logistics, communication, intelligence, and personnel management. By defining fundamental concepts, principles, and strategic goals, the directive seeks to strengthen decision-making, scenario anticipation capacity, and the Army's technological competitiveness, aligning its initiatives with the institution's Information Policy (Brasil 2024b).

Furthermore, the regulation emphasizes the importance of mastering Emerging and Disruptive Technologies (EDT) as an instrument of State security and for the transformation of strategic deterrence. It provides for the

consolidation of institutional competencies for the development, deployment, and ethical use of AI, ensuring that its application is in compliance with the Army’s moral and legal principles. In this context, Ordinance EME/C Ex No. 1,318/2024 represents a structured effort to position the institution in tune with global trends of military modernization, ensuring that technological innovation is integrated in a responsible and strategic manner into its operations (Brasil 2024b).

This analysis evidences that the EBIA, although representing a significant institutional advance as the first formal national policy for AI, presents critical gaps in its conception and structure. The absence of specific treatment for the Defense sector does not constitute a mere punctual omission, but reflects a conceptual approach that disregards the strategic criticality of AI for National Defense, misaligning Brazil from predominant global trends in this field.

The Gap in Defense

The detailed analysis of the EBIA reveals a significant absence of guidelines, objectives, and specific actions for national defense. This gap is not a mere punctual omission, but a structural failure in the strategic conception of the document, with profound implications for Brazilian sovereignty and national security in a global scenario mediated by disruptive technologies.

To measure the extent and gravity of this gap, a systematic textual analysis of the EBIA was conducted, comparing the frequency of key terms related to defense and security with the national AI strategies of other powers. The results in Table 1 evidence a misalignment of the Brazilian approach in relation to predominant international trends.

Table 1: Frequency of Key Terms in Selected National AI Strategies

Keyword	USA	China	UK	France	Russia	Israel	Brazil
National Defense	14	11	24	3	0	6	0
National Security	23	8	18	1	1	4	0
Military	7	13	0	0	0	0	2 (d)
(Internal Security/Public Security)	3	5	3	0	0	0	5(d)

Keyword	USA	China	UK	France	Russia	Israel	Brazil
Sovereignty	0	1 (a)	0	6	1 (a)	4 (a)	0
Explicit Defense/Military Section	Yes	Yes (b)	Yes	Yes	No	No (c)	No
Total Explicit Mentions	47	38	45	4	1	10	7 (d)

Source: prepared by the authors based on the national AI strategies of the countries.

Legend:

(a) When the word “sovereignty” was not found, the emphasis on “independence, autonomy, and technological autonomy” was considered.

(b) In China, there is a section for civil-military integration for technologies of a dual nature;

(c) In Israel, AI is considered transversal to the functions of the State, but the central drive is defense. In that country’s strategy, the word “resilience” was used as a synonym for National Defense;

(d) In Brazil, the key terms were found 7 (seven) times, but out of context, referring to policing and data protection; and

(e) The strategies considered in the analysis were:

-United States of America: Winning the Race: America’s AI Action Plan, 2025.

-China: Next Generation Artificial Intelligence Development Plan, 2017.

-United Kingdom: National Artificial Intelligence Strategy, 2021.

-France: Stratégie Nationale en Intelligence Artificielle (SNIA), 2021.

-Russia: National Strategy for the Development of Artificial Intelligence over the Period Extending up to the Year 2030, 2019.

-Israel: National Program for Artificial Intelligence Program and Snapshot, 2025.

-Brazil: Brazilian Artificial Intelligence Strategy (EBIA), 2021.

(f) Word counts were performed on available public documents and may vary slightly depending on the version or translation used.

Table 1 reveals that while powers like the USA, China, and the UK present a high number of explicit mentions of the key terms (47, 38, and 45 mentions, respectively), the EBIA records only two mentions of “military” and five of “public security,” focused on policing and data protection. There is no mention of “national defense,” “national security,” or “sovereignty” in its main body. The scarce mentions occur in generic or illustrative contexts of the “Public Security” axis, without strategic objectives, concrete actions, or implementation mechanisms for the scope of this study (Brasil 2021). In this sense, the EBIA differs from the other countries. China, for example, formalizes “civil-military fusion” as a strategic pillar, guaranteeing the rapid

incorporation of AI advances into defense (Kania 2020). The USA and the UK, in addition to national AI strategies, have exclusive strategies for Defense.

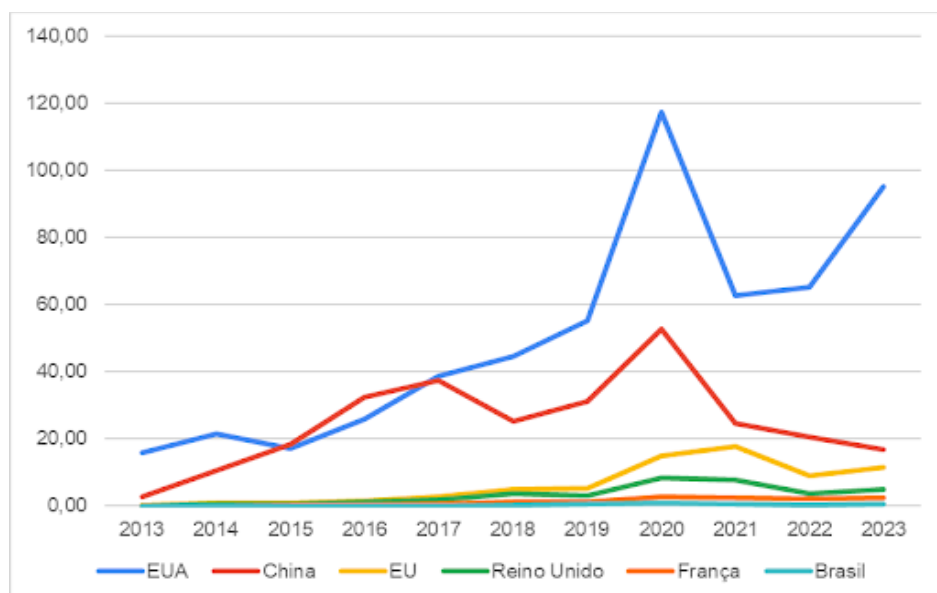
The contrast of the EBIA with the other strategies is notable, even in countries with few direct mentions, where sovereignty is revealing. France (6 mentions of “souveraineté”), Russia (1 mention of “technological sovereignty”) and Israel (4 mentions of “technological sovereignty”) explicitly state AI as a vital component for autonomy and non-technological dependence. The EBIA, however, does not address technological sovereignty in defense. For these nations, AI is not just a tool for efficiency, but a pillar of self-determination and protection of national interests in a complex geopolitical environment. Russia, despite few explicit mentions of defense, underlines “technological sovereignty” as a fundamental principle, suggesting that AI applications for defense are intrinsic to the pursuit of autonomy.

Technologically, the strategic gap results in growing external dependence on critical military systems. According to the Brazilian Academy of Sciences (2023), dependence on foreign nations and multinationals in AI can compromise the security, sovereignty, and competitiveness of domestic companies. To develop new technologies based on AI, it is fundamental to master its principles. The insufficiency of technical knowledge will intensify subordination to large corporations and powers that already dominate the sector.

The Brazilian gap is not limited to the conceptual and lexical dimension. The disparity in AI investments is even more evident. The Brazilian AI Plan (PBIA) forecasts US\$ 4.6 billion for AI until 2028, with no specific budget for military AI. Isolated initiatives by the Armed Forces include, as we have seen, the FAB’s AI Laboratory (US\$ 1.3 million), the development of AI models for aircraft wreckage detection by ITA, and LIARC at IME (Brazilian Air Force 2025a; Brazilian Air Force 2025b; Sá et al. 2025). However, these initiatives are marked by institutional fragmentation and budgetary limitations.

This fragmentation and the volume of investment contrast sharply with the international scenario, especially regarding the fostering of the innovation ecosystem and venture capital. In 2023, for example, the United States attracted US\$ 95.037 billion in venture capital investments in AI, while China recorded US\$ 16.967 billion. In the same period, Brazil attracted only US\$ 482 million in venture capital investments in AI (Chart 1). This abysmal difference in private fostering of innovation is a critical indicator of the fragility of the Brazilian ecosystem and, by extension, of the country’s capacity to develop AI solutions for its Defense needs, compromising military technological autonomy.

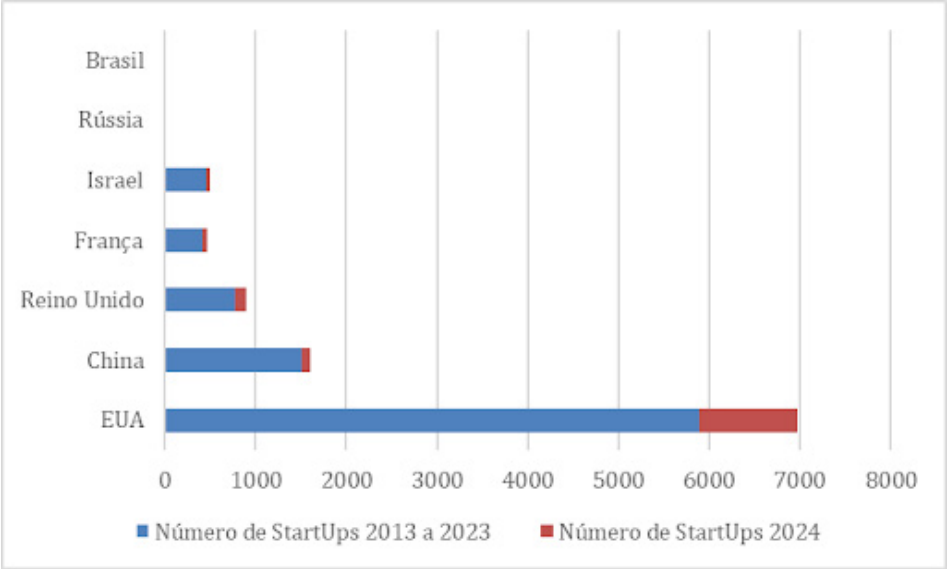
Chart 1: Venture Capital Investments by Country (2013-2023)



Source: OCDE.AI (2025)

Even more worrying is the number of AI startups, essential engines of innovation and agility, including for defense. While the USA has 6,966 AI startups (2013-2024) and China has 1,606, Brazil did not register a significant number in this period (Chart 2). This absence of a vibrant environment for new AI enterprises in Brazil, compared to other countries, reflects a fundamental failure in the capacity to generate and scale innovations in the sector and, consequently, to supply the technological demands of National Defense with cutting-edge domestic solutions.

Chart 2: Number of Startups by Country in the Period 2013-2024



Source: OCDE.AI (2025)

This Brazilian gap contrasts with international trends. Analysis of the ITS report (March 2020) on AI strategies of 20 countries revealed that 7 (35%) contained “defense” and/or “national security” (Instituto de Tecnologia e Sociedade do Rio 2020). Even Finland and Sweden, with a pacifist tradition, include implications of AI for national security in their strategies.

The SIPRI report (2020) demonstrates how AI reconfigures national defense dynamics and strategic power. All eight nuclear states analyzed (USA, Russia, China, France, UK, India, Pakistan, and North Korea) have active programs for integrating AI into strategic systems, but with disparities in capabilities and investments. The USA leads with US\$ 2 billion annually via Defense Advanced Research Projects Agency (DARPA), while Pakistan faces limitations, with only 650 specialized AI researchers.

In intelligence, surveillance, and reconnaissance (ISR), the report documents that seven of the eight countries (87.5%) developed automatic target recognition systems, and four (50%) implemented onboard data processing in unmanned vehicles. China stands out, with significant advances in hypersonic vehicles with AI, such as the DF-ZF. India, despite its advances, still depends on imports for 73% of its critical defense components, evidencing a technological asymmetry that tends to deepen. This dependence creates strategic vulnerabilities, such as risks of embargo and backdoors in

sensitive systems (Boulanin et al., 2020).

In the field of public policies and governance, only three of the eight countries (37.5%) established explicit ethical guidelines for the military use of AI. France allocates €100 million annually for research that prioritizes human oversight, while China imposes no public restrictions on the development of autonomous systems. This normative divergence hinders international agreements; only two significant multilateral initiatives were registered until 2020. The lack of common standards for the development and employment of military AI creates a fragmented and dangerous strategic environment, where incidents or arms races can arise from misinterpretations of adversarial capabilities and intentions (Boulanin et al., 2020).

The SIPRI report on AI in South Asia highlights that India has invested in AI to strengthen its security and stability. That country created a Ministry of Defense task force in 2018, the Centre for Artificial Intelligence and Robotics, to improve intelligence and data analysis. In 2022, it launched the Defence Artificial Intelligence Council and the Defence AI Project Agency, with 75 priority AI projects and a budget of ₹1,000 crore annually until 2026. India also develops emerging technologies, such as unmanned vehicles and cyber warfare, with AI playing a significant role. The application of AI in nuclear and non-nuclear weapons systems is a growing concern, with implications for strategic stability in the region (Topychkanov 2020).

In contrast, Brazil has not yet developed official AI policies with a military or national security focus. Although there are emerging initiatives in the civil field, as suggested by discussions on regulation and investments in AI, there are no programs comparable to India's in scale, institutionalization, or strategic application. The absence of clear public policies and the lack of institutions dedicated to defensive AI research limit Brazil's capacity to effectively integrate AI into its military and national security operations.

Despite the growing incorporation of the term "innovation" in national agendas since the 1990s, Brazil has not yet fully assimilated its systemic and interactive meaning. This is reflected in fragmented policies and reactive, poorly articulated innovative performance (Cassiolato and Lastres 2005). Since the 1960s, empirical studies (SAPPHO Project, UK; Yale Innovation Survey, USA) contributed to replacing the linear view of innovation with a more complex conception. These studies revealed that innovative success is associated with the capacity of firms to interact with external knowledge agents, originating the notion of innovation as a collaborative, cumulative, and institutionally conditioned process.

Understanding the absence of artificial intelligence in Brazilian defense policy gains depth when situated within Latin American structuralist

thinking, notably within the framework of CEPAL. This approach values the centrality of knowledge, productive transformation, and local institutional conditions in development, aligning with contemporary perspectives on innovation systems that emphasize the need for active state policies to foster technical and productive changes (Cassiolato e Lastres 2005). In both analytical frameworks, development does not stem from spontaneous market forces, but from intentional arrangements that coordinate capabilities, institutions, and strategic sectors.

From the perspective of innovation systems, such arrangements are dynamic, historically constructed, and depend on continuous interaction between firms, universities, research centers, government bodies, and civil society. It involves building networks that generate learning, technological diffusion, and endogenous capabilities (Dagnino 2009). In the Brazilian case, however, there is a dissonance between the rhetoric valuing innovation and the institutional practice that sustains it: fragmented policies, poor coordination among initiatives, and a productive structure dominated by low-tech sectors limit the consolidation of a robust national system.

Cassiolato and Lastres (2005) argue that for innovation systems to function effectively in countries like Brazil, it is necessary for the State to act as a coordinator, strengthening internal production chains and ensuring lasting policies capable of building local capabilities. Yet, as Dagnino (2009) points out, Brazil frequently adopts policies that are discontinuous, excessively financial in nature, and insufficiently oriented toward institutional building or the strengthening of the national productive base.

These challenges intensify because the articulation between science, technology and development does not automatically generate socioeconomic progress. Without a conducive institutional environment, intersectoral coordination mechanisms and policies coherent with local capabilities, knowledge production tends to remain disconnected from productive reality, reinforcing historical dependencies and external vulnerabilities. It is at this point that dependency theory, especially in Cardoso and Faletto, contributes to understanding why strategic technologies, such as artificial intelligence, remain absent from central defense guidelines in Brazil.

To these authors, dependency does not operate through the institutional, political and epistemological mechanisms that place peripheral countries in subordinate positions in the global system. The reconfiguration of dependency in the second half of the 20th century shows that, even when external control is not explicit, it reproduces itself through the penetration of international capital, the importation of technologies and the alignment of domestic elites with the external logics of accumulation (Cardoso and Faletto

1970).

Furtado (1974) adds that underdevelopment is a structural phenomenon, functional to the global capitalism itself, in which the domain of innovation remains concentrated in core countries. In these economies, the interplay between science, technology and political power enables the internalization of technical progress; in the periphery, innovation tends to be imported in a subordinate manner, without the domain of the underlying scientific principles or the supporting infrastructures. This critique remains fully valid in the digital age: by importing technologies without mastering their internal logic, a country reinforces its peripheral status, turning technology into a vehicle for subordination rather than autonomy.

These interpretations help explain why AI, despite its global strategic significance, remains marginal to Brazil's defense policy. The absence of a clear guideline reflects a persistent historical pattern of subordinate integration regarding critical technologies. The "integration" into global innovation networks, often interpreted as a sign of modernization, frequently serves merely as a mechanism that deepens dependency, given that knowledge and technology production remain externalized. This pattern is reinforced by national elites who, by adopting imported paradigms and models, neglect to formulate technological strategies aligned with the country's specific vulnerabilities and potential. Consequently, dependency becomes not only economic but also institutional and epistemological.

The result is a persistent dissociation between science, technology, defense, and the project of the nation. Without a strategy that articulates universities, Armed Forces, state agencies, and productive sectors, it becomes unviable to build a sovereign military-technological complex. Even isolated initiatives, such as research labs or modernization programs, tend to lose continuity because of the lack of strategic coordination. In the specific case of AI, this fragmentation entails delegating critical functions to external actors, importing systems, algorithms, and infrastructures over which Brazil lacks full control. This practice exacerbates vulnerabilities, particularly in the cyber domain, where technological dependence can directly compromise national security.

Therefore, the absence of AI in Brazilian defense policy is not an accident, it is the updated expression of a historical pattern of structural subordination. It reflects the reproduction of a model in which the country occupies a peripheral role, consuming technologies conceived at the core without internalizing their production logic. Breaking this pattern requires more than incremental adjustments; it demands a fundamental shift in how Brazil conceives of innovation, sovereignty, and national power. Ultimately,

it requires recognizing that technological sovereignty, especially in strategic areas such as military AI, is not inherited, but built.

Implications of the Absence of an AI Strategy for Defense in Brazil

In the context represented by vulnerabilities brought with the digital revolution, AI interacts as a tool that permeates various areas in the Defense sector. The technological environment incorporated into the operational theater of conflicts presents itself as a new form of employment of violence that uses physical, cybernetic means, irregular elements, political elements, among others (Campany 2021). These elements are part of the constitution of the concept of Hybrid War developed by Hoffman (2007) in his thesis entitled “Conflict in the 21st Century: the rise of Hybrid Wars”.

Starting from this idea, the concept of hybrid threats was developed, which according to the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE n.d.), are: “Harmful activities that are planned and executed with malicious intent. They aim to undermine a target, such as a state or an institution, through a variety of means, often combined.” Although they prioritize the use of non-military tools, they generate significant impacts on the affected societies that, at times, correspond to those of a military aggression. Among these, include cyber attacks, disinformation, sabotage, sponsorship of criminal or terrorist organizations, the exploitation of economic vulnerabilities, and even the corruption of public agents (Campany 2021).

In South America, disinformation has established itself as a recurring hybrid threat, being employed to manipulate public opinion, weaken governments, and influence political processes (Caixeta 2024). This phenomenon aims to destabilize the political scenario by compromising the population’s trust in democratic institutions and fostering internal divisions. In Brazil, the 2022 presidential elections evidenced this scenario, with the digital environment transforming into a strategic space for the fomenting of hybrid threats. The rapid dissemination of information, allied with the difficulty of tracking and attributing these campaigns, makes digital war a highly influential factor with great destabilizing potential (Caixeta 2024).

Advances in information and communication technologies, as well as the expansion of accessible services, enabled the transition from the traditional model of war to the concept of hybrid war. In this new scenario, threats

characteristic of conventional conflicts, such as nuclear ones, were gradually complemented by new forms of threat (Susnea and Ionuț-Cosmin 2021). Among them, cyber threats stand out, which consist of actions conducted by States or international organizations with the objective of attacking and compromising the computer systems and information networks of other nations (Canada 2022).

Therefore, the absence of a specific component for AI in Defense in the Brazilian strategy manifests itself in a particularly critical manner in the domain of cyber defense. For Brundage et al. (2018) AI can be used to expand existing threats, introduce new threats, and alter the typical character of threats, making them more effective, targeted, and difficult to attribute. Furthermore, it can allow cyber attacks to be carried out on a larger scale and with greater efficacy, reducing the need for human intervention and increasing the complexity of necessary responses.

The recent evolution of cyber attacks evidences a fundamental transformation in their nature and complexity. AI-based Advanced Persistent Threats (APTs) are characterized by adaptive capacity, autonomous behavior, and the ability to invade conventional detection systems. Traditional detection and mitigation tools may not be sufficient to deal with these threats, given their evolutionary and stealthy nature. AI, especially deep learning, is seen as a promising solution to improve the detection and defense against APTs (Walsh, Worrell and Scanlon 2024).

The convergence between AI and social media represents a growing risk for the integrity of the informational ecosystem. Generative language models and image synthesis, when combined with automated disinformation networks, allow the coordinated dissemination of false narratives on an industrial scale (Chesney and Citron 2019). The exponential speed of these campaigns increases their efficacy, making the digital environment particularly vulnerable to manipulations (Woolley and Howard 2018).

Advances in technology and trends of power and interdependence have driven the growth of the use of hybrid war, providing innovative capabilities both in the military and non-military domains (Costa 2024). As a consequence, not only the war apparatus will be transformed, but also the human dimension in war will be affected. The reflection of AI applications in hybrid war can be described and explained by the synergistic use of five different instruments and means of power, known as DIME – Diplomatic, Informational, Military, Economic –, which are used to exploit enemy vulnerabilities (Cullen and Reichborn-Kjennerud 2017).

The military dimension includes the use of AI-enabled military systems, encompassing aquatic, aerial, and terrestrial robots. Great progress

has been made in the development of AI-based weapons and technologies. For example, Israel has employed M113 armored personnel carriers, loaded with explosives, to neutralize traps and explosive devices in the Gaza Strip (Monitor do Oriente Médio 2024). Furthermore, AI programs, such as “The Gospel” and “Lavender”, are used to suggest targets for airstrikes and monitor suspected Hamas members, contributing to a rapid identification and elimination of targets, although often resulting in significant civilian casualties (Serhan 2024). These examples illustrate the growing use of AI in military operations, highlighting the need to balance technological efficacy with ethical and legal oversight.

The economic dimension of AI can be explained in the context of hybrid war. When States are targets of hybrid attacks, they often resort to counter-attacks through economic coercion, such as financial isolation and sanctions. AI-based tools are employed to optimize capital investments, assess credit quality, ensure regulatory compliance, monitor commercial transactions, and detect fraud (Zia 2021). AI has great utility in the information domain, which is crucial for shaping political discourse, influencing popular perceptions, and altering political outcomes through the manipulation of information availability (Barbosa 2020).

Another point is the dependence on foreign technologies. Without the autonomous development of AI systems, Brazil may find itself obliged to import solutions from other countries, which can compromise national sovereignty and the security of military information. Furthermore, the absence of an AI strategy can lead to a technological lag in relation to other nations that already incorporate these technologies into their armed forces. This lag can result in operational disadvantages, especially in high-risk missions, such as demining and reconnaissance operations, where AI can be employed to minimize human risks (Sputnik 2024).

Although this work focuses on the EBIA, the recently published Brazilian AI Plan presents the same deficit that we contest. The Plan still focuses on secondary applications, leaving aside core technologies such as language models. To change this scenario, it is essential to articulate innovation policies and the protection of strategic data (Outras Mídias 2024). This approach reproduces the historical pattern of importing know-how, aggravated by the lack of investments in semiconductors and high-performance computational infrastructure (Fernandes 2024).

The analysis of ethical dilemmas in the scope of AI in the military field demands the convergence of three complementary axes: the measurement and monitoring of responsible AI practices (Global Index on Responsible AI), global normative principles consolidated in Responsible AI frameworks, and

the legal-humanitarian reflection on Lethal Autonomous Weapons Systems (LAWS) conducted by organisms such as the International Committee of the Red Cross (ICRC). Although each report addresses distinct dimensions, the integration of the three perspectives reveals that current technological governance is marked by structural asymmetries, with direct implications for international security and the protection of civilians.

From the point of view of measurement, Responsible AI highlights indicators of security, transparency, and accountability as foundations for responsible AI (Responsible AI 2024). However, the military application of AI, especially in lethal contexts, is treated peripherally, without examining in depth dilemmas such as the humanitarian implications documented in recent conflicts, for example, between Israel and Hamas. The absence of specific metrics for military AI capabilities and for the vulnerability of different national contexts, especially in the Global South, limits the index's capacity to capture geopolitical inequalities.

The reports of the UNESCO Recommendation on the Ethics of AI (2021) and the OECD AI Principles (2019), provide a robust normative framework. They emphasize principles such as human-in-the-loop, auditability, mitigation of biases, and compliance with International Humanitarian Law (Jobin, Ienca and Vayena 2019; Floridi 2021). However, these frameworks are predominantly elaborated in the Global North, reflecting its values and priorities. For countries of the Global South, with limited institutional resources, the uncritical adoption of these frameworks can result in technological dependence and in regulatory gaps, perpetuating an asymmetric model of governance.

In turn, the ICRC report on autonomous weapons (ICRC 2016) brings a concrete legal-operational perspective, evidencing how the increase in autonomy in critical attack functions puts at risk principles such as distinction, proportionality, and precaution. The convergence of these reports allows identifying that the central challenge is not only technological, but normative and structural. A truly responsible global AI governance regime needs to include specific metrics for military capabilities within the ethical scope, adapted to the institutional realities of the Global South. Without such an integrated approach, the risk is to consolidate a scenario in which powers unilaterally define the ethical limits of military AI, while other States bear disproportionately the human and strategic costs of its implementation.

The SIPRI report, *Bias in Military Artificial Intelligence* (2024), addresses the risks associated with biases present in military AI systems, emphasizing their ethical, humanitarian, and strategic implications. Although the study does not focus specifically on emerging countries, its

conclusions are highly relevant for these nations, which are in the process of developing or acquiring AI technologies applied to defense. The report defines bias in military AI as the systemically distorted performance of a system that can generate unfair or harmful decisions, influenced by social, cultural, or economic factors, such as race, gender, or class. Such biases can arise from three main sources: bias in society, bias in data and algorithms, and bias in the operational use of the technology, and can compromise the efficacy of operations and generate serious humanitarian consequences, such as incorrect identification of targets or failures in the assessment of critical needs (Blanchard and Bruun 2024).

For emerging countries, the impact of these biases is particularly relevant, given that the research infrastructure and available data often present limitations. The absence of diversity in training data, combined with still incipient regulations on the military use of AI, increases the probability of distorted outcomes, reducing the reliability and ethics of operations. Thus, it is essential that these nations adopt responsible development practices from the outset, incorporating oversight mechanisms, algorithm validation, and review by multiple stakeholders, including universities, industry, and civil society. In this way, it is possible to reduce the risks of biases and strengthen the legitimacy of the use of AI in the context of security and defense (Blanchard and Bruun 2024).

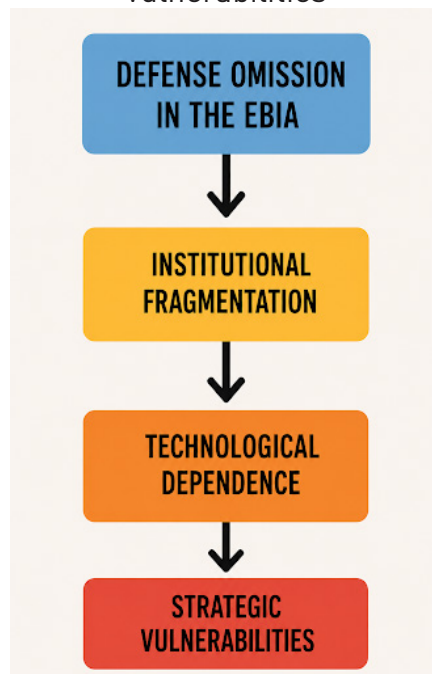
Furthermore, the implementation of transparency in development processes and international cooperation are central strategies to mitigate the risks associated with military AI. Aligning practices and norms to global ethical standards contributes to the construction of more reliable, secure, and consistent systems with the principles of international humanitarian law. For emerging countries, this approach not only strengthens technological capacity but also helps to consolidate credibility and trust in a global strategic scenario where AI plays a growing role in deterrence, decision-making, and the maintenance of regional stability (Blanchard and Bruun 2024).

Bringing the case of the conflict between Israel and Hamas, the use of AI systems, such as Lavender and Gospel by Israel, raises concerns about the dehumanization of the conflict, exacerbating historical inequalities and violating principles of international humanitarian law. This scenario highlights the urgency of establishing international regulations that govern the use of AI in military contexts, ensuring that the technology is employed in an ethical, transparent, and responsible manner, with effective human oversight, to prevent abuses and protect human dignity in times of war.

Given this international landscape, which elucidates systematic integration between AI development and defense capacity among major

powers, the lack of a chapter dedicated to Defense in EBIA triggers a chain of interconnected vulnerabilities, as illustrated in Figure 1. First, without clear strategic guidelines, the country does not establish priorities, coordination mechanisms or specific goals for AI applied to the military sector, enhancing the institutional fragmentation already present in the defense field. Second, this lack of coordination hinders project continuity, limits the development of autonomous capabilities, and reduces long-term planning capacity. Third, a direct consequence is heightened technological dependence on foreign suppliers, particularly in sensitive systems, cyber infrastructure and dual-use technologies, restricting national autonomy in critical areas.

Figure 1: Causal chain - from the omission in the EBIA to strategic vulnerabilities



Source: Prepared by the author (2024).

This cycle culminates in strategic vulnerabilities that directly affect the security of critical infrastructure and the country's ability to respond to hybrid threats and high-complexity conflicts. Thus, the initial omission of Defense in the EBIA not only represents a documental gap, but unleashes a process that connects, linearly and cumulatively, institutional fragmentation,

technological dependency and concrete risks to national sovereignty.

Proposals and recommendations

The analysis developed in the previous sections evidences the pressing need for a strategic reformulation for AI in Brazil, particularly regarding the Defense sector. The EBIA, although an initial milestone, presents significant limitations by neglecting the dimension of AI applied to Defense. To overcome this gap, the revision and amplification of the EBIA is proposed to incorporate specific guidelines for the development of AI in the aforementioned sector, with a focus on dual-use technologies that enable synergy between civilian and military applications.

This approach would allow maximizing investments and accelerating the development of national capabilities, especially in a scenario of budgetary restriction. The implementation of a specific National Program for the development of AI applied to defense emerges as a strategic imperative for Brazil, aligning itself with global trends of strengthening technological sovereignty.

It is understood that such a program should be structured around four fundamental axes: (i) development of sovereign computational infrastructure; (ii) training of specialized human resources; (iii) applied research in priority areas; and (iv) technology transfer to the Defense Industrial Base (BID). Furthermore, the governance of this program should adopt the triple helix model, integrating government, academia, and industry, with agile financing mechanisms and intellectual property protection. This approach would allow overcoming the bureaucratic limitations that historically compromise strategic initiatives in Brazil.

Concretizing the Proposals: International Lessons and National Mechanisms

For the proposals for incorporating AI into Brazilian Defense to become operational, it is essential to detail the “how” of their implementation, drawing inspiration from international models and exploring legal and institutional mechanisms already existing in Brazil.

The prioritization of dual-use technologies is a fundamental strategy to optimize investments in scenarios of limited resources. This approach finds a parallel in China’s “military-civil fusion,” which integrates

universities, industries, and military institutions to accelerate the transfer of innovations from the civilian sector to military applications (Kania 2020). Similarly, the United States seeks collaboration between the Department of Defense, academia, and industry, as exemplified by the “Stargate” project, which foresees massive investments in AI infrastructure with public-private partnerships, with an estimated investment of the order of US\$ 500 billion over the next four years (HuffPost 2025; Open AI 2025). For Brazil, focusing on areas such as cybersecurity or logistical optimization, which have vast civilian and military application, allows leveraging resources from multiple sources.

The implementation of the triple helix in Brazil must be accompanied by mechanisms that facilitate technology transfer to the Defense Industrial Base (BID), combating the historical technological dependence that authors such as Cardoso and Faletto (1970) and Furtado (1974) already pointed out and that persists until today as asserted by Girardi and Galdino (2024). The absence of specific guidelines for AI in defense compromises the development of a national industrial base in this strategic sector, reproducing center-periphery asymmetries. To reverse this framework, it is essential to explore and strengthen instruments such as:

- **Innovation Law (Law No. 10,973/2004 and its updates):** Which already provides mechanisms for interaction between Scientific and Technological Institutions (ICTs) and companies, including laboratory sharing, secondment of researchers, and patent licensing.

- **Technological Commissions:** A powerful instrument for the State to induce the development of specific AI solutions by the national industry, defining the need and sharing the technological risk.

- **Public-Private Partnerships (PPPs) and Joint Development Contracts:** Structures that allow the private sector to share the investment and risk in long-term AI projects, while the public sector guarantees demand and the testing environment.

- **Fostering Intellectual Property (IP):** Clear IP policies are essential to incentivize innovation and facilitate the licensing of technologies developed in universities or military centers to the BID.

The national experience already offers a successful model for this integration: the Integrated Border Monitoring System (SISFRON). It is a strategic project of the Brazilian Army that demonstrates the country's capacity to develop and integrate complex systems, with the active participation of the national industry (such as Savis and Bradar) in supplying advanced technologies. SISFRON serves as an internal “case study” that validates the

premise that Brazil can build sovereign technological capabilities, even in a domain different from AI, providing a roadmap for the future incorporation of AI in Defense.

The adequate dimensioning of investments in R&D constitutes a fundamental element for the development of national capabilities in AI for Defense. China's investment in research and development continues on an ascending trajectory, with expenditures totaling approximately US\$ 500 billion in 2024 (Xinhua 2025). Meanwhile, in the United States, important initiatives in artificial intelligence have been implemented, such as the "Stargate" project, which foresees investments that could reach the same value in the coming years (US\$ 500 billion) (HuffPost, 2025). Although Brazil cannot compete on the same scale of investment, the strategy must focus on the optimization of resources and the induction of an innovation ecosystem that overcomes the "insufficiency of technical knowledge" and the "subordination to large technology corporations and the powers that already dominate this sector" (Brazilian Academy of Sciences 2023).

Finally, we highlight that the revision of the EBIA must contemplate not only technological aspects, but also the ethical dilemmas and humanitarian impacts related to the employment of AI in military systems. The discussion should reference Responsible AI frameworks (such as the OECD principles and the DoD Ethical Principles for AI) and the recent debates on compliance with International Humanitarian Law, using cases such as Israel/Gaza and Ukraine to exemplify the ethical challenges, as already pointed out in section 2.

Conclusion

The analysis developed in this article, based on a multidisciplinary and comparative approach of international models, evidences that the strategic incorporation of Artificial Intelligence in the Defense sector constitutes an unavoidable imperative for the preservation of Brazilian sovereignty and national interests in the 21st century. By performing a critical analysis of the Brazilian Artificial Intelligence Strategy and quantifying the gap in the Defense sector, this work proposes concrete paths for overcoming this strategic vulnerability. The growing digitalization of conflicts and the emergence of hybrid threats demand advanced technological capabilities that Brazil has not yet developed satisfactorily, placing at risk not only its geopolitical projection but also the security of its critical infrastructures.

The lack of strategic autonomy identified in the Brazilian Defense sector

reflects historical patterns of technological dependence and discontinuity of public policies that compromise national development. As demonstrated by the evidence presented, this vulnerability is particularly acute in the field of military AI, where Brazil figures as a mere consumer of foreign technologies, often subject to restrictions and conditionings that limit its operational sovereignty.

The proposals outlined, such as the robust inclusion of defense in the Brazilian AI Strategy, the creation of a specific National Program for the military sector, the amplification of investments in R&D, and the establishment of strategic partnerships, constitute viable paths to reverse this framework. However, success depends on the implementation of State policies with adequate time horizons and consistent resources. The analyzed international experience offers both lessons and warnings for the Brazilian case, evidencing that merely incremental solutions will be insufficient in the face of the accelerated digital transformation of the global strategic environment.

The development of national capabilities in AI for defense demands a systemic approach that integrates multiple actors (government, academia, industry), contemplates diverse dimensions (technological, ethical, legal, operational), and establishes clear priorities aligned with national strategic objectives. In this sense, more than financial resources, Brazil needs strategic vision and adequate institutional arrangements that enable overcoming historical obstacles to its autonomous technological development.

The window of opportunity for the development of significant capabilities in AI for Defense is narrowing rapidly, as technological powers consolidate their leadership and widen the distance in relation to other countries. Brazil, due to its territorial dimension, strategic natural resources, and geopolitical position, cannot abdicate the development of technological capabilities compatible with its national interests and regional responsibilities, also contributing to the stability and security in South America. The question, therefore, is not if the country should invest in AI for Defense, but how to do it efficiently, ethically, and aligned with its national development project.

It is concluded, thus, that the effective incorporation of AI in the Brazilian national defense requires a profound revision of the EBIA to explicitly include the defense dimension, as well as the establishment of governance mechanisms that guarantee the continuity of national efforts in this strategic field. Only through a consistent State policy, which transcends political cycles and mobilizes adequate resources, can Brazil develop the necessary technological capabilities to face the challenges of the 21st century and guarantee its sovereignty in the digital and physical domains.

Acknowledgement

The authors received financial support for this research from the Coordination for the Improvement of Higher Education Personnel (CAPES) through the Program for Support to Teaching and Scientific and Technological Research in National Defense (Pró-Defesa V), under Public Notice No. 36/2023, Process No. 23038.011220/2023-31.

This study was funded by FAPERJ – Carlos Chagas Filho Foundation for Research Support of the State of Rio de Janeiro, SEI Process No. 260003/008748/2026.

References

- Brazilian Academy of Sciences. 2023. *Recomendações para o avanço da inteligência artificial no Brasil*. <https://www.abc.org.br/wp-content/uploads/2023/11/recomendacoes-para-o-avanco-da-inteligencia-artificial-no-brasil-abc-novembro-2023-GT-IA.pdf>
- AI Index Report. 2025. *Stanford University*.
- Allen, Greg and Taniel Chan. 2017. *Artificial intelligence and national security*. Belfer Center for Science and International Affairs.
- Ayres Pinto, Danielle and Sabrina Medeiros. 2022. “Inteligência artificial e seu uso no contexto militar: desafios e dilemas éticos”. *Cadernos Adenauer* 23 (2): 97-112.
- Ayoub, Kareem and Kenneth Payne. 2015. “Strategy in the Age of Artificial Intelligence”. *Journal of Strategic Studies* 39 (6): 793-819.
- Barbosa, Alexandre. 2020. “A Desinformação como Ferramenta da Guerra Híbrida”. PhD diss., Escola de Guerra Naval.
- Barreiros, Daniel and Italo Poty. 2021. “Estratégia Norte-Americana para o desenvolvimento de Inteligência Artificial Militar: um horizonte de curto prazo (2020-2030)”. *Austral* 10 (19): 206-224.
- Blanchard, Alexander and Laura Bruun. 2024. *Bias in Military Artificial Intelligence*. SIPRI.
- Boulanin, Vincent et al. 2020. *Artificial Intelligence, strategic stability and nuclear risk*. SIPRI.
- Brasil. Ministério da Ciência, Tecnologia e Inovação. 2021. *Aprova a Estratégia*

Nacional de artificial.

- Brasil. Ministério da Ciência, Tecnologia e Inovação. 2024a. *Aprova o Plano Brasileiro de Inteligência Artificial*.
- Brasil. Ministério da Defesa. Exército Brasileiro. 2024b. *Aprova a Diretriz Estratégica de Inteligência Artificial para o Exército Brasileiro EB20-D-02.031*.
- Brazilian Air Force. 2024. “FAB aposta em Inteligência Artificial para eficiência, segurança e inovação tecnológica”.
- Brazilian Air Force. 2025a. “CCA-SJ assina convênio inédito na área de Inteligência Artificial”.
- Brazilian Air Force. 2025b. “Pesquisa desenvolvida no ITA utiliza Inteligência Artificial”.
- Brundage, Miles et al. 2018. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Cornell University (Arxiv).
- Caixeta, Alécia. 2024. “A nova fronteira digital: Guerra Híbrida e o impacto da inteligência artificial na soberania dos países da América do Sul”. In *Geografia e sociedade: Compreendendo as dinâmicas globais*, edited by Adilson Basquerote. Atena Editora.
- Campany, Luiggi. 2021. Ameaças híbridas e a segurança marítima do século XXI. PhD diss., Escola de Guerra Naval.
- Canada. 2022. An introduction to cyber threat environment. Canadian Centre for Cybersecurity. *Communications Security Establishment*. <https://www.cyber.gc.ca/sites/default/files/ncta-2022-intro-e.pdf>
- Cardoso, Fernando Henrique, and Enzo Faletto. 1970. *Dependência e desenvolvimento na América Latina: ensaio de interpretação sociológica*. Zahar.
- Cassiolato, José Eduardo, and Helena Lastres. 2005. “Sistemas de inovação e desenvolvimento: as implicações de política.” *São Paulo em Perspectiva* 19 (1): 34-45.
- Chesney, Robert and Danielle Citron. 2019. “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security.” *California Law Review* 107 (6): 1753–1819.
- China. 2017. Ministry of Defence. Next Generation Artificial Intelligence Development Plan.
- Costa, Aristóteles. 2024. Guerra Híbrida: análise das características, impactos e estratégias de defesa no contexto contemporâneo. Diss., Escola de Guerra Naval.

- Cullen, Patrick and Erik Reichborn-Kjennerud. 2017. Understanding hybrid warfare: a multinational capability development campaign project. *MCDC*.
- Dagnino, Renato. 2009. "Elementos para uma teoria crítica da tecnologia." *Revista Brasileira de Ciência e Tecnologia* 1 (1): 3-33.
- United States of America. 2025. *Winning the Race: America's AI Action Plan*.
- Faria, Luis Claudio. 2024. *O impacto da IA para a Defesa Cibernética: proposta para criação do Comando Conjunto de Inteligência Artificial*. Undergraduate Thesis, Escola Superior de Guerra.
- Fattorini et al. 2024. *The Global AI Vibrancy Tool*. Stanford University.
- Fedasiuk, Ryan, Jennifer Melot and Ben Murphy. 2021. *Harnessed Lightning: How the Chinese Military Is Adopting Artificial Intelligence*. Center for Security and Emerging Technology, Georgetown University.
- Fernandes, Miguel. 2024. A regulamentação da IA: como evitar a irrelevância tecnológica em meio à busca por equilíbrio. *Exame*, December 18. <https://exame.com/inteligencia-artificial/a-regulamentacao-da-ia-como-evitar-a-irrelevancia-tecnologica-em-meio-a-busca-por-equilibrio/>.
- Floridi, Luciano. 2021. *The Ethics of Artificial Intelligence*. Oxford University Press.
- Fortune Business Insights. 2025. *Fortune Business Insights*. Accessed July 21, 2025. www.fortunebusinessinsights.com
- France. 2021. Ministry of the Armed Forces. *Stratégie Nationale en Intelligence Artificielle*.
- France. 2024. Ministry of the Armed Forces. *La stratégie française en intelligence artificielle*.
- Furtado, Celso. 1974. *O mito do desenvolvimento econômico*. Paz e Terra.
- Gil, Antônio Carlos. 1999. *Métodos e técnicas de pesquisa social*. Atlas.
- Girardi, Rômulo, and Juraci Ferreira Galdino. 2024. "A 'dualidade' Da Dualidade tecnológica: Implicações para países em desenvolvimento". *Coleção Meira Mattos* 18 (62): 189-216.
- Global Growth Insights. 2025. *Global Growth Insights*. Accessed July 21, 2025. www.globalgrowthinsights.com
- Godoy, Arilda Schmidt. 1995. "Pesquisa qualitativa: tipos fundamentais." *Revista de Administração de Empresas* 35 (3): 20-29.
- Haner, Justin and Denise Garcia. 2019. "The Artificial Intelligence Arms Race: Trends and World Leaders in Autonomous Weapons Development".

Global Policy 10 (3): 331-337.

- Hoffman, Frank. 2007. *Conflict in the 21st century: the rise of hybrid wars*. PhD diss., Potomac Institute for Policy Studies.
- Horowitz, Michael. 2018. "Artificial Intelligence, International Competition, and the Balance of Power". *Texas National Security Review* 1 (3): 36-57.
- HuffPost. 2025. "Trump anuncia una inversión privada de hasta 500.000 millones en inteligencia artificial". *Huffpost*, January 22. <https://www.huffingtonpost.es/global/trump-anuncia-inversion-privada-500000-millones-inteligencia-artificialbr.html>
- Hybrid CoE. n.d. *Hybrid Threats as a Concept*. Accessed March 28, 2025. <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>.
- ICRC. 2016. *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*. International Committee of the Red Cross.
- Instituto de Tecnologia e Sociedade do Rio. 2020. Resumo detalhado dos Planos estratégicos de desenvolvimento de Inteligência Artificial. <https://itsrio.org/wp-content/uploads/2020/03/RelatorioAI.pdf>.
- Israel. Ministry of Defence. 2025. National Program for Artificial Intelligence Program and Snapshot.
- Jobin, Anna, Marcello Ienca, and Effy Vayena. 2019. "The Global Landscape of AI Ethics Guidelines." *Nature Machine Intelligence* 1 (1): 389-399.
- Johnson, James. 2019. "Artificial Intelligence & Future Warfare: Implications for International Security". *Defense & Security Analysis*. Vol. 35 (2): 147-69.
- Kania, Elsa. 2017. *Battlefield singularity. Artificial intelligence, military revolution, and china's future military power*. Center for a new American security.
- Kania, Elsa. 2020. 'AI Weapons' in China's Military Innovation. Brookings Institution.
- Matos, Mauro Esdras. 2024. "A Integração da Inteligência Artificial com a Logística do Exército dos Estados Unidos da América". *Revista Doutrina Militar Terrestre* 12 (38): 38-45.
- Mimran, Tal and Gal Dahan. 2024. Artificial Intelligence in the Battlefield: A Perspective from Israel. *Opinio Juris*, April 20. <https://opiniojuris.org/2024/04/20/artificial-intelligence-in-the-battlefield-a-perspective-from-israel/>.
- Monitor do Oriente Médio. 2024. "Israel usa veículos blindados para limpar bombas na beira da estrada em Gaza". *Monitor do Oriente Médio*, December 30. <https://www.monitordo Oriente.com/20241230-israel->

usa-veiculos-blindados-para-limpar-bombas-na-beira-da-estrada-em-gaza/

Nadibaidze, Anna. 2022. "Great Power Identity in Russia's Position on Autonomous Weapons Systems." *Contemporary Security Policy* 43 (3): 407–35.

OECD. 2019. *Recommendation of the Council on Artificial Intelligence*. Organisation for Economic Co-operation and Development.

OECD.AI. 2025. "Investments in AI and Data." *OECD.AI*. <https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data&selectedVisualization=vc-investments-in-ai-by-country>

Open AI. 2025. "Anunciamos o projeto Stargate." *OpenAI*, January 21.

Outras Mídias. 2024. IA: a chance que o Brasil não pode desperdiçar. *Outras Mídias*, July 11. <https://outraspalavras.net/outrasmidias/ia-a-chance-que-o-brasil-nao-pode-desperdicar/>

Padilha, Luiz. 2025. França e Reino Unido desenvolvem um novo sistema para lidar com ameaças de minas submarinas. *Defesa aérea e naval*, April 4. <https://www.defesaaereanaval.com.br/defesa/franca-e-reino-unido-desenvolvem-novo-sistema-para-lidar-com-ameacas-de-minas-submarinas>.

Payne, Kenneth. 2018. "Artificial Intelligence: A Revolution in Strategic Affairs?" *Survival* 60 (5): 7-32.

United Kingdom. Ministry of Defence. 2021. *National Artificial Intelligence Strategy*.

United Kingdom. Ministry of Defence. 2022. *Defence Artificial Intelligence Strategy*.

United Kingdom. Ministry of Defence. 2025. *AI Opportunities Action Plan*.

Renic, Neil, and Elke Schwarz. 2023. "Crimes of Dispassion: Autonomous Weapons and the Moral Challenge of Systematic Killing." *Ethics & International Affairs* 37 (3): 321–43.

Responsible AI. 2024. *Global Index on Responsible AI*. CIFAR.

Rondepierre, Bertrand. 2024. "French military AI chief: AMIAD has an annual budget of €300 million and will receive a supercomputer". *Politico Europe*, March.

Rosa, Carlos Eduardo, Eduardo Araújo da Silva, and Pedro Barbezani Ribeiro. 2024. "A Geoestratégia dos Drones Aéreos". *Regeo-Revista Interdisciplinar* 15 (1): 1-21.

Russell, Stuart and Peter Norvig. 2016. *Artificial intelligence: a modern approach*.

Pearson.

- Russia. Ministry of Defence. 2019. *National Strategy for the Development of Artificial Intelligence Over the Period Extending up to the Year 2030*.
- Sá, Hebert Azevedo, Romullo Girardi, Julio Cesar Duarte, and Juraci Ferreira Galdino. 2025. “Tendências da inteligência artificial aplicada à defesa: forças, fraquezas, oportunidades e ameaças para o Brasil”. *Boletim De Conjuntura* 21 (62):01-33.
- Scharre, Paul. 2018. *Army of None: Autonomous Weapons and the Future of War*. W. W Norton & Company.
- Schneider, Sergio, and Cláudia Job Schimitt. 1998. “O uso do método comparativo nas Ciências Sociais.” *Cadernos de Sociologia*. 9 (1): 49–87.
- Serhan, Yasmeeen. 2024. “How Israel Uses AI in Gaza—And What It Might Mean for the Future of Warfare”. *Time*, December 18. <https://time.com/7202584/gaza-ukraine-ai-warfare/>
- Sputnik. 2024. “Brasil precisa desenvolver inteligência artificial militar e importar não é opção, diz analista”. *Sputnik*, April 11. <https://noticiabrasil.net.br/20240411/brasil-precisa-desenvolver-inteligencia-artificial-militar-e-importar-nao-e-opcao-diz-analista-34032454.html>
- Susnea, Elena and Ionuț-Cosmin, Buta. 2021. “Artificial intelligence in hybrid warfare: a literature review and classification”. *Strategies XXI* 17 (1): Proceedings of the 17th International Scientific Conference Strategies XXI.
- Topychkanov, Petr, ed. 2020. *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, Volume III: South Asian Perspectives. Stockholm International Peace Research Institute (SIPRI).
- UNESCO. 2021. *Recommendation on the Ethics of Artificial Intelligence*. United Nations Educational, Scientific and Cultural Organization.
- Vincent, Brandi. 2024. “Why the Pentagon Didn’t Request Higher Funding for AI in Fiscal 2025.” *DefenseScoop*, March 11.
- Walsh, Matthew; Worrell, Clarence and Scanlon, Thomas. 2024. *Toward the Use of Artificial Intelligence (AI) for Advanced Persistent Threat Detection*. Carnegie Mellon University.
- Woolley, Samuel and Philip Howard. 2018. *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford University Press.
- Xinhua. 2025. Gastos em pesquisa e desenvolvimento da China registram

rápido crescimento em 2024. *Xinhua*, January 23.

Zequim, Eduarda and Ribeiro, Douglas. 2022. “O papel da inteligência artificial na segurança cibernética: o uso de sistemas inteligentes em benefício da segurança dos dados das empresas”. *Revista Interface Tecnológica* 19 (1): 21–33.

Zia, Haleema. 2021. “The Evolution of Artificial Intelligence: Implications for Cybersecurity and Hybrid Warfare”. *Pakistan Journal of Terrorism Research* 3 (1): 1–28.

ABSTRACT

This article critically analyzes the absence of a National Defense chapter in the Brazilian Artificial Intelligence Strategy (EBIA). It identifies and discusses significant strategic vulnerabilities that this omission poses to national sovereignty, particularly given the current geopolitical landscape and increasing AI militarization. Serious implications of lacking technological autonomy in military AI are explored, considering dynamic contemporary contexts and emerging hybrid threats. The study proposes an integrated, pragmatic model, aligned with public policies, for effectively incorporating AI into Brazil's defense doctrine. This model encompasses autonomous technological development, highly specialized human resource training, and a robust military innovation ecosystem. Conclusions emphasize EBIA's pressing reformulation need, warning of increasing strategic vulnerability in an international scenario where AI is indispensable for state security and autonomy.

KEYWORDS

Artificial Intelligence; National Defense; Brazilian Artificial Intelligence Strategy.

Received on February 17, 2025

Accepted on June 16, 2026