

BRASIL SOB RISCO? A AUSÊNCIA DO SETOR DE DEFESA NA ESTRATÉGIA BRASILEIRA DE INTELIGÊNCIA ARTIFICIAL

Carlos Eduardo Franco Azevedo¹

Rachel Camilly Soares de Souza²

Introdução

A revolução provocada pela Inteligência Artificial (IA) tem reformulado as percepções estratégicas dos Estados no século XXI, podendo influenciar no equilíbrio de poder e nos conflitos internacionais (Horowitz 2018). A capacidade de processamento de dados em larga escala, aprendizagem automática e tomada de decisões em tempo real confere à IA um papel determinante nas doutrinas de defesa contemporâneas (Scharre 2018). As potências militares globais têm incorporado sistemicamente estas tecnologias em suas estratégias de defesa nacional, reconhecendo seu potencial transformador para manutenção da soberania e proteção de interesses nacionais (Payne 2018).

O desenvolvimento de sistemas autônomos de armas, algoritmos de detecção de ameaças, mecanismos de inteligência fundamentados em IA constituem, hoje, elementos essenciais para qualquer potência que pretenda assegurar sua autonomia no cenário internacional (Ayoub e Payne 2015). No Brasil, entretanto, constata-se uma grave lacuna institucional. A Estratégia Brasileira de Inteligência Artificial (EBIA), publicada em 2021, embora abrangente em diversos setores, negligencia aspectos fundamentais relativos à aplicação de IA para fins de defesa nacional (Brasil 2021). Esta

1 Escola de Comando e Estado Maior do Exército (ECEME), Rio de Janeiro, Brasil.
E-mail: francoazevedo@francaevedo.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.

omissão, longe de representar mero lapso documental, configura-se como uma vulnerabilidade estratégica, especialmente considerando o crescente emprego de tecnologias de IA.

Neste contexto, tendo como pergunta de pesquisa: Quais são as implicações da ausência da defesa nacional na Estratégia Brasileira de Inteligência Artificial? Este artigo propõe uma análise crítica da lacuna estratégica brasileira, comparando modelos internacionais de integração de IA às doutrinas de defesa, e avalia as vulnerabilidades resultantes para a defesa nacional. Sugere, ainda, diretrizes para a formulação de uma política pública específica de IA para o setor de defesa ou complementação em uma política pré-existente. A hipótese central sustentada é que a ausência de uma estratégia para incorporação de IA na defesa nacional constitui falha crítica que compromete a soberania brasileira em múltiplas dimensões: tecnológica, militar, econômica e geopolítica.

Para tanto, o estudo adota uma abordagem teórica multidisciplinar, incorporando contribuições de segurança internacional, dos estudos estratégicos contemporâneos e da literatura técnica sobre IA aplicada à defesa. A relevância deste estudo está na necessidade de fomentar o debate acadêmico e político sobre a inserção da IA na defesa do Brasil, de forma a mitigar vulnerabilidades e consolidar uma estratégia de proteção digital compatível com os desafios geopolíticos contemporâneos. Portanto, busca-se cooperar para o preenchimento desta lacuna crítica no pensamento estratégico brasileiro contemporâneo.

Metodologia

Este estudo buscou analisar criticamente a ausência do setor de Defesa na EBIA e suas implicações para a soberania nacional. Para tanto, adotou-se uma abordagem qualitativa (Gil 1999; Godoy 1995), fundamentada em uma análise multidisciplinar que incorporou contribuições da teoria de segurança internacional, dos estudos estratégicos contemporâneos e da literatura técnica sobre IA aplicada à defesa. A escolha por esta abordagem justifica-se pela necessidade de compreender em profundidade as nuances e as interconexões entre as políticas públicas de IA e o setor de defesa, bem como as complexas relações de poder e dependência tecnológica no cenário internacional.

A pesquisa desenvolveu-se pela coleta e análise de dados documentais (Gil 1999), tendo como principal fonte a revisão sistemática de documentos oficiais e relatórios. No âmbito nacional, foram examinados a EBIA, publicada em 2021, e o Plano Brasileiro de Inteligência Artificial (PBIA), de 2024. Esses

documentos foram centrais para identificar a abordagem oficial do Brasil em relação à IA e, mais especificamente, a presença ou ausência de diretrizes voltadas para o setor de defesa.

Complementarmente, consultaram-se estratégias nacionais de IA e documentos de defesa de países de destaque global. A seleção desses países, Estados Unidos, China, Reino Unido, França, Rússia e Israel, baseou-se em três critérios explícitos: (i) liderança internacional em pesquisa e desenvolvimento em IA, segundo indicadores como Stanford AI Index e OCDE.AI; (ii) relevância geopolítica e militar, especialmente no uso de IA de caráter dual ou estritamente militar; e (iii) existência de estratégias nacionais formalizadas, capazes de permitir comparação estrutural com a EBIA. Esses critérios asseguraram diversidade institucional, mas preservaram um mínimo de comparabilidade metodológica entre os casos.

Para garantir consistência na comparação, aplicou-se um protocolo de análise textual às estratégias selecionadas. Esse protocolo consistiu em identificar e quantificar termos-chave relacionados à defesa, como “defesa nacional”, “militar”, “forças armadas”, “segurança nacional” e “soberania”, além de expressões equivalentes utilizadas em diferentes tradições político-estratégicas. Em casos em que traduções literais não capturavam adequadamente o sentido estratégico, adotou-se o critério de equivalência conceitual, considerando termos como *souveraineté*, *autonomie stratégique*, *technological sovereignty* ou *resilience*, quando empregados com a mesma função analítica. Esse cuidado reduziu assimetrias linguísticas e reforçou a validade comparativa.

Os dados coletados foram submetidos a uma análise comparativa e textual (Schneider e Schmitt 1998). Inicialmente, realizou-se uma análise textual sistemática da EBIA e das estratégias internacionais selecionadas. Esta técnica permitiu quantificar a frequência de termos-chave relacionados à defesa e segurança (como “militar”, “forças armadas”, “defesa nacional”, “segurança nacional” e “soberania”) nos documentos, evidenciando a lacuna da dimensão de defesa na estratégia brasileira em comparação com as abordagens de outras nações. Com isso, observou-se as diferenças estruturais entre os documentos, examinando como cada país articula IA com suas doutrinas militares, políticas de inovação e mecanismos institucionais de integração civil-militar. Essa fase buscou identificar a presença de termos, assim como o modo como eles se inscrevem em arranjos institucionais, prioridades estratégicas e concepções de autonomia tecnológica.

Em seguida, procedeu-se a um estudo comparativo aprofundado (Schneider e Schmitt 1998), no qual as abordagens e prioridades do Brasil foram confrontadas com as tendências internacionais. Esta comparação

destacou o desalinhamento do Brasil em relação às potências globais e as vulnerabilidades estratégicas resultantes da omissão do setor de defesa na política nacional de IA.

Reconhecem-se, contudo, limitações inerentes ao método adotado: as estratégias nacionais variam em profundidade, terminologia e grau de transparência; parte das capacidades militares permanece classificada; e diferenças linguísticas podem introduzir nuances interpretativas. Ainda assim, ao explicitar critérios, procedimentos e limites, buscou-se reforçar a confiabilidade, consistência e reprodutibilidade do estudo. Finalmente, com base na lacuna identificada e na análise comparativa internacional, foram discutidas as implicações para a soberania e segurança do Brasil, considerando o contexto de ameaças híbridas e a persistente dependência tecnológica, elementos cruciais para a compreensão do cenário estratégico contemporâneo.

Inteligência Artificial e Defesa Nacional: Panorama Global

Cunhado nos anos 50, o termo inteligência artificial refere-se a programas de computador que simulam inteligência. Conforme Russell e Norvig (2016), a IA pode ser definida como a capacidade de sistemas de computador de executar tarefas que normalmente exigiriam inteligência humana, como reconhecimento de fala, tomada de decisões e solução de problemas. Sob uma ótica brasileira, a IA é definida como sistemas computacionais que, ao processar grandes volumes de dados para objetivos e autonomias específicas, podem prever, classificar, recomendar ou decidir, impactando ambientes físicos e virtuais (Brasil 2024a; Brasil 2024b).

A integração da Inteligência Artificial aos sistemas de defesa representa uma transformação significativa nos paradigmas militares. De acordo com Allen e Chan (2017), o desenvolvimento da IA pode ser tão transformador quanto armas nucleares, aviação e ciberespaço. Diferentemente de inovações incrementais, a IA reconfigurou fundamentalmente capacidades operacionais, táticas e estratégicas das forças armadas globais. Essa tecnologia disruptiva não só aprimora sistemas, mas possibilita novos modelos operacionais, gerando novas capacidades militares (Horowitz 2018).

As aplicações militares da IA abrangem diversas funções, aumentando o poder militar dos Estados. No domínio dos sistemas autônomos, a IA viabilizou o desenvolvimento de plataformas não-tripuladas com maior independência operacional. Segundo Scharre (2018), “A ascensão da inteligência artificial vai transformar a guerra”, tornando veículos aéreos,

terrestres e navais autônomos uma tendência inevitável nas doutrinas militares. O uso da IA na defesa revoluciona diferentes frentes, incluindo automação logística, otimização de decisão e desenvolvimento de armas autônomas. Na logística militar, por exemplo, o Departamento de Logística dos EUA utiliza ferramentas de IA, como o Logistics Federate (LOGFED), para treinar comandantes e estados-maiores em sustentação (Matos 2024).

À medida que essas aplicações vão se multiplicando nos diferentes contextos operacionais, observam-se três movimentos tecnológicos que costumam aparecer de forma recorrente nas estratégias de defesa de diversos países e que ajudam a compreender a direção geral tomada por essa transformação. Eles surgem como tendências que se entrelaçam na prática: o uso crescente da IA para apoiar processos de comando e controle, a expansão de sistemas autônomos em múltiplos domínios e a incorporação cada vez mais profunda de técnicas de IA às operações cibernéticas.

Em primeiro lugar, a IA tem sido incorporada às atividades de comando e controle, ampliando a capacidade de integrar informações, antecipar cenários e apoiar decisões em ambientes marcados pela complexidade e pelo volume crescente de dados. Os exemplos discutidos, como o uso de ferramentas avançadas de apoio à decisão e a otimização de processos logísticos, ilustram como a IA contribui para tornar o processo decisório militar mais responsivo e menos vulnerável ao excesso de informação.

Um segundo conjunto de aplicações aparece nos sistemas autônomos e semi-autônomos, tanto aéreos quanto terrestres ou navais, que se tornaram centrais na forma como as forças armadas conduzem reconhecimento, vigilância e, em alguns casos, até funções ofensivas. Tecnologias descritas no texto, como drones inteligentes, algoritmos de navegação autônoma e sistemas de identificação de alvos, mostram que a autonomização das plataformas é uma transformação estrutural no modo de operar no campo de batalha.

Por fim, a IA também desempenha papel no domínio cibernético, onde atua tanto na detecção de ameaças quanto na automação de respostas e na proteção de infraestruturas críticas. A discussão já presente sobre ataques cibernéticos baseados em IA evidencia como modelos adaptativos e técnicas automatizadas de intrusão modificam o ambiente informacional, introduzindo desafios inéditos para a defesa nacional.

Ademais, a rápida digitalização impulsionada pela IA transformou a defesa cibernética e os conflitos modernos. A IA é essencial para fortalecer a segurança de infraestruturas críticas e sistemas de comando e controle, tanto militar quanto civil, dado que ataques cibernéticos podem comprometer a soberania de um país (Faria 2014). A IA na Segurança da Informação é cada vez mais procurada para prevenir e combater ataques hackers, desafio

que transcende o setor privado e impacta diretamente a segurança nacional (Zequim e Ribeiro 2022).

Apesar do potencial transformador, a IA apresenta riscos inéditos à segurança internacional. A competição tecnológica entre EUA e China pode gerar novas guerras híbridas, com armas autônomas e ataques cibernéticos moldando o futuro dos conflitos (Johnson 2019). A ausência de debate e regulamentação eficaz pode levar à proliferação incontrolada de armas autônomas, ameaçando a estabilidade internacional (Haner e Garcia 2019). A introdução da IA em sistemas autônomos em conflitos é um tema controverso, exigindo acompanhamento ético e jurídico internacional. O uso prático da IA no campo de batalha já é realidade, demonstrado por drones e enxames no conflito russo-ucraniano (Rosa, Silva e Ribeiro 2024). As Forças de Defesa de Israel implantaram sistemas baseados em IA em suas operações, incluindo veículos blindados autônomos e sugestão de alvos como “The Gospel” e “Lavender” (Serhan 2024).

No Brasil, entretanto, as iniciativas de incorporação de IA na defesa permanecem incipientes e fragmentadas. Embora existam esforços pontuais — como o Laboratório de IA da FAB, o LIARC no IME e o Programa Pró-Defesa V – IATQ — essas ações carecem de articulação sistêmica e enquadramento estratégico nacional, conforme será detalhado na análise comparativa a seguir.

A comparação com o cenário internacional evidencia o distanciamento brasileiro em relação às demais nações. Segundo o relatório *The Global AI Vibrancy Ranking* (2024), da Universidade de Stanford, países como EUA, China, Reino Unido e Índia lideram o desenvolvimento de IA, enquanto o Brasil aparece em 34º de 36 Estados (Fattorini et al. 2024). Este descompasso tecnológico compromete a capacidade brasileira de responder autonomamente a conflitos contemporâneos. Para compreender essa lacuna e as abordagens bem-sucedidas, é fundamental analisar os modelos internacionais de IA na defesa, detalhados na próxima seção.

Embora Estados Unidos e China sejam naturalmente mais extensos pela abundância de documentos e escala dos programas de defesa, é possível observar que os demais países analisados partilham direções semelhantes e, em alguns casos, seguem até linhas mais maduras de integração entre IA e defesa. França e Reino Unido, por exemplo, articulam a IA a conceitos operacionais claros, como *information advantage* e *AI ready* no caso britânico e *autonomie stratégique* na doutrina francesa, e traduzem essas orientações em investimentos contínuos em sistemas autônomos, defesa cibernética e aplicações de IA para comando e controle. Esses países, ainda que com menor volume de recursos, apresentam estruturas institucionais consolidadas que vinculam inovação civil e militar, mostrando alto grau de coerência interna

em suas estratégias.

Rússia e Israel, por sua vez, reforçam tendências já discutidas nos casos estadunidense e chinês, especialmente no uso da IA para apoiar operações de larga escala, automatizar processos de seleção de alvos e sustentar ações ofensivas e defensivas no domínio cibernético. A Rússia prioriza capacidades baseadas em automação para compensar restrições industriais, além de integrar IA a sistemas de vigilância e guerra eletrônica; Israel, como já discutido no texto, combina tecnologias de autonomia, análise rápida de dados e integração operacional em ambientes urbanos altamente voláteis. Dessa forma, mesmo que o detalhamento documental seja menor, a direção estratégica é comparável: todos os países incorporam IA aos três eixos centrais, comando e controle, sistemas autônomos e capacidades cibernéticas, refletindo convergência internacional na militarização da IA.

Aspectos relativos aos modelos Internacionais de IA aplicados à Defesa

A revolução tecnológica impulsionada pela IA tem redefinido os paradigmas estratégicos e operacionais na defesa e segurança global. A capacidade da IA de processar dados, aprender padrões e automatizar processos transforma a operação e proteção das nações pelas organizações militares. Essa tecnologia disruptiva aprimora sistemas existentes e possibilita novos modelos operacionais e estratégias de defesa. Pesquisas proeminentes no setor nos últimos cinco anos incluem segurança cibernética, aprendizado de máquina, robótica, sensoramento, análise de dados, apoio à decisão, simulação e processamento de linguagem neural (Sá et al. 2025).

A crescente importância da IA reflete-se nos dados de mercado. Segundo a Fortune Business Insights, o mercado global de IA foi avaliado em US\$233,46 bilhões em 2024, projetando um crescimento de 29,2% até US\$1.771,62 bilhões em 2033 (Fortune Business Insights 2025). Nesse ecossistema, a IA aplicada à Defesa, embora menor, demonstra notável dinamismo, avaliada em US\$7,15 bilhões em 2024 e projetada para US\$23,06 bilhões até 2033 (Global Growth Insights 2025). Esse crescimento é impulsionado por orçamentos de defesa, preocupações com segurança global e avanços em IA, que aprimoram capacidades em vigilância, detecção de ameaças e sistemas autônomos. Assim, a IA não é só uma ferramenta de eficiência, mas um ativo que confere superioridade estratégica e aprimora defesas, tornando-se um setor competitivo em evolução. Governos e privados investem pesadamente para obter essa vantagem, resultando em inovações

contínuas.

Este panorama de investimentos e avanços tecnológicos serve de base para compreender as abordagens de diferentes nações. Modelos internacionais revelam abordagens diversificadas, mas com um comum denominador: a IA é pilar da segurança e soberania nacional. A seguir, detalham-se as principais iniciativas de países-chave.

Os EUA mantêm a liderança global em IA (1^o no The Global AI Vibrancy Ranking 2024 de Stanford) e demonstram forte compromisso com a integração da tecnologia em sua defesa. Sua estratégia nacional, “Mantendo a Liderança Americana em IA-2025” (2025), visa consolidar a liderança em P&D, sistemas autônomos, logística, infraestrutura de dados e IA de código aberto (Fattorini et al. 2024). Um pilar é o “Projeto StarGate” (2025), parceria público-privada que estima US\$ 500 bilhões em investimentos para infraestrutura e data centers (Open AI 2025). Os EUA também possuem estratégia de IA exclusiva para Defesa, materializada pela criação do Joint Artificial Intelligence Center (JAIC), em 2018 e, posteriormente, do Chief Data and Analytics Officers (CDAOs), em 2022, que absorveu o JAIC, centralizando a integração da IA nas operações militares (Barreiros e Poty 2021). O DoD (Departamento de Defesa) planeja investir US\$ 1,8 bilhão em IA em 2025 (US\$ 874 milhões em 2022) (Vincent 2024). Projetos importantes incluem Maven, JADC2 e Drones Loyal Wingman.

A China (2^o no The Global AI Vibrancy Ranking 2024) pretende se tornar o principal centro global de inovação em IA até 2030, desafiando a liderança dos EUA (Fattorini et al. 2024). Sua estratégia de IA na defesa inclui o programa “Inteligência Militar 2030”, integrado ao “Made in China 2025”, que transfere inovações civis para aplicações militares (Kania, 2017). A estratégia chinesa de IA, como observa Kania (2020), se destaca pela fusão militar-civil, que integra universidades, indústrias e militares no desenvolvimento tecnológico. Essa abordagem visa eliminar barreiras entre setores, promovendo inovação em tecnologias de uso dual para aplicações civis e militares. Permite que as mesmas tecnologias e equipes atuem simultaneamente, acelerando a incorporação de avanços de IA na defesa. Embora os gastos em P&D sejam abrangentes (US\$ 500 bilhões em 2024), o investimento em equipamentos com IA para fins militares variou entre US\$ 1,6 bilhão e US\$ 2,7 bilhões anuais (2018-2020). A China foca em “Guerra com IA”, vigilância, drones autônomos e suporte à decisão, consolidando-se como potência emergente em IA aplicada à defesa (Fedasiuk, Melot e Murphy 2021; Fattorini et al. 2024).

O Reino Unido (3^o no The Global AI Vibrancy Ranking 2024) adota abordagem dual, com estratégias nacionais de IA e específica para defesa

(Fattorini et al. 2024). Sua AI National Strategy (2021) e AI Opportunities Action Plan (2025) visam US\$ 500 bilhões na economia britânica até 2030 (Reino Unido 2021; Reino Unido 2025). O país investe em Centros de Doutorado em IA (US\$ 127 milhões) e “AI Growth Zones” (AIGZs), fomentando inovação em regiões estratégicas (Reino Unido 2025). Na defesa, a Defence AI Strategy (2022) busca tornar o Reino Unido uma organização eficaz e influente em IA, promovendo desenvolvimento militar seguro e responsável (Reino Unido 2022). Reino Unido e França colaboraram no Sistema de Contramedidas de Minas Marítimas (MMCM), solução inovadora com IA para detectar e neutralizar minas sem risco a marinheiros. O sistema, entregue em 2025, emprega sonar em barco drone para mapear minas, neutralizadas por veículo remoto. A IA acelera o processo e reduz a necessidade de navios tripulados, oferecendo vantagens em eficiência e segurança (Padilha, 2025). Combinando inovação e segurança nacional, o Reino Unido demonstra compromisso robusto com IA, reforçando sua posição como ator global em inteligência artificial.

A França (6^{ffi} no The Global AI Vibrancy Ranking 2024) busca soberania em IA para defesa, com investimentos em infraestrutura e inovação (Fattorini et al. 2024). Em março de 2024, lançou a “Stratégie ministérielle sur l’intelligence artificielle”, visando orientar e acelerar o uso de uma “IA de defesa” credível e eficaz. Uma iniciativa principal é a criação da Agência Ministerial para a IA de Defesa (AMIAD), que centraliza recursos e busca garantir o domínio francês dessas tecnologias, evitando dependência (França 2024). A estratégia também destaca a importância de um supercomputador dedicado à IA até 2025, o maior da Europa, capaz de processar dados classificados (França 2024). Como parte do esforço, a França anunciou US\$ 126 bilhões para infraestrutura e data centers, reforçando sua capacidade tecnológica e estratégica. O plano “França 2030” dedica 2,5 bilhões de euros (US\$ 2,7 bilhões) para IA na defesa, consolidando o papel estratégico da tecnologia (Rondepierre 2024). Com investimentos robustos, infraestrutura avançada e colaboração internacional, a França reforça sua posição como ator global em IA na defesa.

Israel (16^{ffi} no The Global AI Vibrancy Ranking 2024) é reconhecido pela inovação tático-operacional e integração sistêmica de IA, focando em aplicações militares e de segurança (Fattorini et al. 2024). O país investiu US\$ 300 milhões no Programa Nacional de IA, incluindo um supercomputador nacional e uma “Fábrica de IA” para integrar algoritmos à estratégia militar. Essa abordagem abrange operações militares, identificação de alvos, logística e sistemas autônomos, consolidando a IA como central nas doutrinas das Forças de Defesa Israelenses (IDF) (Mimran e Dahan 2024). Oficiais da IDF

destacaram o uso crescente de IA, especialmente no conflito Israel-Hamas (2023). Sistemas como Alchemist, Fire Factory e Depth of Wisdom coletam e analisam vastos volumes de inteligência (sinal, geográfica, humana e vigilância), permitindo disseminação eficiente de informações entre unidades e ataques militares precisos com veículos não tripulados e outras tecnologias autônomas (Renic e Schwarz 2023). Adicionalmente, Israel utiliza Gospel e Lavender para sugestão de alvos e monitoramento, e veículos blindados autônomos para limpeza de bombas. A integração de IA oferece vantagem tecnológica contínua, permitindo assimilar e aplicar inteligência de diversos domínios de guerra de forma eficiente e precisa.

A Rússia (29^o no The Global AI Vibrancy Ranking 2024) lançou em 2019 sua Estratégia Nacional de IA até 2030, priorizando Defesa, saúde, educação e automação empresarial. A estratégia busca reduzir dependência estrangeira e modernizar capacidades tecnológicas. Desde 2017, a Rússia enfatiza que a liderança em IA é essencial para soberania e posição global (Rússia 2019; Fattorini et al. 2024). Militarmente, a Rússia desenvolveu o Conceito para Uso de Sistemas Robóticos para Fins Militares até 2030, visando robotizar 30% do poder de combate até 2025, com orçamento de US\$ 346 bilhões até 2021. Criou também um departamento de IA no Ministério da Defesa, reforçando o compromisso com a automação (Nadibaidze 2022). A aplicação prática de IA foi anunciada por Putin durante a invasão da Ucrânia (2022), com mísseis hipersônicos como o Kinzhal, demonstrando integração de tecnologias avançadas (Ayres e Medeiros 2022). Esses avanços refletem o esforço russo em modernizar suas forças armadas e competir, consolidando sua posição geopolítica.

Por fim, o Brasil (34^o no The Global AI Vibrancy Ranking 2024) apresenta iniciativas incipientes e fragmentadas em IA para defesa (Fattorini et al. 2024). A EBIA não foca explicitamente na defesa, e o PBIA prevê investir R\$ 23 bilhões (US\$ 4.6 bilhões) em IA até 2028, sem orçamento específico para IA militar. No contexto brasileiro, as iniciativas de defesa em IA incluem: o Laboratório de IA da FAB (R\$ 6,5 milhões/US\$ 1,3 milhão), o LIARC no IME, o desenvolvimento de modelos de IA para detecção de destroços de aeronaves pelo ITA, a inclusão de disciplinas de IA nas Escolas Militares, a liderança no Programa Pró-Defesa V – IATQ, a promoção do simpósio “Inteligência Artificial na Expressão Militar do Poder Nacional” e a publicação da Diretriz Estratégica de IA do Exército Brasileiro (2024). Contudo, estas iniciativas carecem de articulação sistêmica e fundamentação doutrinária consolidada, refletindo a ausência de política nacional específica para a IA em defesa.

A Estratégia Brasileira de Inteligência Artificial e a Lacuna na Defesa

A Estratégia Brasileira de Inteligência Artificial, instituída pela Portaria MCTI nº 4.617, de 6 de abril de 2021, representa o primeiro esforço sistemático de formulação de política pública nacional para este campo tecnológico emergente (Brasil 2021). O documento estabelece visão, objetivos e eixos temáticos para orientar o desenvolvimento e aplicação de IA no país, buscando posicionar o Brasil como protagonista na chamada “Quarta Revolução Industrial” (Brasil 2021).

A EBIA estrutura-se em nove eixos temáticos: Legislação, Regulação e Uso Ético; Governança de IA; Aspectos Internacionais; Educação; Força de Trabalho e Capacitação; Pesquisa, Desenvolvimento, Inovação (PD&I) e Empreendedorismo; Aplicação nos Setores Produtivos; Aplicação no Poder Público; e Segurança Pública (Brasil 2021). Para cada eixo, o documento estabelece objetivos estratégicos e ações indicativas, delineando responsabilidades institucionais e prazos estimados de implementação.

Em análise crítica da estrutura e conteúdo da EBIA, observa-se uma ênfase em aspectos regulatórios, educacionais e de pesquisa básica, sem aprofundamento adequado em aplicações setoriais específicas. Com isso, apontamos que apesar da EBIA apresentar estrutura conceitual abrangente, demonstra um desequilíbrio entre formulações generalistas e diretrizes operacionais concretas, resultando em documento que, embora meritório como primeira iniciativa, carece de especificidade implementável.

O eixo Aspectos Internacionais destaca a cooperação global em IA, mas não menciona parcerias estratégicas para o desenvolvimento de tecnologias de defesa. Em um cenário global competitivo, onde países investem pesadamente em IA militar, o Brasil demonstra ignorar essa dimensão essencial. Embora o documento incentive a pesquisa e o desenvolvimento em IA, ele não direciona esforços para tecnologias voltadas à defesa. Países líderes em IA frequentemente priorizam projetos com aplicações duais (civis e militares), aspecto não considerado na estratégia brasileira (Brasil 2021).

Embora exista um eixo dedicado à segurança pública, ele se limita a aspectos como policiamento preditivo e combate ao crime organizado. Não há, contudo, menção ao papel da IA na defesa contra ameaças externas ou no fortalecimento da defesa cibernética do Brasil ou mesmo na defesa de infraestruturas críticas. Em um mundo onde ataques cibernéticos podem comprometer a soberania de um país, a falta dessa abordagem é preocupante (Brasil 2021).

Ainda que a EBIA não mencione a defesa, o Exército Brasileiro, por sua vez, formalizou a Diretriz Estratégica de Inteligência Artificial (Portaria EME/C Ex nº 1.318, de 14 de maio de 2024), estabelecendo orientações institucionais para a integração da IA no âmbito da organização. Seu objetivo central é promover a modernização e a eficiência operacional do Exército, por meio do emprego responsável de sistemas de IA em diferentes áreas, como logística, comunicação, inteligência e gestão de pessoal. Ao definir conceitos fundamentais, princípios e metas estratégicas, a diretriz busca fortalecer a tomada de decisão, a capacidade de antecipação de cenários e a competitividade tecnológica do Exército, alinhando suas iniciativas à Política de Informação da instituição (Brasil 2024b).

Além disso, a normativa enfatiza a importância do domínio de Tecnologias Emergentes e Disruptivas (TED) como instrumento de segurança do Estado e de transformação da dissuasão estratégica. Ela prevê a consolidação de competências institucionais para o desenvolvimento, implantação e uso ético da IA, garantindo que sua aplicação esteja em conformidade com os princípios morais e legais do Exército. Nesse contexto, a Portaria EME/C Ex nº 1.318/2024 representa um esforço estruturado para posicionar a instituição em sintonia com tendências globais de modernização militar, assegurando que a inovação tecnológica seja integrada de forma responsável e estratégica em suas operações (Brasil 2024b).

Esta análise evidencia que a EBIA, embora represente avanço institucional significativo como primeira política nacional formal para IA, apresenta lacunas críticas em sua concepção e estrutura. A ausência de tratamento específico para o setor de defesa não constitui mera omissão pontual, mas reflete abordagem conceitual que desconsidera a criticidade estratégica da IA para defesa nacional, desalinhando o Brasil de tendências globais predominantes neste campo.

A Lacuna na Defesa

A análise detalhada da EBIA revela uma ausência significativa de diretrizes, objetivos e ações específicas para a defesa nacional. Esta lacuna não é mera omissão pontual, mas uma falha estrutural na concepção estratégica do documento, com implicações profundas para a soberania e segurança nacional brasileira em um cenário global mediado por tecnologias disruptivas.

Para mensurar a extensão e gravidade desta lacuna, realizou-se análise textual sistemática da EBIA, comparando a frequência de termos-chave relacionados à defesa e segurança com as estratégias nacionais de IA de

outras potências. Os resultados na Tabela 1 evidenciam um desalinhamento da abordagem brasileira em relação às tendências internacionais predominantes.

Tabela 1: Frequência de Termos-Chave em Estratégias Nacionais de IA Seleccionadas

Termo-Chave	EUA	China	Reino Unido	França	Rússia	Israel	Brasil
Defesa Nacional	14	11	24	3	0	6	0
Segurança Nacional	23	8	18	1	1	4	0
Militar	7	13	0	0	0	0	2 (d)
(Segurança Interna/ Segurança Pública)	3	5	3	0	0	0	5(d)
Soberania	0	1 (a)	0	6	1 (a)	4 (a)	0
Seção Explícita de Defesa/ Militar	Yes	Yes (b)	Yes	Yes	No	No (c)	No
Total de Menções Explícitas	47	38	45	4	1	10	7 (d)

Fonte: elaborado pelos autores com base nas estratégias nacionais de IA dos países.

Legenda:

- (a) Quando não encontrada a palavra soberania, foi considerada a ênfase em “independência, autonomia e autonomia tecnológica”.
- (b) Na China, há uma seção para integração civil-militar para tecnologias de natureza dual;
- (c) Em Israel, a IA é considerada transversal às funções do Estado, porém o drive central é defesa. Na estratégia daquele país utilizou-se a palavra resiliência como sinônimo de Defesa Nacional;
- (d) No Brasil, os termos-chave foram encontrados 7 (sete) vezes, mas fora de contexto, se referindo a policiamento e proteção de dados; e
- (e) As estratégias consideradas na análise foram:
 - Estados Unidos: Winning the Race: America’s AI Action Plan, 2025.
 - China: Next Generation Artificial Intelligence Development Plan, 2017.
 - Reino Unido: National Artificial Intelligence Strategy, 2021.
 - França: Stratégie Nationale en Intelligence Artificielle (SNIA), 2021.
 - Rússia: 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.

- Brasil: Estratégia Brasileira de Inteligência Artificial (EBIA), 2021.

(f) As contagens de palavras foram realizadas nos documentos públicos disponíveis e podem variar ligeiramente dependendo da versão ou tradução utilizada.

A Tabela 1 revela que, enquanto potências como EUA, China e Reino Unido apresentam um número elevado de menções explícitas aos termos-chave (47, 38 e 45 menções, respectivamente), a EBIA registra apenas duas menções a “militar” e cinco a segurança pública, focadas em policiamento e proteção de dados. Não há menção a “defesa nacional”, “segurança nacional” ou “soberania” em seu corpo principal. As escassas menções ocorrem em contextos genéricos ou ilustrativos do eixo “Segurança Pública”, sem objetivos estratégicos, ações concretas ou mecanismos de implementação para o escopo deste estudo (Brasil 2021). Nesse sentido, a EBIA difere dos demais países. A China, por exemplo, formaliza a “fusão civil-militar” como pilar estratégico, garantindo rápida incorporação de avanços em IA à defesa (Kania 2020). EUA e Reino Unido, além de estratégias nacionais de IA, possuem estratégias exclusivas para a Defesa.

O contraste da EBIA com as demais estratégias é notório, mesmo em países com poucas menções diretas, onde a soberania é reveladora. França (6 menções a “*souveraineté*”), Rússia (1 menção a “*technological sovereignty*”) e Israel (4 menções a “*technological sovereignty*”) explicitam a IA como componente vital para autonomia e não dependência tecnológica. A EBIA, contudo, não aborda a soberania tecnológica na defesa. Para essas nações, a IA não é só ferramenta de eficiência, mas pilar da autodeterminação e proteção de interesses nacionais em ambiente geopolítico complexo. A Rússia, apesar de poucas menções explícitas à defesa, sublinha a “soberania tecnológica” como princípio fundamental, sugerindo que as aplicações de IA para defesa são intrínsecas à busca por autonomia.

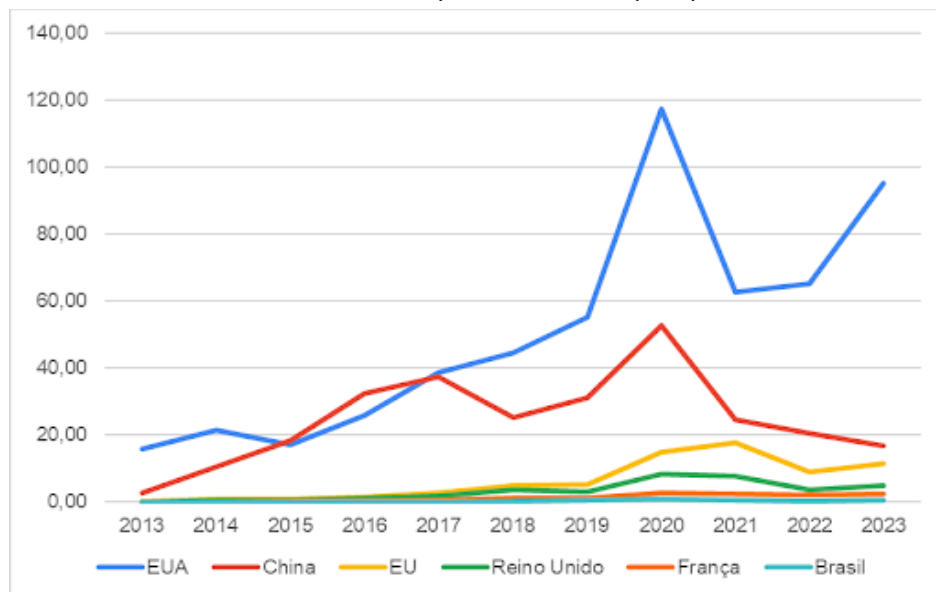
Tecnologicamente, a lacuna estratégica resulta em crescente dependência externa em sistemas militares críticos. Segundo a Academia Brasileira de Ciências (2023), a dependência de nações estrangeiras e multinacionais em IA pode comprometer a segurança, soberania e competitividade de empresas domésticas. Para desenvolver novas tecnologias baseadas em IA, é fundamental dominar seus princípios. A insuficiência de conhecimento técnico intensificará a subordinação a grandes corporações e potências que já dominam o setor.

A lacuna brasileira não se limita à dimensão conceitual e lexical. A disparidade de investimentos em IA é ainda mais evidente. O PBIA prevê

US\$ 4,6 bilhões em IA até 2028, sem orçamento específico para IA militar. Iniciativas isoladas das Forças Armadas incluem, como vimos, o Laboratório de IA da FAB (US\$ 1,3 milhão), o desenvolvimento de modelos de IA para detecção de destroços de aeronaves pelo ITA, e o LIARC no IME (Força Aérea Brasileira 2025a; Força Aérea Brasileira 2025b; Sá et al. 2025). Contudo, estas iniciativas são marcadas pela fragmentação institucional e limitação orçamentária.

Essa fragmentação e o volume de investimento contrastam agudamente com o cenário internacional, especialmente no que tange ao fomento do ecossistema de inovação e ao capital de risco. Em 2023, por exemplo, os Estados Unidos atraíram US\$ 95,037 bilhões em investimentos de capital de risco em IA, enquanto a China registrou US\$ 16,967 bilhões. No mesmo período, o Brasil atraiu apenas US\$ 482 milhões em investimentos de capital de risco em IA (Gráfico 1). Essa diferença abissal no fomento privado à inovação é um indicador crítico da fragilidade do ecossistema brasileiro e, por extensão, da capacidade do país de desenvolver soluções de IA para suas necessidades de defesa, comprometendo a autonomia tecnológica militar.

Gráfico 1: Investimentos de Capital de Risco por países (2013-2023)

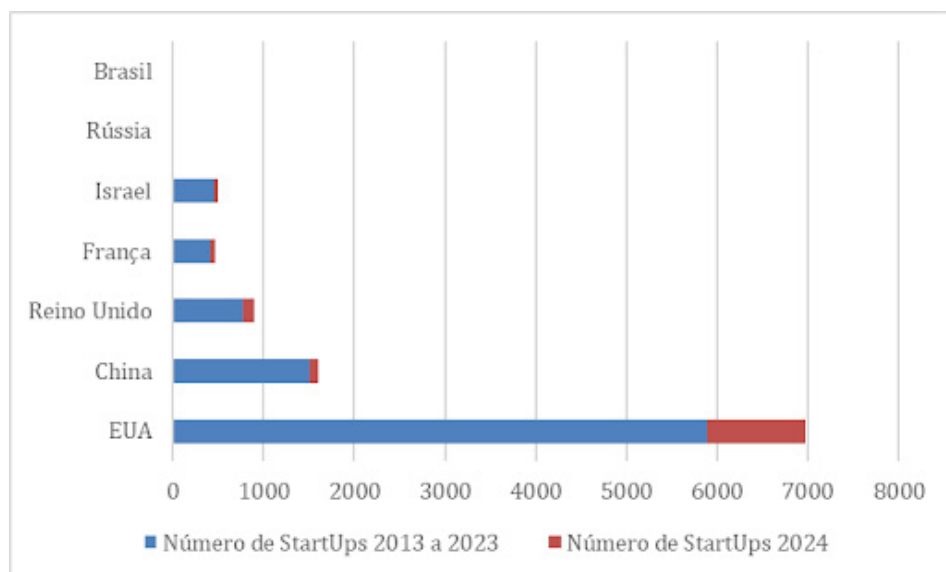


Fonte: OCDE.AI (2025)

Ainda mais preocupante é o número de startups de IA, motores

essenciais de inovação e agilidade, inclusive para a defesa. Enquanto EUA contam com 6.966 startups de IA (2013-2024) e a China com 1.606, o Brasil não registrou número significativo nesse período (Gráfico 2). Essa ausência de um ambiente vibrante de novas empresas de IA no Brasil, comparado a outros países, reflete falha fundamental na capacidade de gerar e escalar inovações no setor e, conseqüentemente, de suprir as demandas tecnológicas da defesa nacional com soluções domésticas de ponta.

Gráfico 2: Número de Startups por país no período de 2013-2024



Fonte: OCDE.AI (2025)

Essa lacuna brasileira contrasta com as tendências internacionais. Análise do relatório do ITS (março de 2020) sobre estratégias de IA de 20 países revelou que 7 (35%) continham “defesa” e/ou “segurança nacional” (Instituto de Tecnologia e Sociedade do Rio 2020). Mesmo Finlândia e Suécia, de tradição pacifista, incluem implicações da IA para a segurança nacional em suas estratégias.

O relatório do SIPRI (2020) demonstra como a IA reconfigura as dinâmicas de defesa nacional e poder estratégico. Todos os oito Estados nucleares analisados (EUA, Rússia, China, França, Reino Unido, Índia, Paquistão e Coreia do Norte) possuem programas ativos de integração de IA em

sistemas estratégicos, mas com disparidades em capacidades e investimentos. Os EUA lideram com US\$ 2 bilhões anuais via Defense Advanced Research Projects Agency (DARPA), enquanto o Paquistão enfrenta limitações, com apenas 650 pesquisadores especializados em IA.

Na inteligência, vigilância e reconhecimento (ISR), o relatório documenta que sete dos oito países (87,5%) desenvolveram sistemas de reconhecimento automático de alvos, e quatro (50%) implementaram processamento de dados onboard em veículos não tripulados. A China destaca-se, com avanços significativos em veículos hipersônicos com IA, como o DF-ZF. A Índia, a despeito de seus avanços, ainda depende de importações para 73% de seus componentes críticos de defesa, evidenciando assimetria tecnológica que tende a se aprofundar. Essa dependência cria vulnerabilidades estratégicas, como riscos de embargo e backdoors em sistemas sensíveis (Boulanin et al., 2020).

No campo de políticas públicas e governança, apenas três dos oito países (37,5%) estabeleceram diretrizes éticas explícitas para o uso militar de IA. A França destina € 100 milhões anuais para pesquisas que priorizam a supervisão humana, enquanto a China não impõe restrições públicas ao desenvolvimento de sistemas autônomos. Essa divergência normativa dificulta acordos internacionais; apenas duas iniciativas multilaterais significativas foram registradas até 2020. A falta de padrões comuns para desenvolvimento e emprego de IA militar cria um ambiente estratégico fragmentado e perigoso, onde incidentes ou corridas armamentistas podem surgir de interpretações equivocadas sobre capacidades e intenções adversárias (Boulanin et al., 2020).

O relatório SIPRI sobre IA no Sul da Ásia destaca que a Índia tem investido em IA para fortalecer sua segurança e estabilidade. Aquele país criou uma força-tarefa do Ministério da Defesa em 2018, o Centre for Artificial Intelligence and Robotics, para melhorar a inteligência e análise de dados. Em 2022, lançou o Defence Artificial Intelligence Council e o Defence AI Project Agency, com 75 projetos prioritários em IA e orçamento de 1.000 crore anuais até 2026. A Índia também desenvolve tecnologias emergentes, como veículos não tripulados e guerra cibernética, com a IA desempenhando papel significativo. A aplicação da IA em sistemas de armas nucleares e não nucleares é preocupação crescente, com implicações para a estabilidade estratégica na região (Topychkanov 2020).

Em contraste, o Brasil ainda não desenvolveu políticas oficiais de IA com foco militar ou de segurança nacional. Embora existam iniciativas emergentes no campo civil, como sugerido por discussões sobre regulamentação e investimentos em IA, não há programas comparáveis aos da Índia em escala, institucionalização ou aplicação estratégica. A ausência de políticas públicas

claras e a falta de instituições dedicadas à pesquisa defensiva em IA limitam a capacidade do Brasil de integrar a IA eficazmente em suas operações militares e de segurança nacional.

Apesar da crescente incorporação do termo “inovação” nas agendas nacionais desde os anos 1990, o Brasil ainda não assimilou plenamente seu significado sistêmico e interativo. Isso se reflete em políticas fragmentadas e desempenho inovativo reativo e pouco articulado (Cassiolato e Lastres 2005). Desde os anos 1960, estudos empíricos (Projeto SAPPHO, Reino Unido; Yale Innovation Survey, EUA) contribuíram para substituir a visão linear da inovação por uma concepção mais complexa. Esses estudos revelaram que o sucesso inovador se associa à capacidade das empresas de interagir com agentes externos de conhecimento, originando a noção de inovação como processo colaborativo, cumulativo e institucionalmente condicionado.

A compreensão da ausência de inteligência artificial na política de defesa brasileira ganha profundidade quando situada no pensamento estruturalista latino-americano, especialmente no âmbito da CEPAL. Essa abordagem destaca a centralidade do conhecimento, da transformação produtiva e das condições institucionais locais no desenvolvimento, convergindo com perspectivas contemporâneas de sistemas de inovação que enfatizam a necessidade de políticas estatais ativas para promover mudanças técnicas e produtivas (Cassiolato e Lastres 2005). Em ambos os quadros analíticos, o desenvolvimento não decorre de forças espontâneas do mercado, mas de arranjos intencionais que coordenam capacidades, instituições e setores estratégicos.

Na perspectiva dos sistemas de inovação, tais arranjos são dinâmicos, historicamente construídos e dependem da interação contínua entre empresas, universidades, centros de pesquisa, órgãos governamentais e sociedade civil. Trata-se de articular redes que gerem aprendizado, difusão tecnológica e capacidades endógenas (Dagnino 2009). No caso brasileiro, contudo, há uma dissonância entre o discurso de valorização da inovação e a prática institucional que a sustenta: políticas fragmentadas, baixa coordenação entre iniciativas e uma estrutura produtiva dominada por setores de baixa intensidade tecnológica limitam a consolidação de um sistema nacional robusto.

Cassiolato e Lastres (2005) argumentam que, para que sistemas de inovação sejam eficazes em países periféricos, é fundamental que o Estado atue como coordenador, fortalecendo encadeamentos produtivos internos e garantindo políticas duradouras capazes de construir capacidades locais. Entretanto, como aponta Dagnino (2009), o Brasil frequentemente adota políticas descontinuadas, excessivamente financeiras e pouco orientadas à

construção institucional ou ao fortalecimento da base produtiva nacional.

Esses desafios se intensificam porque a articulação entre ciência, tecnologia e desenvolvimento não gera automaticamente progresso socioeconômico. Sem um ambiente institucional propício, mecanismos de coordenação intersetorial e políticas coerentes com as capacidades locais, a produção de conhecimento tende a permanecer desconectada da realidade produtiva, reforçando dependências históricas e vulnerabilidades externas. É nesse ponto que a teoria da dependência, especialmente em Cardoso e Faletto, contribui para compreender por que tecnologias estratégicas, como a inteligência artificial, permanecem ausentes das diretrizes centrais de defesa no Brasil.

Para esses autores, a dependência não opera por meio de mecanismos institucionais, políticos e epistemológicos que inserem países periféricos em posições subordinadas no sistema global. A reconfiguração da dependência na segunda metade do século XX mostra que, mesmo quando o controle externo não é explícito, ele se reproduz por meio da penetração do capital internacional, da importação de tecnologias e do alinhamento das elites domésticas às lógicas externas de acumulação (Cardoso e Faletto 1970).

Furtado (1974) acrescenta que o subdesenvolvimento é um fenômeno estrutural, funcional ao próprio capitalismo global, no qual o domínio da inovação permanece concentrado nos países centrais. Nessas economias, a articulação entre ciência, tecnologia e poder político possibilita a internalização do progresso técnico; já na periferia, a inovação tende a ser importada de forma subordinada, sem domínio dos fundamentos científicos ou das infraestruturas que a sustentam. Essa crítica continua plenamente válida na era digital: ao importar tecnologias sem domínio de sua lógica interna, o país reforça sua posição periférica, transformando a tecnologia em vetor de subordinação e não de autonomia.

Essas interpretações ajudam a explicar por que a IA, apesar de seu caráter estratégico global, permanece marginal na política de defesa do Brasil. A ausência de uma diretriz clara reflete na persistência de um padrão histórico de inserção subordinada em tecnologias críticas. A “integração” às redes globais de inovação, frequentemente interpretada como sinal de modernização, é, em muitos casos, apenas um mecanismo de aprofundamento da dependência, na medida em que a produção de conhecimento e tecnologia permanece externalizada. Esse padrão é reforçado por elites nacionais que, ao aderir a paradigmas e modelos importados, negligenciam a formulação de estratégias tecnológicas coerentes com as vulnerabilidades e potencialidades do país. A dependência torna-se, assim, não apenas econômica, mas institucional e epistemológica.

O resultado é uma dissociação persistente entre ciência, tecnologia, defesa e projeto de nação. Sem uma estratégia que articule universidades, Forças Armadas, agências governamentais e setores produtivos, torna-se inviável construir um complexo militar-tecnológico soberano. Mesmo iniciativas pontuais, como laboratórios de pesquisa ou programas de modernização, tendem a perder continuidade por falta de coordenação estratégica. No caso específico da IA, essa fragmentação significa delegar funções críticas a atores externos, importando sistemas, algoritmos e infraestruturas que o Brasil não controla plenamente. Essa prática amplia vulnerabilidades, sobretudo no domínio cibernético, onde a dependência tecnológica pode comprometer diretamente a segurança nacional.

Portanto, a ausência de IA na política de defesa brasileira não é um evento acidental, mas a atualização de um padrão histórico de subordinação estrutural. Ela reflete a reprodução de um modelo no qual o país ocupa funções periféricas, consumindo tecnologias concebidas no centro sem internalizar sua lógica de produção. Romper com esse padrão exige mais do que ajustes incrementais: requer uma inflexão profunda no modo como o Brasil concebe inovação, soberania e poder nacional. Em última instância, exige reconhecer que a soberania tecnológica, especialmente em áreas estratégicas como IA militar, não se herda: constrói-se.

Implicações da ausência de uma Estratégia de IA para Defesa no Brasil

No contexto representado por vulnerabilidades trazidas com a revolução digital, a IA interage como uma ferramenta que perpassa diversas áreas no setor de defesa. O ambiente tecnológico incorporado no teatro operacional dos conflitos, apresenta-se como uma nova forma de emprego da violência que utiliza meios físicos, cibernéticos, elementos irregulares, políticos, dentre outros (Campany 2021). Esses elementos são parte da constituição do conceito de Guerra Híbrida desenvolvido por Hoffman (2007) em sua tese intitulada “Conflict in the 21st Century: the rise of Hybrid Wars”.

Partindo dessa ideia, desenvolveu-se o conceito de ameaças híbridas, que de acordo com o Centro Europeu de Excelência para o Combate a Ameaças Híbridas (Hybrid CoE), são: “Atividades prejudiciais que são planejadas e executadas com intenção maligna. Elas visam minar um alvo, como um estado ou uma instituição, por meio de uma variedade de meios, geralmente combinados.” Embora priorizem o uso de ferramentas não militares, geram impactos significativos nas sociedades afetadas que, por vezes, correspondem

aos de uma agressão militar. Dentre esses, incluem-se os ataques cibernéticos, a desinformação, as sabotagens, o patrocínio a organizações criminosas ou terroristas, a exploração de vulnerabilidades econômicas e até a corrupção de agentes públicos (Campany 2021).

Na América do Sul, a desinformação tem se consolidado como uma ameaça híbrida recorrente, sendo empregada para manipular a opinião pública, enfraquecer governos e influenciar processos políticos (Caixeta 2024). Esse fenômeno visa desestabilizar o cenário político ao comprometer a confiança da população nas instituições democráticas e fomentar divisões internas. No Brasil, as eleições presidenciais de 2022 evidenciaram esse cenário, com o ambiente digital se transformando em um espaço estratégico para o fomento de ameaças híbridas. A rápida disseminação de informações, aliada à dificuldade de rastreamento e atribuição dessas campanhas, faz da guerra digital um fator altamente influente e com grande potencial desestabilizador (Caixeta 2024).

Os avanços nas tecnologias da informação e comunicação, assim como a ampliação dos serviços acessíveis, possibilitaram a transição do modelo tradicional de guerra para o conceito de guerra híbrida. Nesse novo cenário, ameaças características dos conflitos convencionais, como as nucleares, foram gradualmente complementadas por novas formas de ameaça (Susnea e Ionuț-Cosmin 2021). Entre elas, destacam-se as ciberameaças, que consistem em ações conduzidas por Estados ou organizações internacionais com o objetivo de atacar e comprometer sistemas computacionais e redes de informação de outras nações (Canadá 2022).

Sendo assim, a ausência de componente específico para IA em defesa na estratégia brasileira manifesta-se de forma particularmente crítica no domínio da ciberdefesa. Para Brundage et al. (2018) a IA pode ser usada para expandir ameaças existentes, introduzir novas ameaças e alterar o caráter típico das ameaças, tornando-as mais eficazes, direcionadas e difíceis de atribuir. Ademais, pode permitir que ataques cibernéticos sejam realizados em maior escala e com maior eficácia, reduzindo a necessidade de intervenção humana e aumentando a complexidade das respostas necessárias.

A evolução recente de ataques cibernéticos evidencia transformação fundamental em sua natureza e complexidade. Ataques de Persistência Avançada (APTs) baseados em IA caracterizam-se por capacidade adaptativa, comportamento autônomo e habilidade de invadir sistemas convencionais de detecção. As ferramentas tradicionais de detecção e mitigação podem não ser suficientes para lidar com essas ameaças, dada a sua natureza evolutiva e sigilosa. A IA, especialmente o *deep learning*, é vista como uma solução promissora para melhorar a detecção e a defesa contra APTs (Walsh, Worrell

e Scanlon 2024).

A convergência entre IA e as mídias sociais representa um risco crescente para a integridade do ecossistema informacional. Modelos generativos de linguagem e síntese de imagens, quando combinados com redes automatizadas de desinformação, permitem a disseminação coordenada de narrativas falsas em escala industrial (Chesney e Citron 2019). A velocidade exponencial dessas campanhas aumenta sua eficácia, tornando o ambiente digital particularmente vulnerável a manipulações (Woolley e Howard 2018).

Os avanços na tecnologia e as tendências de poder e interdependência têm impulsionado o crescimento do uso da guerra híbrida, proporcionando capacidades inovadoras tanto no domínio militar quanto no não militar (Costa 2024). Como consequência, não apenas o aparato bélico será transformado, mas também a dimensão humana na guerra será afetada. O reflexo das aplicações de IA na guerra híbrida pode ser descrito e explicado pelo uso sinérgico de cinco diferentes instrumentos e meios de poder, conhecidos como MPECI – Militar, Político, Econômico, Civil e Informacional –, que são utilizados para explorar vulnerabilidades dos inimigos (Cullen e Reichborn-Kjennerud 2017).

A dimensão militar inclui o uso de sistemas militares habilitados por IA, abrangendo robôs aquáticos, aéreos e terrestres. Grandes progressos foram feitos no desenvolvimento de armas e tecnologias baseadas em IA. Por exemplo, Israel tem empregado veículos blindados de transporte de pessoal M113, carregados com explosivos, para neutralizar armadilhas e dispositivos explosivos na Faixa de Gaza (Monitor do Oriente 2024). Além disso, programas de IA, como “The Gospel” e “Lavender”, são utilizados para sugerir alvos para ataques aéreos e monitorar membros suspeitos do Hamas, contribuindo para uma rápida identificação e eliminação de alvos, embora frequentemente resultando em baixas civis significativas (Serhan 2024). Esses exemplos ilustram o uso crescente de IA em operações militares, destacando a necessidade de equilibrar a eficácia tecnológica com a supervisão ética e legal.

A dimensão econômica da IA pode ser explicada no contexto da guerra híbrida. Quando Estados são alvos de ataques híbridos, frequentemente recorrem a contra-ataques por meio de coerção econômica, como isolamento financeiro e sanções. Ferramentas baseadas em IA são empregadas para otimizar investimentos de capital, avaliar qualidade de crédito, garantir conformidade regulatória, monitorar transações comerciais e detectar fraudes (Zia 2021). A IA tem grande utilidade no domínio da informação, que é crucial para moldar o discurso político, influenciar percepções populares e alterar resultados políticos por meio da manipulação da disponibilidade de

informações (Barbosa 2020).

Outro ponto é a dependência de tecnologias estrangeiras. Sem o desenvolvimento autônomo de sistemas de IA, o Brasil pode se ver obrigado a importar soluções de outros países, o que pode comprometer a soberania nacional e a segurança das informações militares. Além disso, a ausência de uma estratégia de IA pode levar a uma defasagem tecnológica em relação a outras nações que já incorporam essas tecnologias em suas forças armadas. Essa defasagem pode resultar em desvantagens operacionais, especialmente em missões de alto risco, como operações de desminagem e reconhecimento, onde a IA pode ser empregada para minimizar riscos humanos (Sputnik 2024).

Apesar deste trabalho ter como foco a EBIA, o recém-publicado Plano Brasileiro de Inteligência Artificial apresenta o mesmo déficit que contestamos. O Plano ainda foca em aplicações secundárias, deixando de lado tecnologias centrais como modelos de linguagem. Para mudar esse cenário, é essencial articular políticas de inovação e proteção de dados estratégicos (Outras mídias 2024). Essa abordagem reproduz o padrão histórico de importação de know-how, agravado pela falta de investimentos em semicondutores e infraestrutura computacional de alto desempenho (Fernandes 2024).

A análise dos dilemas éticos no âmbito da IA no campo militar demanda a convergência de três eixos complementares: a mensuração e monitoramento das práticas de IA responsável (*Global Index on Responsible AI*), os princípios normativos globais consolidados em frameworks de Responsible AI e a reflexão jurídico-humanitária sobre sistemas de armas autônomas letais (*Lethal Autonomous Weapons Systems – LAWS*) conduzida por organismos como o *International Committee of the Red Cross* (ICRC). Embora cada relatório aborde dimensões distintas, a integração das três perspectivas revela que a governança tecnológica atual é marcada por assimetrias estruturais, com implicações diretas para a segurança internacional e a proteção de civis.

Do ponto de vista da medição, o *Responsible AI* destaca indicadores de segurança, transparência e prestação de contas como fundamentos para uma IA responsável (Responsible AI 2024). Contudo, a aplicação militar da IA, especialmente em contextos letais, é tratada de forma periférica, sem examinar com profundidade dilemas como as implicações humanitárias documentadas em conflitos recentes, por exemplo, entre Israel e Hamas. A ausência de métricas específicas para capacidades militares de IA e para a vulnerabilidade de diferentes contextos nacionais, sobretudo do Sul Global, limita a capacidade do índice de capturar desigualdades geopolíticas.

Já os relatórios da *UNESCO Recommendation on the Ethics of AI* (2021) e os *OECD AI Principles* (2019), fornecem um arcabouço normativo

robusto. Eles enfatizam princípios como *human-in-the-loop*, auditabilidade, mitigação de vieses e conformidade com o Direito Internacional Humanitário (Jobin, Ienca e Vayena 2019; Floridi 2021). No entanto, esses marcos são predominantemente elaborados no Norte Global, refletindo seus valores e prioridades. Para países do Sul Global, com recursos institucionais limitados, a adoção acrítica desses *frameworks* pode resultar em dependência tecnológica e em lacunas regulatórias, perpetuando um modelo assimétrico de governança.

Por sua vez, o relatório do ICRC sobre armas autônomas (ICRC 2016) traz uma perspectiva jurídico-operacional concreta, evidenciando como o aumento da autonomia nas funções críticas de ataque coloca em risco princípios como distinção, proporcionalidade e precaução. A convergência desses relatórios permite identificar que o desafio central não é apenas tecnológico, mas normativo e estrutural. Um regime global de governança de IA verdadeiramente responsável precisa incluir métricas específicas de capacidades militares no âmbito ético, adaptado às realidades institucionais do Sul Global. Sem tal abordagem integrada, o risco é consolidar um cenário no qual as potências definem unilateralmente os limites éticos da IA militar, enquanto os outros Estados arcam de forma desproporcional com os custos humanos e estratégicos de sua implementação.

O relatório do SIPRI, *Bias in Military Artificial Intelligence* (2024), aborda os riscos associados aos vieses presentes em sistemas de IA militar, enfatizando suas implicações éticas, humanitárias e estratégicas. Embora o estudo não se concentre especificamente em países emergentes, suas conclusões são altamente relevantes para essas nações, que estão em processo de desenvolvimento ou aquisição de tecnologias de IA aplicadas à defesa. O relatório define o viés em IA militar como o desempenho sistemicamente distorcido de um sistema que pode gerar decisões injustas ou prejudiciais, influenciadas por fatores sociais, culturais ou econômicos, tais como raça, gênero ou classe. Tais vieses podem surgir de três fontes principais: viés na sociedade, viés nos dados e algoritmos, e viés no uso operacional da tecnologia, podendo comprometer a eficácia das operações e gerar consequências humanitárias graves, como identificação incorreta de alvos ou falhas na avaliação de necessidades críticas (Blanchard e Bruun 2024).

Para países emergentes, o impacto desses vieses é particularmente relevante, dado que a infraestrutura de pesquisa e os dados disponíveis frequentemente apresentam limitações. A ausência de diversidade nos dados de treinamento, combinada com regulamentações ainda incipientes sobre uso militar de IA, aumenta a probabilidade de resultados distorcidos, reduzindo a confiabilidade e a ética das operações. Assim, é essencial que essas nações adotem práticas de desenvolvimento responsável desde o início, incorporando

mecanismos de supervisão, validação de algoritmos e revisão por múltiplos stakeholders, incluindo universidades, indústria e sociedade civil. Dessa forma, é possível reduzir os riscos de vieses e fortalecer a legitimidade do uso da IA no contexto de segurança e defesa (Blanchard e Bruun 2024).

Além disso, a implementação de transparência nos processos de desenvolvimento e a cooperação internacional são estratégias centrais para mitigar os riscos associados à IA militar. Alinhar práticas e normas a padrões éticos globais contribui para a construção de sistemas mais confiáveis, seguros e consistentes com os princípios de direito internacional humanitário. Para países emergentes, essa abordagem não apenas fortalece a capacidade tecnológica, mas também ajuda a consolidar credibilidade e confiança em um cenário estratégico global onde a IA desempenha um papel crescente na dissuasão, na tomada de decisão e na manutenção da estabilidade regional (Blanchard e Bruun 2024).

Trazendo o caso do conflito entre Israel e Hamas, o uso de sistemas de IA, como o *Lavender* e o *Gospel* por Israel, levanta preocupações sobre a desumanização do conflito, exacerbando desigualdades históricas e violando princípios do direito internacional humanitário. Esse cenário destaca a urgência de estabelecer regulamentações internacionais que governem o uso de IA em contextos militares, assegurando que a tecnologia seja empregada de maneira ética, transparente e responsável, com supervisão humana efetiva, para prevenir abusos e proteger a dignidade humana em tempos de guerra.

A partir desse panorama internacional, que evidencia a integração sistemática entre desenvolvimento de IA e capacidades de defesa nas principais potências, a ausência de um capítulo dedicado à Defesa na EBIA desencadeia uma cadeia de vulnerabilidades interconectadas, conforme ilustrado na Figura 1. Primeiro, sem diretrizes estratégicas claras, o país não estabelece prioridades, mecanismos de coordenação ou metas específicas para IA aplicada ao setor militar, intensificando a fragmentação institucional já presente no campo de defesa. Segundo, essa desarticulação dificulta a continuidade de projetos, limita a formação de capacidades autônomas e reduz a capacidade de planejamento de longo prazo. Terceiro, como consequência direta, acentua-se a dependência tecnológica em relação a fornecedores estrangeiros, especialmente em sistemas sensíveis, infraestrutura cibernética e tecnologias dual-use, restringindo a autonomia nacional em áreas críticas.

Figura 1: Cadeia causal: da omissão na EBIA às vulnerabilidades estratégicas vulnerabilities



Fonte: Elaborada pelo autor (2024).

Esse ciclo culmina em vulnerabilidades estratégicas que afetam diretamente a segurança de infraestruturas essenciais e a capacidade do país de responder a ameaças híbridas e conflitos de alta complexidade. Assim, a omissão inicial da Defesa na EBIA não representa apenas uma lacuna documental, mas desencadeia um processo que conecta, de forma linear e cumulativa, fragmentação institucional, dependência tecnológica e riscos concretos à soberania nacional.

Propostas e recomendações

A análise desenvolvida nas seções anteriores evidencia a necessidade premente de uma reformulação estratégica para a IA no Brasil, particularmente no que tange ao setor de defesa. A EBIA, embora seja um marco inicial, apresenta limitações significativas ao negligenciar a dimensão de IA aplicada à Defesa. Para superar esta lacuna, propõe-se a revisão e ampliação da EBIA para incorporar diretrizes específicas para o desenvolvimento de IA no

referido setor, com foco em tecnologias de uso dual que possibilitem sinergia entre aplicações civis e militares.

Esta abordagem permitiria maximizar os investimentos e acelerar o desenvolvimento de capacidades nacionais, especialmente em um cenário de restrição orçamentária. A implementação de um Programa Nacional específico para o desenvolvimento de IA aplicada à defesa surge como imperativo estratégico para o Brasil, alinhando-se às tendências globais de fortalecimento da soberania tecnológica.

Entende-se que tal programa deveria estruturar-se em quatro eixos fundamentais: (i) desenvolvimento de infraestrutura computacional soberana; (ii) formação de recursos humanos especializados; (iii) pesquisa aplicada em áreas prioritárias; e (iv) transferência tecnológica para a Base Industrial de Defesa (BID). Ademais, a governança deste programa deve adotar o modelo de tríplice hélice, integrando governo, academia e indústria, com mecanismos ágeis de financiamento e proteção de propriedade intelectual. Esta abordagem permitiria superar as limitações burocráticas que historicamente comprometem iniciativas estratégicas no Brasil.

Concretizando as Propostas: Lições Internacionais e os Mecanismos Nacionais

Para que as propostas de incorporação da IA na defesa brasileira se tornem operacionais, é essencial detalhar o “como” de sua implementação, inspirando-se em modelos internacionais e explorando mecanismos legais e institucionais já existentes no Brasil.

A priorização de tecnologias de uso dual é uma estratégia fundamental para otimizar investimentos em cenários de recursos limitados. Essa abordagem encontra paralelo na “fusão militar-civil” da China, que integra universidades, indústrias e instituições militares para acelerar a transferência de inovações do setor civil para aplicações militares (Kania 2020). Da mesma forma, os Estados Unidos buscam a colaboração entre o Departamento de Defesa, a academia e a indústria, como exemplificado pelo projeto “Stargate”, que prevê investimentos massivos em infraestrutura de IA com parcerias público-privadas, com estimativa de investimentos da ordem de US\$ 500 bilhões nos próximos quatro anos (HuffPost 2025; Open AI 2025). Para o Brasil, focar em áreas como cibersegurança ou otimização logística, que possuem vasta aplicação civil e militar, permite alavancar recursos de múltiplas fontes.

A implementação da tríplice hélice no Brasil deve ser acompanhada

por mecanismos que facilitem a transferência de tecnologia para a Base Industrial de Defesa (BID), combatendo a histórica dependência tecnológica que autores como Cardoso e Faletto (1970) e Furtado (1974) já apontavam e que persiste até hoje conforme asseveram Girardi e Galdino (2024). A ausência de diretrizes específicas para IA em defesa compromete o desenvolvimento de base industrial nacional neste setor estratégico, reproduzindo assimetrias centro-periferia. Para reverter esse quadro, é essencial explorar e fortalecer instrumentos como:

- **Lei de Inovação (Lei nº 10.973/2004 e suas atualizações):** Que já prevê mecanismos de interação entre Instituições Científicas e Tecnológicas (ICTs) e empresas, incluindo compartilhamento de laboratórios, cessão de pesquisadores e licenciamento de patentes.

- **Encomendas Tecnológicas:** Instrumento poderoso para o Estado induzir o desenvolvimento de soluções específicas de IA pela indústria nacional, definindo a necessidade e compartilhando o risco tecnológico.

- **Parcerias Público-Privadas (PPPs) e Contratos de Desenvolvimento Conjunto:** Estruturas que permitem ao setor privado compartilhar o investimento e o risco em projetos de IA de longo prazo, enquanto o setor público garante a demanda e o ambiente de teste.

- **Fomento à Propriedade Intelectual (PI):** Políticas claras de PI são essenciais para incentivar a inovação e facilitar o licenciamento de tecnologias desenvolvidas em universidades ou centros militares para a BID.

A experiência nacional já oferece um modelo de sucesso para essa integração: o Sistema Integrado de Monitoramento de Fronteiras (SISFRON). Trata-se de um projeto estratégico do Exército Brasileiro que demonstra a capacidade do país de desenvolver e integrar sistemas complexos, com a participação ativa da indústria nacional (como Savi e Bradar) no fornecimento de tecnologias avançadas. O SISFRON serve como um “*case study*” interno que valida a premissa de que o Brasil pode construir capacidades tecnológicas soberanas, mesmo em um domínio diferente da IA, fornecendo um roteiro para a futura incorporação de IA na defesa.

O dimensionamento adequado de investimentos em P&D constitui elemento fundamental para o desenvolvimento de capacidades nacionais em IA para defesa. O investimento da China em pesquisa e desenvolvimento continua em trajetória ascendente, com gastos totalizando aproximadamente US\$ 500 bilhões em 2024 (Xinhua 2025). Enquanto isso, nos Estados Unidos, iniciativas importantes em inteligência artificial têm sido implementadas, como o projeto “*Stargate*”, que prevê investimentos que podem alcançar o mesmo valor nos próximos anos (US\$ 500 bilhões) (HuffPost, 2025). Embora

o Brasil não possa competir na mesma escala de investimento, a estratégia deve focar na otimização de recursos e na indução de um ecossistema de inovação que supere a “insuficiência de conhecimento técnico” e a “subordinação às grandes corporações tecnológicas e às potências que já dominam este setor” (Academia Brasileira de Ciências 2023).

Por fim, destacamos que a revisão da EBIA deve contemplar não apenas aspectos tecnológicos, mas também os dilemas éticos e impactos humanitários relacionados ao emprego de IA em sistemas militares. A discussão deve referenciar *frameworks* de *Responsible AI* (como os princípios da OCDE e do *DoD Ethical Principles for AI*) e os debates recentes sobre conformidade com o Direito Internacional Humanitário, utilizando casos como Israel/Gaza e Ucrânia para exemplificar os desafios éticos, como já apontado na seção 2.

Conclusão

A análise desenvolvida neste artigo, fundamentada em uma abordagem multidisciplinar e comparativa de modelos internacionais, evidencia que a incorporação estratégica da Inteligência Artificial no setor de defesa constitui imperativo incontornável para a preservação da soberania e dos interesses nacionais brasileiros no século XXI. Ao realizar uma análise crítica da Estratégia Brasileira de Inteligência Artificial e quantificar a lacuna do setor de defesa, este trabalho propõe caminhos concretos para a superação dessa vulnerabilidade estratégica. A crescente digitalização dos conflitos e a emergência de ameaças híbridas demandam capacidades tecnológicas avançadas que o Brasil ainda não desenvolveu de forma satisfatória, colocando em risco não apenas sua projeção geopolítica, mas também a segurança de suas infraestruturas críticas.

A falta de autonomia estratégica identificada no setor de defesa brasileiro reflete padrões históricos de dependência tecnológica e descontinuidade de políticas públicas que comprometem o desenvolvimento nacional. Como demonstrado pelas evidências apresentadas, esta vulnerabilidade é particularmente aguda no campo da IA militar, onde o Brasil figura como mero consumidor de tecnologias estrangeiras, frequentemente sujeitas a restrições e condicionamentos que limitam sua soberania operacional.

As propostas delineadas, como a inclusão robusta da defesa na Estratégia Brasileira de IA, a criação de um Programa Nacional específico para o setor militar, a ampliação de investimentos em P&D e o estabelecimento de parcerias estratégicas, constituem caminhos viáveis para reverter este

quadro. Contudo, o sucesso depende de implementação de políticas de Estado com horizontes temporais adequados e recursos consistentes. A experiência internacional analisada oferece tanto lições quanto advertências para o caso brasileiro, evidenciando que soluções meramente incrementais serão insuficientes diante da acelerada transformação digital do ambiente estratégico global.

O desenvolvimento de capacidades nacionais em IA para defesa demanda uma abordagem sistêmica que integre múltiplos atores (governo, academia, indústria), contemple diversas dimensões (tecnológica, ética, jurídica, operacional) e estabeleça prioridades claras alinhadas aos objetivos estratégicos nacionais. Neste sentido, mais que recursos financeiros, o Brasil necessita de visão estratégica e arranjos institucionais adequados que viabilizem a superação de entraves históricos ao seu desenvolvimento tecnológico autônomo.

A janela de oportunidade para o desenvolvimento de capacidades significativas em IA para defesa está se estreitando rapidamente, à medida que potências tecnológicas consolidam sua liderança e ampliam a distância em relação aos demais países. O Brasil, por sua dimensão territorial, recursos naturais estratégicos e posição geopolítica, não pode abdicar do desenvolvimento de capacidades tecnológicas compatíveis com seus interesses nacionais e responsabilidades regionais, contribuindo também para a estabilidade e segurança na América do Sul. A questão, portanto, não é se o país deve investir em IA para defesa, mas como fazê-lo de forma eficiente, ética e alinhada a seu projeto de desenvolvimento nacional.

Conclui-se, assim, que a incorporação efetiva da IA na defesa nacional brasileira requer uma revisão profunda da EBIA para incluir explicitamente a dimensão de defesa, bem como o estabelecimento de mecanismos de governança que garantam a continuidade dos esforços nacionais nesse campo estratégico. Somente através de uma política de Estado consistente, que transcenda ciclos políticos e mobilize recursos adequados, o Brasil poderá desenvolver as capacidades tecnológicas necessárias para enfrentar os desafios do século XXI e garantir sua soberania no domínio digital e físico.

Agradecimentos

Os autores receberam apoio financeiro para a realização desta pesquisa da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), por meio do Programa de Apoio ao Ensino e à Pesquisa Científica e Tecnológica em Defesa Nacional – Pró-Defesa V, referente ao Edital n. 36/2023, Processo

n. 23038.011220/2023-31.

Este estudo foi financiado pela FAPERJ - Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro, Processo SEI 260003/008748/2026.

Referências

- Academia Brasileira de Ciências. 2023. “Recomendações para o avanço da inteligência artificial no Brasil”. Novembro, 2023. <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: Stanford University.
- Allen, Greg e Taniel Chan. 2017. *Artificial intelligence and national security*. Belfer Center for Science and International Affairs.
- Ayres Pinto, Danielle e Sabrina Medeiros. 2022. “Inteligência artificial e seu uso no contexto militar: desafios e dilemas éticos”. *Cadernos Adenauer* 23 (2): 97-112.
- Ayoub, Kareem e Kenneth Payne. 2015. “Strategy in the Age of Artificial Intelligence”. *Journal of Strategic Studies* 9 (6): 793-819.
- Barbosa, Alexandre. 2020. *A Desinformação como Ferramenta da Guerra Híbrida*. (Tese Doutorado). Rio de Janeiro, Escola de Guerra Naval.
- Barreiros, Daniel e 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 e 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.
- 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* organizado por Adilson Basquerote, 127-135. Atena Editora.
- Campany, Luiggi. 2021. *Ameaças híbridas e a segurança marítima do século XXI*. (Tese de Doutorado). Rio de Janeiro, Escola de Guerra Naval.
- Canadá. 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, e Enzo Faletto. 1970. *Dependência e desenvolvimento na América Latina: ensaio de interpretação sociológica*. Zahar.
- Cassiolo, José Eduardo, e Helena Lastres. 2005. “Sistemas de inovação e desenvolvimento: as implicações de política.” *São Paulo em Perspectiva* 19 (1): 34-45.
- Chesney, Robert e Danielle Citron. 2019. “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security.” *California Law Review* 107 (6): 1753-1819.
- China. Ministério da Defesa. 2017. Next Generation Artificial Intelligence Development Plan.
- Costa, Aristóteles. 2024. *Guerra Híbrida: análise das características, impactos e estratégias de defesa no contexto contemporâneo*. (Monografia), Rio de Janeiro, Escola de Guerra Naval.
- Cullen, Patrick e 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.
- Estados Unidos da América. 2018. Summary of the 2018 Department of Defense Artificial Intelligence Strategy, DoD, 2018.
- Estados Unidos da América. 2019. Artificial intelligence for the American people. <https://trumpwhitehouse.archives.gov/ai/ai-american-values/>
- Estados Unidos da América. 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*. (Trabalho

- de Conclusão de Curso), Rio de Janeiro, Escola Superior de Guerra.
- Fattorini et al. 2024. The Global AI Vibrancy Tool. Stanford University.
- Fedasiuk, Ryan, Jennifer Melot e 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*. <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.
- Força Aérea Brasileira. 2024. FAB aposta em Inteligência Artificial para eficiência, segurança e inovação tecnológica.
- Força Aérea Brasileira. 2025a. CCA-SJ assina convênio inédito na área de Inteligência Artificial.
- Força Aérea Brasileira. 2025b. Pesquisa desenvolvida no ITA utiliza Inteligência Artificial.
- Fortune Business Insights, última modificação 21 de julho de 2025. www.fortunebusinessinsights.com
- França. 2021. Ministério da Defesa. *Stratégie Nationale en Intelligence Artificielle*.
- França. 2024. Ministério da Defesa. *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*. 5. ed. Atlas.
- Girardi, Rômulo, e Juraci Ferreira Galdino. 2024. “A ‘dualidade’ Da Dualidade tecnológica: Implicações para países em desenvolvimento”. *Coleção Meira Mattos* 18 (62), 189-216.
- Global Growth Insights, última modificação 21 de julho de 2025. www.globalgrowthinsights.com
- Godoy, Arilda Schmidt. 1995. “Pesquisa qualitativa: tipos fundamentais.” *Revista de Administração de Empresas* 35(3): 20–29.
- Haner, Justin e 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*. (Tese de Doutorado). Arlington: Potamac 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. <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. 2023. *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. Ministério da Defesa. 2025. National Program for Artificial Intelligence Program and Snapshot.
- Jobin, Anna, Marcello Ienca, e 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* 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 e Gal Dahan. 2024. Artificial Intelligence in the Battlefield: A Perspective from Israel. *Opinio Juris*. <https://opiniojuris.org/2024/04/20/artificial-intelligence-in-the-battlefield-a-perspective-from-israel/>.
- Monitor do Oriente. 2024. Israel usa veículos blindados para limpar bombas na beira da estrada em Gaza. Atualizado em 30 de dezembro de 2024. <https://www.monitordooriente.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*, 21 de janeiro de 2025.
- Outras Mídias. 2024. IA: a chance que o Brasil não pode desperdiçar. <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*. <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.
- Reino Unido. Ministério da Defesa. 2021. National Artificial Intelligence Strategy.
- Reino Unido. Ministério da Defesa. 2022. Defence Artificial Intelligence Strategy.
- Reino Unido. Ministério da Defesa. 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*, março 2024.
- Rosa, Carlos Eduardo, Eduardo Araújo da Silva, e Pedro Barbezani Ribeiro. 2024. "A Geoestratégia dos Drones Aéreos". *Regeo-Revista Interdisciplinar* 15 (1): 1-21.
- Russell, Stuart e Peter Norvig. 2016. *Artificial intelligence: a modern approach*. Pearson.
- Rússia. Ministério da Defesa. 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, e 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, e 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*. Atualizado em 18 de dezembro de 2024. <https://time.com/7202584/gaza-ukraine-ai-warfare/>
- Sputnik. 2024. Brasil precisa desenvolver inteligência artificial militar e importar não é opção, diz analista. <https://noticiabrasil.net.br/20240411/brasil-precisa-desenvolver-inteligencia-artificial-militar-e-importar-nao-e-opcao-diz-analista--34032454.html>
- Susnea, Elena e Ionuț-Cosmin, Buta. 2021. Artificial intelligence in hybrid warfare: a literature review and classification. Vol. 17 (1): Anais da 17th Conferência Científica Internacional Estratégias 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. Paris: United Nations Educational, Scientific and Cultural Organization.
- Vincent, Brandi. 2024. “Why the Pentagon Didn’t Request Higher Funding for AI in Fiscal 2025.” *DefenseScoop*, 11 de março de 2024.
- Walsh, Matthew; Worrell, Clarence e Scanlon, Thomas. 2024. *Toward the Use of Artificial Intelligence (AI) for Advanced Persistent Threat Detection*. Carnegie Mellon University.
- Woolley, Samuel e 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.
- Zequim, Eduarda e 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.

RESUMO

Este artigo analisa criticamente a ausência de um capítulo de Defesa Nacional na Estratégia Brasileira de Inteligência Artificial (EBIA). Discute as vulnerabilidades estratégicas que essa omissão impõe à soberania nacional, especialmente frente ao cenário geopolítico e à militarização da IA. Explora as implicações da falta de autonomia tecnológica em IA militar, considerando o contexto contemporâneo e as ameaças híbridas. O trabalho propõe um modelo integrado para incorporar a IA na doutrina de defesa do Brasil, alinhado às políticas públicas vigentes. Este modelo abrange desenvolvimento tecnológico autônomo, formação de recursos humanos especializados e um ecossistema de inovação militar. As conclusões enfatizam a urgência de reformular a EBIA, alertando para o risco de crescente vulnerabilidade estratégica onde a IA é essencial para a segurança e autonomia dos Estados.

PALAVRAS-CHAVE

Inteligência Artificial; Defesa Nacional; Estratégia Brasileira de Inteligência Artificial.

Recebido em 17 de fevereiro de 2025

Aprovado em 16 de junho de 2026