UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 3, e98714, p. 1-29, 2026 • https://dx.doi.org/10.5902/2357797598714
Submissão: 07/09/2026 • Aprovação: 14/09/2026 • Publicação: 02/10/2026

Artigos Dossiê

Soberania decisória e IA de defesa no Sul Global: o caso brasileiro

Decision sovereignty and defense AI in the Global South: the Brazilian case

Everton Antônio Ramos[I]

[I]Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, RJ, Brasil

Resumo

Este artigo identifica, a partir do caso brasileiro, condições para preservar a soberania decisória no desenvolvimento de uma estrutura de inteligência artificial (IA) de Defesa em contextos do Sul Global marcados por vulnerabilidades tecnológicas e restrições de comunicação em redes contestadas. Adota abordagem predominantemente qualitativa, apoiada por indicadores quantitativos descritivos, e utiliza o Brasil como estudo de caso único incorporado, com os Estados Unidos como contraste contextual. O corpus reúne normas e políticas de defesa, doutrina militar, documentos multilaterais, literatura acadêmica, indicadores de prontidão tecnológica, dados de infraestrutura em nuvem e registros de empresas credenciadas pelo Ministério da Defesa. A análise distingue dependência tecnológica externa e opacidade algorítmica como problemas distintos. No caso brasileiro, a exposição externa aparece com maior clareza na infraestrutura computacional, enquanto as capacidades relativas a modelos permanecem menos determinadas pelas fontes públicas. Há competências documentadas em integração, comunicações, segurança da informação e comando e controle. A análise do processo decisório mostra que opacidade, carga cognitiva, calibração da confiança e degradação das comunicações condicionam a avaliação dos resultados produzidos por IA. Os achados são organizados nas dimensões de controle e autoridade, verificação, explicabilidade e continuidade. Conclui-se que a soberania decisória não exige produção doméstica integral da cadeia tecnológica, desde que o Estado preserve capacidades suficientes para controlar, avaliar e sustentar as funções que condicionam o emprego militar da IA.

Palavras-chave: IA de defesa; Processo decisório militar; Soberania decisória; Dependência tecnológica; Redes contestadas

Artigo publicado por InterAção sob uma licença CC BY-NC-SA 4.0.

Abstract

This article identifies, from the Brazilian case, conditions for preserving decision sovereignty in the development of a Defense artificial intelligence (AI) structure in Global South contexts marked by technological vulnerabilities and communication constraints in contested networks. It adopts a predominantly qualitative approach, supported by descriptive quantitative indicators, and uses Brazil as an embedded single-case study, with the United States as a contextual contrast. The corpus combines defense legislation and policy, military doctrine, multilateral documents, academic literature, technology-readiness indicators, cloud-infrastructure data, and records of firms accredited by the Brazilian Ministry of Defense. The analysis treats external technological dependence and algorithmic opacity as distinct problems. In Brazil, external exposure is clearest in computing infrastructure, while capabilities related to AI models remain less clearly determined by public sources. Documented capabilities are more visible in integration, communications, information security, and command and control. The analysis of military decision-making shows that opacity, cognitive load, trust calibration, and degraded communications condition the assessment of AI-generated outputs. The findings are organized around control and authority, verification, explainability, and continuity. The article concludes that decision sovereignty does not require complete domestic production of the technological chain, provided that the state preserves sufficient capabilities to control, assess, and sustain the functions that condition the military use of AI.

Keywords: Defense AI; Military decision-making; Decision sovereignty; Technological dependence; Contested networks

1 INTRODUÇÃO

A Inteligência Artificial (IA) deixou de ocupar o debate militar apenas como componente de sistemas de armas e passou a integrar atividades de comando e controle, gestão da informação, logística, planejamento e apoio à decisão. Levantamento anterior identificou dezoito tarefas militares apoiadas por IA antes da seleção e do engajamento de alvos, distribuídas entre funções como comando e controle, processamento de informação, logística e treinamento (Grand-Clément, 2023). No Brasil, essa ampliação ganhou referência normativa própria com a aprovação, em agosto de 2026, da Política de IA de Defesa (Brasil, 2026b).

A Política define a IA de Defesa a partir de tecnologias baseadas em software, hardware, métodos e sistemas destinadas a apoiar processos decisórios das Forças Armadas. Também incorpora o ciclo OODA ao referencial de comando e controle, atribuindo à orientação a formação da representação da nova situação que antecede

a decisão, e inclui a explicabilidade entre os atributos associados ao emprego desses sistemas (Brasil, 2026b). Essa configuração aproxima três elementos que interessam diretamente a este artigo: a tecnologia que produz informação ou recomendação, a infraestrutura necessária ao seu funcionamento e o decisor que precisa avaliar o resultado antes de empregá-lo.

Nesse processo, a opacidade algorítmica representa uma dificuldade própria. Modelos complexos, designados na literatura como modelos de "caixa-preta", podem produzir classificações, previsões ou recomendações sem tornar suficientemente acessíveis ao usuário as relações internas que conduziram ao resultado, o que limita a possibilidade de compreender erros, vieses e condições de validade (Hassija et al., 2024). Essa característica não decorre da nacionalidade do desenvolvedor. Sistemas produzidos domesticamente podem ser opacos, enquanto sistemas estrangeiros podem admitir maior inspeção, documentação ou explicação. Dependência tecnológica externa e opacidade algorítmica constituem, portanto, problemas distintos e devem ser examinados separadamente.

A distinção torna-se relevante no caso brasileiro porque a exigência normativa de explicabilidade convive com capacidades tecnológicas distribuídas de forma desigual entre os componentes que sustentam o emprego da IA. Infraestrutura computacional, dados, modelos, integração, interfaces e comunicações podem estar submetidos a fornecedores, contratos e condições de acesso diferentes. A análise considera, em cada segmento, as capacidades efetivamente disponíveis para testar, compreender, controlar e manter as funções apoiadas pela IA. Neste artigo, soberania decisória designa a capacidade estatal de conservar autoridade suficiente para avaliar e empregar os resultados produzidos pela IA no processo decisório militar. O problema reside em identificar quais capacidades sustentam essa autoridade nos diferentes segmentos da cadeia de suporte à decisão.

Essa questão se torna mais exigente em redes degradadas ou contestadas. A redução da conectividade pode afetar a atualização de dados, o acesso a serviços, a

disponibilidade de modelos ou a transmissão de informações necessárias à avaliação da recomendação. Ao mesmo tempo, o emprego da IA tende a ocorrer justamente em ambientes nos quais velocidade, incerteza e sobrecarga informacional pressionam o processo decisório. As restrições de comunicação podem limitar mecanismos empregados para compensar a opacidade algorítmica, como a comparação com outras fontes, a atualização de informações, a verificação técnica e o acesso a serviços externos. A opacidade possui origem distinta dessas restrições. A estrutura tecnológica e as condições cognitivas da decisão passam, assim, a integrar o mesmo problema analítico.

Diante desse cenário, a investigação responde à seguinte questão: Quais condições, identificadas a partir do caso brasileiro, permitem preservar a soberania decisória no desenvolvimento de uma estrutura de IA de Defesa em contextos do Sul Global marcados por vulnerabilidades tecnológicas e restrições de comunicação em redes contestadas? O Brasil constitui o caso principal por oferecer corpus normativo recente, registros administrativos sobre sua Base Industrial de Defesa e indicadores que permitem examinar diferentes segmentos tecnológicos. O Sul Global constitui o domínio de referência da inferência analítica. O alcance dos resultados concentra-se em contextos nos quais capacidades domésticas coexistem com dependência de tecnologias, serviços ou fornecedores externos, preservadas as diferenças institucionais, industriais e estratégicas entre os Estados.

O objetivo geral consiste em identificar, a partir do caso brasileiro, condições para o desenvolvimento de uma estrutura de IA de Defesa capaz de preservar a soberania decisória em contextos caracterizados por vulnerabilidades tecnológicas e restrições de comunicação em redes contestadas. Para alcançá-lo, o artigo caracteriza mecanismos de concentração e dependência tecnológica, examina capacidades e dependências presentes no caso brasileiro, analisa como a opacidade algorítmica afeta a interpretação e o emprego de resultados no processo decisório militar e organiza esses resultados em uma estrutura analítica aplicada à cadeia de suporte à decisão.

A literatura recente examina partes desse problema em vertentes predominantemente separadas. Probasco et al. (2025) discutem capacidades, limitações e medidas de mitigação para sistemas de IA empregados no apoio à decisão militar, com atenção ao contexto de uso, aos dados e à interação humano-máquina. Shandler, Gross e Shereshevsky (2026) mostram experimentalmente que a explicabilidade pode alterar a relação de militares com recomendações algorítmicas, sem demonstrar que maior explicação produza automaticamente melhor decisão.

Em outra vertente, estudos sobre soberania e aquisição digital tratam da transparência sobre fornecedores, componentes e condições de contratação como condição do controle institucional (Kamphorst et al., 2026). Wei e Shu (2026), em formulação convergente, definem soberania decisória como a autoridade estatal sobre política de decisão, versões, comportamento de contingência, auditabilidade e aprovação final da ação, e a tratam como problema de arquitetura de sistema. A articulação entre essas evidências permanece menos explorada quando se consideram, em conjunto, a estrutura tecnológica disponível a um país importador, a avaliação da saída algorítmica e a preservação dessas funções sob restrições de comunicação.

A contribuição deste artigo consiste em aproximar esses problemas por meio de uma estrutura analítica que relaciona os segmentos da cadeia de suporte à decisão às dimensões de controle e autoridade, verificação, explicabilidade e continuidade. O argumento não pressupõe que nacionalidade da tecnologia, explicabilidade, dependência e autonomia sejam equivalentes. A análise busca identificar onde essas condições se manifestam e quais mecanismos institucionais e técnicos permitem avaliá-las no caso brasileiro.

A vigência da Política de IA de Defesa torna essa discussão particularmente relevante, porque a incorporação de atributos como explicabilidade, auditabilidade, testes, resiliência e redução de dependência exige compreender como eles podem ser observados em sistemas formados por componentes distribuídos ao longo de diferentes segmentos tecnológicos.

O artigo está organizado em sete seções. Após esta introdução, é apresentado o percurso metodológico. A terceira seção examina, a partir dos Estados Unidos, mecanismos de concentração tecnológica e dependência como contraste contextual. A quarta caracteriza capacidades, dependências e elementos da Base Industrial de Defesa brasileira. A quinta analisa a opacidade algorítmica e seus efeitos sobre o processo decisório militar. A sexta aplica a estrutura analítica ao caso brasileiro. A seção final reúne os resultados e responde à questão de pesquisa.

2 PERCURSO METODOLÓGICO

A pesquisa adota abordagem predominantemente qualitativa, com uso subsidiário de indicadores quantitativos descritivos, e organiza-se como estudo de caso único, decomposto em unidades internas de análise. O Brasil constitui o caso, examinado por segmentos da cadeia tecnológica que sustenta o emprego da IA no processo decisório militar. Os Estados Unidos comparecem apenas como contraste contextual, para caracterizar mecanismos de concentração tecnológica e dependência. A inferência pretendida é analítica e se dirige a contextos que compartilhem com o caso brasileiro a combinação entre capacidades domésticas e exposição a tecnologias, serviços ou fornecedores externos.

O Brasil foi selecionado pela disponibilidade de registros administrativos e indicadores multilaterais capazes de caracterizar capacidades tecnológicas e industriais. Foram utilizados o Frontier Technology Readiness Index, dados sobre infraestrutura de computação em nuvem e o registro de empresas credenciadas pelo Ministério da Defesa. Esses instrumentos medem objetos distintos e foram interpretados segundo o alcance definido por cada fonte, sem tratar as contagens como medida direta da capacidade produtiva nacional.

O corpus reuniu legislação, políticas e doutrina militar brasileira, documentos oficiais estrangeiros e multilaterais, literatura acadêmica e bases estatísticas, tendo a Política de IA de Defesa como principal referencial normativo nacional. A análise

documental foi complementada por estudos de Defesa, Relações Internacionais, fatores humanos, interação humano-computador, governança de IA e economia política da tecnologia, e o cruzamento entre fontes produzidas para finalidades distintas foi empregado para conferir a consistência dos achados.

A busca bibliográfica concentrou-se em trabalhos publicados entre 2018 e agosto de 2026, admitindo estudos anteriores quando constituíam referências fundacionais ou evidência necessária ao mecanismo analisado. A seleção privilegiou artigos revisados por pares, documentos primários e textos integrais; preprints e working papers foram empregados de forma subsidiária, sem sustentar isoladamente proposições centrais. Ferramentas de busca assistida por IA, inclusive o Consensus, auxiliaram a identificação inicial dos trabalhos, posteriormente conferidos em texto integral.

A análise do corpus foi organizada por categorias, em dois níveis. No primeiro, foram identificados os atributos expressos no corpus brasileiro, entre eles explicabilidade, auditabilidade, testes, controle, supervisão, resiliência e redução de dependência, com apoio nos seguintes dispositivos da Política de IA de Defesa: art. 2º V; art. 3º VIII e IX; art. 5º II, III, X, XI, XIII e XVI; e, para os instrumentos de implementação, art. 5º I, art. 8º e arts. 7º III e 9º (Brasil, 2026b). No segundo, esses atributos foram agrupados segundo a função que exercem sobre o emprego da IA, resultando em quatro dimensões analíticas: controle e autoridade, verificação, explicabilidade e continuidade. Foram retidas as dimensões com rastreabilidade documental, correspondência em fonte de natureza distinta e relação direta com a capacidade de avaliar, supervisionar, verificar ou preservar o emprego da IA.

Para examinar onde essas dimensões se manifestam, a cadeia de suporte à decisão foi decomposta em cinco segmentos: infraestrutura computacional, dados, modelos, integração e interface, e comunicações e emprego. A decomposição constitui síntese analítica do artigo e organiza os componentes tecnológicos e operacionais identificados no corpus em uma sequência funcional que se estende da infraestrutura computacional ao segmento de comunicações e emprego. O conhecimento das

dependências e as redes contestadas foram tratados como condições transversais, a segunda considerada pelos seus efeitos sobre a disponibilidade de dados, serviços, enlaces e mecanismos de verificação, com incidência principal no segmento de comunicações e emprego e na dimensão de continuidade. Aquisição, contratação e transferência tecnológica foram analisadas como mecanismos institucionais capazes de alterar a distribuição das capacidades observadas.

A pesquisa apresenta limitações decorrentes da natureza pública do corpus e da heterogeneidade dos indicadores utilizados. A ausência de registro foi tratada como lacuna documental, sem inferência automática de inexistência de capacidade. As quatro dimensões e a sua distribuição pelos cinco segmentos resultam de síntese documental e não foram submetidas a validação por especialistas nem a comparação sistemática entre múltiplos casos, o que confere à estrutura analítica alcance exploratório compatível com o desenho da pesquisa.

3 O COMPLEXO MILITAR-TECNOLÓGICO E A GEOPOLÍTICA DA INTELIGÊNCIA ARTIFICIAL

A expressão complexo militar-industrial descreve a relação consolidada no século XX, na qual o Estado contratava empresas privadas para produzir plataformas e sistemas de armas. A configuração formada em torno da IA tem outra natureza. Cientistas de dados e programadores de empresas privadas passam a integrar quartéis-generais operacionais e a trabalhar ao lado do pessoal militar, o que produz uma configuração híbrida entre setor privado e setor público, civil e militar, que King (2025) denomina complexo militar-tecnológico. Este capítulo examina as implicações dessa configuração para a capacidade estatal.

Os Estados Unidos são utilizados como contraste de alta capacidade tecnológica e estatal. Lideram o investimento privado mundial em IA, com 67 bilhões de dólares em 2023, equivalentes a 70% do total global, à frente da China, com 7,8 bilhões, e da Índia, com 1,4 bilhão (UNCTAD, 2025). King (2025) oferece estudo monográfico recente

sobre a relação entre defesa e tecnologia privada. O caso oferece um contraste de alta capacidade em investimento, base científica e acesso a fornecedores, permitindo observar dependências mesmo nesse contexto. Qualquer extensão a outros países do Norte Global fica assinalada como inferência deste artigo.

A concentração alcança a produção de conhecimento e a infraestrutura. No período de 2000 a 2023, a China e os Estados Unidos responderam por cerca de um terço das publicações mundiais em IA e por 60% das patentes (UNCTAD, 2025). Na camada física, a Nvidia detinha 90% do mercado de unidades de processamento gráfico no terceiro trimestre de 2024, dado que o relatório atribui à Jon Peddie Research. Na camada de serviço, Alphabet, Amazon e Microsoft controlavam mais de dois terços do mercado mundial de computação em nuvem (UNCTAD, 2025). A parcela empresarial no financiamento da pesquisa nos Estados Unidos passou de cerca de 50% nos anos 1980 para perto de 80% em 2025, conforme working paper de economia da inovação (Crespi; Guarascio; Reljic, 2026).

A natureza do ativo explica por que a concentração se mantém. Srnicek (2017) associa esse padrão à centralidade dos dados como insumo econômico e à consolidação da plataforma como modelo de negócio, do que resulta forte concentração de mercado. Nesse modelo, a plataforma funciona como infraestrutura de intermediação e concentra o controle das condições de acesso. Esse controle constitui um ativo de posição que alcança os agentes dependentes da infraestrutura, inclusive as forças armadas.

A concentração localiza a produção de IA fora do aparelho de Estado. A dependência da defesa em relação a empresas privadas decorre dessa posição na cadeia de produção e antecede qualquer decisão de compra. A dependência já se manifestou em operação militar real. A força armada ucraniana conduziu operações contando, além dos aliados tradicionais, com Google, Microsoft, Starlink, Palantir e Anduril para obter os dados, a IA e o software necessários à execução, conforme registra King (2025). O caso comparece como evidência pontual, sem generalização.

King (2025) identifica quatro fontes dessa dependência da defesa norte-americana em relação às empresas civis de tecnologia. A primeira está no capital da pesquisa, e o Pentágono investiu 1,1 bilhão de dólares em pesquisa e desenvolvimento de IA em 2023. A segunda está no pessoal qualificado, que segue para as empresas de tecnologia, onde programadores podem iniciar com remuneração anual entre 200 mil e 300 mil dólares. A terceira está no regime de aquisição, que fixa requisitos no início e recebe a entrega ao fim de um ciclo longo, desenho adequado a plataformas e desfavorável ao desenvolvimento de software. A quarta está na burocracia, e as organizações criadas para contorná-la resolvem problemas individuais sem se expandir para o Departamento de Defesa.

O Estado reconheceu essas restrições e atuou sobre parte delas. Em 2014, a Terceira Estratégia de Compensação levou o governo a reformar a aquisição para atrair empresas de tecnologia, seguindo-se a criação da Unidade de Inovação em Defesa e do Centro Conjunto de Inteligência Artificial (King, 2025). O esforço orçamentário tem continuidade na Lei Pública 119-21, de 2025, que destinou 2 bilhões de dólares à expansão daquela unidade e 250 milhões ao ecossistema de IA (Congressional Research Service, 2025). A dependência do fornecedor privado permaneceu. Capital e pessoal exigem horizonte de investimento e de formação que excede o ciclo de uma administração, e o complexo militar-tecnológico constitui o resíduo dessas restrições, operando como estrutura da produção de capacidade militar.

A dependência manifestada na Ucrânia teve consequência operacional documentada. A SpaceX forneceu quinze mil terminais Starlink até julho de 2022, a comunicação segura entre o governo e as forças armadas passou a depender desse enlace e o sistema ucraniano de gestão de batalha Delta operava sobre ele. O dirigente da empresa bloqueou o acesso ao serviço para impedir um ataque à Crimeia, após tratar do assunto com autoridades norte-americanas, conforme narra King (2025). O episódio mostra que o fornecedor do enlace detém capacidade de interromper uma operação em curso, e que essa capacidade não pertence ao Estado que emprega o meio.

O fornecedor tem domicílio jurídico, e o Estado de origem regula o que ele exporta. O plano de ação norte-americano determina exportar a pilha tecnológica completa, incluindo hardware, modelos, software, aplicações e padrões, a países dispostos a integrar sua aliança em IA (Estados Unidos, 2025b). A orientação do Bureau of Industry and Security (BIS) sobre a Proibição Geral 10 afirma que o uso dos circuitos chineses nela tratados pode violar controles de exportação norte-americanos e sujeitar empresas a medidas de fiscalização (BIS, 2025), inclusive quando o usuário está situado em terceiro país.

A escolha do fornecedor também expõe o adquirente à jurisdição do Estado de origem, inclusive a controles de exportação e condições de acesso. A dependência de plataformas norte-americanas e chinesas intensifica a subordinação dos governos estrangeiros (Crespi; Guarascio; Reljic, 2026). Os mesmos autores distinguem as economias dotadas de poder de barganha e de controle sobre infraestruturas críticas daquelas em que a soberania tecnológica se apresenta fraca, com hiato entre autoridade formal e controle efetivo. A tipologia não classifica o Brasil. Localizar a posição brasileira nessa cadeia é a tarefa do capítulo seguinte.

4 ESTRUTURA DE INTELIGÊNCIA ARTIFICIAL DE DEFESA NO BRASIL: CAPACIDADES E DEPENDÊNCIAS TECNOLÓGICAS

A Política de IA de Defesa associa a implementação ao desenvolvimento da Base Industrial de Defesa, à integração com comunicações e segurança cibernética e à obtenção de capacidades para projetar, desenvolver, produzir, controlar e proteger infraestrutura digital e sistemas críticos de IA (Brasil, 2026b). A questão é onde o Brasil apresenta capacidades documentadas nos segmentos que sustentam a IA de Defesa e em quais deles a exposição a fornecedores externos aparece com maior nitidez.

O índice de prontidão em tecnologias de fronteira oferece uma primeira aproximação, desde que seu alcance seja preservado. Ele mede tecnologias de fronteira em conjunto e não IA isoladamente. Em 2024, o Brasil ocupava a 38ª posição

entre 170 economias, com melhor posição em pesquisa e desenvolvimento, 18º lugar, do que em capacidade industrial, 50º, e competências, 59º. A Índia registrava o mesmo escore agregado, 0,74, mas ocupava o 3º lugar em pesquisa e desenvolvimento e o 10º em capacidade industrial, ao mesmo tempo que aparecia em 113º em competências (UNCTAD, 2025). A comparação mostra que a posição agregada oculta configurações internas distintas e, por isso, não permite inferir capacidade de IA de Defesa sem decomposição adicional.

Os indicadores específicos de IA ajudam a estreitar essa leitura. A UNCTAD inclui o Brasil entre poucos países em desenvolvimento com supercomputadores de grande porte ou grandes centros de dados e entre aqueles com contingente relevante de desenvolvedores de IA. O relatório registra ainda 22 serviços de infraestrutura de nuvem no País em meados de 2024, oferecidos pelos oito provedores considerados na figura III.9 do relatório, todos sediados no exterior (UNCTAD, 2025). Esses registros confirmam presença territorial de recursos humanos e infraestrutura, mas não informam sua escala disponível para a defesa, o controle sobre hardware e serviços nem a capacidade de sustentar treinamento e atualização de modelos. Presença física, capacidade científica e controle tecnológico representam, assim, dimensões diferentes.

A aproximação ao setor de defesa exige um instrumento de outra natureza. A Lei nº 12.598 condiciona o credenciamento de Empresa Estratégica de Defesa a requisitos como sede e estabelecimento industrial no País, conhecimento científico ou tecnológico comprovado e continuidade produtiva em território nacional, enquanto o Decreto nº 7.970 regulamenta esse credenciamento (Brasil, 2012; Brasil, 2013). O registro consultado reunia 338 empresas em 2026 (Brasil, 2026a). Como o credenciamento oficial não informa o segmento tecnológico de atuação, este artigo classificou as empresas com base na razão social e na descrição pública de suas atividades. A classificação foi utilizada para localizar presença empresarial credenciada nos segmentos analisados. As contagens não medem diretamente capacidade nacional de IA, escala produtiva ou domínio tecnológico.

A distribuição resultante concentra maior presença em criptografia e segurança da informação, comunicações e espaço, e software de comando e controle e engenharia de sistemas, com mais de dez empresas em cada grupo. Montagem eletrônica e componentes reúne oito empresas, enquanto nuvem e centros de dados reúnem duas e semicondutores e fundição, uma (Brasil, 2026a). A diferença não autoriza transformar quantidade de empresas em medida de capacidade. Ela indica onde a capacidade empresarial credenciada é mais visível. Para o objeto deste artigo, o dado sugere maior presença em segmentos habilitadores de integração, comunicação, proteção e comando e controle do que nos segmentos associados à infraestrutura computacional de base.

A evidência técnica disponível reforça essa leitura apenas para o segmento de integração. Gomes et al. (2024) mapeiam requisitos de alto nível de sistemas de comando e controle em rede e examinam serviços e arquiteturas aplicáveis a redes militares, em trabalho com participação do Centro de Desenvolvimento de Sistemas do Exército Brasileiro. A fonte não mede capacidade nacional de IA e não trata de dependência ou aquisição. Seu valor neste capítulo é mais restrito. Ela demonstra competência técnica documentada em redes e integração militar, áreas que a Política de IA de Defesa associa à interoperabilidade, às comunicações e ao comando e controle. Essa evidência técnica complementa o registro administrativo ao demonstrar competência documentada em redes e integração militar, sem transformar a presença empresarial em medida de capacidade nacional de IA.

O corpus permite, portanto, conclusões com graus diferentes de segurança. Na infraestrutura computacional, a combinação entre serviços de nuvem prestados por empresas sediadas no exterior e a pequena presença credenciada em nuvem, centros de dados e semicondutores documenta exposição externa mais clara. Esse resultado não mede a disponibilidade de computação de alto desempenho para emprego militar e não autoriza estimar seu grau de dependência. No segmento de modelos, a evidência é ainda mais limitada. Nenhum dos instrumentos empregados

mede diretamente a capacidade brasileira de desenvolver, treinar, adaptar, atualizar ou manter modelos destinados à Defesa. A baixa visibilidade documental desse segmento deve ser tratada como lacuna de mensuração, e não como demonstração de inexistência de capacidade nacional.

O caso brasileiro apresenta, assim, uma distribuição desigual das capacidades que podem sustentar a IA de Defesa. O corpus registra produção científica e recursos computacionais no País, além de presença empresarial e competência técnica em integração, comunicações, segurança da informação e comando e controle. A exposição externa aparece com maior clareza na infraestrutura computacional, enquanto a capacidade relativa a modelos permanece menos determinada pelas fontes disponíveis. O diagnóstico localiza o problema em segmentos específicos da cadeia de suporte à decisão. Em redes contestadas, dependências em infraestrutura, serviços e comunicações podem afetar o acesso às informações e às funções necessárias para avaliar a saída algorítmica. O capítulo seguinte examina como essas condições tecnológicas se combinam com opacidade, carga cognitiva e pressão temporal no processo decisório militar.

5 O PROCESSO DECISÓRIO MILITAR SOB CAIXAS-PRETAS: OPACIDADE, CARGA COGNITIVA E CONFIANÇA

A adoção de IA no apoio à decisão militar decorre de uma vantagem concreta associada à capacidade de processar grandes volumes de dados e identificar relações em escala e velocidade superiores às capacidades humanas. Esse ganho, porém, não elimina a função do julgamento. Predição, dados e julgamento são elementos complementares da decisão, e a redução do custo de predizer aumenta o valor dos demais componentes do processo (Goldfarb; Lindsay, 2022). Em aplicações militares, essa distinção assume maior relevância porque erros precisam ser reconhecidos em ambientes de alta consequência e sob condições distintas das observadas no desenvolvimento do sistema (Tomsett et al., 2020). A vantagem computacional começa

no processamento, enquanto a decisão permanece dependente da avaliação humana da saída produzida.

A saída algorítmica alcança uma etapa específica do ciclo de comando e controle. O ciclo OODA, desenvolvido no pensamento estratégico de John Boyd, articula observação, orientação, decisão e ação, atribuindo à orientação papel central na construção da representação a partir da qual o decisor interpreta a situação e orienta sua conduta (Boyd, 2018). A Política de IA de Defesa incorporou esse referencial e define a orientação como a produção da imagem mental da nova situação (Brasil, 2026b). Para este artigo, o ponto de interesse está na função exercida pela saída algorítmica nesse processo. Ao integrar a representação construída pelo comandante, ela precisa ser interpretada, contrastada com outras informações e avaliada quanto às condições em que foi produzida.

A primeira dificuldade dessa avaliação decorre da opacidade algorítmica. Como observado na introdução, a opacidade dos modelos de caixa-preta não decorre da nacionalidade do desenvolvedor (Hassija et al., 2024). Além disso, compreender uma explicação não equivale automaticamente a melhorar a decisão, porque os efeitos da explicabilidade dependem de como a informação é apresentada e percebida pelo usuário (Reinhard et al., 2026). A questão relevante é, assim, quanto o decisor consegue conhecer sobre a saída nas condições concretas de emprego.

O ambiente militar acrescenta outra fonte de incerteza, pois o desempenho observado em treinamento ou teste pode não se reproduzir nas condições concretas da operação. Essa dificuldade assume especial relevância na orientação, que envolve a construção cognitiva da situação sob condições de complexidade, novidade e incerteza (Johnson, 2023). Tomsett et al. (2020) mostram que, em operações de coalizão, serviços de IA podem atuar sobre dados diferentes daqueles empregados em treinamento, sofrer alteração de disponibilidade e ser utilizados por operadores que não conhecem integralmente suas fronteiras de erro. A consequência decisória central está na dificuldade de reconhecer quando a recomendação perdeu aderência

à situação, especialmente porque a possibilidade de falha está presente em qualquer sistema. Goldfarb e Lindsay (2022) localizam risco semelhante na automação prematura, quando objetivos relativamente claros são executados em ambiente incerto e a velocidade da resposta reduz a oportunidade de perceber o descompasso entre a situação real e a representação codificada.

A capacidade de avaliar essas condições encontra, por sua vez, limites humanos. A memória de trabalho dispõe de capacidade restrita para tratar simultaneamente elementos novos, especialmente quando a tarefa exige comparação, atualização e escolha sob pressão (Sweller; Ayres; Kalyuga, 2011). O problema já possui evidência em contexto militar. Hollands, Spivak e Kramkowski (2019) observaram, em soldados submetidos a cenário tático, que maior velocidade de apresentação de mensagens aumentou a carga cognitiva e reduziu a consciência situacional. Aumentar a quantidade de informação disponibilizada ao decisor, portanto, não produz necessariamente maior compreensão. Informação útil precisa chegar em volume e forma compatíveis com a capacidade de processá-la no intervalo disponível.

Essa limitação condiciona também a explicabilidade. Explicações podem oferecer elementos para interpretar uma recomendação, detectar inconsistências e decidir quanto confiar nela, mas também exigem atenção e esforço cognitivo. A revisão sistemática de Reinhard et al. (2026), baseada em 107 estudos experimentais, mostra que os efeitos da explicabilidade sobre confiança, desempenho e detecção de erros variam conforme características da explicação, do usuário e da tarefa. No ambiente militar, a informação oferecida deve ser adequada à função desempenhada pelo sistema, à consequência da decisão e ao tempo disponível. Explicabilidade útil é aquela que acrescenta capacidade de avaliação sem transformar a própria explicação em nova fonte de sobrecarga.

O resultado esperado é uma confiança calibrada, ajustada ao desempenho demonstrado pelo sistema nas condições de emprego. Tomsett et al. (2020) associam a calibração à capacidade de ajustar o grau de confiança ao desempenho

demonstrado pelo sistema em cada situação. A literatura de fatores humanos distingue tanto o uso excessivo da automação quanto a rejeição de auxílio potencialmente útil (Parasuraman; Riley, 1997). Evidência militar recente mostra que a segunda possibilidade também é concreta. Shandler, Gross e Shereshevsky (2026), em dois experimentos com 2.015 militares, diante de réplica de um sistema de apoio à seleção de alvos, identificaram aversão à recomendação algorítmica em cenários de elevado dano colateral e observaram alteração desse comportamento quando recursos de explicabilidade estavam presentes. O desenho experimental não isola o mecanismo causal responsável por esse efeito. A evidência sustenta, portanto, a importância da calibração, sem autorizar presumir que mais explicação produzirá necessariamente melhor decisão.

O tempo disponível condiciona todo esse processo. Na decisão militar, a pressão temporal reduz o tempo disponível para compensar a opacidade por meio de informação adicional, comparação independente ou consulta a outras fontes. Forma-se, assim, uma tensão operacional em que a menor transparência ou previsibilidade do comportamento do sistema amplia a necessidade de avaliação, ao mesmo tempo que a urgência que favorece o emprego da IA reduz o tempo disponível para realizá-la. A contribuição da IA depende da velocidade com que produz a saída e da possibilidade de o decisor qualificá-la antes de incorporá-la à etapa de orientação.

Em redes contestadas, a dependência tecnológica pode afetar as condições de acesso, teste e continuidade do sistema. Tomsett et al. (2020) observam que os serviços disponíveis ao usuário podem variar conforme localização física, estado da rede e prioridades operacionais. Johnson (2023) acrescenta que ataques às comunicações eletrônicas podem comprometer estruturas de comando dependentes desses enlaces. A degradação da conectividade pode restringir o recebimento, a verificação e a continuidade da capacidade que produz a recomendação. A disponibilidade da infraestrutura e das informações necessárias à avaliação passa, assim, a integrar as condições de emprego da IA.

A velocidade do ciclo decisório, por si só, não assegura a qualidade da decisão. Quando a percepção do ambiente é incompleta, imprecisa ou inadequadamente interpretada, a aceleração do processamento pode apenas antecipar uma decisão deficiente. A opacidade algorítmica, o desconhecimento das condições de falha, a carga cognitiva, a pressão temporal e a degradação da rede podem afetar justamente a qualidade da orientação que precede a decisão. O problema desloca-se, portanto, da simples adoção de IA para as condições sob as quais sua saída pode ser avaliada e empregada. O capítulo seguinte sistematiza essas condições e as aplica ao caso brasileiro.

6 CONTROLE, VERIFICAÇÃO, EXPLICABILIDADE E CONTINUIDADE NO CASO BRASILEIRO

O capítulo anterior identificou fatores que condicionam a interpretação e o uso da saída produzida pela IA no processo decisório militar. Este capítulo organiza os atributos extraídos dos documentos segundo a função que exercem sobre o emprego da IA e examina como se distribuem ao longo da cadeia de suporte à decisão.

A Política de IA de Defesa enuncia os atributos que originam as quatro dimensões, ao enunciar auditabilidade e explicabilidade entre os seus princípios e ao estabelecer como diretriz a obtenção de capacidades já referidas no capítulo 4, com redução da dependência de fornecedores externos (Brasil, 2026b). As quatro dimensões descrevem capacidades distintas e podem variar de forma independente em um mesmo sistema. As dimensões e a sua distribuição constituem síntese analítica deste artigo e os documentos estrangeiros empregados a seguir exercem função exclusivamente comparativa.

O conhecimento das dependências atravessa as quatro dimensões. Em estudo do setor público neerlandês, Kamphorst et al. (2026) mostram que instituições sem informação sobre o que adquirem, de quem e sob quais condições ficam restritas para exercer controle e planejar alternativas. O arcabouço de gestão de risco do Instituto

Nacional de Padrões e Tecnologia dos Estados Unidos inclui componentes de terceiros ao longo do ciclo de vida (Tabassi, 2023).

Controle e autoridade abrangem as condições pelas quais o Estado define limites de emprego, supervisiona funções e conserva capacidade de intervenção ao longo do ciclo de vida do sistema. A posição brasileira no Grupo de Peritos Governamentais sobre sistemas de armas letais autônomos propõe a passagem do operador manual à posição de supervisor, com capacidade de supervisionar, intervir e desativar (Brasil, 2020). Em escopo restrito aos sistemas de armas autônomos, a Diretiva 3000.09, do Departamento de Defesa dos Estados Unidos, exige nível apropriado de julgamento humano sobre o uso da força e procedimentos claros de ativação e desativação (Estados Unidos, 2023). A Política de IA de Defesa concentra a participação humana nas decisões de maior criticidade.

A verificação produz evidência documentada sobre o comportamento do sistema nas condições de emprego pretendidas. A Política de IA de Defesa associa essa dimensão à realização de testes rigorosos e à adoção de processos auditáveis, rastreáveis e justificáveis, que permitem examinar e documentar o comportamento do sistema ao longo de seu ciclo de vida (Brasil, 2026b). A estratégia revisada da OTAN também prevê uma estrutura de teste, avaliação, verificação e validação de IA e instalações capazes de testar e validar aplicações sob diferentes condições tecnológicas, procedimentais e operacionais (OTAN, 2024). No emprego militar, a verificação precisa considerar a correspondência entre as condições de desenvolvimento e teste e aquelas encontradas na operação. Probasco et al. (2025) mostram que mudanças de contexto podem reduzir a validade do desempenho anteriormente observado, problema agravado pela escassez de dados representativos de situações de combate.

A explicabilidade trata das informações necessárias para que o decisor compreenda e avalie o resultado produzido pelo sistema. A Política de IA de Defesa a define como capacidade de fornecer explicação compreensível e interpretável por humanos, produzir intuições sobre suas causas e permitir transparência, auditoria

e responsabilização (Brasil, 2026b). O arcabouço norte-americano distingue explicabilidade, interpretabilidade e transparência e relaciona a informação fornecida ao papel de quem utiliza o sistema (Tabassi, 2023). Pfaff (2026) corrobora essa leitura ao sustentar que o valor do sistema está na compreensão utilizável e adaptável do ambiente operacional que ele permite formar, acima da rapidez da resposta.

A informação necessária para explicar o resultado produzido pela IA varia conforme a função desempenhada pelo sistema e a criticidade da decisão que ele apoia. Em aplicações de maior criticidade operacional, como aquelas que podem influenciar o emprego da força, torna-se mais importante que o decisor conheça as incertezas, as limitações e as condições de validade do resultado antes de utilizá-lo. Isso não implica estabelecer níveis fixos de explicabilidade para cada aplicação. O parâmetro é funcional e depende do que o decisor precisa compreender para avaliar adequadamente a recomendação. No contexto dos sistemas de comando e controle, o ADP 6-0 estabelece que o conhecimento produzido pelos sistemas seja apresentado ao comandante como recomendação, preservando o julgamento humano antes da decisão (Estados Unidos, 2026).

Neste artigo, continuidade designa a capacidade de preservar a função apoiada pela IA quando falhas, degradação das comunicações ou mudanças nas condições de acesso afetam o sistema. A Política de IA de Defesa exige requisitos mínimos de tolerância a falhas e degradação controlada, de modo a preservar a operação segura em condições adversas ou sob ataque, e adota a resiliência em ambientes contestados como princípio (Brasil, 2026b). Em sentido convergente, a doutrina de comando e controle do Exército dos Estados Unidos estabelece que os sistemas devem permanecer capazes de desempenhar suas funções em ambientes degradados (Estados Unidos, 2026). Em estruturas dependentes de componentes externos, a continuidade implica ainda identificar quais serviços, atualizações, enlaces e suportes são necessários para manter a função disponível durante o emprego.

O Quadro 1 cruza as dimensões analíticas com os segmentos da cadeia definidos no percurso metodológico. As colunas acompanham o percurso da infraestrutura computacional até as comunicações e o emprego. As linhas transformam cada dimensão em uma pergunta sobre quem controla a função, que evidências demonstram seu funcionamento, o que o decisor precisa compreender e como a função pode ser mantida diante de falhas ou restrições. Cada célula indica o que deve ser examinado em cada segmento. O diagnóstico considera o grau de capacidade que o Estado possui, as dependências envolvidas e a possibilidade de manter essa capacidade durante o emprego. Quando essas condições são insuficientes, a matriz permite localizar a vulnerabilidade e identificar qual função pode ser afetada. A relevância de cada aspecto depende da função apoiada pela IA, da criticidade da decisão e das dependências presentes no sistema.

Quadro 1 – Matriz analítica da cadeia de suporte à decisão militar com IA

Dimensões analíticas	**1 Infraestrutura computacional**	**2 Dados**	**3 Modelos**	**4 Integração e interface**	**5 Comunicações e emprego**
Controle e autoridade *Quem controla, limita ou interrompe?*	Acesso, configuração e hospedagem	Acesso, uso e atualização dos dados	Versão autorizada, função e limites de emprego	Ativação e desativação de funções	Autoridade sobre o uso operacional
Verificação *Que evidência demonstra o funcionamento?*	Desempenho, segurança e disponibilidade	Procedência, integridade e adequação ao contexto	Validade no escopo declarado e monitoramento	Teste da configuração operacional integrada	Comportamento sob degradação
Explicabilidade *O que o decisor precisa compreender?*	Limitações do provimento que afetam a interpretação do resultado	Origem e limite de validade do dado	Incerteza e limites do resultado	Estado do sistema e resultado compreensíveis ao decisor	Atraso, perda ou incompletude da informação
Continuidade *Como a função é preservada diante de falha, degradação ou dependência?*	Recuperação, suporte e alternativa de provimento	Fluxo de atualização e validade com dado defasado	Manutenção e substituibilidade	Preservação da função integrada	Resiliência diante de degradação e interrupção

Fonte**:** Autor (2026)

Aplicada ao diagnóstico do capítulo 4, a matriz permite distinguir presença tecnológica de capacidade estatal sobre a função correspondente. Na infraestrutura computacional, por exemplo, o acesso a capacidade contratada informa apenas parte do diagnóstico. A avaliação da continuidade exige examinar também suporte, recuperação e alternativas de provimento, enquanto a verificação requer evidências sobre desempenho, segurança e disponibilidade.

A maior presença documentada em integração, comunicações e comando e controle localiza capacidade empresarial, e não informa o grau de controle que o Estado exerce sobre a função. A maior exposição externa da infraestrutura computacional e a menor determinação documental sobre modelos indicam onde a avaliação depende de informação adicional sobre acesso, teste e suporte. Os documentos examinados preveem a avaliação de desempenho, segurança e disponibilidade de componente de terceiro, mas não especificam quais direitos de verificação acompanham capacidade computacional obtida externamente. Essa ausência delimita o alcance do material e impede inferir inexistência de capacidade.

A aquisição constitui um dos mecanismos pelos quais essa distribuição pode ser alterada. A política brasileira de compensação tecnológica prevê, em aquisições de interesse da Defesa, instrumentos como transferência de tecnologia, capacitação tecnológica, coprodução e cooperação industrial (Brasil, 2023). Esses instrumentos podem ampliar conhecimento, competência ou capacidade de intervenção conforme o conteúdo obtido, e a sua previsão não demonstra controle sobre o sistema adquirido.

A análise permite derivar três elementos contratuais e uma condição institucional. O primeiro é o acesso à documentação sobre versão, dados, escopo e limites de validade. O segundo é a possibilidade de realizar ou supervisionar ensaio e avaliação independentes. O terceiro é a definição das condições de suporte, continuidade e substituição no ciclo de vida. A condição institucional é a capacidade nacional para realizar, supervisionar ou interpretar esses ensaios, sem a qual o aproveitamento técnico desses elementos permanece limitado.

Como referência comparativa de aquisição pública, o Memorando M-25-22 do Office of Management and Budget (OMB) prevê medidas para reduzir a dependência de fornecedores, entre elas transferência de conhecimento, portabilidade de dados e modelos, avaliação independente, monitoramento ao longo do contrato e possibilidade de reversão de versões. O documento exclui de seu escopo a IA adquirida como componente de sistemas de segurança nacional (Estados Unidos, 2025a). No caso brasileiro, os elementos identificados resultam da síntese do corpus e podem ser incorporados aos instrumentos de implementação previstos pela Política de IA de Defesa.

O capítulo organiza as dimensões pelas quais essas exigências podem ser examinadas em cada segmento da cadeia e indica quais instrumentos vigentes poderiam incorporar essas exigências. Duas questões permanecem abertas, a especificação dos direitos de verificação em capacidade computacional contratada, que o corpus não fornece, e qual capacidade institucional de ensaio e avaliação está disponível para sustentar essas dimensões. Ambas retornam na síntese final.

7 CONCLUSÃO

A pesquisa examinou, no caso brasileiro, as condições que permitem preservar a soberania decisória em uma estrutura de IA de Defesa no Sul Global, sob dependência tecnológica e comunicações contestadas. A análise mostra que essas condições se distribuem pelos diferentes segmentos da cadeia de suporte à decisão, submetidos a distintas formas de acesso, controle e dependência. Os segmentos participam da formação e do emprego do resultado produzido pela IA e podem apresentar graus distintos de domínio nacional sem eliminar, por essa razão, a autoridade estatal sobre sua utilização.

O contraste com os Estados Unidos mostrou que mesmo países situados na fronteira tecnológica organizam capacidades militares de IA por meio de relações entre Estado e empresas privadas, com concentração de infraestrutura, capital, conhecimento

e serviços em número restrito de atores. A dependência tecnológica também se manifesta em contextos de alta capacidade tecnológica. Em contextos do Sul Global caracterizados por maior exposição a tecnologias, serviços ou fornecedores externos, essa dependência pode adquirir maior relevância quando alcança segmentos cuja indisponibilidade, alteração ou restrição de acesso compromete funções necessárias ao processo decisório. O problema passa a ser identificar onde a dependência produz vulnerabilidade operacional e quais capacidades permitem administrá-la.

O caso brasileiro evidencia uma distribuição desigual dessas capacidades. O corpus registra competências em integração, comunicações, segurança da informação e comando e controle. Na infraestrutura computacional, a dependência externa se torna mais visível. A capacidade relacionada ao desenvolvimento, treinamento, atualização e manutenção de modelos permanece menos determinada pelas fontes públicas disponíveis. Esses resultados não autorizam medir um grau único de dependência nacional. Eles permitem localizar segmentos em que o conhecimento sobre fornecedores, condições de acesso, suporte, atualização e alternativas se torna particularmente relevante para avaliar a autonomia de emprego.

A análise do processo decisório acrescentou uma restrição distinta. A opacidade algorítmica não decorre da dependência externa e tampouco desaparece com a produção doméstica. Ela resulta das condições pelas quais determinados sistemas produzem resultados que não são integralmente acessíveis ou interpretáveis por seus usuários. Sua importância militar aparece sobretudo quando classificações, previsões ou recomendações passam a integrar a orientação e influenciam a representação a partir da qual o decisor interpreta o ambiente. Sob pressão temporal e elevada carga informacional, a utilidade da IA depende também da possibilidade de reconhecer incertezas, limitações e condições de validade antes que o resultado seja incorporado ao julgamento.

As redes degradadas ou contestadas introduzem outra camada ao problema. Elas não produzem opacidade algorítmica, mas podem restringir a atualização de

dados, o acesso a serviços, a transmissão de informações e os mecanismos disponíveis para verificar ou contextualizar o resultado. A contribuição operacional da IA depende, por isso, tanto do desempenho do modelo quanto da capacidade de manter as funções que sustentam seu emprego quando as condições de comunicação se deterioram. A continuidade deixa de ser apenas atributo técnico de disponibilidade e passa a integrar a avaliação da estrutura que apoia a decisão.

A partir do caso brasileiro, a resposta à questão de pesquisa indica que a preservação da soberania decisória em uma estrutura de IA de Defesa depende da capacidade estatal de exercer controle e autoridade, verificação, explicabilidade e continuidade sobre as funções que condicionam a formação, a avaliação e o emprego dos resultados no processo decisório militar. A produção doméstica integral da cadeia tecnológica não constitui requisito para esse resultado. A estrutura analítica proposta oferece referência para contextos do Sul Global em que capacidades domésticas coexistam com dependências externas nos segmentos examinados.

Essa conclusão atribui papel específico à aquisição e à capacidade institucional do Estado. Documentação sobre versões, dados, escopo e limitações, possibilidade de ensaio e avaliação independentes e condições de suporte, continuidade e substituição constituem mecanismos pelos quais relações de dependência podem ser administradas. Seu valor, contudo, depende da existência de capacidade nacional para interpretar documentação, realizar ou supervisionar avaliações e decidir sobre a continuidade do emprego. A soberania decisória se apoia na capacidade de exercer autoridade informada sobre funções críticas ao longo do ciclo de vida.

Essa capacidade institucional ultrapassa o âmbito exclusivo do Ministério da Defesa. A estrutura tecnológica examinada envolve competências distribuídas entre Defesa, ciência e tecnologia, infraestrutura digital, indústria e outros atores responsáveis pela produção, regulação e sustentação das capacidades empregadas. A soberania decisória associada à IA de Defesa depende, por isso, de articulação interinstitucional capaz de conectar as necessidades militares às capacidades tecnológicas mantidas no

Estado e no ecossistema nacional de inovação. A implementação da Política de IA de Defesa deve ser compreendida dentro dessa articulação mais ampla, preservadas as competências institucionais de cada ator.

O alcance desses resultados permanece condicionado pelo desenho da pesquisa. O estudo baseia-se em documentação pública, indicadores heterogêneos e um único caso decomposto em unidades internas de análise. A ausência de evidência documental não foi tratada como demonstração de inexistência de capacidade, e as quatro dimensões propostas ainda não foram submetidas à validação por especialistas ou à comparação sistemática entre múltiplos países. Pesquisas futuras podem testar a estrutura analítica em outros Estados do Sul Global, aprofundar a mensuração de capacidades relativas a modelos e infraestrutura computacional e examinar empiricamente como requisitos de controle, verificação, explicabilidade e continuidade são incorporados a processos de aquisição e emprego militar.

Ainda com essas limitações, o caso brasileiro indica que a questão decisiva para a IA de Defesa está na capacidade de conservar condições efetivas para conhecer, avaliar, empregar e sustentar a tecnologia quando o processo decisório militar depende dela.

REFERÊNCIAS

BOYD, John R. **A discourse on winning and losing**. Editado e compilado por Grant T. Hammond. Maxwell AFB, AL: Air University Press, 2018.

BRASIL. **Decreto nº 7.970, de 28 de março de 2013**. Regulamenta dispositivos da Lei nº 12.598, de 21 de março de 2012. Brasília, DF: Presidência da República, 2013.

BRASIL. **LAWS and human control: Brazilian proposals for working definitions**. Genebra: United Nations, 2020. Documento CCW/GGE.1/2020/WP.4.

BRASIL. **Lei nº 12.598, de 21 de março de 2012**. Estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas de defesa e dá outras providências. Brasília, DF: Presidência da República, 2012.

BRASIL. Ministério da Defesa. **Empresas de Defesa (ED) e Empresas Estratégicas de Defesa (EED)**. Brasília, DF: Ministério da Defesa, 2026a. Base de dados. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/industria-de-defesa/comissao-mista-da-industria-de-defesa-cmid-1/empresas-de-defesa-ed-e-empresas-estrategicas-de-defesa-eed. Acesso em: 26 ago. 2026.

BRASIL. Ministério da Defesa. **Portaria GM-MD nº 3.990, de 3 de agosto de 2023**. Estabelece a Política de Compensação Tecnológica, Industrial e Comercial de Defesa, PComTIC Defesa. **Diário Oficial da União,** Brasília, DF, n. 156, seção 1, p. 18, 16 ago. 2023. Disponível em: https://mdlegis.defesa.gov.br/norma_pdf/?NUM=3990&ANO=2023&SER=A. Acesso em: 20 ago. 2026.

BRASIL. Ministério da Defesa. **Portaria GM-MD nº 4.360, de 24 de agosto de 2026**. Aprova a Política de Inteligência Artificial de Defesa. Brasília, DF: Ministério da Defesa, 2026b. Disponível em: https://www.in.gov.br/web/dou/-/portaria-gm-md-n-4.363-de-24-de-agosto-de-2026-728283524. Acesso em: 28 ago. 2026.

BUREAU OF INDUSTRY AND SECURITY (BIS). **Guidance on application of General Prohibition 10 (GP10) to People's Republic of China (PRC) advanced-computing integrated circuits (ICs)**. Washington, DC: U.S. Department of Commerce, 13 maio 2025. Disponível em: https://www.bis.gov/media/documents/general-prohibition-10-guidance-may-13-2025.pdf. Acesso em: 20 ago. 2026.

CONGRESSIONAL RESEARCH SERVICE. **Federal Research and Development (R&D) Funding: FY2026**. Washington, DC: Congressional Research Service, 3 set. 2025. R48694. Disponível em: https://www.congress.gov/crs_external_products/R/PDF/R48694/R48694.2.pdf. Acesso em: 20 ago. 2026.

CRESPI, Francesco; GUARASCIO, Dario; RELJIC, Jelena. **Technological Sovereignty, Big Tech and the Military-Digital complex**. Pisa: Laboratory of Economics and Management, Sant'Anna School of Advanced Studies, 2026. LEM Working Paper Series, n. 2026/20. DOI: 10.57838/sssa/exxw-mf60.

ESTADOS UNIDOS (EUA). Department of Defense. **DoD Directive 3000.09: Autonomy in Weapon Systems**. Washington, DC: Office of the Under Secretary of Defense for Policy, 25 jan. 2023.

ESTADOS UNIDOS (EUA). Department of the Army. **ADP 6-0: Command and Control**. Washington, DC: Headquarters, Department of the Army, 7 jul. 2026.

ESTADOS UNIDOS (EUA). Executive Office of the President. Office of Management and Budget. **Driving Efficient Acquisition of Artificial Intelligence in Government**. Washington, DC: Office of Management and Budget, 3 abr. 2025a. Memorandum M-25-22. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf. Acesso em: 22 ago. 2026.

ESTADOS UNIDOS (EUA). Executive Office of the President. **Winning the Race: America's AI Action Plan**. Washington, DC: The White House, jul. 2025b.

GOLDFARB, Avi; LINDSAY, Jon R. Prediction and judgment: why artificial intelligence increases the importance of humans in war. **International Security**, v. 46, n. 3, p. 7-50, 2022. DOI: 10.1162/isec_a_00425.

GOMES, João Eduardo Costa et al. Surveying emerging network approaches for military command and control systems. **ACM Computing Surveys**, v. 56, n. 6, art. 143, p. 1-38, 2024. DOI: 10.1145/3626090.

GRAND-CLÉMENT, Sarah. **Artificial Intelligence Beyond Weapons: application and impact of AI in the military domain**. Genebra: United Nations Institute for Disarmament Research, 2023. Disponível em: https://unidir.org/wp-content/uploads/2023/10/UNIDIR_AI_Beyond_Weapons_Application_Impact_AI_in_the_Military_Domain.pdf. Acesso em: 22 ago. 2026.

HASSIJA, Vikas et al. Interpreting black-box models: a review on explainable artificial intelligence. **Cognitive Computation**, v. 16, p. 45-74, 2024. DOI: 10.1007/s12559-023-10179-8.

HOLLANDS, Justin G.; SPIVAK, Tzvi; KRAMKOWSKI, Eric W. Cognitive load and situation awareness for soldiers: effects of message presentation rate and sensory modality. **Human Factors**, v. 61, n. 5, p. 763-773, 2019. DOI: 10.1177/0018720819825803.

JOHNSON, James. Automating the OODA loop in the age of intelligent machines: reaffirming the role of humans in command-and-control decision-making in the digital age. **Defence Studies**, v. 23, n. 1, p. 43-67, 2023. DOI: 10.1080/14702436.2022.2102486.

KAMPHORST, Bart Anthony; DE LIGNY, Sofie de Wilde; FERRARI, Fabian; SCHÄFER, Mirko Tobias. Opaque procurement: how transparency deficits compromise democratic digital sovereignty. **Journal of Responsible Technology**, v. 26, art. 100178, 2026. DOI: 10.1016/j.jrt.2026.100178.

KING, Anthony. **AI, Automation, and War: the rise of a military-tech complex**. Princeton, NJ: Princeton University Press, 2025. DOI: 10.1515/9780691265155.

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE (OTAN). **Summary of NATO's revised Artificial Intelligence (AI) strategy**. [S. l.]: OTAN, 10 jul. 2024. Disponível em: https://www.nato.int/fr/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy. Acesso em: 22 ago. 2026.

PARASURAMAN, Raja; RILEY, Victor. Humans and automation: use, misuse, disuse, abuse. **Human Factors**, v. 39, n. 2, p. 230-253, 1997. DOI: 10.1518/001872097778543886.

PFAFF, C. Anthony. **Fighting with Data: design implications for AI-enabled mission-command systems**. Carlisle Barracks, PA: U.S. Army War College Press, 2026. Disponível em: https://press.armywarcollege.edu/monographs/988. Acesso em: 17 ago. 2026.

PROBASCO, Emelia S.; TONER, Helen; BURTELL, Matthew; RUDNER, Tim G. J. **AI for Military Decision-Making: harnessing the advantages and avoiding the risks**. Washington, DC: Center for Security and Emerging Technology, Georgetown University, 2025. Issue Brief. DOI: 10.51593/20240028.

REINHARD, Philipp; LI, Mahei Manhai; PETERS, Christoph; LEIMEISTER, Jan Marco. Effects of explanations in human-AI interaction: a systematic review and framework for future research on explainable AI. **Information Systems Frontiers**, v. 28, p. 1233-1266, 2026. DOI: 10.1007/s10796-026-10716-4.

SHANDLER, Ryan; GROSS, Michael L.; SHERESHEVSKY, Yahli. Black Box Warfare: human judgment and military decision-making in the age of AI. **Journal of Conflict Resolution**, OnlineFirst, 2026. DOI: 10.1177/00220027261463443.

SRNICEK, Nick. **Platform Capitalism**. Cambridge: Polity Press, 2017.

SWELLER, John; AYRES, Paul; KALYUGA, Slava. **Cognitive Load Theory**. New York, NY: Springer, 2011. DOI: 10.1007/978-1-4419-8126-4.

TABASSI, Elham. **Artificial Intelligence Risk Management Framework (AI RMF 1.0)**. Gaithersburg, MD: National Institute of Standards and Technology, 2023. NIST AI 100-1. DOI: 10.6028/NIST.AI.100-1.

TOMSETT, Richard et al. Rapid trust calibration through interpretable and uncertainty-aware AI. **Patterns**, v. 1, n. 4, art. 100049, 2020. DOI: 10.1016/j.patter.2020.100049.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD). **Technology and Innovation Report 2025: inclusive artificial intelligence for development**. Genebra; Nova York: United Nations, 2025. UNCTAD/TIR/2025. ISBN 978-92-1-003283-4. Disponível em: https://unctad.org/publication/technology-and-innovation-report-2025. Acesso em: 17 ago. 2026.

WEI, Peng; SHU, Wesley. Preserving decision sovereignty in military AI: a trade-secret-safe architectural framework for model replaceability, human authority, and state control. **arXiv**, 26 mar. 2026. arXiv:2604.20867v1. Disponível em: https://arxiv.org/abs/2604.20867. Acesso em: 10 ago. 2026.

Autoria

1 Everton Antônio Ramos

Oficial de Infantaria do Exército Brasileiro; Curso de Formação de Oficiais pela Academia Militar das Agulhas Negras; Bacharelado em Educação Física pela Escola de Educação Física do Exército; Curso de Aperfeiçoamento de Oficiais na Escola de Aperfeiçoamento de Oficiais; Mestrado Profissional em Ciências Militares com Ênfase em Gestão Operacional pela Escola de Aperfeiçoamento de Oficiais; Em andamento o curso de Comando e Estado Maior na Escola de Comando e Estado-Maior; Doutorando https://orcid.org/0009-0005-7557-058X • everton.a.ramos@gmail.com

Como citar este artigo

RAMOS, E. A. Soberania decisória e IA de defesa no Sul Global: o caso brasileiro. **InterAção**, Santa Maria, v. 17, n. 3, e98714, p. 1-29, 2026. DOI 10.5902/2357797598714. Disponível em: https://dx.doi.org/10.5902/2357797598714. Acesso em: dia mês abreviado. ano.