RISCOS DO USO DE INTELIGÊNCIA ARTIFICIAL ESTRANGEIRA NAS FORÇAS ARMADAS

*Por Carlos Alexandre Klomfahs**



Imagem meramente ilustrativa, gerada por inteligência artificial.

IA estrangeira nas Forças Armadas: entre ganhos operacionais e riscos à soberania, a exposição de dados militares e familiares abre brechas para espionagem, engenharia social e sabotagem, exigindo uma estratégia de contrainteligência que proteja toda a rede ao redor do militar.

A adoção de sistemas de inteligência artificial desenvolvidos por potências estrangeiras pelas Forças Armadas brasileiras introduz vulnerabilidades que transcendem a dimensão técnica. O presente artigo, baseado em nossas consultorias estratégicas prestadas a governos (TCMS) e empresas, examina três eixos de risco: a exposição das novas gerações de militares a dependências cognitivas e operacionais; a vulnerabilidade dos militares mais experientes a sofisticados ataques de engenharia social; e, principalmente, a captura massiva de dados, incluindo informações de saúde, biométricas e geolocalização, por plataformas privadas estrangeiras, que podem ser empregado indevidamente por forças especiais e serviços de inteligência estrangeiros para espionagem, sabotagem e monitoramento de alvos.

Como pressuposto, este artigo argumenta que os familiares de militares constituem o elo mais frágil dessa cadeia, servindo como via indireta de acesso ao alvo principal. Por isso, as Forças Armadas brasileiras, por meio do Ministério da Defesa, precisam reconhecer os elevados riscos a que estão expostos, desde o gerenciamento de riscos cibernéticos, até a adoção de protocolos rígidos de contrainteligência e de segurança orgânica.

INTRODUÇÃO

A inteligência artificial (IA) deixou de ser promessa para se tornar uma realidade operacional nas Forças Armadas brasileiras, seja nas academias militares, nos cursos de aperfeiçoamento ou nas entidades de estudos superiores, bem como no âmbito tático-operacional, em serviço e fora dele.

Pois bem.

A IA é um conceito amplo que engloba qualquer sistema capaz de imitar a inteligência humana para analisar dados, tomar decisões ou reconhecer padrões (como filtros de *spam* e recomendações de filmes), enquanto a IA generativa é um subconjunto específico dessa tecnologia cujo foco principal é criar conteúdos inéditos e originais, como textos, imagens, áudios e códigos, a partir de comandos recebidos.



Figura 1: Enquanto as Forças Armadas ampliam o uso da IA, plataformas privadas utilizadas por militares e familiares capturam dados de localização, documentos, saúde e biometria. Agregadas, essas informações compõem perfis de rotinas, vínculos e vulnerabilidades, tornando a proteção das famílias parte indispensável da contrainteligência e da segurança orgânica.

Embora a IA tradicional não seja o foco deste artigo, e sim a IA generativa, o Exército, por exemplo, mantém 48 projetos de pesquisa financiados pela FINEP, abrangendo desde enxames de drones até defesa cibernética e tecnologias quânticas. A Marinha emprega visão computacional para vigilância da Amazônia Azul, e a FAB desenvolve sistemas de manutenção preditiva e de apoio à decisão. O Ministério da Defesa inclusive instituiu, em agosto de 2026, a **Política de Inteligência Artificial de Defesa**[1], que estabelece princípios para o uso responsável da tecnologia, porém, o foco é no desenvolvimento interno, não na proteção contra plataformas já em uso.

Por exemplo, a diretriz XI (capacidades autóctones) e o princípio VII (autonomia tecnológica) orientam o futuro: desenvolver tecnologia nacional. Contudo, neste artigo apontamos os riscos presentes e cotidianos: militares e seus familiares já utilizam plataformas estrangeiras privadas (mensagens, redes sociais, nuvem) que capturam dados continuamente. A Portaria não aborda esse uso difuso e não institucional, nem estabelece regras sobre o uso de plataformas privadas estrangeiras por militares em sua vida pessoal ou em comunicações informais. Além disso, a origem desses sistemas raramente é nacional.

A dependência de modelos, infraestrutura de nuvem e plataformas desenvolvidas por empresas estrangeiras[2], majoritariamente sediadas nos Estados Unidos, cria uma assimetria estrutural de poder. Como alertou o secretário[3] de Ciência e Tecnologia para a Transformação Digital do Ministério da Ciência, Tecnologia e Inovação, “você não tem como se defender se não usar ferramentas capazes de criar sua defesa”. O problema é que, ao usar ferramentas alheias, a defesa passa a ser condicionada por interesses alheios.

Este artigo não trata de cenários especulativos de ficção científica. Trata, sim, de riscos concretos, documentados e crescentes, que afetam desde o soldado recém-incorporado até o oficial-general, e que encontram nos familiares dos militares o vetor mais negligenciado e, paradoxalmente, o mais explorável.

---

1 ***BRASIL***. *Portaria GM-MD N° 4.360, de 24 de agosto de 2026. Diário Oficial da União, 01/09/2026, Ed. 165-A, Seção 1, Extra A, Pág. 1. Disponível em: https://www.in.gov.br/web/dou/-/portaria-gm-md-n-4.360-de-24-de-agosto-de-2026-729333487.*

2 ***CANZI***, *Leonardo Sant’Anna. Inteligência Artificial (IA) e Operações Militares: O Emprego da IA no Exame de Situação do Comandante de Operações Militares. Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/15708/1/MO%207384%20-%20LEONARDO%20SANT%20ANNA%20CANZI.pdf.*

3 ***AMOÊDO***, *Julia. Dependência externa em IA amplia risco geopolítico, diz governo. Poder360, 16 de maio de 2026. Disponível em: https://www.poder360.com.br/poder-governo/dependencia-externa-em-ia-amplia-risco-geopolitico-diz-governo/.*

DIRETRIZ ESTRATÉGICA DE IA DO EB E PRINCÍPIOS DO DIH

A Diretriz Estratégica de Inteligência Artificial do Exército Brasileiro (EB20-D-02.031) foi aprovada pela Portaria C Ex Nº 1.318/2024 e publicada no *Boletim do Exército nº 21*, de 24 de maio de 2024. Seu escopo abrange a aplicação da IA em sistemas de comando e controle (C^2), apoio à decisão em tempo real no ciclo OODA (Observar, Orientar, Decidir e Agir), proteção de infraestruturas críticas e otimização logística.

A Diretriz estabelece as orientações para implantação e uso da IA na Força, priorizando controle humano em decisões de uso da força. Contudo, a diretriz não faz menção aos riscos do uso de plataformas estrangeiras, nem detalha mecanismos concretos de auditoria, explicabilidade e prestação de contas exigidos pelo Direito Internacional Humanitário (DIH). Embora alguns desses pontos não sejam objeto do presente artigo, tal lacuna que representa um risco significativo para a conformidade legal em cenários de conflito armado.

NO ÂMBITO DO MINISTÉRIO DA DEFESA

A Portaria GAB CHEC-MD[4] nº 3.742, de 13 de julho de 2026, disciplina o uso de ferramentas de Inteligência Artificial Generativa (IA-G) nas atividades acadêmicas da Escola Superior de Guerra (ESG) e da Escola Superior de Defesa (ESD). Seu eixo central é a proteção de dados estratégicos e a responsabilização humana integral pelo conteúdo produzido com auxílio de IA.

A Portaria representa um avanço normativo relevante ao vedar expressamente o processamento de informações classificadas, sigilosas ou operacionais em nuvem pública, determinando que ferramentas sem garantias suficientes sobre retenção, reaproveitamento de dados ou compartilhamento com terceiros sejam tratadas como “não aprovadas” para informações protegidas.

Contudo, seu alcance é setorial e limitado às atividades acadêmicas apenas da ESG e ESD, deixando descobertas outras instituições militares de ensino superior e o uso cotidiano de plataformas estrangeiras por militares em contextos operacionais e, sobretudo, por seus familiares, vetores que este artigo identifica como os elos mais vulneráveis da cadeia de captura de dados.

Ademais, a Portaria concentra a responsabilização no usuário individual, sem estabelecer exigências de auditoria algorítmica independente ou certificação de fornecedores estrangeiros, de modo que mitiga o sintoma (o uso indevido pelo usuário)

4 *Gabinete da Chefia de Educação e Cultura do Ministério da Defesa.*

sem enfrentar a causa estrutural (a dependência de infraestrutura alheia) que este artigo diagnostica.



Figura 2: Os atos estabelecem salvaguardas em contextos específicos: a Diretriz do Exército prioriza o controle humano; a Política de IA de Defesa orienta o desenvolvimento nacional; e a Portaria da ESG e da ESD regula o uso acadêmico. Ainda falta orientação abrangente para o uso cotidiano de plataformas privadas por militares e familiares.

RISCOS PARA AS NOVAS GERAÇÕES

Os militares mais jovens, a chamada “geração nativa digital”, sejam praças, cadetes e jovens oficiais, chegam às fileiras com uma familiaridade intuitiva com tecnologias que seus superiores levaram décadas para dominar. Essa fluência, no entanto, converte-se em vulnerabilidade quando aplicada a plataformas estrangeiras de IA generativa.

O primeiro risco é a dependência cognitiva precoce. Jovens oficiais e praças formam seus hábitos profissionais em contato com assistentes de IA generativa, sistemas de recomendação tática e ferramentas de análise de dados cujos algoritmos são caixas-pretas proprietárias, além dos riscos de informações pessoais que exponham a tropa, os exercícios, os adestramentos ou as operações, ou o *upload* de documentos confidenciais, doutrinários ou acadêmicos, classificados ou não, que podem ser utilizados em “engenharia de inteligência reversa” para reconstrução de informações de defesa.

A explicabilidade – a capacidade de compreender e auditar decisões automatizadas –, torna-se letra morta quando o modelo pertence a uma empresa estrangeira que não revela seus parâmetros. A formação doutrinária nacional cede lugar a uma lógica operacional desenhada sob premissas alheias.

O segundo risco é a exposição a mecanismos de controle remoto, equipamentos e *softwares* estrangeiros podem conter *kill switches* ou *backdoors*[5], dispositivos lógicos que permitem a negação de funcionamento à distância.

Não sem razão, o presidente[6] da Associação das Indústrias Aeroespaciais do Brasil alerta que, ainda que um equipamento funcione por décadas sem interferência, “isso não representa garantia de que funcionarão da mesma forma numa eventual guerra”.



Figura 3: Os três riscos interligados para os militares mais jovens: dependência cognitiva, vulnerabilidade operacional e conformidade acrítica. Formação crítica e autonomia tecnológica são fundamentais para preservar a capacidade de decisão e a doutrina nacional.

Basta recordar que o Brasil já sofreu negação de acesso ao GPS em 1997 e 1999 durante lançamentos do VLS, e questionamentos semelhantes surgiram em 2024 sobre o uso da rede Starlink pelas Forças Armadas[7]. Para os jovens militares que operam drones, sistemas de comando e controle e plataformas de análise em tempo real, a confiança em *hardware* e *software* estrangeiros é uma aposta cujo custo pode ser a própria missão.

5 *Kill switch e backdoor são mecanismos de controle digital, mas funcionam para finalidades opostas de segurança e acesso.* ***Kill switch****: É um botão de emergência projetado para desligar ou inutilizar remotamente um sistema, dispositivo ou rede para conter uma ameaça ou evitar vazamento de dados.* ***Backdoor****: É uma porta dos fundos oculta que permite acessar ou controlar um sistema secretamente, ignorando os mecanismos normais de autenticação e segurança.*

6 ***SHIDARA****, Júlio. A Ameaça dos Kill Switches Para a Soberania Nacional. Velho General, 10 de novembro de 2026. Disponível em: https://velhogeneral.com.br/2026/11/10/a-ameaca-dos-kill-switches-para-a-soberania-nacional/.*

7 ***FREITAS****, Caio de. Starlink: Militares usam internet via satélite de Elon Musk sem teste de segurança da rede. A Pública, 31 de outubro de 2024. Disponível em: https://apublica.org/2024/10/starlink-militares-usam-internet-via-satelite-de-elon-musk-sem-teste-de-seguranca-da-rede/.*

O terceiro risco é a formação de uma cultura de conformidade acrítica. Se as ferramentas de IA disponíveis são estrangeiras, e se não há alternativas nacionais em escala, os jovens militares aprendem dentro de limites epistêmicos impostos por terceiros.

RISCOS PARA OS MILITARES MAIS VELHOS

Se os jovens estão expostos pela imersão acrítica, os militares mais experientes, especialmente os oficiais superiores que compõe um Estado-Maior e os oficiais-generais enfrentam uma vulnerabilidade distinta: a erosão da base de conhecimento tácito e a exposição a ataques de engenharia social cada vez mais sofisticados, que enganam até os mais experientes e cautelosos.

O oficial veterano construiu sua carreira sobre um repertório de experiências, intuições e procedimentos que a IA não replica. Contudo, à medida que sistemas de apoio à decisão estrangeiros ganham espaço, esse conhecimento tácito é progressivamente desvalorizado ou, pior, capturado.

Plataformas de IA registram consultas, decisões e análises de oficiais superiores, que acumulam um acervo sobre doutrina, capacidades e limitações nacionais. Esse acervo reside em servidores estrangeiros, sujeitos a jurisdições estrangeiras.

A engenharia social, mesmo contra militares experientes, é igualmente sofisticada. Ataques modernos utilizam IA para gerar comunicações personalizadas, *deep fakes* de voz e texto, e perfis falsos em redes sociais que exploram redes de contato profissionais e pessoais.

Um oficial superior que utilize uma plataforma estrangeira de mensagens ou rede profissional para manter contato com colegas, incluindo estrangeiros, prática comum em adidos e alunos de cursos no exterior, torna-se alvo de campanhas de *phishing* direcionadas.

Note-se que mesmo o Departamento de Guerra dos Estados Unidos reconhece que “todo soldado é um alvo potencial, independentemente de posto ou especialidade” e que “pequenos erros podem ter consequências estratégicas”.

O risco mais insidioso, contudo, é a normalização da vigilância. Militares experientes que utilizam plataformas privadas estrangeiras para comunicação como *e-mails*, armazenamento de documentos em nuvens e até mesmo aplicativo de monitoramento de saúde criam, involuntariamente, um arquivo vivo de informações sensíveis.

A infraestrutura que faz varredura de conversas para identificar crimes violentos, como revelado no caso OpenAI, “é a mesma que identifica segredos industriais, pesquisas científicas de ponta ou planejamento estratégico de governos”. O militar veterano, por

sua posição e conhecimento acumulado, é precisamente o alvo de maior valor para esse tipo de coleta.



Figura 4: Pistas digitais e redes de contato favorecem mensagens personalizadas e phishing direcionado, com familiares também como via indireta de acesso. Gestão de riscos cibernéticos, contrainteligência e segurança orgânica devem integrar a resposta.

CAPTURA DE DADOS POR PLATAFORMAS PRIVADAS E SERVIÇOS DE INTELIGÊNCIA

O núcleo do problema reside na assimetria informacional entre o usuário militar e o provedor estrangeiro de IA. Quando um membro das Forças Armadas utiliza uma plataforma privada, seja um aplicativo de mensagens, aplicativos de navegação por GPS, uma rede social, um assistente de voz ou um serviço de armazenamento em nuvem, ele fornece, voluntária ou involuntariamente, um conjunto de dados às Forças Especiais e Serviços de Inteligência estrangeiros, que inclui:

• **Informações de Geolocalização**: rotinas, deslocamentos, locais de trabalho e residência, padrões de comportamento;

• **Documentos**: arquivos pessoais e/ou classificados, outros aparentemente inócuos que, agregados, revelam estruturas organizacionais, capacidades e vulnerabilidades;

• **Informações de Saúde**: dados médicos, históricos de exames, condições físicas e mentais, obtidos por meio de aplicativos de monitoramento ou armazenamento de documentos;

• **Dados Biométricos**: impressões digitais, reconhecimento facial, padrões de voz, padrões de escrita, pegadas digitais capturadas por sensores de dispositivos e autenticação em plataformas.



Figura 5: A agregação de dados de localização, documentos, saúde e biometria pode formar perfis detalhados das rotinas, redes de contato e vulnerabilidades de militares.

A legislação brasileira reconhece a sensibilidade desses dados. A Lei Geral de Proteção de Dados (LGPD)[8] classifica dados biométricos e de saúde como informações pessoais sensíveis, mas o foco não é a lei e sim protocolos nacionais de contrainteligência e segurança orgânica.

Contudo, a jurisdição estrangeira dos provedores cria um vazio de proteção: o militar brasileiro não tem como exigir que uma empresa sediada nos Estados Unidos, na Europa ou na China apague seus dados, limite seu uso ou preste contas sobre compartilhamento com agências governamentais daquele país.

A legislação americana, em particular, permite que o governo acesse dados armazenados por empresas nacionais americanas por meio de ordens judiciais sigilosas ou de programas de vigilância em massa. A revelação de que a OpenAI vinha escaneando conversas de usuários para identificar crimes, infraestrutura que pode ser redirecionada para outros fins, ilustra a plasticidade desses sistemas. A oferta de 5% de participação

8 ***PRESIDÊNCIA DA REPÚBLICA***. *Secretaria-Geral, Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.*

acionária da OpenAI ao governo americano, noticiada em julho de 2026, apenas institucionaliza essa proximidade.

Para as forças especiais e os serviços de inteligência estrangeiros, esses dados constituem um arquivo de alvos em potencial. A agregação de informações dispersas – uma postagem em rede social, um histórico de localização, um documento compartilhado em nuvem –, permite construir perfis detalhados de militares brasileiros: suas rotinas, suas redes de contato, suas vulnerabilidades pessoais e profissionais. Esse arquivo pode ser armazenado por anos, aguardando o momento em que se torne útil para operações de engenharia social, espionagem, sabotagem ou, em cenário extremo, neutralização de alvos.

A doutrina de contrainteligência brasileira reconhece a necessidade de "produzir conhecimento sobre elementos do público interno com capacidade de serem cooptados". O que a doutrina parece não ter previsto foi que a cooptação pudesse ocorrer indiretamente por parentes próximos do militar e não por abordagem direta, como pela captura silenciosa de dados em plataformas privadas estrangeiras, sem que o alvo sequer perceba que está sendo mapeado.

OS FAMILIARES COMO ELO MAIS FRÁGIL

A cadeia de vulnerabilidade não termina no militar. Ela se estende, e encontra seu ponto de menor resistência, nos familiares. Cônjuges, filhos, pais e companheiros de militares utilizam as mesmas plataformas estrangeiras de comunicação, redes sociais e serviços digitais.

Ora, eles não passam por treinamento de segurança operacional, não têm obrigação de sigilo e não compreendem, necessariamente, o valor estratégico de uma informação aparentemente trivial: uma foto de família em frente à residência funcional, um passeio no *shopping*, uma viagem turística, uma postagem sobre a ausência do militar durante uma operação, um comentário sobre a rotina de trabalho do cônjuge, etc.

Para um serviço de inteligência estrangeiro, os familiares são a via indireta de acesso ao alvo principal. A engenharia social contra um cônjuge, por meio de um perfil falso em rede social, um anúncio de emprego atraente, um *link* aparentemente inofensivo, pode render credenciais de acesso, informações sobre a localização do militar, ou até mesmo a instalação de *spyware* no dispositivo da família.

O Departamento de Guerra americano alerta que "postagens aparentemente inofensivas em redes sociais, como fotos em zona de guerra, reclamações sobre a unidade, ou mesmo atualizações familiares, podem ser montadas como um quebra-cabeça que revela um

quadro: prontidão da unidade, cronogramas, vulnerabilidades". O alerta vale, *a fortiori*, para as famílias de militares brasileiros.

O elo familiar é explorado de três formas principais. Primeiro, pela **coleta passiva**: os familiares publicam, compartilham e curtem conteúdo que, agregado, revela padrões de vida, localização e relações do militar. Segundo, pelo **engajamento ativo**: perfis falsos, golpes românticos, ofertas de emprego e mensagens personalizadas exploram a confiança e a vulnerabilidade emocional dos familiares. Terceiro, pela **coerção**: em cenários de crise ou conflito, a exposição de informações sobre familiares pode ser utilizada como instrumento de pressão psicológica sobre o militar.



Figura 6: A exposição digital de familiares pode revelar padrões de vida, localização e relações do militar, além de abrir caminho para engenharia social e pressão psicológica. A orientação e a proteção da família pode ampliar o perímetro de segurança orgânica e contrainteligência.

Sob esta perspectiva, pode-se inferir que a doutrina de contrainteligência e de segurança orgânica das Forças Armadas brasileiras dedica atenção limitada a esse vetor. O treinamento de segurança operacional tende a focar no militar, não em sua rede familiar. Contudo, a experiência em nossas consultorias estratégicas a governos e empresas, bem como os conflitos recentes, demonstram que a guerra informacional não respeita a distinção entre combatente e não combatente, especialmente quando o não combatente carrega, no bolso, um dispositivo conectado a plataformas estrangeiras.

CONSIDERAÇÕES FINAIS

À luz das evidências apresentadas, pode-se inferir que o uso de inteligência artificial estrangeira nas Forças Armadas não é, em si, um risco, embora tenhamos visto que a Diretriz EB20-D-02.031 do Exército representa um avanço ao formalizar a governança de IA no Exército e ao afirmar o controle humano sobre o uso da força. Contudo, é imperativo incorporar mecanismos concretos de orientação de uso de IA dentro e fora de serviço, aos militares e seus familiares, bem como auditoria, explicabilidade e prestação de contas.



Figura 7: A proteção da Defesa exige medidas complementares: soberania sobre infraestrutura, dados e algoritmos; governança institucional com controle humano; e formação e orientação que incluam militares e familiares no perímetro de proteção.

Assim, a Portaria nº 3742/2026 do Ministério da Defesa, que por ter sido elaborada no âmbito acadêmico, teve foco setorial e restrito a ESD e ESG, deixa a descoberto todas as instituições de ensino superior militar e no âmbito das competências do Ministério da Defesa, carece de um alcance nacional sobre protocolos de contrainteligência e segurança orgânica, como a “defesa cibernética” e “inteligência estratégica e operacional no interesse da defesa”, as organizações militares.

Vê-se que a tecnologia é uma realidade incontornável, e a recusa em utilizá-la criaria uma assimetria de capacidades igualmente perigosa. O problema reside na ausência de controle soberano e em âmbito nacional sobre a infraestrutura, os dados e os algoritmos que sustentam essa tecnologia.

As novas gerações de cadetes precisam de formação crítica que as conscientize sobre os limites dos sistemas estrangeiros como uso de IA para trabalhos acadêmicos ou operacionais em instituições e organizações militares. Por outro lado, os militares mais experientes precisam de protocolos que protejam seu conhecimento tácito da captura por plataformas alheias.

Acima de tudo, as Forças Armadas precisam reconhecer, no gerenciamento de riscos cibernéticos, que os dados de seus membros – e de suas famílias – não são um subproduto inevitável da vida digital, mas um ativo estratégico que está sendo transferido, gratuitamente, para jurisdições estrangeiras.

A construção de soberania tecnológica exige mais do que discursos. Exige infraestrutura nacional de nuvem, modelos de IA desenvolvidos e auditados no país, e uma doutrina de segurança operacional que contemple a família do militar como parte integrante do perímetro de proteção. Enquanto isso não ocorrer, o elo mais frágil continuará sendo aquele que menos sabe que está na mira.

***Carlos Alexandre Klomfahs** é advogado, especialista em Direito Internacional dos Conflitos Armados e operador de Inteligência. Egresso curso de geopolítica da ECEME e estratégia marítima da Escola de Guerra Naval. É mestrando no Programa de Pós-Graduação em Segurança Internacional e Defesa (PPGSID) da Escola Superior de Guerra.*
