Cadernos Adenauer

ANO XXVII
2026

KONRAD ADENAUER STIFTUNG

2

Indústria de defesa e novas tecnologias

www.kas.de/brasil

Indústria de defesa e novas tecnologias

Cadernos Adenauer
ANO XXVII
2026
2

Indústria de defesa e novas tecnologias

KONRAD ADENAUER STIFTUNG

EDITOR RESPONSÁVEL
Maximilian Hedrich

CONSELHO EDITORIAL
Antônio Jorge Ramalho
Fátima Anastasia
Humberto Dantas
José Mario Brasiliense Carneiro
Leonardo Nemer Caldeira Brant
Lúcia Avelar
Mario Monzoni
Rodrigo Perpétuo
Silvana Krause

COORDENAÇÃO EDITORIAL
Reinaldo J. Themoteo

REVISÃO
Reinaldo J. Themoteo

CAPA, PROJETO GRÁFICO E DIAGRAMAÇÃO
Claudia Mendes

ISSN 1519-0951
Cadernos Adenauer XXVII (2026), nº2
Indústria de defesa e novas tecnologias
Rio de Janeiro: Fundação Konrad Adenauer, junho 2026.
ISBN 978-65-89432-66-1

FUNDAÇÃO KONRAD ADENAUER
Representação no Brasil: Rua Guilhermina Guinle, 163 · Botafogo
Rio de Janeiro · RJ · 22270-060
Tel.: 0055-21-2220-5441 · Telefax: 0055-21-2220-5448
adenauer-brasil@kas.de · www.kas.de/brasil

Sumário

Apresentação

A indústria de defesa ocupa um papel estratégico na segurança nacional e na projeção de poder dos Estados, sendo também um dos setores que mais impulsiona o desenvolvimento tecnológico em escala global. Historicamente, inovações como a internet, o GPS e os drones nasceram de projetos militares e, posteriormente, transformaram-se em ferramentas de uso civil, demonstrando como a defesa atua como catalisadora de avanços científicos. No cenário contemporâneo, marcado por tensões geopolíticas, guerras híbridas e ameaças cibernéticas, a integração de novas tecnologias torna-se essencial para garantir superioridade operacional e capacidade de resposta rápida. Inteligência artificial, big data, sistemas autônomos, nanotecnologia e biotecnologia são apenas alguns dos campos que vêm redefinindo o conceito de defesa, ampliando tanto as possibilidades de proteção quanto os dilemas éticos e jurídicos. Além disso, a cooperação internacional e a participação da iniciativa privada têm se mostrado fundamentais para acelerar a inovação, ao mesmo tempo em que levantam questões sobre soberania e dependência tecnológica.

O objetivo desta edição da série Cadernos Adenauer, a segunda de 2026, é apresentar um conjunto de artigos que analisem os principais aspectos da interseção entre a indústria de defesa e as novas tecnologias, oferecendo aos leitores textos que ajudem a compreender como esse setor se reinventa diante das transformações digitais e científicas, com atenção especial aos impactos econômicos, sociais e políticos no contexto brasileiro.

Esta publicação é composta por seis capítulos. O primeiro apresenta um panorama das novas tecnologias e suas aplicações militares, explorando como inovações recentes estão sendo incorporadas às doutrinas e capacidades das forças armadas ao redor do mundo. O segundo capítulo é dedicado à biotecnologia e à nanotecnologia no setor militar, discutindo as fronteiras entre avanço científico e os riscos associados ao uso dessas tecnologias em contextos de conflito. No terceiro capítulo, a análise recai sobre a economia da defesa e seu impacto industrial, com ênfase nas cadeias produtivas, no fomento à inovação e nas implicações para o desenvolvimento nacional. O quarto capítulo trata das implicações éticas das novas tecnologias militares, refletindo sobre os limites do uso de sistemas avançados e a responsabilidade dos Estados e das empresas envolvidas. O quinto capítulo dedica-se ao conceito de guerra híbrida, explicando suas características, seus mecanismos e os desafios que representa para as democracias contemporâneas. Por fim, o sexto capítulo projeta cenários e tendências para o futuro da defesa, convidando o leitor a refletir sobre o papel da inovação na construção de um ambiente internacional mais resiliente e equilibrado.

Agradecemos a cada autora e a cada autor que participam nesta publicação, cujos artigos contribuem para um debate qualificado sobre segurança, tecnologia e soberania. Cada capítulo convida leitoras e leitores a uma reflexão crítica sobre os desafios e as oportunidades que emergem da convergência entre defesa e inovação, propondo perspectivas para um Brasil mais preparado para os cenários que se avizinham. Boa leitura!

Maximilian Hedrich
Diretor da Fundação Konrad Adenauer no Brasil

Novas tecnologias e sua aplicação militar

Thiago Borne

Resumo

O presente artigo examina a relação entre tecnologia e guerra a partir de uma perspectiva histórica, institucional e estratégica. Parte-se do argumento de que as dinâmicas contemporâneas não representam uma ruptura absoluta, mas a intensificação de padrões recorrentes de interação entre inovação tecnológica e conflito armado, agora potencializados pela centralidade do setor privado e pela difusão de tecnologias de uso dual. A primeira seção reconstitui a genealogia institucional dessa relação, desde a "era da automação" até o deslocamento do eixo de inovação do Estado para o mercado privado, articulando evidências dos conflitos em curso na Ucrânia e em Gaza como ilustração direta dessas dinâmicas. A segunda seção discute as implicações estratégicas desse processo a partir de duas dimensões complementares: a tradição das *offset strategies* norte-americanas e o problema estrutural da escala na adoção de novas tecnologias. Conclui-se que a vantagem estratégica contemporânea depende menos da posse de tecnologias avançadas do que da capacidade de integrá-las em ecossistemas operacionais coerentes, o que exige reforma institucional, coordenação público-privada e mecanismos eficazes de aquisição.

Abstract

This paper examines the relationship between technology and warfare from historical, institutional, and strategic perspectives. It argues that

contemporary dynamics do not represent an absolute break with the past, but rather an intensification of recurring patterns of interaction between technological innovation and armed conflict, now amplified by the growing centrality of the private sector and the diffusion of dual-use technologies. The first section reconstructs the institutional genealogy of this relationship, from the "age of automation" to the shift of the innovation axis from the state to the private market, drawing on empirical evidence from the ongoing conflicts in Ukraine and Gaza. The second section discusses the strategic implications of this process through two complementary lenses: the American tradition of offset strategies and the structural challenge of scaling new technologies for operational use. The article concludes that contemporary strategic advantage depends less on the possession of advanced technologies than on the capacity to integrate them into coherent operational ecosystems, a goal that requires institutional reform, public-private coordination, and agile acquisition mechanisms.

Introdução

O século XXI tem sido marcado pela aceleração do progresso tecnológico. Tecnologias que por décadas permaneceram restritas à ficção científica passaram não apenas a ser empregadas no campo de batalha, como também a se difundir amplamente no cotidiano. O ritmo dessa transformação permanece elevado, e seu impacto sobre a forma como sociedades e forças militares operam é inegável. Esse processo abrange múltiplas frentes, incluindo a inteligência artificial (IA), os sistemas autônomos e as dimensões espacial e cibernética da guerra.

Essa transformação ocorre em paralelo a um momento crítico no ambiente de segurança internacional, caracterizado pela transição do eixo de poder econômico e militar do Atlântico para o Pacífico. À medida que o equilíbrio de poder global se torna cada vez mais contestado, a competição, em suas diversas formas, tende a se intensificar. O enfraquecimento da noção tradicional de "Ocidente", historicamen-

te liderada pelos Estados Unidos e ancorada em valores e instituições consolidados no pós-guerra, amplia as margens de manobra de potências revisionistas como Rússia e Coreia do Norte, ao mesmo tempo em que corrói a confiança em foros multilaterais como a OTAN, a ONU e o Banco Mundial. Não por acaso, os conflitos em curso na Ucrânia e no Oriente Médio, caracterizados por sua escala, duração e pela integração de tecnologias avançadas, sugerem que o sistema internacional atravessa uma inflexão dessa natureza. Nesse cenário, premissas centrais da teoria estratégica do século XX tornam-se progressivamente insuficientes.

Esses conflitos têm, ademais, levado potências ocidentais a redescobrir lições clássicas da história militar parcialmente negligenciadas no pós-Guerra Fria: a centralidade da produção industrial em larga escala e a persistência da guerra de atrito (Jones; Daniels, 2025). Diferentemente dos conflitos daquele período, frequentemente breves e geograficamente delimitados, as guerras contemporâneas são interconectadas em escala global e altamente disruptivas para infraestruturas civis. Esse conjunto de características impõe novos imperativos tanto à análise acadêmica quanto ao planejamento de defesa.

Os dados orçamentários confirmam essa inflexão. Os gastos globais de defesa passaram de US$ 2,23 trilhões em 2023 para US$ 2,46 trilhões em 2024, tendência impulsionada pelo aumento de 50% nos orçamentos dos membros europeus da OTAN entre 2022 e 2025 e por um suplemento extraordinário de US$ 156 bilhões aprovado pelo Congresso norte-americano em 2025 (Jones; Daniels, 2025, p. 119-122). O número de aliados da OTAN que atingem a meta de 2% do PIB em gastos militares, que era de apenas três em 2014, subiu para mais de vinte em 2025 – uma transformação que não teria ocorrido sem a invasão russa à Ucrânia como catalisador. Esse reequipamento acelerado, combinado com a modernização contínua das forças armadas chinesas, sinaliza que o ambiente estratégico contemporâneo é menos caracterizado por competição difusa do que por uma corrida armamentista com contornos cada vez mais definidos.

Esse ambiente competitivo repercute diretamente sobre o desenvolvimento e o emprego de tecnologias militares. Tradicionalmente, dois modelos têm orientado a análise das transformações na guerra: o evolucionismo gradual, baseado em mudanças incrementais, e o equilíbrio pontuado, que enfatiza rupturas abruptas seguidas de estabilidade. A realidade contemporânea, no entanto, desafia essa distinção. A guerra passa a evoluir simultaneamente por acumulação e por descontinuidades, combinando processos incrementais com mudanças qualitativas que reconfiguram premissas doutrinárias consolidadas.

Este artigo tem por objetivo retomar o debate sobre tecnologia e guerra a partir de uma perspectiva que articula suas dimensões históricas, institucionais e estratégicas. Parte-se do argumento de que as dinâmicas contemporâneas não representam uma ruptura absoluta, mas a intensificação de padrões recorrentes de interação entre inovação tecnológica e conflito armado, agora potencializados pela centralidade do setor privado e pela difusão de tecnologias de uso dual. O artigo desenvolve esse argumento em duas seções. A primeira reconstitui a relação histórica entre guerra e inovação e examina o deslocamento do eixo de desenvolvimento tecnológico do Estado para o mercado, articulando evidências dos conflitos contemporâneos como ilustração direta dessas dinâmicas. A segunda discute as implicações estratégicas desse processo a partir de duas dimensões complementares: a tradição das estratégias de compensação norte-americanas e o problema estrutural da escala na adoção de novas tecnologias.

Desenvolvimento tecnológico, indústria e mercado

Para compreender como a tecnologia chegou ao centro do conflito contemporâneo, é preciso reconstituir sua genealogia institucional. A origem de grande parte das tecnologias atualmente empregadas no campo de batalha está diretamente associada a esforços de pesquisa conduzidos sob a liderança do governo dos Estados Unidos. Inovações como a internet, o sistema de posicionamento global (GPS), e os microprocessa-

dores emergiram de um ecossistema em que investimentos públicos em pesquisa básica e aplicada contribuíram não apenas para avanços tecnológicos, mas para a formação de setores industriais inteiros.

Esse padrão de retroalimentação entre conflito e inovação se aprofundou a partir da Segunda Guerra Mundial com o que se convencionou chamar de "era da automação" (Van Creveld, 1991): o período em que a transmissão, o processamento e o armazenamento de dados passaram a ser desafios centrais das forças armadas, demandando sistemas computadorizados que substituíram parte da mão de obra e aceleraram, paradoxalmente, o próprio volume de dados produzidos. O desenvolvimento da internet e do GPS como subprodutos de investimentos militares norte-americanos é expressão direta desse ciclo. O conceito de "revolução nos assuntos militares", que ganhou força política nos anos 1990 a partir das lições da Guerra do Golfo, traduziu institucionalmente esse reconhecimento: tratava-se de transformar as forças armadas norte-americanas por meio da integração de tecnologias de informação e comunicação em todos os níveis operacionais, do planejamento à logística (Borne, 2019).

Essa dinâmica não é nova. Ao longo da história, a guerra atuou reiteradamente como catalisadora da inovação: a Primeira e a Segunda Guerras Mundiais aceleraram o desenvolvimento de rádio, aviação, radar, medicina de campo e computação; a Guerra Fria impulsionou corridas tecnológicas em propulsão a jato, energia nuclear e nos fundamentos da computação em rede. Cada ciclo de conflito produziu não apenas armas mais letais, mas plataformas cujos desdobramentos civis redefiniram a economia e a vida cotidiana. Esses momentos, em que múltiplas ondas tecnológicas convergem simultaneamente, amplificando o potencial disruptivo de cada inovação e tornando o ritmo de transformação particularmente difícil de antecipar pelas estruturas político-militares, foram denominados "revoluções científicas paralelas" (Kadtke; Wells II, 2014). É precisamente esse o cenário contemporâneo.

Esse deslocamento não foi apenas econômico: teve raízes na reestruturação política do pós-Guerra Fria. O fim da União Soviética justi-

ficou cortes orçamentários e processos de privatização nas forças armadas de diversos países, enquanto nos Estados Unidos a crescente aversão pública a guerras de alto custo humano pressionava o planejamento militar a buscar alternativas tecnológicas à presença massiva de tropas. A digitalização passou a ser vista não apenas como fator de superioridade tática, mas como instrumento para reduzir a "fricção" política do uso da força (Borne, 2019). A lógica era clara: forças menores, mais tecnológicas e mais letais poderiam ser projetadas com menor custo político do que os exércitos de massa do século XX.

A partir dos anos 1990, e de forma acelerada na década seguinte, esse eixo de inovação deslocou-se do setor público para o privado. Nos anos 2000, com a consolidação da economia digital, empresas privadas passaram a liderar o desenvolvimento tecnológico, enquanto o papel do governo norte-americano em pesquisa e desenvolvimento (P&D) se tornou relativamente menos central. No caso dos Estados Unidos, em particular, a desvinculação entre a indústria de software e os objetivos estratégicos nacionais criou uma lacuna crítica na capacidade do Estado de direcionar a inovação para fins de segurança, comprometendo a base tecnológica de sua superioridade militar (Karp; Zamiska, 2024).

Os dados tornam esse diagnóstico ainda mais preciso. Em 2025, o gasto público norte-americano em P&D correspondia a 17% do orçamento de defesa, contra apenas 4% na Europa, uma razão de quatro para um que reflete não uma retirada do Estado do campo da inovação, mas uma assimetria estrutural no papel que esse Estado desempenha de cada lado do Atlântico (Lang et al., 2026). No setor privado, a diferença é marginal: as maiores empresas de defesa europeias investem em média 5% da receita em P&D, contra 4,5% das norte-americanas. O que separa os dois ecossistemas não é, portanto, a ambição privada, mas a intensidade e a continuidade do financiamento público. Onde o Estado recuou sem deixar substituto equivalente, criou-se um vácuo que o mercado, orientado por retornos de curto prazo, não tem incentivo estrutural para preencher.

Esse rearranjo tem implicações diretas para a segurança nacional. As motivações que orientam o investimento privado em P&D diferem substancialmente daquelas que historicamente guiaram a ação estatal: enquanto o setor público tende a priorizar objetivos estratégicos de longo prazo, a indústria concentra-se em retornos mais imediatos, com foco em aplicações comerciais e na rápida disseminação de tecnologias. Considerações relativas ao uso adversarial dessas inovações frequentemente ocupam posição secundária, o que representa uma vulnerabilidade estrutural para as democracias ocidentais.[1]

O setor privado não é apenas um fornecedor passivo de tecnologia: tornou-se um ator com agenda própria na reforma das estruturas de aquisição do Estado. Em 2024, as empresas Palantir e Anduril formaram um consórcio explicitamente desenhado para desafiar contratantes tradicionais, argumentando oferecer "uma forma mais eficiente de vender ao governo tecnologia de ponta" (Goussac; Boulanin, 2026, p. 7). O relatório *NatSec100* do Silicon Valley Defense Group, publicado em 2025, vai além e advoga pela substituição do foco em "inovação" pelo foco em "adoção acelerada" de capacidades já existentes, pressionando o Estado a simplificar processos de certificação e aprovação para que produtos privados cheguem mais rapidamente ao campo de batalha. Ao Parlamento britânico, representantes dessas empresas afirmaram que ciclos de produto no setor de IA se medem em semanas ou meses, tornando os processos de aquisição tradicionais, que operam em anos ou décadas, estruturalmente incompatíveis com o ritmo da inovação contemporânea (SVDG, 2025). A questão que esse movimento levanta não é apenas de eficiência: é de quem define, afinal, as prioridades da defesa nacional.

---

1 Esse descompasso é reconhecido pelas próprias instituições de defesa ocidentais. A OTAN identifica nove áreas de tecnologias emergentes e disruptivas, entre elas inteligência artificial, computação quântica, sistemas autônomos, biotecnologia e tecnologias hipersônicas, como centrais para a transformação em curso, e reconhece que a vantagem estratégica passa a depender da capacidade de coletar, processar e agir sobre dados em tempo real, reduzindo o ciclo de decisão e ampliando a eficácia operacional em ambientes multidomínio (LANG et al., 2026).

Os conflitos em curso oferecem evidências empíricas diretas dessas dinâmicas. Na Ucrânia, o chamado "ciclo de aprendizado de seis semanas" expressa uma realidade em que ambos os lados desenvolvem contramedidas eletrônicas, adaptam plataformas e testam novos sistemas com uma agilidade sem precedentes (Jones; Daniels, 2025). Diante da eficácia crescente dos drones com inteligência IA para localizar alvos blindados, as forças russas chegaram a recorrer a animais de carga para movimentação de suprimentos, o que demonstra que pressão tecnológica suficiente pode forçar adversários a recuar a soluções pré-tecnológicas. No plano das comunicações, a adoção de drones operados por cabos de fibra óptica (imunes ao *jamming*[2] eletrônico e com alcance de até dez quilômetros) ilustra como soluções de baixo custo podem neutralizar vantagens tecnológicas consideráveis.

A guerra da informação avançou de forma igualmente acelerada. A Ucrânia empregou software de reconhecimento facial com IA para identificar mais de 250 mil soldados russos e localizar crianças levadas para a Rússia, enquanto esta lançou *deepfakes*[3] de figuras políticas ucranianas para fins de desinformação em escala industrial. Ao mesmo tempo, drones ISR[4] coletam vastos volumes de dados, com IA analisando imagens de satélite e relatórios de campo para produzir listas de alvos em tempo real, comprimindo os ciclos de decisão a um grau que desafia as estrutu-

2 *Jamming* (ou interferência eletrônica) é a técnica de emissão deliberada de sinais de rádio frequência para bloquear ou degradar as comunicações e os sistemas de navegação do adversário, tornando inoperantes drones telecomandados, mísseis guiados por GPS e redes de comunicação tática.

3 *Deepfakes* são vídeos, áudios ou imagens sintéticos gerados por algoritmos de aprendizado profundo (*deep learning*) que simulam, de forma convincente, declarações ou ações de pessoas reais. No contexto da guerra da informação, são empregados para fabricar evidências, disseminar desinformação e minar a confiança pública em líderes políticos e militares.

4 ISR é o acrônimo de *Intelligence, Surveillance and Reconnaissance* (Inteligência, Vigilância e Reconhecimento). Refere-se ao conjunto de sistemas (satélites, drones, sensores terrestres e plataformas aéreas tripuladas) dedicados à coleta, processamento e disseminação de informações sobre o ambiente operacional e as forças adversárias.

ras de comando tradicionais (Jones; Daniels, 2025). Em Gaza, as Forças de Defesa de Israel (IDF, na sigla em inglês) utilizaram sistemas de apoio à decisão com IA, como o sistema Gospel, para processar bilhões de pontos de dados e gerar listas de alvos em velocidade e escala sem precedentes.[5] Isso produziu uma "cegueira seletiva" (Gvaryahu, 2026). É importante distinguir, nesse contexto, dois tipos de sistemas: os sistemas autônomos de armas (AWS), que executam decisões letais diretamente, e os sistemas de apoio à decisão com IA (AI-DSS), como o *Gospel*, que influenciam a decisão sem a executar formalmente. O problema documentado em Gaza não é, portanto, que a máquina decidiu sozinha – é que o processo de validação humana foi comprimido a aprovações de vinte segundos de recomendações algorítmicas, criando o que pesquisadores denominam *automation bias*: a tendência de operadores a confiar mais nos outputs automatizados do que em seu próprio julgamento crítico, especialmente sob pressão de tempo (Blanchard; Bruun, 2025, p. 12). A responsabilidade dilui-se no processo, o erro é naturalizado pela linguagem da probabilidade estatística, e o questionamento é neutralizado pela aparente objetividade da máquina.

A dimensão logística emerge desses conflitos com força renovada. A invasão russa à Ucrânia expôs vulnerabilidades críticas nas bases industriais de defesa tanto dos EUA quanto da Europa, especialmente em termos de preparação para conflito prolongado e produção de munições. Nenhuma das forças estava preparada para a intensidade do consumo, e o apoio a Kiev tensionou as cadeias de produção aliadas de forma sem precedentes desde a Guerra Fria. A lição é direta: a vantagem tecnológica sem capacidade industrial de sustentação torna-se frágil em conflitos de atrito prolongado. Esses conflitos produziram ainda uma inovação institucional relevante: a Ucrânia reduziu drasticamente os prazos de aquisição de sistemas não tripulados, de meses ou anos para semanas,

5 O sistema Gospel (*Habsora*) é uma plataforma avançada de IA desenvolvida por Israel, utilizada para identificar automaticamente alvos militares, aumentando significativamente a velocidade e a escala na geração de alvos.

ao adotar tecnologia comercial de prateleira e criar incentivos para empresas privadas (Jones; Daniels, 2025). Esse modelo contrasta com os processos tradicionais das democracias ocidentais, marcados por regulações que, embora necessárias, frequentemente criam rigidez incompatível com o ritmo de inovação contemporâneo.

No entanto, a tensão central que atravessa todos esses desenvolvimentos é a que existe entre a geração de inovação e sua adoção operacional em escala. O principal desafio contemporâneo não reside na capacidade de inventar, mas na capacidade de integrar. A consolidação de um sistema de defesa modernizado depende não apenas do desenvolvimento de tecnologias emergentes, mas da coordenação entre atores, da criação de mecanismos eficazes de financiamento e aquisição e da capacidade de integrar essas tecnologias em sistemas operacionais complexos (Swartz; Brukardt; Hujsak, 2025).

O caso europeu ilustra esse ponto de forma aguda: apesar de sólida base científica, a Europa enfrenta dificuldades estruturais em converter conhecimento em capacidades militares operacionais. Análises comparativas de dados de patentes revelam que a participação europeia em patentes de alta qualidade é sistematicamente inferior à sua participação em publicações científicas, padrão oposto ao dos Estados Unidos, onde a conversão de pesquisa em produto patenteado é consistentemente superior (Lang et al., 2026). O Fundo de Defesa Europeu (EDF, na sigla em inglês) representa um esforço de correção, mas a fragmentação do mercado europeu de defesa e os diferentes regimes de propriedade intelectual entre os Estados-membros continuam a limitar os resultados (Comissão Europeia, 2025).

Ecossistemas de inovação e a lógica da vantagem estratégica

As evidências dos conflitos contemporâneos e as fragilidades institucionais identificadas na seção anterior convergem para um problema analítico de ordem mais geral: como sustentar a vantagem estratégi-

ca em um ambiente em que a tecnologia é abundante, mas a integração é escassa? A tradição das chamadas *offset strategies*, estratégias de compensação desenvolvidas pelos Estados Unidos desde os anos 1950, oferece um fio condutor histórico para responder a essa pergunta.

O conceito de *offset* refere-se ao esforço de neutralizar vantagens do adversário por meio de uma combinação de conceitos operacionais e tecnologia. A primeira *offset* compensou a superioridade numérica soviética na Europa com arsenais nucleares táticos e forças aerotransportadas de longo alcance. A segunda, desenvolvida a partir dos anos 1970, valeu-se de mísseis de precisão, sensores avançados e redes de inteligência para multiplicar a eficácia de forças menores. A terceira, formulada em meados de 2010 diante da modernização acelerada das Forças Armadas da China, apostou na integração entre sistemas autônomos, inteligência artificial e forças humanas, antecipando o ciclo que a guerra na Ucrânia tornaria empírico. O que essas três gerações têm em comum é a lógica segundo a qual "a tecnologia torna possível a revolução, mas a revolução em si só acontece quando novos conceitos de operação se desenvolvem" (apud Jones; Daniels, 2025, p. 147). Tecnologia sem doutrina é potencial não realizado.

O contraponto histórico mais imediato é o das operações norte-americanas no Afeganistão e no Iraque após 2001. Os Estados Unidos dispunham, nesses conflitos, de superioridade tecnológica absoluta em sensores, comunicações, precisão de armamentos e logística. Ainda assim, foram incapazes de traduzir essa vantagem em vitória estratégica, porque seus adversários adaptaram seus métodos de combate para anular precisamente os trunfos tecnológicos norte-americanos: combatendo entre civis em ambientes urbanos, recorrendo à insurgência e ao terrorismo, e explorando as limitações políticas que restringem o uso da força por democracias. A tecnologia havia avançado; a doutrina, a organização e a compreensão do ambiente estratégico não acompanharam no mesmo ritmo (Borne, 2019). Esse fracasso foi o que tornou politicamente urgente o debate sobre uma nova *offset*, não como substituição, mas como aprendizado.

A proposta de uma nova *offset* , ou quarta geração, emerge precisamente desse diagnóstico, com ênfase na integração entre humanos, máquinas e organizações (Nazil, 2025, p. 1999). Nessa perspectiva, o valor da inteligência artificial não reside na automação de decisões letais (com todos os problemas éticos que o caso de Gaza ilustra), mas na capacidade de ampliar a cognição humana, processar informações em escala incompatível com capacidades biológicas e liberar operadores para julgamentos de ordem superior. Essa tensão entre velocidade algorítmica e julgamento humano é constitutiva do modelo e precisa ser reposicionada como desafio de design organizacional e doutrinário, não apenas técnico (Gvaryahu, 2026). A vantagem sustentável não reside na posse de uma tecnologia singular, mas na capacidade de adaptá-la e integrá-la mais rapidamente do que o adversário: argumento que ecoa diretamente o ciclo ucraniano de seis semanas descrito na seção anterior.

O problema central que essa nova geração de compensação enfrenta é precisamente o da escala: a capacidade de transformar inovação em impacto operacional sustentado. Dados recentes sobre os ecossistemas de defesa ocidentais revelam um padrão preocupante: o investimento público e privado em P&D cresce, mas a transição de tecnologias do laboratório para o campo de batalha permanece lenta e fragmentada. Três gargalos estruturais explicam essa dinâmica: a ausência de mecanismos de financiamento adequados para tecnologias em estágio intermediário de maturação, a falta de demanda estatal coordenada que sinalize prioridades ao setor privado, e a rigidez dos processos de aquisição que impedem a integração ágil de sistemas prontos (Swartz; Brukardt; Hujsak, 2025). O caso europeu é particularmente revelador: apesar de sólida base científica, a participação europeia em patentes de alta qualidade é sistematicamente inferior à sua participação em publicações científicas de ponta, padrão oposto ao dos Estados Unidos, evidenciando que a lacuna não está na geração do conhecimento, mas na sua conversão em capacidade operacional (Lang et al., 2026, p. 8).

Esse diagnóstico tem orientado reposicionamentos estratégicos concretos. A diretiva de janeiro de 2026 do Departamento de Guerra

dos EUA torna explícita a aposta numa força "voltada para IA": a superioridade militar norte-americana dependerá da capacidade de integrar IA como elemento estruturante de todas as capacidades, aproveitando vantagens assimétricas em poder computacional, dinamismo empreendedor e dados operacionais de combate que nenhum outro exército do mundo pode replicar (EUA, 2026). Na ausência de adaptações institucionais consistentes, o risco de obsolescência tecnológica é significativo, e a janela para agir, progressivamente mais estreita (Kadtke; Wells II, 2014). A guerra contemporânea é cada vez menos definida por plataformas isoladas e cada vez mais por ecossistemas integrados de inovação: velocidade de adaptação, capacidade organizacional e integração institucional tornaram-se variáveis tão decisivas quanto a própria tecnologia.

Considerações finais

O percurso analítico desenvolvido neste artigo permite formular três conclusões articuladas. A primeira é histórica: a relação entre guerra e inovação tecnológica obedece a uma lógica de retroalimentação estrutural, em que conflitos aceleram inovações e inovações reconfiguram conflitos. A atual aceleração não rompe com esse padrão: pelo contrário, ela o intensifica, comprimindo os ciclos de aprendizado e ampliando a escala dos efeitos.

A segunda conclusão é institucional: o deslocamento do eixo de inovação do Estado para o mercado privado criou uma lacuna estratégica que as democracias ocidentais ainda não souberam equacionar plenamente. A ambivalência do setor tecnológico privado em relação a aplicações militares, combinada com processos de aquisição pouco ágeis e ecossistemas de defesa fragmentados, produz uma assimetria perigosa: a velocidade de inovação do setor civil supera a capacidade de adoção operacional das forças armadas. Os conflitos na Ucrânia e em Gaza confirmaram essa leitura, mas também demonstraram que o problema não é intratável. A reestruturação do processo de aquisições ucraniano e a integração intensiva de tecnologia comercial de prateleira oferecem um

modelo, ainda que imperfeito, de como democracias podem aumentar sua agilidade institucional sem abrir mão do controle civil sobre o emprego da força.

A terceira conclusão é operacional: a vantagem no campo de batalha do século XXI depende menos da posse de tecnologias avançadas do que da capacidade de integrá-las, adaptá-las e sustentá-las em ritmo superior ao do adversário. Gaza, por sua vez, adicionou uma dimensão normativa incontornável a esse argumento: sem mecanismos adequados de responsabilização, a velocidade que a IA confere às operações militares pode produzir não superioridade estratégica, mas erosão da legitimidade, um custo político que as democracias ocidentais não podem ignorar.

Em última instância, a vitória no século XXI dependerá menos da capacidade de vencer batalhas e mais da habilidade de evitar que elas ocorram por meio da superioridade informacional, da antecipação e da adaptação contínua. Para isso, é preciso que o conhecimento tecnológico e o propósito estratégico voltem a convergir: entre o Vale do Silício e Washington, entre laboratórios e quartéis-generais, entre inovação e doutrina. Reconstituir essa convergência é o desafio político central que as democracias ocidentais enfrentam nesta década. Esse desafio inclui uma dimensão normativa que não pode ser tratada como agenda exclusivamente futura. O debate sobre marcos internacionais para sistemas autônomos letais está em curso e já produziu resultados concretos. O problema não é a ausência de iniciativas, mas a dificuldade de transformá-las em obrigações vinculantes em um ambiente de competição estratégica intensa, no qual os principais atores têm incentivos para preservar sua liberdade de ação.[6]

---

6 Por exemplo, o Grupo de Especialistas Governamentais (GGE) sobre Tecnologias Emergentes na Área de Sistemas de Armas Autônomas Letais (LAWS) vem deliberando ativamente desde 2014; a Cúpula REAIM (Inteligência Artificial Responsável no Domínio Militar) adotou um "Blueprint for Action" em setembro de 2024; e os Estados Unidos emitiram em novembro de 2023 uma Declaração Política sobre o uso responsável de IA militar (BLANCHARD; BRUUN, 2025).

Dimensões relevantes permanecem, mesmo assim, em aberto para pesquisas futuras: o papel de potências não-ocidentais, em particular China, na redefinição dos padrões globais de inovação militar; os efeitos da difusão tecnológica sobre atores não-estatais e países do Sul Global; e a questão de como fazer avançar marcos normativos quando os Estados com maior capacidade tecnológica são também os que mais resistem à regulação.

Referências

ARAYA, Daniel; KING, Meg. The impact of artificial intelligence on military defence and security. **CIGI Papers**, Waterloo, n. 263, mar. 2022. 28 p. Disponível em: https://www.cigionline.org/static/documents/no.263.pdf. Acesso em: abr. 2026.

BLANCHARD, Alexander; BRUUN, Laura. Autonomous weapon systems and AI-enabled decision support systems in military targeting: a comparison and recommended policy responses. Solna: Stockholm International Peace Research Institute (SIPRI), jun. 2025. 34 p. DOI: 10.55163/YQBY3151. Disponível em: https://www.sipri.org/publications/2025/other-publications/autonomous-weapon-systems-and-ai-enabled-decision-support-systems-military-targeting-comparison-and. Acesso em: abr. 2026.

BORNE, Thiago. Tecnologias militares emergentes: digitalização e a Third Offset Strategy estadunidense. **Revista Brasileira de Estudos de Defesa**, v. 6, n. 1, 2019. DOI: 10.26792/rbed.v6n1.2019.75118. Disponível em: https://rbed.abedef.org/rbed/article/view/75118. Acesso em: abr. 2026.

BUJEK, Małgorzata. New rules of the contemporary war. **Security Forum**, Dęblin, n. 2, 2017. DOI: 10.26410/SF_2/17/11. Disponível em: https://wsb.edu.pl/files/pages/634/security_forum_02_2017_11.pdf. Acesso em: abr. 2026.

CLAPP, Sebastian. **Defence and artificial intelligence**. Bruxelas: European Parliamentary Research Service, EPRS Briefing PE 569.580, abr. 2025. 12 p. Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf. Acesso em: abr. 2026.

COMISSÃO EUROPEIA. Directorate-General for Defence Industry and Space. **From AI to quantum:** how the European Defence Fund shapes the future of EU defence technologies. Bruxelas: European Commission, 15 dez. 2025. 4 p. Disponível em: https://defence-industry-space.ec.europa.eu/ai-quantum-how-european-defence-fund-shapes-future-eu-defence-technologies-2025-12-15_en. Acesso em: abr. 2026.

ESTADOS UNIDOS DA AMÉRICA. Department of War. **Artificial Intelligence Strategy for the Department of War:** Accelerating America's Military AI Dominance. Washington, DC: Department of War, 9 jan. 2026. 6 p. Disponível em: https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF. Acesso em: abr. 2026.

GOUSSAC, Netta; BOULANIN, Vincent. **Responsible procurement of military artificial intelligence**. Solna: Stockholm International Peace Research Institute (SIPRI), fev. 2026. 39 p. DOI: 10.55163/YOLG1827. Disponível em: https://www.sipri.org/publications/2026/other-publications/responsible-procurement-military-artificial-intelligence. Acesso em: abr. 2026.

GVARYAHU, Avner. These aren't AI firms, they're defense contractors. We can't let them hide behind their models. **The Guardian**, Londres, 15 mar. 2026. Disponível em: https://www.theguardian.com/us-news/ng-interactive/2026/mar/15/ai-defense-warfare-companies. Acesso em: abr. 2026.

JONES, Seth G.; DANIELS, Seamus P. (eds.). **War and the modern battlefield:** insights from Ukraine and the Middle East. Washington, DC: CSIS; New York: Bloomsbury Academic, set. 2025. ISBN: 979-8-7651-9851-3. Disponível em: https://features.csis.org/war-modern-battlefield/. Acesso em: abr. 2026.

KADTKE, James; WELLS II, Linton. **Policy challenges of accelerating technological change:** security policy and strategy implications of parallel scientific revolutions. Washington, DC: National Defense University, Center for Technology and National Security Policy, set. 2014. 73 p. Disponível em: https://digitalcommons.ndu.edu/defense-tech-papers/3. Acesso em: abr. 2026.

KARP, Alexander C.; ZAMISKA, Nicholas W. **The technological republic**. New York: Crown Currency, 2024. ISBN: 9780593798690.

KING, Anthony. Digital targeting: artificial intelligence, data, and military intelligence. **Journal of Global Security Studies**, Oxford, v. 9, n. 2, 2024, ogae009. DOI: 10.1093/jogss/ogae009. Disponível em: https://academic.oup.com/jogss/article/9/2/ogae009/7667104. Acesso em: abr. 2026.

LANG, Nikolaus et al. The defense technology frontier: how Europe could lead. [S.l.]: Boston Consulting Group (BCG), 9 fev. 2026. Disponível em: https://www.bcg.com/publications/2026/the-new-frontier-of-defense-technology-and-security. Acesso em: abr. 2026.

NAZIL, Ashikur Rahman. AI at war: the next revolution for military and defense. **World Journal of Advanced Research and Reviews**, Lagos, v. 27, n. 1, p. 1998–2004, 2025. DOI: 10.30574/wjarr.2025.27.1.2735. Disponível em: https://wjarr.com/sites/default/files/fulltext_pdf/WJARR-2025-2735.pdf. Acesso em: abr. 2026.

SILICON VALLEY DEFENSE GROUP (SVDG). **NatSec100: top 100 venture capital-backed defense tech startups – 2025 edition**. [S.l.]: Silicon Valley Defense Group; J.P. Morgan, 6 jul. 2025. 40 p. Disponível em: https://static1.squarespace.com/static/6824e488de9281397c0dfb01/t/686b55531ac6cd419b922258/1751864662805/SVDG_2025_NatSec100_20250706.pdf. Acesso em: abr. 2026.

SWARTZ, Dale; BRUKARDT, Ryan; HUJSAK, Karl. **Creating a modernized defense technology frontier**. [S.l.]: McKinsey & Company, 12 fev. 2025. Disponível em: https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/creating-a-modernized-defense-technology-frontier. Acesso em: abr. 2026.

Thiago Borne é doutor em Estudos Estratégicos Internacionais pela Universidade Federal do Rio Grande do Sul (UFRGS). Lecionou em diversas instituições públicas e privadas no campo das Relações Internacionais. Atualmente atua como consultor da Organização das Nações Unidas (ONU) no campo da segurança alimentar e nutricional. As opiniões expressas neste artigo são de responsabilidade exclusiva do autor, não refletindo necessariamente o posicionamento institucional da organização à qual o mesmo está vinculado.

A Convergência NBIC: origem, atualidade e projeção de futuro

Clóvis Eduardo Godoy Ilha
Fábio Netto Pinheiro Grande
Hugo Fernandes Marques Freitas

Resumo

Este artigo analisa a origem, a evolução e as perspectivas futuras da Convergência NBIC – a integração entre nanotecnologia, biotecnologia, tecnologia da informação e ciências cognitivas. Essa convergência inspira-se nos debates das Conferências Macy e na cibernética, podendo ser entendida como um instrumento para potencializar as capacidades humanas físicas, cognitivas e sociais. O tema provoca a divergência entre duas correntes filosóficas: a tecnoética, baseada na responsabilidade ética do avanço tecnológico, e o transumanismo, que defende o aperfeiçoamento contínuo do ser humano por meio da tecnologia. O artigo também compara as estratégias de Estados Unidos, União Europeia, China e Rússia diante da NBIC, destacando sua relevância geopolítica e militar. Por fim, examina aplicações atuais, como interfaces cérebro-computador e terapias avançadas, além de discutir os riscos éticos, psicológicos e estratégicos associados ao chamado "soldado do futuro".

Abstract

This article analyzes the origins, evolution, and future prospects of NBIC Convergence – the integration of nanotechnology, biotechnology, in-

formation technology, and cognitive science. This convergence draws inspiration from the debates at the Macy Conferences and from cybernetics, and can be understood as a tool for enhancing human physical, cognitive, and social capabilities. The topic sparks a divergence between two philosophical currents: technoethics, based on the ethical responsibility of technological advancement, and transhumanism, which advocates for the continuous improvement of human beings through technology. The article also compares the strategies of the United States, the European Union, China, and Russia regarding NBIC, highlighting its geopolitical and military relevance. Finally, it examines current applications, such as brain-computer interfaces and advanced therapies, and discusses the ethical, psychological, and strategic risks associated with the so-called "soldier of the future."

1. Introdução

1.1 Transformações tecnológicas contemporâneas

Vivemos um período de aceleração tecnológica sem precedentes, em que diferentes campos científicos amadurecem simultaneamente e passam a interagir de forma profunda. Quando combinadas, tecnologias que já eram transformadoras isoladamente ampliam mutuamente seu alcance.

É nesse contexto que se insere a Convergência NBIC, cuja origem, atualidade e projeções de futuro serão examinadas neste trabalho. Tratase de um modelo de integração tecnológica orientado ao aprimoramento das capacidades humanas, mas que também expõe uma tensão filosófica fundamental: de um lado, uma visão que busca subordinar o avanço científico a princípios de responsabilidade social e limites éticos; de outro, uma perspectiva que entende a ciência como vetor legítimo, e desejável, de transformação radical do ser humano.

O eixo central deste estudo é demonstrar como essa tensão orienta a forma como as grandes potências incorporam a Convergência NBIC em suas estratégias tecnológicas, condicionando sua busca por superioridade científica, econômica e militar.

1.2 Conceito de convergência tecnológica

A convergência tecnológica ocorre quando diferentes tecnologias passam a operar de forma integrada em uma mesma plataforma funcional. Para que essa integração seja possível, três condições fundamentais devem ser atendidas: (1) compatibilidade de escala física; (2) viabilidade de comunicação, com uma linguagem comum entre os componentes; e (3) viabilidade intelectual, entendida como o domínio dos processos e princípios que regem essa interação (Andler et al., 2008). Um exemplo ilustrativo é o dos biossensores, nos quais a biologia realiza a detecção e a eletrônica processa a informação, combinando dois domínios distintos em um único sistema operacional.

2. Origem do termo NBIC

2.1 A Convergência tecnológica do início do Século XXI

Nas tecnologias convergentes, o avanço em uma área tende a impulsionar o progresso em outras, gerando capacidades mais eficientes, rápidas e com aplicações cada vez mais amplas. No início do século XXI, já se percebia a aproximação entre campos como biologia, física, química, ciência dos materiais e engenharias mecânica e elétrica, todos avançando rumo à manipulação de estruturas na faixa de 1 a 100 nanômetros. Apesar desse movimento comum, cada disciplina parecia desenvolver sua própria forma de "nanotecnologia", ainda sem uma integração efetiva entre si (Spohrer e Engelbart, 2003).

2.2 A nanotecnologia como revolução científica e estratégica

À época, a nanotecnologia era vista como um campo ainda em sua infância, em quel apenas nanoestruturas rudimentares podiam ser produzidas com algum grau de controle. Apesar disso, já se reconhecia nela uma "revolução em curso", com potencial para gerar impactos profundos na economia e na sociedade, comparáveis aos provocados pela tecnologia da informação e pela biologia celular e genética. Esse cenário levou, no início dos anos 2000, à criação da *National*

Nanotechnology Initiative (NNI), concebida para posicionar os Estados Unidos na vanguarda da nanotecnologia e assegurar sua competitividade global e superioridade militar ao longo do século XXI (Estados Unidos, 2000).

O cientista Mihail Roco, então conselheiro sênior da National Science Foundation (NSF), a principal agência de fomento à pesquisa científica básica dos Estados Unidos, foi o arquiteto e a figura central da NNI. Ele compreendia que a nanotecnologia não constituía apenas um novo campo acadêmico, mas uma tecnologia estruturante, capaz de transformar a ciência e a sociedade. Além disso, via na convergência entre nanotecnologia e biotecnologia uma oportunidade singular de expandir as fronteiras da capacidade humana, abrangendo suas dimensões físicas, intelectuais e sociais (Grebenshchikova, 2016).

Em dezembro de 2001, Roco e William Bainbridge, então diretor de programas da NSF, organizaram um seminário dedicado às tecnologias convergentes voltadas ao aprimoramento do desempenho humano. O encontro reuniu dezenas de representantes de agências governamentais, universidades, corporações tecnológicas e setores industriais, consolidando um espaço de diálogo estratégico sobre o futuro da integração tecnológica.

O relatório resultante daquele encontro cunhou o termo "**Convergência NBIC**" e lançou as bases para uma estratégia nacional de pesquisa e desenvolvimento que integrasse a ciência básica à indústria, sob fomento e normatização do governo, com o intuito de aprimorar as capacidades humanas e, consequentemente, promover o crescimento econômico (Roco e Bainbridge, 2002).

2.3 Significado estratégico da sigla NBIC

A sigla NBIC designa a interseção estratégica entre sistemas computacionais avançados e a biologia molecular, aliada à precisão da nanotecnologia e à modelagem das funções cerebrais. A Nanotecnologia fornece a manipulação da matéria; a Biotecnologia permite a aplicação em sistemas vivos; a Tecnologia da Informação oferece o controle e o proces-

samento de dados; e as Ciências Cognitivas fornecem os fundamentos para compreender o funcionamento da mente humana e desenvolver interfaces capazes de interagir diretamente com seus processos.

3. Ligação do NBIC com as Conferências Macy e a cibernética

3.1 O Seminário de 2001 e sua herança intelectual

O Seminário de 2001 foi motivado pela oportunidade criada pelo avanço da nanotecnologia, mas também herdou o caráter multidisciplinar que regeu os debates das "Conferências Macy". Estas foram uma série de reuniões realizadas nas décadas de 1940 e 1950 e cuja gênese remonta à busca de uma solução para um problema eminentemente militar: o desenvolvimento de sistemas de controle para a artilharia antiaérea (Fredrikzon, 2016).

3.2 O problema militar que originou a cibernética

Durante a Segunda Guerra Mundial, os cientistas Norbert Wiener e Julian Bigelow foram encarregados de melhorar a precisão dos canhões antiaéreos contra aviões alemães, que estavam se tornando rápidos e manobráveis demais para os cálculos manuais. O desafio era melhorar a eficácia dos sistemas de interceptação antiaérea, o que exigia prever o comportamento futuro de um sistema complexo composto pelo piloto (homem) e o avião (máquina) (Fredrikzon, 2016).

Naquela mesma época, um evento em Nova Iorque marcaria o início de uma série de encontros científicos que teriam significativo impacto na ciência e, em última análise, encaminhariam a solução daquele problema da artilharia antiaérea.

3.3 O encontro de 1942 e o nascimento do diálogo interdisciplinar

Em maio de 1942, Frank Fremont-Smith, que era diretor da Fundação Josiah Macy Jr, organizou um encontro científico em Nova Iorque, cha-

mado *Cerebral Inhibition Meeting*, dedicado à hipnose e à fisiologia do reflexo condicionado. Foi um evento de caráter interdisciplinar reunindo dois grupos distintos de cientistas, de um lado, matemáticos, médicos, biólogos e engenheiros, e do outro, psicólogos, antropólogos e cientistas sociais (Masaro, 2010).

O encontro de 1942 estabeleceu as bases para uma nova forma de investigar sistemas vivos e artificiais. Essa abertura intelectual seria decisiva para o surgimento da cibernética e, posteriormente, para abordagens contemporâneas que tratam processos biológicos e tecnológicos sob uma lógica comum de informação e controle.

3.4 O artigo de 1943 e o conceito de feedback

Em 1943, Norbert Wiener, Julian Bigelow e o fisiologista Arturo Rosenblueth publicaram o artigo *Behavior, Purpose and Teleology*, no qual propuseram que o comportamento de máquinas e organismos vivos poderia ser compreendido a partir de princípios comuns de finalidade (propósito) e controle.

Nesse enquadramento, o sistema homem-máquina passa a ser concebido como um arranjo dinâmico que requer mecanismos de correção contínua de desvios em relação a um objetivo, o que conduz diretamente à formulação do conceito de *Feedback* (retroalimentação), elemento central da cibernética e fundamento para o desenvolvimento de sistemas capazes de ajustar seu comportamento com base em informações do ambiente (Masaro, 2010).

O artigo de 1943 não apenas ofereceu uma solução teórica para o problema militar da época, mas também inaugurou uma nova forma de pensar a relação entre organismos vivos e máquinas, abrindo caminho para uma intensa atividade intelectual nos anos seguintes e para a consolidação da cibernética como campo interdisciplinar emergente.

3.5 As Conferências Macy e a consolidação da Cibernética

Dando continuidade aos encontros iniciados em 1942, Frank Fremont-Smith organizou, entre 1946 e 1953, uma série de dez reuniões intitula-

das *Feedback Mechanisms and Circular Causal Systems in Biology and the Social Sciences*, posteriormente conhecidas como Conferências Macy. Esses encontros reuniram matemáticos, engenheiros, médicos, psicólogos e cientistas sociais em um ambiente de diálogo interdisciplinar sem precedentes, no qual Norbert Wiener e Julian Bigelow se destacaram como figuras centrais.

Em 1948, Wiener publicou *Cybernetics: Or Control and Communication in the Animal and the Machine*, obra que formalizou o termo "cibernética" e estabeleceu as bases conceituais para um campo dedicado ao estudo dos mecanismos de controle e comunicação em sistemas naturais e artificiais. A partir da sexta reunião, em 1949, o binômio homemmáquina ganhou protagonismo, com debates sobre a substituição de receptores sensoriais por dispositivos protéticos e sobre a possibilidade de integração funcional entre organismos vivos e máquinas.

Nas reuniões subsequentes, temas como aprendizagem, emoções, comunicação humana e funcionamento do sistema nervoso ampliaram o escopo das discussões, mas mantiveram um eixo comum: a busca por princípios unificadores capazes de explicar o comportamento de sistemas complexos. Esse esforço consolidou a cibernética como um campo interdisciplinar emergente e preparou o terreno conceitual para abordagens contemporâneas que tratam processos biológicos e tecnológicos sob uma mesma lógica de controle e informação.

3.6 Legado das Conferências Macy

As Conferências Macy consolidaram a compreensão de que máquinas e organismos vivos podem ser analisados como sistemas regidos por princípios comuns de controle e comunicação. Tal perspectiva encontra ressonância no pressuposto central da Convergência NBIC, segundo o qual áreas como a nanotecnologia e a biotecnologia podem ser compreendidas e manipuladas sob a lógica de sistemas de informação, um conceito de profundas repercussões políticas, tecnológicas e até mesmo filosóficas (Fredrikzon, 2016).

4. Discussões éticas quanto à Convergência NBIC

4.1 NBIC como oportunidade para o melhoramento do corpo humano

A ideia de que a Convergência NBIC oferece oportunidades para aprimorar o desempenho humano remete à concepção do organismo como um sistema composto por partes passíveis de reparo, aprimoramento ou substituição. O aprimoramento físico envolveria o desenvolvimento de novas capacidades sensoriais, bem como na utilização de implantes capazes de ampliar a força humana; o aprimoramento intelectual poderia ocorrer, por exemplo, por meio da integração do cérebro a supercomputadores portáteis; e, adicionalmente, vislumbrava-se a possibilidade de interfaces cérebro-cérebro como forma de aprimoramento social (Yoon e Cho, 2024).

No desenvolvimento dessas ideias, a Convergência NBIC passou a ser interpretada à luz de duas correntes filosóficas com graus distintos de divergência: a tecnoética e o transumanismo.

4.2 A tecnoética

O conceito de tecnoética, formulado pelo filósofo Mario Bunge em 1977, refere-se à responsabilidade moral e social dos agentes envolvidos no progresso tecnológico. Nessa perspectiva, torna-se necessária a construção de uma matriz ética capaz de orientar não apenas a eficiência técnica das inovações, mas também a avaliação crítica de suas implicações sociais e morais (Grebenshchikova, 2016).

Tal abordagem exerceu influência significativa sobre a perspectiva europeia acerca da Convergência NBIC. Em 2004, o relatório *Converging Technologies – Shaping the Future of European Societies* apresentou as conclusões de um grupo de especialistas incumbido de analisar os impactos da convergência tecnológica. Nesse contexto, foi proposta a abordagem denominada CTEKS (*Converging Technologies for the European Knowledge Society*), voltada à integração entre nanotecnologia, biotecnologia, tecnologias da informação e ciências cognitivas, com o objetivo de impulsionar a competitividade e o dinamismo da economia europeia, sem desconside-

rar demandas sociais, valores de diversidade e princípios de justiça, característicos da sociedade europeia (European Commission, 2004).

A concepção de Bunge – segundo a qual o desenvolvimento tecnológico deve ser orientado por critérios éticos capazes de prevenir danos sociais – alinha-se diretamente a essa abordagem europeia, que compreende a convergência tecnológica como um projeto normativo orientado ao bem comum, e não apenas à maximização da eficiência técnica.

4.3 O transumanismo

Em contraste com a tecnoética, destaca-se a perspectiva do Transumanismo, cujas origens remontam à década de 1950 e que foi posteriormente sistematizado, nos anos 1990, pelo filósofo Nick Bostrom. Essa corrente interpreta a Convergência NBIC como um vetor para a superação de limitações biológicas humanas, tais como o envelhecimento e, em última instância, a própria morte.

Sob essa ótica, o corpo humano é concebido como uma plataforma suscetível e, em certa medida, desejável, de otimização tecnológica, por meio de recursos como interfaces cérebro-máquina e engenharia genética. A natureza humana, por sua vez, é entendida como um estágio evolutivo transitório, passível de aperfeiçoamento contínuo mediante intervenções científicas e tecnológicas (Bostrom, 2005).

5. A postura dos principais atores geopolíticos quanto à Convergência NBIC

As posturas dos Estados Unidos, da União Europeia, da China e da Rússia em relação à Convergência NBIC refletem, de modo direto, seus valores e objetivos estratégicos. Nesse contexto, o contraste entre o transumanismo e a tecnoética constitui um eixo interpretativo central para compreender, sobretudo, as posições dos Estados Unidos e da União Europeia.

Nos Estados Unidos, a convergência NBIC é frequentemente associada a uma visão otimista e instrumental da tecnologia, fortemente ali-

nhada aos princípios do transumanismo. Tal perspectiva busca superar as limitações biológicas por meio do aprimoramento de capacidades físicas, cognitivas e emocionais, concebendo o desempenho humano ampliado como um vetor para a obtenção de superioridade econômica e militar (Yoon e Cho, 2024).

Em contraste, a União Europeia, que, no âmbito da convergência NBIC, desenvolve uma vasta gama de tecnologias com um forte foco em aplicações civis e médicas, adota uma abordagem mais cautelosa. Essa postura, ancorada em princípios tecnoéticos, compreende a tecnologia como inseparável de seus impactos sociais e normativos. Assim, privilegia-se a promoção do bem comum e a observância de critérios éticos em detrimento da mera maximização da eficiência técnica. No âmbito institucional, destaca-se ainda a tendência de dissociar o desenvolvimento de tecnologias convergentes de aplicações explicitamente militares (Burt, 2023).

No caso da China, a convergência NBIC é orientada por objetivos estratégicos vinculados ao fortalecimento do poder estatal. Tal orientação materializa-se na Fusão Civil-Militar, que promove a integração entre inovações civis e aplicações militares, em uma lógica pragmática de aceleração tecnológica. Nesse contexto, o melhoramento humano é concebido como instrumento para ampliar a competitividade e a capacidade de dissuasão do país (Global X., 2020).

Por último, a Rússia desenvolveu uma formulação própria, ao incorporar as ciências sociais e humanidades ao acrônimo original, denominando-a NBICS. Essa abordagem enfatiza aplicações militares de alta intensidade, incluindo o desenvolvimento de combatentes com capacidades ampliadas, como a operação de sistemas por meio de sinais neurais e maior resistência a condições extremas. Em comparação com a postura europeia, observa-se menor ênfase em restrições éticas formais, bem como uma maior tolerância ao risco e menor transparência regulatória (Timashev, 2019).

De modo geral, as estratégias desses atores moldam o avanço científico e tecnológico no campo da convergência NBIC, especialmente no que se refere às suas aplicações militares. Nesse cenário, enquanto a

abordagem europeia impõe freios normativos mais robustos e a Rússia enfrenta limitações decorrentes de seu contexto geopolítico recente, os Estados Unidos e a China emergem como os principais protagonistas na disputa pela liderança em áreas estratégicas, notadamente a nanotecnologia e a biotecnologia.

6. Situação atual e importância estratégica da nanotecnologia e da biotecnologia

No prosseguimento da discussão sobre a convergência NBIC, será apresentada uma breve síntese da atual situação da nanotecnologia e da biotecnologia em termos de principais atividades e volume de mercado; bem como uma rápida descrição de sua importância estratégica.

6.1 Nanotecnologia

6.1.1 Situação atual da Nanotecnologia

Atualmente, a nanotecnologia está num momento de transição da experimentação laboratorial para a escala industrial massiva, com o mercado global em forte expansão. Vários fatores contribuem para quadro, com destaque para a crescente adoção de nanodispositivos no setor aeroespacial e de defesa; e a incorporação da nanotecnologia em diagnósticos e outras aplicações na medicina. Por outro lado, o alto custo da infraestrutura de nanomateriais restringe o crescimento de um mercado muito segmentado em diferentes setores como eletrônica, saúde, manufatura, energia, automotivo, aeroespacial e defesa, alimentos e bebidas, dentre outros (Fortune Business Insights, 2024).

O segmento dos nanodispositivos desempenha um papel importante na nanotecnologia, permitindo a manipulação e o controle da matéria em nanoescala. Eles são essenciais para diversas aplicações, incluindo diagnósticos médicos, eletrônica, dispensação de brocas e ciência dos materiais.

A título de ilustração, vale a pena citar um exemplo de nanodispositivo que representa a convergência da nanotecnologia com a biotecno-

logia. Trata-se dos tipos de vacinas utilizadas no contexto da pandemia de Covid-19 cujo funcionamento baseou-se no princípio de que o RNA Mensageiro (mRNA) será traduzido em um antígeno após ser introduzido nas células hospedeiras. Naquelas vacinas, o mRNA é encapsulado em nanopartículas lipídicas, que são estruturas em escala nanométrica (geralmente entre 1 e 100 nanômetros), um procedimento que protege o mRNA e facilita sua entrada nas células (Park, 2021).

6.1.2 Importância estratégica da nanotecnologia.

Os dois maiores atores globais da atualidade, Estados Unidos e China, consideram a nanotecnologia como uma ferramenta indispensável em sua disputa pelo domínio de tecnologias críticas e emergentes. A aplicação militar da nanotecnologia foca na possibilidade de obtenção de materiais leves que suportem altas pressões e temperaturas, adequados para empregos diversos, como em drones ou em sistemas hipersônicos e espaciais. Além disso, a nanotecnologia tem sido utilizada em programas voltados para a defesa química, biológica, radiológica e nuclear (DQBRN), e na indústria de comunicações e eletrônica (Estados Unidos, 2026).

Embora a China já lidere em volume de pesquisas de alto impacto em diversas áreas de nanotecnologia e materiais avançados, há um grande esforço transpor o gargalo da fabricação física. Os chineses buscam reduzir a dependência de tecnologias ocidentais para garantir que sua infraestrutura crítica não seja vulnerável a sanções ou interrupções na cadeia de suprimentos. A disputa entre as potências pelo domínio da manufatura em escalas nanométricas ou menores é determinante na corrida pela vantagem em capacidades de defesa (Gaida, 2023).

6.2 Biotecnologia

6.2.1 Situação atual da biotecnologia

A análise da Biotecnologia pode ser estruturada a partir de dois de seus principais ramos: a biologia sintética e a bioinformática.

6.2.1.1 Biologia sintética

A biologia sintética redesenha sistemas biológicos para produzir funções específicas, valendo-se de engenharia genômica, sequenciamento e edição genética. Abrange áreas como síntese de DNA, engenharia de proteínas e desenvolvimento de sistemas celulares artificiais, alcançando valores expressivos e sendo impulsionado pela inovação tecnológica e pelo lançamento contínuo de novos produtos.

No cenário internacional, destacam-se os Estados Unidos, com sua liderança em medicamentos, diagnósticos e biomanufatura; a China, atuando fortemente em sequenciamento e síntese genética; o Japão, com ênfase em medicina regenerativa e doenças associadas ao envelhecimento; e a Europa, com foco em soluções biológicas sustentáveis (Fortune Business Insights, 2026b).

6.2.1.2 Bioinformática

A Bioinformática consiste no uso de ferramentas computacionais para coletar, processar e interpretar dados biológicos, contribuindo para o estudo de processos fisiológicos e patológicos, bem como para a descoberta de novos fármacos.

Os Estados Unidos lideram esse setor, com significativa participação da aplicação da bioinformática na área da saúde. A Europa se destaca pelos investimentos em pesquisa genômica, enquanto a China amplia sua presença por meio do crescimento no número de ensaios clínicos. No Japão, observa-se ênfase no desenvolvimento de plataformas genômicas baseadas em inteligência artificial, uma tendência global que conduz à medicina personalizada e acelera a descoberta de novos medicamentos (Fortune Business Insights, 2026a).

6.2.2 Importância estratégica da biotecnologia

A biotecnologia também é objeto de intensa competição entre Estados Unidos e China. Um relatório oficial do governo dos Estados Unidos destaca que a integração entre biotecnologia e inteligência artificial tende a repercutir fortemente nos setores de defesa, agricultura e saú-

de, além de alertar para o risco daquele país perder sua liderança global em biotecnologia (National Security Commission on Emerging Biotechnology, 2025).

Outro relatório, dessa vez do Pentágono, reforça a ideia de que a biotecnologia é uma das tecnologias críticas para a segurança nacional, citando aplicações como o desenvolvimento de biopolímeros, que são materiais leves e resistentes de interesse da Defesa, bem como de soluções médicas avançadas. O objetivo central do Departamento de Defesa dos Estados Unidos é acelerar a transição entre pesquisa e a aplicação prática, fortalecendo sua superioridade tecnológica e operacional frente aos demais países do mundo (Estados Unidos. 2023).

Por sua vez, a China inclui a biotecnologia na categoria de Indústria Emergente Estratégica (SEI), considerando-a essencial tanto para a competitividade econômica quanto para a segurança nacional. Essa estratégia integra o esforço de transição para uma economia baseada em inovação de alta tecnologia. A biotecnologia é tratada como tecnologia de uso dual, na qual os avanços em áreas como medicina e biologia sintética podem ser adaptados para aplicações em defesa biológica, assim como para o aumento da resiliência e das capacidades operacionais das forças armadas (Global X, 2020).

As possibilidades de integração e a importância estratégica da nanotecnologia e da biotecnologia reforçam a pertinência de se analisar a situação da Convergência NBIC e suas implicações em termos militares.

7. A situação atual e futura da Convergência NBIC e seu uso militar

7.1 Situação atual

Observa-se, na atualidade, uma integração acelerada das tecnologias associadas à Convergência NBIC, com destaque para algumas aplicações práticas atualmente em fase de consolidação.

7.1.1 Nanotecnologia e microeletrônica

Na interface entre a Nanotecnologia e a tecnologia da informação, a indústria de semicondutores já opera em escalas de 5 nm e 3 nm. Paralelamente, o desenvolvimento de materiais como grafeno, nanomateriais de carbono e componentes eletrônicos flexíveis tem viabilizado a produção de dispositivos vestíveis. Nesse cenário, a China atualmente desponta como o líder global em patentes na área de nanotecnologia (National Center for Nanoscience and Technology, 2025)

7.1.2 Biotecnologia e saúde

A convergência entre nanotecnologia e Biotecnologia amplia a precisão e a eficácia de tratamentos médicos, com destaque para o desenvolvimento de terapias direcionadas, como fármacos antitumorais capazes de atingir alvos específicos com maior seletividade e menor toxicidade sistêmica.

7.1.3 Interfaces cérebro-computador e neurotecnologia

No âmbito da Neurotecnologia, as interfaces cérebro-computador integram biotecnologia, tecnologia da informação e ciências cognitivas, apresentando aplicações tanto médicas quanto militares. No campo clínico, sobressaem programas de restauração sensório-motora, que viabilizam próteses controladas neuralmente e capazes de fornecer feedback sensorial por meio de estimulação direta do córtex cerebral (Perry World House, 2016).

Adicionalmente, tecnologias de aprimoramento cognitivo baseadas nessas interfaces permitem monitorar fadiga, otimizar desempenho e ampliar a capacidade analítica, com aplicações potenciais em atividades como inteligência e tomada de decisão. No âmbito militar, iniciativas como o programa "Soldado Ciborgue 2050" exploram a viabilidade de comunicação bidirecional direta entre cérebro e sistemas autônomos (Burt, 2023).

7.1.4 Digitalização e inteligência artificial

A convergência entre tecnologia da informação e ciências cognitivas, impulsionada pela Inteligência Artificial, tem possibilitado o desenvolvimento de sistemas autônomos capazes de mimetizar processos biológicos e cognitivos, ampliando o grau de automação e adaptabilidade em diversos domínios.

7.2 A Convergência NBIC e o soldado na guerra do futuro

Algumas projeções para o ano de 2050 indicam que os conflitos ocorrerão simultaneamente no ciberespaço e no ambiente físico, com a convergência NBIC integrando ambas as dimensões. Isso explica os esforços atuais e futuros em aperfeiçoar as capacidades humanas nas suas dimensões físicas, sensoriais e cognitivas, por meio de aprimoramentos tecnológicos (Burt, 2023).

Pode-se imaginar inúmeras possibilidades de aplicação da convergência NBIC na fabricação de um "soldado do futuro", um combatente que seria capaz, por exemplo, de controlar de sistemas autônomos por meio de interfaces neurais, dotado de ampla percepção sensorial (como visão em múltiplos espectros), ou provido de sensores subcutâneos e fibras ópticas integradas ao sistema neuromuscular. Certamente, tal soldado teria excepcional eficiência operacional, não sofreria tanto com a fadiga de combate e seria dotado de ampla consciência situacional do campo de batalha, mas, qual seria o preço a ser pago pelo homem debaixo da armadura?

7.3 Desafios e riscos

A incorporação intensiva de tecnologias NBIC em combatentes introduz desafios significativos. A grande dependência de sistemas digitais aumenta a vulnerabilidade a ataques cibernéticos e a pulsos eletromagnéticos. A integração homem-máquina também poderá gerar relevantes impactos psicológicos, incluindo transtornos durante e após o combate, assim como dificuldades na posterior reintegração à vida civil. Tudo isso sem se falar no debate ético de se investir tempo e dinheiro para

fabricar o tal soldado do futuro, num mundo repleto de pessoas descapacitadas sem acesso mesmo a serviços médicos básicos.

8. Conclusão

A Convergência NBIC é mais do que um fenômeno tecnológico, mas um marco civilizacional que redefine a relação entre ciência, sociedade, ética e poder. Desde suas raízes na cibernética e nas Conferências Macy até sua consolidação como estratégia nacional no início do século XXI, a NBIC evoluiu de um projeto intelectual interdisciplinar para um eixo estruturante das capacidades científicas e militares contemporâneas.

A integração entre nanotecnologia, biotecnologia, tecnologia da informação e ciências cognitivas é um instrumento para a manipulação da matéria, da vida e da mente de forma simultânea e interdependente e que gera discussões éticas que transcendem mesmo para a esfera religiosa. Afinal, o homem deve ou não se submeter aos limites impostos por Deus?

A disputa entre modelos normativos, tais como o transumanismo norte-americano, a tecnoética europeia e as abordagens pragmáticas de China e Rússia, evidencia que a convergência NBIC é também um campo de disputa de valores. A capacidade de ampliar o desempenho humano, integrar sistemas biológicos a plataformas digitais e desenvolver aplicações de uso dual exige mecanismos robustos de governança, capazes de equilibrar inovação, segurança e responsabilidade social. O que é mais certo? Limitar o avanço de uma tecnologia com tal capacidade disruptiva em nome de princípios éticos ou atirar primeiro antes que o seu adversário o faça?

À medida que a convergência NBIC avança, especialmente em aplicações militares e de segurança, torna-se essencial reconhecer que seus benefícios vêm acompanhados de vulnerabilidades profundas. A dependência crescente de sistemas digitais, a possibilidade de impactos psicológicos decorrentes da integração homem-máquina e os riscos de

assimetrias tecnológicas entre Estados reforçam a necessidade de reflexão crítica e regulação internacional.

O futuro da convergência NBIC dependerá, em grande medida, da solução de dilemas éticos e civilizatórios, ou seja, seu destino não está tanto no que o cientista realiza no laboratório, mas será o resultado de qual visão predominará no choque de interesses entre os principais centros de poder global.

Referências

ANDLER, Daniel et al. **Converging Technologies and their impact on the Social Sciences and Humanities (CONTECS)**: An analysis of critical issues and a suggestion for a future research agenda: Final Report. Coordenadores: Bernd Beckert; Michael Friedewald. Karlsruhe: Fraunhofer Institute for Systems and Innovation Research, maio 2008. 421 p. Disponível em: http://www.contecs.fraunhofer.de. Acesso em: 17 abr. 2026.

ALVES, Marcos Antonio; VALENTE, Alan Rafael. **O estatuto científico da ciência cognitiva em sua fase inicial:** uma análise a partir da estrutura das revoluções científicas de Thomas Kuhn. Marília: Oficina Universitária; São Paulo: Cultura Acadêmica, 2021. 148 p.

BOSTROM, Nick. **Transhumanist Values**. Oxford: Oxford University, 2005. p. 3-14. (Ethical Issues for the Twenty-First Century). Disponível em: http://www.nickbostrom.com. Acesso em: 3 abr. 2026.

BURT, Peter. **Cyborg dawn?:** the military use of human augmentation for war fighting. Shaftesbury: Drone Wars UK, maio 2023. Disponível em: https://dronewars.net. Acesso em: 8 abr. 2026.

ESTADOS UNIDOS. National Science and Technology Council. Committee on Technology. Subcommittee on Nanoscale Science, Engineering and Technology. National Nanotechnology Initiative: The Initiative and Its Implementation Plan. Washington, D.C.: NSTC, 2000.

ESTADOS UNIDOS. Executive Office of the President. National Nanotechnology Initiative Supplement to the President's 2026 Budget. Washington, DC: National Science and Technology Council, 2026.

ESTADOS UNIDOS. Department of Defense. Department of Defense Biomanufacturing Strategy. Washington, DC: Office of the Under Secretary of Defense for Research and Engineering, 2023. Disponível em: [arquivo anexo]. Acesso em: 17 abr. 2026.

EUROPEAN COMMISSION. **High Level Expert Group "Foresighting the New Technology Wave"**. Converging Technologies – Shaping the Future of European Societies:

Report 2004. Rapporteur: Alfred Nordmann. Brussels: European Commission, 2004. 64 p.

FORTUNE BUSINESS INSIGHTS. **Nanotechnology Market Size, Share & Industry Analysis, By Type (Nanosensors and Nanodevices), By Application (Electronics, Healthcare, Manufacturing, Energy, and Others), and Regional Forecast, 2024-2032**. [S. l.], 2024. Disponível em: https://www.fortunebusinessinsights.com/nanotechnology-market-108466. Acesso em: 23 maio 2024.

FORTUNE BUSINESS INSIGHTS. **Synthetic Biology Market Size, Share, Growth & Forecast, 2034**. [S. l.], mar. 2026. Disponível em: https://www.fortunebusinessinsights.com/synthetic-biology-market-107168. Acesso em: 17 abr. 2026.

FORTUNE BUSINESS INSIGHTS. **Bioinformatics Market Size, Share, Growth & Forecast, 2032**. [S. l.], 2024. Disponível em: https://www.fortunebusinessinsights.com/bioinformatics-market-109493. Acesso em: 17 abr. 2026.

FREDRIKZON, Johan. Review: Cybernetics: The Macy Conferences. **Sensorium Journal**, v. 3, n. 2021, p. 56-59, 2021. Resenha de: PIAS, Claus (ed.). Cybernetics: The Macy Conferences 1946-1953: The Complete Transactions. Zurich: Diaphanes, 2016.

GAIDA, Jamie et al. **ASPI's Critical Technology Tracker:** The global race for future power. Canberra: Australian Strategic Policy Institute, 2023. (Report No. 69/2023). Disponível em: https://www.aspi.org.au/report/critical-technology-tracker. Acesso em: 17 abr. 2026.

GLOBAL X. **China Government Initiatives in Biotechnology.** Hong Kong: Global X by Mirae Asset, 2020. Disponível em https://www.globalxetfs.com.hk/content/files/China_Government_Initiatives_in_Biotechnology.pdf. Acesso em: 17 abr. 2026.

GREBENSHCHIKOVA, Elena. NBIC-Convergence and Technoethics: Common Ethical Perspective. **International Journal of Technoethics**, [s. l.], v. 7, n. 1, p. 77-84, jan./jun. 2016.

MASARO, Leonardo**. Cibernética:** ciência e técnica. 2010. 213 f. Dissertação (Mestrado em Sociologia) – Instituto de Filosofia e Ciências Humanas, Universidade Estadual de Campinas, Campinas, 2010.

NATIONAL CENTER FOR NANOSCIENCE AND TECHNOLOGY (China); NANOTECHNOLOGY INDUSTRY INNOVATION STRATEGIC ALLIANCE. **White Paper:** China Nanotechnology Industry (2025): Global Leadership and Technological Breakthrough Empowered by the tiny, Empowering the industry. Beijing: NCNST, ago. 2025. 862 p.

NATIONAL SECURITY COMMISSION ON EMERGING BIOTECHNOLOGY (NSCEB). **Charting the Future of Biotechnology:** An action plan for American security and prosperity. Washington, D.C.: NSCEB, abr. 2025. Disponível em: [arquivo anexo]. Acesso em: 17 abr. 2026.

PARK, Jung Woo et al. mRNA vaccines for COVID-19: what, why and how. International **Journal of Biological Sciences**, [S. l.], v. 17, n. 6, p. 1446-1460, abr. 2021. Disponível em: https://doi.org/10.7150/ijbs.59233. Acesso em: 16 abr. 2026.

PERRY WORLD HOUSE. **When neuroscience leads to neuroweapons.** Chicago: Bulletin of the Atomic Scientists, out. 2016. Disponível em: https://thebulletin.org/2016/10/when-neuroscience-leads-to-neuroweapons/. Acesso em: 8 abr. 2026.

ROCO, Mihail C.; BAINBRIDGE, William Sims (ed.). **Converging Technologies for Improving Human Performance:** Nanotechnology, Biotechnology, Information Technology and Cognitive Science (NBIC). [S. l.]: National Science Foundation, 2002. 405 p. Disponível em: https://www.wtec.org/ConvergingTechnologies/1/NBIC_report.pdf. Acesso em: 17 abr. 2026.

SANTOS, Dalci Maria dos. **Convergência Tecnológica:** Implicações e Desafios para os Neurocientistas na América Latina. 2012. 133 f. Tese (Doutorado em Ciências) – Escola Paulista de Medicina, Universidade Federal de São Paulo, São Paulo, 2012.

SPOHRER, James C.; ENGELBART, Douglas C. **Converging Technologies for Enhancing Human Performance:** Science and Business Perspectives. [S. l.]: [s. n.], 2003. (Draft).

YOON, Youngsam; CHO, Il-Joo. **A review of human augmentation and individual combat capability:** focusing on MEMS-based neurotechnology. Micro and Nano Systems Letters, [s. l.], v. 12, n. 17, p. 1-9, 2024.

TIMASHEV, S. A. **Infranetics:** The New MAICS-convergent Technology Science. IOP Conference Series: Materials Science and Engineering, [S. l.], v. 481, n. 012023, p. 1-12, 2019. DOI: 10.1088/1757-899X/481/1/012023. Disponível em: https://doi.org/10.1088/1757-899X/481/1/012023. Acesso em: 9 abr. 2026.

Clóvis Eduardo Godoy Ilha é engenheiro-militar e doutor em química pela Universidade de Brasília (UnB). Foi diretor do Arsenal de Guerra General Câmara (AGGC), chefe do Centro de Imagens e Informações Geográficas do Exército (CIGEx) e supervisor do Projeto de Reestruturação do Sistema de Defesa Química, Biológica, Radiológica e Nuclear do Exército Brasileiro (Pjt Retta DQBRNEx). Também foi membro titular da Comissão Técnica Nacional de Biossegurança (CTNBio), foi inspetor de armas químicas na Organização das Nações Unidas (ONU) e atuou no Ministério da Ciência e Tecnologia (MCT), no Centro Gestor e Operacional do Sistema de Proteção da Amazônia (CENSIPAM) e na Indústria de Material Bélico do Brasil (IMBEL). Integra o Grupo IlhaGrande, com campo de atuação focado na cientometria. E-mail clovis.ilha@gmail.com

Fábio Netto Pinheiro Grande é tecnólogo em redes de computadores, com pós-graduação em Big Data e Analytics e é mestrando em Economia pela Fundação Getúlio Vargas (FGV). Trabalha na Caixa Econômica Federal (CEF) como Gerente Executivo na área de Gestão de Relacionamento com o Cliente (CRM), atuando com marketing digital. Também atuou no processo de tratamento de dados de Open Finance e na implantação de modelos IFRS9 e PLDFT na área de risco. No grupo IlhaGrande, exerce a função de engenheiro de dados. Email speedsrj@gmail.com

Hugo Fernandes Marques Freitas é engenheiro Mecânico formado pelo Centro de Universitário do Distrito Federal (UDF), com pós-graduação em Gestão estratégica de Pessoas, e trabalha na Caixa Econômica Federal (CEF). Atualmente como auditor interno trabalha na Célula de Auditoria de Dados e Informações. Foi representante da CEF em três grupos de trabalho junto à Federação Brasileira de Bancos (FEBRABAN): GT Serviços, GT Dados Abertos e GT SandBox, tendo sido o coordenador do GT de Dados Abertos. Integra o Grupo IlhaGrande, onde atua na modelagem, mineração e consolidação de dados. E-mail hugofmfreitas@gmail.com

Economia da defesa e impacto industrial

Eduardo Siqueira Brick

Resumo

A indústria de defesa não pode ser avaliada pelos mesmos critérios aplicados à indústria civil. Sua finalidade última é estratégica – a defesa da soberania e dos interesses nacionais –, e não econômica. Partindo dessa premissa, o artigo examina a relação entre economia, defesa e indústria, alertando para o risco de textos acadêmicos subestimarem a finalidade primordial dos investimentos no setor. Os conflitos recentes na Ucrânia e no Irã evidenciam que capacidade militar pressupõe uma indústria de defesa apta a suprir as Forças Armadas com meios, insumos e serviços essenciais. Nesse quadro, a logística de defesa – compreendida como a atividade destinada a criar e sustentar o emprego de capacidade militar – ocupa posição central na análise. O artigo reconstrói a evolução histórica dessa logística e propõe um arcabouço conceitual para examinar as relações entre defesa, economia, indústria e tecnologia à luz dos conflitos contemporâneos.

Abstract

The defense industry cannot be evaluated using the same criteria applied to the civilian sector. Its ultimate purpose is strategic – the defense of sovereignty and national interests – rather than economic. Based on this premise, this article examines the relationship between the economy, defense, and industry, warning against the risk that academic texts

may underestimate the primary purpose of investments in the sector. Recent conflicts in Ukraine and Iran demonstrate that military capability presupposes a defense industry capable of supplying the Armed Forces with essential resources, inputs, and services. In this context, defense logistics – understood as the activity aimed at creating and sustaining the employment of military capability – occupies a central position in the analysis. The article traces the historical evolution of these logistics and proposes a conceptual framework for examining the relationships between defense, the economy, industry, and technology in light of contemporary conflicts.

1. Introdução

> "*Nonetheless, the purpose of defense expenditure is not economic stimulation, economic growth, or employment (or politics) but must be justified on the basis of the nation's national security needs*"
> (Jacques S. Gansler)

O título deste artigo menciona três entidades, economia, defesa e indústria, e sugere uma interdependência entre elas. Entretanto, é preciso alertar para o principal corolário da frase de Jacques Gansler (2011) no caput desta sessão. Indústrias de defesa não podem ser tratadas da mesma maneira que aquelas voltadas para aplicações civis. Elas têm que ter, no que concerne a investimentos do Estado, o mesmo tratamento dado às Forças Armadas (FFAA). O critério com que devem ser avaliadas é a eficácia dos seus produtos em combate e, não, sua eficiência, ou o lucro, ou geração de empregos, ou arrecadação de impostos, ou geração de divisas. Ou seja, sua finalidade última não é econômica, mas, estratégica, voltada para a defesa da soberania e dos interesses nacionais.

Muito se tem escrito sobre essa ligação. Temas como relação entre defesa e desenvolvimento, defesa e inovação tecnológica, dualidade en-

tre aplicações militares e civis, transbordamento de investimentos em defesa, investimentos em defesa como política industrial, entre outros, têm sido abordados em artigos acadêmicos.

Entretanto, muitas vezes esses textos ignoram a finalidade principal dos investimentos em defesa, como alerta Gansler (2011), ou dão pouca ênfase à relação umbilical que passou a existir entre indústria e defesa a partir da revolução industrial do século XVIII e que, cada vez mais, se acentua com o desenvolvimento tecnológico.

Os recentes conflitos na Ucrânia e no Irã têm demonstrado que não existe capacidade militar sem uma indústria de defesa capaz de suprir as FFAA com meios adequados para se contrapor às ameaças e apoiar o seu emprego, nos ambientes de sua atuação, abastecendo as unidades militares, assim criadas, com os insumos e serviços essenciais tais como, munições, sobressalentes, medicamentos, alimentos, combustíveis, serviços médicos, de manutenção, de armazenamento e de transporte, entre outros. Capacidade industrial em produtos de defesa também é essencial para repor ativos militares, que sofrem perdas elevadas durante os combates.

Pode-se dizer que, do ponto de vista conceitual, sempre foi assim.

Logística de defesa pode ser entendida como a atividade destinada a criar e sustentar o emprego de capacidade militar. Ou seja, prover as unidades militares de combate com os meios necessários, sejam eles recursos humanos, armas, fortificações e meios de transporte e fornecer os insumos (produtos e serviços) para seu emprego. Essa atividade sempre existiu em toda a história dos conflitos humanos. Entretanto, a forma como ela foi desenvolvida ao longo do tempo foi mudando com a evolução das sociedades e formas de governo, com os avanços tecnológicos na arte da guerra e com a própria estrutura da economia como um todo.

Dessa forma, para melhor analisar o impacto industrial da economia de defesa, é importante, não só usar um arcabouço teórico com aderência à realidade, mas, também, conhecer como a logística de defesa evoluiu ao longo do tempo.

Na sessão 2 será apresentado um resumo da evolução da logística de defesa no ocidente e oriente próximo.

A sessão 3 introduz o arcabouço conceitual usado para fundamentar análises relacionadas à logística de defesa e descreve algumas relações que existem entre defesa, economia, indústria e tecnologia.

A sessão 4 apresenta alguns ensinamentos que os conflitos recentes oferecem.

2. Um breve retrospecto histórico da logística de defesa

"*Igitur qui desiderat pacem, praeparet bellum.*"
(Públio Flávio Vegécio Renato)

Segundo Eccles (1965), as decisões militares de alto nível exigem uma mistura dinâmica de:

a) Estratégia, que procura traçar um caminho exequível entre objetivos políticos e meios;
b) Tática, que diz respeito ao uso de meios em combate; e
c) Logística (de defesa) que é responsável pelo preparo e apoio ao emprego de capacidade militar em combate.

Em tempos de paz, estratégia e logística preponderam. Em tempos de guerra, todos os três componentes devem atuar sinergicamente.

Durante alguns milhares de anos, até a revolução industrial em meados do século XVII, que introduziu e generalizou o uso da máquina a vapor, a maneira como a logística de defesa foi executada sofreu poucas alterações. Nesse período, as inovações foram causadas, principalmente, por demografia e por organização e capacidade econômica do Estado. É importante ressaltar que existem quatro tipos de inovação, também aplicáveis na defesa: de produtos (armas), de processos (táticas), de marketing e organizacional.

A primeira grande inovação é creditada aos assírios, que teriam sido os primeiros a organizar exércitos permanentes. Portanto, uma inovação organizacional. Além de maior eficácia em combate, isso lhes permitiu realizar campanhas que não fossem limitadas pelos períodos de plantio e colheita dos alimentos. Sítios de cidades e fortalezas, por exemplo, podiam se prolongar pelo tempo necessário a que os defensores exaurissem seus recursos e se vissem obrigados à rendição. Isso só foi possível porque o Estado conseguiu acumular recursos para adotar esse tipo de organização e a demografia permitiu.

As inovações seguintes podem ser creditadas aos romanos. Inicialmente, o sistema de recrutamento de legionários entre os povos subjugados da península itálica, permitiu que, mesmo após desastres militares contundentes, como os sofridos frente aos cartagineses na segunda guerra púnica, fosse possível uma rápida recuperação da capacidade militar, recompondo as legiões perdidas. Sistema semelhante só foi utilizado quase dois mil anos após, quando Napoleão Bonaparte implantou a conscrição obrigatória, gerando o mesmo efeito. Resiliência para recriar capacidade de combate, mesmo após grandes perdas.

A segunda grande inovação romana ocorreu na reforma feita por Gaius Marius no século II AC. Basicamente, a transformação do serviço militar temporário em permanente e a expansão do universo de classes sociais que poderiam fornecer recrutas para as legiões, com o concomitante fornecimento, pelo Estado, de todos os equipamentos que os combatentes necessitavam: espadas, uniformes, armaduras, capacetes, lanças, escudos, cavalos etc. Anteriormente, somente cidadãos com recursos próprios podiam compor as legiões, porque eram os únicos capazes de custear seus próprios armamentos. A reforma permitiu a profissionalização do exército romano, maiores efetivos, padronização do armamento e adoção de novas formações e táticas para combate. Aumentou, dessa forma, a eficácia das legiões em combate e a resiliência de Roma face a desastres em batalhas. Novamente, demografia e a possibilidade de acumular recursos por parte do Estado viabilizaram essas inovações organizacionais e de processo.

A principal característica desse período é que quase toda a logística de defesa de Roma era de responsabilidade das legiões. Desde a fabricação de armas, meios de transporte, inclusive navios, fortificações, quartéis e, até mesmo, a construção de estradas e pontes. Ou seja, a própria infraestrutura de transporte que o império construiu, fator importante na sua economia, teve participação direta das legiões. Essas eram praticamente autônomas, vivendo, sempre que possível, dos recursos que podiam encontrar nas regiões onde operavam, sem necessidade de longas rotas de reabastecimento. A campanha de Júlio Cesar na Gália (58 a 50 AC) ilustra bem essa realidade.

Após a queda de Roma, da idade média, até o início do século XVI, essa estrutura desapareceu. Sem um governo central, controlando vastos territórios e populações, diminuiu a capacidade dos governantes extraírem recursos da sociedade para custear armas e realizar o recrutamento em larga escala. O paradigma mais comum passou a ser o uso de mercenários, ou tropas fornecidas por senhores feudais. Esse fato não permitiu a sustentação de grandes exércitos, como foi possível para os grandes impérios da antiguidade.

Duas inovações de produto permitiram o ressurgimento de grandes impérios europeus, do início do século XVI a meados do século XX, agora em escala global. O uso da pólvora em armas de fogo e o advento dos navios para longas navegações oceânicas. Com base nesses ativos, inicialmente Portugal e Espanha, logo seguidos por Inglaterra, Holanda, França e, posteriormente, Alemanha, Itália e Bélgica, conseguiram conquistar vastos territórios nas américas, África e em todo o oriente. O descompasso proporcionado por esses meios substituiu a necessidade de usar grandes efetivos. Mesmo considerando a influência de outros fatores muito relevantes, como a ocorrência de pandemias trazidas pelos europeus ao novo mundo, que dizimaram populações e desestruturaram os governos centrais que existiam nas américas (astecas e incas), chega a ser inacreditável que apenas algumas centenas de espanhóis foram suficientes para conquistar impérios estabelecidos que controlavam milhões de pessoas e possuíam exércitos com muitas dezenas de milhares de guerreiros.

Vastas riquezas extraídas desses territórios, incialmente na forma de ouro, prata, pedras preciosas, madeiras, especiarias, matérias primas diversas e, posteriormente, grandes plantações, retroalimentaram esse poder inicial adquirido. Foi a época de ouro das potências europeias. Nesse interim, meados do século XVII, ocorreu a revolução industrial. Esta, criou uma nova realidade e aumentou o fosso econômico e militar entre as potências europeias e o resto do mundo.

A revolução industrial e tecnológica ao longo dos séculos XVIII e XIX, teve três impactos importantes na guerra em geral e na logística de defesa em particular. Em primeiro lugar, inovações de produto, tais como armas mais letais (metralhadoras e canhões mais precisos e de maior alcance), a propulsão a vapor para navios, tornando-os independentes das condições de vento e a construção de ferrovias. Essas duas últimas, possibilitaram a movimentação rápida de grandes quantidades de homens e materiais em longas distâncias, com grande impacto nas operações militares e no abastecimento. O segundo impacto foi a padronização e a produção em massa de armas e munições. O terceiro impacto foi a inserção de empresas privadas nos esforços de guerra. Armas e munições, antes de responsabilidade exclusiva de órgãos estatais, passaram também a ser fornecidas por empresas privadas. Esses fatores levaram ao que se chamou de paradigma da guerra industrial, pelo efeito de massificação, tanto das mortes em combate, quanto da produção de armas e munições. A mobilização de todos os recursos do país para o esforço de guerra, passou a ser necessária. Esta foi possível porque os produtos de defesa ainda eram razoavelmente simples tecnologicamente e usados em grandes quantidades, o que facilitou a adaptação do parque manufatureiro para o esforço de guerra. Quem melhor conceituou essa nova realidade foi Thorpes (1917).

Duas consequências inevitáveis dessas mudanças foram a inclusão dos ativos industriais e de transporte dos contendores como alvos de ações militares e a necessidade de aumentar exponencialmente os efetivos das forças combatentes. O abastecimento dessas forças nos teatros de operações exigia uma enorme estrutura de logística de transporte (ferrovias, rodovias, rotas marítimas e fluviais).

Na segunda guerra mundial, o ápice desse paradigma para conflitos, esses efetivos se contavam na faixa de milhões e, não apenas de algumas dezenas ou centenas de milhares. Além disso, toda a economia dos adversários e até mesmo suas cidades, passaram a ser considerados alvos legítimos, porque faziam parte da logística de defesa.

Inovações de produto importantes também ocorreram no fim desse período. O surgimento da aviação, dos submarinos, dos meios de comunicação e de sensoreamento, dos carros de combate e dos foguetes.

A destacar, nesse período, é a adoção de organizações de alto nível na administração pública (ministérios), independentes das FFAA, para cuidar da logística de defesa, tratando diretamente com a indústria. Os ministérios do Armamento na França (Primeira Grande Guerra) e Alemanha (Segunda Grande Guerra) ilustram essa inovação organizacional na logística de defesa.

O fator nuclear, inovação de produto disruptiva, mudou tudo isso. Inviabilizou a guerra industrial entre potências nucleares, porque, se a mesma lógica usada até então fosse empregada, acarretaria a destruição mútua.

Teve início, então, o período da chamada Guerra Fria entre duas grandes potências nucleares: os Estados Unidos da América (EUA) e a União das Repúblicas Socialistas Soviéticas (URSS). Como não podiam se enfrentar diretamente, ambas se envolveram em inúmeros conflitos por procuração, ou apoiaram lados distintos em conflitos outros. Destacam-se as inúmeras guerras entre Israel e países árabes e as guerras de libertação que ocorreram em diversas colônias europeias e que levaram, finalmente, à independência de quase todas essas colônias. Os países industrializados se beneficiaram dessa demanda por armas, pois isso representou um reforço não desprezível para ajudar a sustentar suas indústrias de defesa, durante o período em que não estiveram envolvidos diretamente em conflitos com potências de mesmo porte.

A forma como a logística de defesa foi conduzida nesse período sofreu mudanças muito significativas. A base dessas inovações foi o re-

conhecimento da necessidade de elevados investimentos estatais para viabilizar o domínio de tecnologias críticas, em especial para defesa. O texto de Vannevar Bush para o presidente Truman em 1945 (*Science, The Endless Frontier*) representa um divisor de águas nesse aspecto. Recomendava que o governo deveria financiar, de forma permanente, a pesquisa científica, mesmo em tempos de paz. Propôs a criação de um sistema colaborativo entre universidade, governo e indústria, gerando o que ficou conhecido como complexo científico-tecnológico, ou complexo militar-industrial. Nesse modelo a universidade faria pesquisa básica e formação de recursos humanos, a indústria se encarregaria de desenvolvimentos e o governo atuaria como motor, gerando a demanda e financiando os investimentos, quase sempre a fundo perdido. Posteriormente, com o trabalho de Etzkowitz e Leydesdorff (1995), o modelo da hélice tríplice ampliou as funções desses três entes. A universidade passou também a criar incubadoras e empresas, a indústria se envolveu com pesquisa básica de alto nível e o governo assumiu o papel de capitalista de risco. Nos EUA esse complexo científico-industrial operou de forma descentralizada, de modo a incentivar competição e inovação, mas sob forte indução por parte do Departamento de Defesa (DoD). A França adotou uma estrutura mais centralizada, criando, em 1961, um órgão executivo, independente das FFAA, para cuidar da aquisição de produtos de defesa e da pesquisa e desenvolvimento de tecnologias e produtos de defesa: a *Délegation Ministérielle pour l'Armement* (DMA), atualmente *Direction Générale de l'Armement* (DGA) subordinada diretamente ao Ministro da Defesa. A evolução da logística de defesa da França no século XX está bem documentada por Giovachini (2000). Recentemente, quase todos os países com significativa capacidade militar adotaram modelos semelhantes ao francês. Alguns exemplos de organizações independentes das FFAA para cuidar de aquisições e desenvolvimentos são SSB (*Presidency of Defense Industries*), Turquia, DE&S (*Defence Equipment and Support*), Reino Unido, FMV (*Defence Materiel Administration*), Suécia, DPP (*Directory for Procurement and Production*), Israel, AIN (*Equipment, Information Technology and*

in Service Support Directorate), Alemanha, ARMSCOR (*Armaments Corporation of South Africa*), Africa do Sul e DPP (*Department for Defence* Production), Índia.

Os resultados práticos dessa visão, de atribuir ao Estado a responsabilidade para investimentos em CT&I para defesa, podem ser vistos no percentual dos gastos com P&D feitos pelos governos de vários países, que foram gerenciados pelo setor de defesa. Segundo Mowery (2012), no período de 1980 a 2010 esses valores, para Estados Unidos, Reino Unido, França e Suécia, chegaram, respectivamente a 70%, 49%, 40% e 28%. Os avanços tecnológicos proporcionados por esses investimentos foram substanciais. Satélites, armas nucleares diversas, mísseis balísticos e guiados contra todos os tipos de alvos, aeronaves cada vez mais sofisticadas, submarinos e navios com propulsão nuclear, entre outras. Este avanço aumentou o fosso de capacidade militar entre países mais desenvolvidos e os demais.

Esse período foi caracterizado, também, por ações dos EUA e países alinhados para impedir que outros, fora desse entorno, obtivessem tecnologias críticas para uso militar. O problema é que o critério adotado para definir o que deveria, ou não, ser controlado, muitas vezes foi abrangente demais. Na prática, essas ações tiveram o efeito de dificultar, ou mesmo impedir, que muitos países conseguissem desenvolver bases industriais de defesa próprias. O fenômeno, conhecido por cerceamento tecnológico, teve grande impacto negativo no desenvolvimento e sustentação de uma base industrial em dezenas de países em fase de desenvolvimento. A justificativa inicial foi a de evitar que essas tecnologias caíssem nas mãos do adversário do bloco ocidental na Guerra Fria, mas essas ações não se encerraram com a dissolução da USSR, que ocorreu formalmente em 26 de dezembro de 1991, fruto de um processo de decadência que durou alguns anos, e que marcou o fim desse período da história.

A queda da USSR deu início a um novo período na história dos conflitos, com amplas repercussões na logística de defesa. O fim da história, como preconizou Fukuyama, com um domínio incontestável da

potência vencedora e a predominância final da democracia liberal, nos moldes ocidentais, reduziria a probabilidade de conflitos e a necessidade de grandes investimentos em defesa. Paralelamente, no campo econômico, o chamado Consenso de Washington, formulado no final da década de 1980, majoritariamente por economistas ligados ao Fundo Monetário Internacional (FMI), Banco Mundial e Departamento do Tesouro dos EUA, preconizava que fosse adotada uma agenda liberal, envolvendo, entre outros, abertura comercial e para investimentos estrangeiros, desregulamentação, privatizações e redução de gastos públicos. As forças do mercado passariam a comandar o desenvolvimento com pouca, ou nenhuma, intervenção estatal, inclusive em setores estratégicos para a defesa. As consequências para a logística de defesa foram enormes. De uma maneira geral, a redução dos orçamentos, obrigou à reformulação de todo o setor industrial de defesa, com fusões, aquisições e falências, reduzindo significativamente a quantidade de empresas e gerando alta concentração no setor. Em 1993, no evento que passou a ser conhecido como *the last supper*, o Secretário de Defesa americano, Les Aspin, informou aos executivos (CEO) das grandes empresas de defesa que os investimentos seriam reduzidos drasticamente e que o governo não iria sustentar as empresas, recomendando que essas buscassem fundir suas operações. Nesse período, ocorreu ampla desnacionalização de empresas, antes protegidas pelo Estado. A globalização da economia, levou a que cadeias de suprimento de componentes críticos, migrassem para o exterior. Praticamente, em muitos países, o único critério para definir a origem dos insumos, se externa ou interna, passou a ser o econômico. A geopolítica e segurança nacional ficaram em segundo plano. Evidentemente, os impactos dessas mudanças não foram uniformes em todos os países. No oriente, muitos países, como a China, mantiveram suas políticas de planejamento central da economia e pesados investimentos do Estado em indústrias, tecnologia e infraestrutura de transporte, energia e comunicações. No ocidente, nos países em desenvolvimento, que aderiram a essa agenda liberal, o impacto negativo sobre o setor industrial e o crescimen-

to econômico foi muito grande. O caso do Brasil é emblemático. O país foi um dos que mais se desenvolveram no período de 1930-80, com crescimento anual médio do produto interno bruto (PIB) na faixa de 7%, com forte intervenção do Estado, industrialização acelerada e grandes investimentos em infraestrutura. De 1980 até 2025, com a mudança do modelo, que passou a seguir a agenda liberal do Consenso de Washington a partir dos anos 90, o crescimento médio foi da ordem de 2%, com grandes oscilações. Um exemplo marcante dessa influência foi a Emenda Constitucional número 6, de 1995, que revogou o Artigo 171 da Constituição Federal. Este artigo permitia ao Estado, entre outras coisas, dar tratamento preferencial a empresas genuinamente nacionais para aquisição de bens e serviços pelo Poder Público e conceder proteção e benefícios especiais temporários para desenvolver atividades consideradas estratégicas para a defesa nacional ou imprescindíveis ao desenvolvimento do País.

Na prática, essa mudança impediu que o Estado brasileiro financiasse o desenvolvimento de tecnologias e produtos de defesa e atuasse para sustentar suas empresas estratégicas, em direção oposta ao que preconizava o modelo sugerido por Vannevar Bush e adotado pelos EUA e muitos outros países.

O impacto negativo dessa nova política no desenvolvimento industrial do país foi significativo. Segundo dados da Federação das Indústrias do Estado de São Paulo (FIESP) o percentual do PIB industrial do Brasil em relação ao PIB total, cresceu de 11,9 a 21,6% no período de 1947 a 1985, regredindo para apenas 11,4% em 2015. Em 1980 o PIB industrial do Brasil era cerca de 117,3% da soma dos PIBs industriais de China, Coreia do Sul, Malásia e Tailândia. Em 2010 esse percentual caiu para 10 %. Ou seja, o Brasil, além de baixo crescimento da economia, sofreu um acelerado processo de desindustrialização nesse período. A indústria de defesa brasileira, que havia se desenvolvido muito no período anterior, produzindo navios, carros de combate, aeronaves, munições, artilharia, foguetes, misseis, radares e equipamentos de comunicações e guerra ele-

trônica, chegando a ser um importante país exportador de produtos de defesa, acabou encolhendo e perdendo muito de sua capacidade, sem que o Estado agisse para sustentá-la, já que os instrumentos constitucionais pertinentes foram revogados. Essa postura do Estado brasileiro persiste até os dias de hoje. Atualmente, o que restou dessa capacidade depende muito de exportações e é quase que totalmente dependente de tecnologias, materiais e componentes críticos importados.

Apesar das expectativas geradas pelo fim da guerra fria, os conflitos não terminaram, mas adquiriram novas características. Tornaram-se comuns o que se convencionou chamar de guerras assimétricas, entre países com capacidades militares muito desequilibradas. O avanço tecnológico também não parou. Sistemas de monitoramento global do planeta e de navegação a partir do espaço, armas de longo alcance e grande precisão, veículos não tripulados (VNT), aeronaves e navios furtivos, inteligência artificial, sistemas de defesa aérea cada vez mais eficazes, capacidade de monitoramento e interferência em redes de comunicações e de computadores, entre outros. Essas evoluções transformaram a natureza da guerra e da própria base logística de defesa. O fato de muitos produtos e sistemas de defesa terem se tornado muito complexos e caros, inviabiliza a possibilidade de mobilização nos moldes da que foi feita na segunda guerra mundial. Para muitos produtos, é necessária uma prontidão industrial desde os tempos de paz, com capacidade de aumento de escala produtiva em curto espaço de tempo. Por outro lado, muitas inovações, como é o caso de VNT, podem ser mais simples e baratas, permitindo o rápido aumento de sua produção via mobilização.

Finalizando este resumo, como já foi ressaltado na introdução, os recentes conflitos na Ucrânia e Irã, mostraram que sem uma capacidade de logística de defesa própria, não é possível ter capacidade militar efetiva. Por esse motivo, assiste-se a um movimento internacional de retorno à busca de autonomia em logística de defesa, amparado por aumentos expressivos nos orçamentos de defesa.

3. Um arcabouço conceitual para logística de defesa

> "Sem um consenso sobre conceitos fundamentais, são remotas as possibilidades de se criar a harmonia de pensamento e de ação, que é essencial para se prover segurança nacional em um mundo confuso" (Henry E. Eccles).

Os conceitos apresentados nesta sessão, de forma resumida, foram desenvolvidos em inúmeros trabalhos anteriores do autor, em especial Brick (2016, 2019, 2022 e 2022a).

Defesa comporta duas macros atividades: emprego e preparo de capacidade militar. Emprego (de capacidade militar) é atividade executada em períodos de conflito ou catástrofes que atinjam a população. Preparo (de capacidade militar) é atividade executada ininterruptamente, tanto em períodos de paz como de guerra. Como já visto nas sessões 1 e 2, logística de defesa é essencial tanto para o preparo, quanto para o emprego.

Capacidade militar só pode ser valorada em termos de proficiência efetiva em combate nas contingências possíveis que o país possa vir a ter que enfrentar. Essas, podem ser caracterizadas, de uma forma muito simplificada, como uma combinação de tarefas (tipos de emprego tático de unidades militares), ameaças (as unidades militares dos inimigos) e cenários (geografia; condições climáticas; ambiente urbano ou rural; existência, ou não. de aliados com que se possa contar; etc.). O acrônimo TAC (tarefa/ameaça/cenário) serve para identificar cada uma das situações em que a capacidade militar poderá ser usada.

É importante ressaltar que o resultado do emprego de capacidade militar só pode ser valorado no contexto maior representado pela TAC, e associado aos objetivos políticos e estratégicos que se tenha no conflito. A recente guerra dos EUA e Israel contra o Irã oferece um bom exemplo. A capacidade militar iraniana é muito inferior à de seus adversários. Entretanto, a capacidade de retaliação, proporcionada pelos sistemas de

mísseis e drones guiados que o Irã desenvolveu, e é capaz de produzir em grandes quantidades, associada à geografia do país, mostrou-se bastante efetiva nesse cenário.

Capacidade militar tem dois componentes essenciais: a capacidade operacional de combate (ou capacidade militar propriamente dita) e a capacidade de logística de defesa.

Esses dois componentes de capacidade militar devem trabalhar sinergicamente para que esta possa apresentar proficiência em combate. Isto porque a capacidade operacional de combate de uma unidade militar depende de muitos fatores que podem ser resumidos em quatro grandes categorias:

a) Estrutura das unidades – efetivo, treinamento, liderança, organização, informação, interoperabilidade.
b) Modernidade - grau de sofisticação e atualização do agregado tecnológico (sistemas de armas, equipamentos, instalações) e, também, doutrina e tática, todos adequados às ameaças possíveis.
c) Prontidão – o fato de a unidade estar pronta para cumprir a missão para a qual foi projetada. Ou seja, ter os seus meios materiais e humanos disponíveis para pronto emprego (aprestada).
d) Sustentabilidade - a capacidade de manter o nível de prontidão durante a atividade operacional.

Modernidade e sustentabilidade dependem diretamente da capacidade de logística de defesa. Para ter essa capacidade o país deve desenvolver e sustentar unidades fabris (indústrias) e institutos de ciência, tecnologia e inovação (ICT) específicos para defesa, conhecidos, no seu conjunto, como Base Industrial de Defesa (BID).

O desenvolvimento e sustentação de uma parte dessa BID, que deve ser considerada estratégica para o país, também é uma atividade importante da logística de defesa. Este aspecto será abordado com maiores detalhes mais adiante, ao se propor uma taxonomia para logística de defesa.

É importante destacar que a logística de defesa tem dois lados: um lado da oferta, representado pela BID e um lado da demanda, normalmente representado por uma organização do Estado, responsável pelas atividades de inovação, pesquisa e desenvolvimento (P&D) e aquisição de produtos de defesa e pela gestão de políticas industriais e de ciência, tecnologia e inovação (CT&I) específicas para defesa. Esse conjunto, envolvendo oferta e demanda, constitui um sistema único que deve trabalhar de forma sinergética e integrada, visando ao desenvolvimento e sustentação da capacidade militar. É por esse motivo que um termo mais adequado para ser usado no lugar de BID é Base Logística de Defesa (BLD), que inclui tanto o lado da demanda quanto o da oferta.

Existem três tipos distintos, mas interdependentes, de logística de defesa. Duas voltadas diretamente para a construção e emprego de capacidade operacional de combate (FFAA) e uma voltada para o desenvolvimento e sustentação da capacidade de logística de defesa (BLD), principalmente aquela que é considerada estratégica para o país:

a) Logística de Operações (do consumidor, ou "pequena" logística): cuida do apoio direto às operações; também é conhecida como logística militar nas FFAA.
b) Logística de Aparelhamento das FFAA (do produtor, "grande" logística, ou economia de defesa): cuida da criação da capacidade operacional de combate das unidades militares das FFAA; envolve as estratégicas atividades de aquisição de produtos de defesa e inovação tecnológica, fundamentais para o terceiro tipo de logística de defesa.
c) Logística de Aparelhamento e Sustentação da BLD (da política industrial e tecnológica para defesa): cuida do desenvolvimento e da sustentação da capacidade de logística de defesa. Ou seja, da BID, principalmente de sua parte considerada estratégica e da própria BLD como um todo, porque também tem que cuidar do preparo das organizações que gerenciam a demanda. A atenção que os EUA dedicam ao preparo de sua Acquisition Work Force (cerca de 154.000

profissionais de logística de defesa, a maioria civis) é emblemático a esse respeito.

Para que um país possa empregar capacidade militar ele tem que, previamente, preparar (construir e sustentar) esses dois Instrumentos da Defesa

Existem três questões básicas de cujas respostas depende todo o processo de planejamento da defesa:

a. preparar para quais **possíveis contingências futuras** (ameaças e cenários)?
b. qual a **capacidade militar** necessária para enfrentar essas contingências?
c. como desenvolver e sustentar os **instrumentos da defesa** que proverão a capacidade militar necessária?

A resposta à primeira questão, que diz respeito a uma definição de "o que" constitui o problema da defesa, depende muito de uma Grande Estratégia, que defina objetivos nacionais e a posição e o papel que o país deseja ocupar no sistema internacional em algum momento no futuro e, também, em certa medida, de uma avaliação de cenário, que aponte possíveis obstáculos e opositores a essas pretensões.

A definição da capacidade militar necessária é uma atividade bem mais complexa. Ela envolve o desenvolvimento dos dois Instrumentos de Defesa que irão prover os componentes dessa capacidade militar: operacional de combate (FFAA) e de logística de defesa (BLD). No caso de capacidade operacional de combate, quais unidades militares deverão ser construídas e sustentadas. No caso de capacidade de logística de defesa, quais indústrias estratégicas de defesa (EED), institutos de ciência e tecnologia (ICT) e tecnologias e produtos de defesa. Ela depende de considerações sobre a capacidade militar de possíveis ameaças, da geografia, da capacidade econômica, industrial e tecnológica própria, de possíveis alianças e fontes de suprimento, entre outros fatores.

A terceira questão diz respeito às soluções de compromisso entre alocações de orçamento para desenvolver e sustentar os Instrumentos de Defesa. Em períodos de paz, a prioridade deve ser para desenvolver e sustentar a capacidade de logística de defesa. Isto porque essa é muito mais difícil e demorada para construir e, em períodos de paz, as restrições orçamentárias para defesa são normalmente muito grandes, pois existe a competição para atender a outras necessidades mais prementes. Já em períodos de conflito, a prioridade deve ser para a capacidade operacional de combate, usando todos os meios possíveis, inclusive recorrendo a importações de armas e munições. A vantagem aqui é que as restrições orçamentárias praticamente inexistem.

Uma questão frequentemente abordada é a existência de impacto direto do gasto com defesa no desenvolvimento econômico. Defensores de maiores gastos argumentam que esses impactos são positivos, enquanto outros discordam. Desde os trabalhos pioneiros de Benoit (1973, 1978), muitos autores procuraram responder a essa questão, entre eles Brumm (1997), Dunne et al. (2005), Alptekin & Levine (2012) e Chen et al. (2014). Até o presente momento não existe uma resposta que seja universalmente aplicável. Smith (2009), afirma que efeitos macroeconômicos só existem quando os orçamentos de defesa superam 5% do PIB.

Por outro lado, existem muitas evidências de que impactos indiretos existem e são muito relevantes. Esses impactos derivam da dualidade de algumas tecnologias e produtos de defesa e, também, da capacidade industrial que lhes deram origem. Podemos incluí-los em duas categorias: geração de novos setores industriais para explorar novas tecnologias e produtos e aprimoramento e utilização de capacidade industrial, originalmente criada para atender à defesa, para gerar produtos de uso civil.

Exemplos do primeiro caso são a internet, motores aeronáuticos a reação, radar, sistemas de posicionamento global, satélites e foguetes. Os impactos do transbordamento dessas tecnologias para uso civil dispensam maiores explicações, pois elas estão presentes no dia a dia das pessoas e geraram uma nova economia. Não é exagerado dizer que a economia moderna é altamente baseada e dependente dessas tecnologias.

O outo tipo de impacto, no aprimoramento e fortalecimento da capacidade industrial e sua utilização dual, embora não tão impactante quanto o primeiro, não é desprezível. Capacidade industrial deve ser entendida como uma combinação de instalações, tecnologia (saber fazer), bens de capital e recursos humanos. Um caso bastante expressivo desse impacto é a Embraer. Os dois efeitos podem ser observados nessa empresa: tanto o aprimoramento de sua capacidade industrial, derivado de investimentos da defesa, que a tornaram extremamente competitiva, quanto o uso dessa capacidade para produzir aeronaves para uso civil. Vários estudos relacionam as despesas com defesa e o desenvolvimento e sustentação de capacidade e competitividade industrial em empresas europeias e americanas, especialmente para produtos de alta e média alta tecnologias (Mollas-Gallart, 1992; Wang et al., 2012 e Winthrop et al., 2002).

A conclusão é que existe realmente um impacto positivo de investimentos em defesa no desenvolvimento econômico e tecnológico-industrial de um país, principalmente quando esses investimentos estão associados ao desenvolvimento de novas tecnologias e capacidade industrial para produtos de média-alta e alta tecnologias. Entretanto, como enfatizado na introdução, esse é um transbordamento positivo desses investimentos, mas não é o seu objetivo principal.

4. Lições apreendidas nos conflitos recentes

"A introdução de novas armas frequentemente muda
a própria natureza da guerra" (Liddel Hart)

Para finalizar, é importante identificar quais os principais ensinamentos que se pode extrair dos recentes conflitos assimétricos, típicos dessa era em que vivemos, em especial na Ucrânia e no oriente médio. Em ambos os conflitos, de um lado, temos duas das maiores potências militares e, do outro, países médios. No caso da Ucrânia, com expressivo apoio dos países da OTAN e, no caso do Irã, com uma BLD própria,

voltada para desenvolver armas de longo alcance e alta precisão (mísseis balísticos e drones) que se mostraram muito adequadas para dissuasão, no ambiente em que são usadas.

Em primeiro lugar, que não é possível ter capacidade militar efetiva e crível, sem se dispor de uma Base Logística de Defesa própria e adequada às características e necessidades específicas do país. Apoios externos podem ser importantes, mas não se pode contar com eles.

Em segundo lugar, a consolidação do entendimento de que a logística de defesa tem como função primordial o preparo e apoio ao emprego de capacidade militar e não se destina a gerar empregos, divisas, ou impostos e o critério para se avaliar indústrias estratégicas de defesa não é a eficiência, ou capacidade de gerar lucros, mas, sim, a eficácia em combate dos produtos que desenvolve e produz.

Em terceiro lugar, a consolidação do uso de mísseis e veículos não tripulados de baixo custo, de todos os tipos, de variados alcances e alta precisão. Esses podem ser produzidos em massa, com relativa facilidade e saturar defesas que utilizam mísseis muito mais sofisticados e caros. Primeiros passos de um processo, que parece ser inevitável, de robotização da guerra. Dependendo do cenário geográfico, esse novo tipo de armas pode ser uma solução para países de médio porte se prepararem para enfrentar conflitos assimétricos.

Referências

ALPTEKIN, A., & LEVINE, P. Military expenditure and economic growth: A meta-analysis. **European Journal of Political Economy**, 28, p. 636-650, 2012. http://dx.doi.org/10.1016/j.ejpoleco.2012.07.002

BENOIT, E. **Defence and Economic Growth in Developing Countries**. Boston, MA, USA: Lexington Books, 1973.

BENOIT, E. Growth and Defence in Developing Countries. **Economic Development and Cultural Change**, 26, p. 271-280, 1978. https://doi.org/10.1086/451015

BRICK, E.S. Logística de defesa: uma subárea do conhecimento de importância estratégica para as ciências de gestão**. Revista Brasileira de Gestão e Desenvolvimento Regional**, 12(2), p. 301-331, 2016.

BRICK, E. S. A conceptual framework for defense logistics. **Gestão & Produção**, 26(4). e4062, 2019. https://doi.org/10.1590/0104-530X4062-19

BRICK, E. S. Base logística de defesa: o instrumento de defesa estratégico para o preparo e sustentação do emprego da capacidade militar. **Revista Brasileira de Estudos Estratégicos REST** V14 No 28, 2022.

BRICK, E. S. **Política Industrial e Tecnológica para a Defesa Nacional**. Federação das Indústrias do Estado de São Paulo, 2022a.

BRUMM, H. Military spending, government disarray and economic growth: a crosss-country empirical analysis. **Journal of Macroeconomics**, 19, p. 827-838, 1997. https://doi.org/10.1016/S0164-0704(97)00044-X

CHEN, P. F., Lee, C. C. & Chiu, Y. B. The nexus between defense expenditure and economic growth: new global evidence. **Economic Modelling**, 36, p. 474-483, 2014. http://dx.doi.org/10.1016/j.econmod.2013.10.019

DUNNE, J., SMITH, R., & WILLENBOCKEL, D. Models of military expenditure and growth: a critical view. **Defence and Peace Economics**, 16, p. 449-461, 2005. doi:10.1080/10242690500167791

ECCLES, H. **Military Concepts and Philosophy**. New Brunswick, NJ, USA: Rutgers University Press, 1965.

ETZKOWITZ, H. e LEYDESDORFF, L. The triple helix-university-industry-government relations: a laboratory for knowledge based economic development. **EASST Review 14** (1995, nr. 1) 14-19, 1995.

GANSLER, J. **Democracy's Arsenal:** Creating a Twenty-First-Century Defense Industry. The MIT Press, 2011.

GIOVACHINI, L. L'armement français au XXe siècle: une politique à L'épreuve de l'histoire. Paris, France: Ellipses Édition Marketing S.A, 2000.

MOLLAS-GALLART, J. **Military Production and Innovation in Spain**. London: Harwood, 1992.

MOWERY, D.C. Defense-related R&D as a model for "Grand Challenges" technology policies**. Research Policy 41,** 2012.

SMITH, R. **Military economics:** the interaction of power and money. Hampshire, United Kingdon: Palgrave Macmillan, 2009.

THORPES, G. (1917). **Pure Logistics:** the science of war preparation. Introduced by Stanley Falk (3 ed.). Washington, DC, USA: National Defense University Press, 1996.

WANG, T., SHYU, S., & CHOU, H. The impact of defense expenditures on economic productivity in OECD countries. **Economic Modelling**, 29, p. 2104-2114, 2012. http://dx.doi.org/10.1016/j.econmod.2012.06.041

WINTHROP, M. F., DECKRO, R. F., & KLOEBER, Jr., J. M. Government R&D expenditures and US technology advancement in the aerospace industry: a case study. **Journal of Engineering and Technology Management**, 19, p. 287-305, 2002. doi: 10.1016/S0923-4748(02)00022-X

Eduardo Siqueira Brick · Professor Titular (aposentado) da Universidade Federal Fluminense. Pesquisador do UFFDEFESA – Núcleo de Estudos de Defesa, Inovação, Capacitação e Competitividade Industrial.

Implicações éticas da inteligência artificial em sistemas autônomos no contexto da defesa

Joelmir Ramos

Resumo

A incorporação crescente de inteligência artificial (IA) em sistemas autônomos tem reconfigurado de maneira estrutural a indústria de defesa contemporânea, deslocando o eixo da superioridade estratégica do domínio puramente físico para o domínio informacional, algorítmico e infraestrutural. Este artigo analisa as implicações éticas, políticas e geopolíticas dessa transformação, com ênfase na delegação de decisões críticas a sistemas automatizados e na natureza dual-use das tecnologias emergentes. Adotando o conceito de soberania algorítmica como eixo analítico, argumenta-se que o controle sobre dados, modelos e infraestruturas digitais constitui elemento central da autonomia estatal no século XXI. Discute-se o dilema da responsabilidade moral em decisões mediadas por algoritmos, os riscos associados à opacidade e à dependência tecnológica, bem como os desafios regulatórios no contexto brasileiro. Sustenta-se que a adoção da inteligência artificial na defesa não representa apenas uma evolução técnica incremental, mas uma reconfiguração das estruturas de poder, com implicações profundas para a soberania, a responsabilidade e os limites da ação humana em cenários críticos.

Abstract

The increasing incorporation of artificial intelligence (AI) into autonomous systems has structurally reshaped the contemporary defense industry, shifting the axis of strategic superiority from the purely physical domain to informational, algorithmic, and infrastructural dimensions. This article examines the ethical, political, and geopolitical implications of this transformation, with particular emphasis on the delegation of critical decisions to automated systems and the dual-use nature of emerging technologies. Adopting the concept of algorithmic sovereignty as its analytical framework, the study argues that control over data, models, and digital infrastructures has become a central element of state autonomy in the 21st century. It further discusses the dilemma of moral responsibility in algorithm-mediated decisions, the risks associated with opacity and technological dependence, and the regulatory challenges within the Brazilian context. The paper contends that the adoption of artificial intelligence in defense does not merely represent incremental technical progress, but rather a reconfiguration of power structures, with profound implications for sovereignty, accountability, and the limits of human agency in critical scenarios.

1. Introdução

A incorporação de inteligência artificial em sistemas autônomos de defesa representa uma transformação estrutural no modo como o poder é exercido e distribuído no sistema internacional contemporâneo. Longe de constituir apenas um avanço tecnológico incremental, essa mudança redefine os fundamentos da ação estatal, deslocando o eixo da superioridade estratégica do domínio físico para o domínio informacional, algorítmico e infraestrutural. Nesse novo cenário, a capacidade de processar dados em tempo real, identificar padrões complexos e executar decisões automatizadas torna-se um elemento central na configuração do poder.

A crescente integração de inteligência artificial em contextos estratégicos redefine as bases tradicionais da ação estatal. Se, ao longo do século XX, a superioridade militar esteve associada à capacidade industrial e ao domínio de recursos físicos, o século XXI assiste à consolidação de um novo paradigma, no qual a capacidade de coletar, processar e interpretar dados em tempo real se torna central (Hurochkina, 2025). Essa mudança não apenas amplia a eficiência operacional, mas também altera a própria natureza da tomada de decisão em ambientes de alta complexidade.

Essa transformação introduz um paradoxo fundamental: quanto mais sofisticados e autônomos se tornam os sistemas de decisão, menos transparentes e compreensíveis se tornam seus processos internos. Sistemas baseados em aprendizado de máquina operam frequentemente por meio de arquiteturas complexas, nas quais a relação entre dados de entrada e decisões de saída não é plenamente explicável (Nalbant, 2025). A opacidade desses sistemas compromete a rastreabilidade das decisões e impõe desafios significativos à responsabilização e à governança.

Ao mesmo tempo, a velocidade de operação desses sistemas excede a capacidade humana de supervisão, especialmente em cenários de alta criticidade, como operações militares e defesa cibernética. Nesse contexto, decisões potencialmente irreversíveis podem ser executadas sem validação humana direta, ampliando o risco de erros sistêmicos e reduzindo a margem para intervenção corretiva. A delegação de decisões a sistemas automatizados, portanto, não apenas redefine a eficiência operacional, mas também tensiona os limites da responsabilidade humana.

Além disso, a crescente centralidade de sistemas algorítmicos na tomada de decisão estratégica implica uma reconfiguração das estruturas institucionais que sustentam a ação estatal. A dependência de infraestruturas digitais e de modelos de inteligência artificial desenvolvidos por atores externos introduz novas formas de vulnerabilidade, associadas não apenas à segurança técnica, mas também ao controle político e econômico desses sistemas. Nesse contexto, a autonomia estatal passa a

depender, em medida crescente, da capacidade de compreender, desenvolver e governar tecnologias complexas.

Diante desse cenário, este artigo propõe uma análise crítica da incorporação da inteligência artificial na defesa a partir da noção de soberania algorítmica. Argumenta-se que o domínio sobre sistemas inteligentes constitui um novo eixo de poder, redefinindo as fronteiras da autonomia estatal e introduzindo desafios éticos e políticos que transcendem o campo técnico. Ao explorar essas dimensões, busca-se contribuir para o debate sobre os limites e as possibilidades da ação humana em um mundo cada vez mais mediado por sistemas automatizados.

2. Inteligência artificial e a reconfiguração da defesa contemporânea

A emergência de sistemas autônomos baseados em inteligência artificial representa uma mudança qualitativa na evolução das tecnologias de defesa. Esses sistemas operam por meio de ciclos integrados de percepção, decisão e ação (*sense–decide–act*), nos quais sensores capturam dados, algoritmos identificam padrões e módulos de decisão executam respostas em tempo real (Nazil, 2025).

Essa arquitetura permite não apenas a automação de tarefas, mas a delegação de funções cognitivas tradicionalmente associadas a operadores humanos. A capacidade de identificar padrões em grandes volumes de dados, prever comportamentos e reagir a eventos em tempo real redefine a natureza da ação estratégica.

A literatura recente destaca a progressiva transição entre diferentes níveis de autonomia, variando de sistemas com supervisão humana (*human-in-the-loop*) até sistemas totalmente autônomos (*human-out-of-the-loop*). Essa transição não é meramente técnica, mas implica uma redefinição das relações entre humanos e máquinas na tomada de decisão (Natarajan, 2025).

Além disso, a incorporação de IA em sistemas de defesa está diretamente associada à lógica da competição estratégica entre Estados. Países

que dominam tecnologias avançadas de inteligência artificial tendem a obter vantagens significativas em termos de capacidade de resposta, precisão e eficiência operacional (Baeza, 2025).

Nesse sentido, a inteligência artificial não deve ser compreendida apenas como uma ferramenta tecnológica, mas como uma infraestrutura de poder, capaz de reconfigurar as relações de força no sistema internacional.

A crescente complexidade desses sistemas também impõe novos desafios operacionais relacionados à confiabilidade e à previsibilidade das decisões automatizadas. Em ambientes dinâmicos e incertos, a capacidade de generalização dos modelos de inteligência artificial torna-se um fator crítico, uma vez que decisões baseadas em dados incompletos ou enviesados podem produzir resultados inesperados. Essa limitação evidencia que a eficácia dos sistemas autônomos não depende apenas de sua sofisticação técnica, mas da qualidade dos dados e dos contextos nos quais são empregados.

Adicionalmente, a integração de sistemas autônomos em arquiteturas militares amplia a interdependência entre diferentes camadas tecnológicas, incluindo sensores, redes de comunicação, infraestrutura computacional e modelos de aprendizado. Essa interdependência cria novos pontos de vulnerabilidade, especialmente em cenários de guerra híbrida e cibernética, nos quais ataques direcionados a componentes específicos podem comprometer o funcionamento de todo o sistema. Dessa forma, a robustez tecnológica passa a ser um elemento central da estratégia de defesa.

A difusão dessas tecnologias no sistema internacional tende a intensificar dinâmicas de corrida tecnológica, nas quais Estados buscam acelerar o desenvolvimento de capacidades autônomas para evitar desvantagens estratégicas. Esse movimento pode reduzir o espaço para reflexão ética e regulação, favorecendo a adoção de soluções tecnológicas antes da consolidação de mecanismos adequados de governança. Nesse contexto, a inteligência artificial não apenas transforma a condução de operações, mas também redefine os próprios ritmos e lógicas da competição internacional.

3. Soberania algorítmica e a nova geopolítica do poder

A transformação digital exige uma revisão profunda do conceito de soberania. No contexto contemporâneo, o domínio sobre dados, algoritmos e infraestruturas digitais torna-se tão relevante quanto o controle territorial. A soberania algorítmica pode ser compreendida como a capacidade de um Estado de desenvolver, controlar e auditar sistemas inteligentes que influenciam decisões críticas (Badawy, 2025). Essa capacidade envolve não apenas infraestrutura tecnológica, mas também domínio sobre fluxos de dados, modelos de aprendizado e arquiteturas computacionais.

A dependência tecnológica, especialmente em áreas como inteligência artificial e semicondutores, introduz vulnerabilidades estruturais. Sistemas desenvolvidos por atores externos podem incorporar vieses, limitações ou mecanismos de controle que escapam à supervisão nacional. Esse cenário tem sido interpretado como uma forma de colonialismo digital, caracterizado pela concentração do poder tecnológico em poucos atores globais e pela dependência de países periféricos (Abiade, 2025).

Além disso, a soberania algorítmica está diretamente relacionada à capacidade de um Estado de proteger seus interesses estratégicos em um ambiente cada vez mais mediado por sistemas digitais. A ausência de domínio sobre essas tecnologias pode comprometer a autonomia decisória e limitar a capacidade de atuação internacional.

Nesse contexto, a soberania algorítmica também assume uma dimensão econômica, uma vez que o controle sobre infraestruturas digitais e plataformas tecnológicas está diretamente associado à geração de valor e à competitividade global. Grandes corporações tecnológicas, muitas vezes sediadas em poucos países, concentram não apenas capacidade técnica, mas também poder de influência sobre mercados, fluxos informacionais e processos decisórios. Essa concentração reforça assimetrias globais e amplia a dependência de países que não possuem capacidade de desenvolvimento tecnológico equivalente.

Adicionalmente, a governança dos dados emerge como um elemento central da soberania contemporânea. A capacidade de coletar, armazenar e processar dados em larga escala não apenas sustenta o funcionamento de sistemas de inteligência artificial, mas também influencia diretamente a produção de conhecimento e a tomada de decisão. Nesse sentido, o controle sobre dados estratégicos torna-se um ativo crítico, cuja ausência pode limitar significativamente a capacidade de um Estado de formular políticas públicas eficazes e responder a desafios complexos.

É notável que a soberania algorítmica está intrinsecamente ligada à capacidade institucional de formular, implementar e fiscalizar políticas tecnológicas. Não se trata apenas de desenvolver tecnologia, mas de criar estruturas de governança capazes de garantir seu uso alinhado a interesses nacionais e valores democráticos. Nesse cenário, Estados que não conseguem articular capacidades técnicas e institucionais tendem a ocupar posições periféricas em um sistema internacional cada vez mais orientado por dinâmicas tecnológicas.

4. Ética da decisão algorítmica

A delegação de decisões críticas a sistemas algorítmicos introduz dilemas éticos complexos, especialmente no que diz respeito à responsabilidade, transparência e legitimidade das decisões. Em contextos de alta criticidade, como os sistemas de defesa, essas questões assumem uma dimensão ainda mais sensível, uma vez que decisões automatizadas podem produzir efeitos irreversíveis.

Um dos principais desafios refere-se à atribuição de responsabilidade em sistemas autônomos. Quando uma decisão é tomada por um algoritmo, a cadeia de responsabilidade torna-se difusa, envolvendo desenvolvedores, operadores e instituições (Cecez-Kecmanovic, 2025). Essa fragmentação dificulta a identificação de agentes responsáveis por eventuais falhas, comprometendo mecanismos tradicionais de accountability.

Além disso, a opacidade dos modelos de aprendizado de máquina compromete a transparência das decisões. A ausência de explicabilidade dificulta a auditoria e a avaliação ética das ações realizadas pelos sistemas. Em contextos nos quais decisões precisam ser justificadas, seja do ponto de vista jurídico, político ou moral, essa limitação representa um desafio significativo para a legitimidade das ações automatizadas.

Outro aspecto relevante diz respeito à formalização de princípios éticos em estruturas computacionais. Conceitos como justiça, proporcionalidade e responsabilidade são intrinsecamente contextuais e dificilmente traduzíveis em regras formais. A tentativa de codificar esses princípios em algoritmos implica simplificações que podem comprometer sua aplicação em cenários reais.

A literatura recente tem enfatizado a necessidade de desenvolver abordagens interdisciplinares para lidar com esses desafios, integrando perspectivas da filosofia, da ciência política e da engenharia. Nesse contexto, a ética da inteligência artificial não pode ser reduzida a um conjunto de diretrizes técnicas, mas deve ser compreendida como um campo de disputa normativa, no qual diferentes valores e interesses são negociados.

Paralelamente, a natureza dual-use das tecnologias emergentes amplia a complexidade desses dilemas. Tecnologias desenvolvidas para fins civis podem ser rapidamente adaptadas para aplicações militares, criando um ambiente de ambiguidade estratégica. Sistemas de inteligência artificial utilizados em áreas como saúde, transporte ou educação podem ser reconfigurados para vigilância, monitoramento e tomada de decisão em contextos de defesa.

Essa dualidade torna difícil estabelecer fronteiras claras entre inovação e risco. A mesma tecnologia que promove ganhos sociais pode ser empregada para fins estratégicos, muitas vezes sem alterações estruturais significativas. Como resultado, a regulação dessas tecnologias torna-se particularmente desafiadora, exigindo mecanismos flexíveis e adaptativos.

Essa característica impõe desafios significativos para a governança tecnológica. A regulação precisa equilibrar a promoção da inovação

com a mitigação de riscos, evitando tanto a estagnação quanto o uso irresponsável das tecnologias. Organismos internacionais, como a OCDE e a UNESCO, têm buscado estabelecer diretrizes para o uso ético da inteligência artificial, mas ainda há lacunas significativas, especialmente no que se refere a aplicações militares.

Além disso, a natureza dual-use das tecnologias intensifica os dilemas éticos associados à sua aplicação, uma vez que decisões sobre desenvolvimento e implementação frequentemente ocorrem em contextos distintos daqueles em que seus efeitos se manifestam. Essa dissociação entre intenção e impacto dificulta a antecipação de riscos e amplia a complexidade da responsabilidade moral.

Por fim, a convergência entre ética algorítmica e tecnologias dual -use evidencia a necessidade de repensar os modelos tradicionais de regulação. Em um cenário no qual as fronteiras entre civil e militar se tornam cada vez mais difusas, torna-se fundamental desenvolver estruturas de governança capazes de lidar com essa ambiguidade. Isso implica não apenas a criação de normas e diretrizes, mas também o fortalecimento de capacidades institucionais e mecanismos de cooperação internacional que permitam responder de forma coordenada aos desafios emergentes.

5. Brasil: Inserção periférica, dependência tecnológica e desafios estruturais

O Brasil apresenta uma inserção periférica no sistema tecnológico global, caracterizada pela dependência de infraestruturas críticas e tecnologias desenvolvidas no exterior. Essa condição limita a capacidade do país de atuar de forma autônoma em setores estratégicos, especialmente aqueles relacionados à defesa, à segurança cibernética e à inteligência artificial. Em um cenário no qual o poder é cada vez mais mediado por sistemas digitais, a ausência de domínio tecnológico compromete não apenas a competitividade econômica, mas também a soberania nacional (Sá, 2025).

A ausência de uma indústria robusta de semicondutores, a dependência de plataformas digitais estrangeiras e a limitada capacidade de desenvolvimento de modelos de IA constituem fatores estruturais dessa vulnerabilidade. O controle sobre dados e infraestruturas digitais tornou-se um dos principais determinantes do poder econômico e político contemporâneo, reforçando assimetrias globais e consolidando a posição dominante de poucos atores internacionais.

Ao mesmo tempo, o Brasil possui potencial significativo, especialmente no campo acadêmico e científico. Universidades públicas, centros de pesquisa e iniciativas de inovação desempenham papel fundamental na formação de recursos humanos altamente qualificados e na geração de conhecimento. Essa base representa um ativo estratégico relevante, que pode ser mobilizado para reduzir a dependência externa e fomentar o desenvolvimento de tecnologias nacionais.

Nesse contexto, a construção de soberania algorítmica no Brasil depende de políticas públicas consistentes, investimentos contínuos em pesquisa e desenvolvimento e fortalecimento das capacidades institucionais. A Estratégia Brasileira de Inteligência Artificial (EBIA) e os debates em torno da regulação da IA representam avanços importantes, mas ainda insuficientes diante da magnitude dos desafios.

Adicionalmente, é necessário considerar que a dependência tecnológica não se limita ao acesso a produtos e serviços, mas envolve também a incorporação de padrões técnicos, protocolos e arquiteturas definidas externamente. Essa dependência normativa pode restringir a capacidade do país de formular políticas tecnológicas alinhadas a seus próprios interesses estratégicos, reforçando sua posição periférica no sistema internacional.

Outro aspecto relevante diz respeito à fragmentação do ecossistema de inovação brasileiro. A ausência de integração efetiva entre universidades, setor produtivo e políticas públicas limita a capacidade de transformar conhecimento científico em soluções tecnológicas aplicadas. O papel do Estado como indutor da inovação é fundamental para a construção de capacidades tecnológicas estratégicas, especialmente em países em desenvolvimento.

Além disso, a crescente centralidade da inteligência artificial na economia global exige a formação de competências específicas, tanto no nível técnico quanto institucional. A escassez de profissionais qualificados, aliada à competição internacional por talentos, representa um desafio adicional para o Brasil, que precisa não apenas formar, mas também reter capital humano especializado.

A construção de soberania algorítmica no país está intrinsecamente ligada à capacidade de articular uma visão estratégica de longo prazo, que integre desenvolvimento tecnológico, políticas industriais e governança digital. Sem essa articulação, o risco é que o Brasil permaneça como consumidor de tecnologias externas, limitado em sua capacidade de influenciar os rumos da transformação digital e de proteger seus interesses estratégicos em um ambiente cada vez mais competitivo e tecnologicamente orientado.

6. Limitações sistêmicas e desafios de governança da inteligência artificial

Apesar de seu potencial transformador, sistemas de inteligência artificial apresentam limitações técnicas significativas que se tornam particularmente críticas em contextos estratégicos, como a defesa. Erros de classificação, vieses nos dados de treinamento e dificuldades de generalização podem comprometer a precisão das decisões, especialmente em ambientes dinâmicos e incertos. Além disso, esses sistemas são vulneráveis a ataques adversariais, nos quais pequenas perturbações nos dados de entrada podem induzir comportamentos inesperados ou decisões equivocadas. A dependência de grandes volumes de dados também introduz riscos associados à qualidade, integridade e representatividade das informações utilizadas no treinamento dos modelos.

Essas limitações técnicas não são apenas problemas operacionais, mas configuram riscos sistêmicos, uma vez que decisões automatizadas podem produzir efeitos amplos e, em alguns casos, irreversíveis. Em contextos de defesa, a ausência de mecanismos robustos de validação,

supervisão e controle pode amplificar esses riscos, comprometendo tanto a eficácia operacional quanto a legitimidade das ações realizadas por sistemas autônomos.

Diante desse cenário, a governança da inteligência artificial emerge como um dos principais desafios contemporâneos. A complexidade dos sistemas, a velocidade de inovação e a natureza transnacional das tecnologias dificultam a construção de marcos regulatórios eficazes e adaptáveis. No caso brasileiro, o debate regulatório encontra-se em desenvolvimento, refletindo a necessidade de equilibrar a promoção da inovação tecnológica com a garantia de responsabilidade, transparência e segurança.

A construção de um framework regulatório eficaz exige a articulação entre diferentes atores, incluindo governo, academia e setor privado, além do fortalecimento de capacidades institucionais para monitoramento e fiscalização. Ao mesmo tempo, é fundamental considerar as especificidades do contexto nacional, evitando a simples importação de modelos regulatórios externos que podem não se adequar às realidades locais. Nesse sentido, enfrentar as limitações técnicas da inteligência artificial e desenvolver estruturas de governança adequadas são processos indissociáveis, essenciais para garantir que a incorporação dessas tecnologias ocorra de forma segura, responsável e alinhada aos interesses estratégicos do Estado.

7. Conclusão

A incorporação de sistemas baseados em inteligência artificial na defesa contemporânea não constitui apenas um avanço tecnológico, mas uma transformação estrutural na forma como decisões estratégicas são concebidas e executadas. Ao deslocar o eixo da ação estatal para arquiteturas algorítmicas e infraestruturas digitais, essa mudança redefine os fundamentos do poder, introduzindo novas dinâmicas de dependência, vulnerabilidade e competição no sistema internacional. Nesse contexto, a noção de soberania algorítmica emerge como elemento central

para a compreensão da autonomia estatal no século XXI, na medida em que o domínio sobre dados, modelos e sistemas de decisão condiciona diretamente a capacidade dos Estados de formular e executar estratégias de forma independente.

Paralelamente, os desafios éticos associados à delegação de decisões a sistemas autônomos evidenciam os limites de uma abordagem puramente técnica. A opacidade dos modelos, a difusão da responsabilidade e a dificuldade de traduzir princípios normativos em estruturas computacionais demonstram que a inteligência artificial é, fundamentalmente, uma tecnologia política. Assim, sua incorporação na defesa deve ser compreendida como uma escolha estratégica e normativa, cuja condução definirá não apenas a posição dos Estados no sistema internacional, mas também os limites da autonomia humana em um mundo cada vez mais mediado por sistemas automatizados.

Referências

ABIADE, Sheriffdeen Folaranmi. Algorithmic Sovereignty and the New Security Dependencies: How Foreign AI Surveillance Technologies Reshape Domestic Autonomy in the Global South. **World Journal of Advanced Research and Reviews**, 2025. *https://doi. org/10.30574/wjarr* 2

BADAWY, Wael. Algorithmic sovereignty and democratic resilience: rethinking AI governance in the age of generative AI. **AI and Ethics 5.5**, 2025, p. 4855-4862.

BAEZA, Victor Monzon, et al. **AI-driven tactical communications and networking for defense:** A survey and emerging trends, 2025. arXiv preprint arXiv:2504.05071.

CECEZ-KECMANOVIC, Dubravka. "Ethics in the world of automated algorithmic decision-making–a posthumanist perspective." **Information and Organization 35.3,** 2025, 100587.

HUROCHKINA, Viktoriia, Svitlana Bondarenko, and Tomasz Szapiro. The implementation of artificial intelligence technologies in the military domain: Opportunities and risks. **2025 15th International Conference on Advanced Computer Information Technologies** (ACIT). IEEE, 2025.

NALBANT, Kemal Gokhan, and TOKACI, Tuba. Developments in the defense industry with the impact of machine learning and artificial intelligence. **International Journal of Applied Sciences & Development 4**, p. 37-47, 2025.

NATARAJAN, Sriraam, et al. Human-in-the-loop or AI-in-the-loop? Automate or Collaborate?. **Proceedings of the AAAI Conference on Artificial Intelligence**. Vol. 39. No. 27, 2025.

NAZIL, Ashikur Rahman. "AI at War: The next revolution for military and defense." (2025).

SÁ, Hebert Azevedo, et al. Tendências da inteligência artificial aplicada à defesa: forças, fraquezas, oportunidades e ameaças para o Brasil. **Boletim de Conjuntura (BOCA)**, 21.62, p. 01-33, 2025.

Joelmir Ramos- Graduado em Engenharia Elétrica / Eletrônica pela UERJ. Mestre em Engenharia Eletrônica pela UERJ. MBA em Data Science and Analytics pela USP. Doutorando Ciência da Computação e Gestão de Sistemas Complexos pela UFRJ. Criador do primeiro robô humanoide do Brasi: o Sistema 14-bis. Atua nas áreas de inteligência artificial, computação visual e robótica humanoide.

Guerra híbrida como coerção politicamente dirigida: tecnologia, ambiguidade e vulnerabilidade estratégica

Jorge M. Lasmar

Resumo

A guerra híbrida constitui uma forma contemporânea de coerção politicamente dirigida, na qual instrumentos militares e não militares são combinados para produzir efeitos estratégicos sob condições de ambiguidade. O artigo compara conceitos, autores e debates doutrinários a partir de uma abordagem qualitativa e teórico-conceitual, revendo conceitos sobre guerra híbrida, ambiguidade estratégica, tecnologia, fricção, vulnerabilidades sistêmicas, e o pensamento de Clausewitz. Sustenta-se que a guerra híbrida não representa uma essência inteiramente nova da guerra, mas um modo específico de integrar coerção, ambiguidade e exploração de vulnerabilidades. Sua eficácia depende da capacidade de intensificar incertezas, dificultar a atribuição de responsabilidade, retardar respostas e pressionar vulnerabilidades informacionais, institucionais, infraestruturais e sociais já existentes. Por fim, a tecnologia exerce papel central nas ameaças híbridas ao ampliar a escala, a velocidade, a opacidade e o alcance dessas ações, mas não substitui sua lógica política. Assim, a guerra híbrida pode ser compreendida como exploração coordenada de vulnerabilidades sob condições de ambiguidade.

Abstract

Hybrid warfare constitutes a contemporary form of politically directed coercion in which military and non-military instruments are combined to produce strategic effects under conditions of ambiguity. The article compares concepts, authors, and doctrinal debates through a qualitative and theoretical-conceptual approach, reviewing discussions on hybrid warfare, strategic ambiguity, technology, friction, systemic vulnerabilities, and Clausewitz's thought. It argues that hybrid warfare does not represent an entirely new essence of war, but rather a specific way of integrating coercion, ambiguity, and the exploitation of vulnerabilities. Its effectiveness depends on the ability to intensify uncertainty, complicate attribution of responsibility, delay responses, and pressure pre-existing informational, institutional, infrastructural, and social vulnerabilities. Finally, technology plays a central role in hybrid threats by expanding the scale, speed, opacity, and reach of these actions, but it does not replace their political logic. Thus, hybrid warfare can be understood as the coordinated exploitation of vulnerabilities under conditions of ambiguity.

Introdução

O conflito contemporâneo é cada vez mais conduzido por meio da combinação de ações cibernéticas disruptivas, campanhas de desinformação, atores por procuração, sabotagem, pressão econômica, manipulação jurídica e uso calibrado da força. Casos como a guerra na Ucrânia reforçaram a percepção de que o conflito frequentemente se desenrola por meio de instrumentos militares e não militares que operam de forma combinada, tornando menos nítidas as distinções convencionais entre guerra e paz, pressão interna e externa, e ação cinética e não cinética. No entanto, essa amplitude também pode tornar o conceito teoricamente impreciso. Este artigo aceita a crítica de que o termo guerra híbrida tem sido, por vezes, excessivamente elástico, mas não

conclui que seu uso deva ser abandonado. Ao contrário, argumenta que a guerra híbrida permanece analiticamente útil quando definida por sua lógica estratégica: o uso coordenado de instrumentos combinados para produzir efeitos políticos sob condições de ambiguidade.

Este artigo conecta três debates que frequentemente são tratados separadamente: a expansão excessiva do conceito de guerra híbrida, o problema clausewitziano do propósito político e do atrito, e a coerção tecnologicamente mediada como forma de exploração de vulnerabilidades. O argumento aqui apresentado é que a guerra híbrida deve ser compreendida não como um tipo inteiramente novo de guerra, mas como uma forma contemporânea de coerção politicamente dirigida. Seu caráter distintivo está na coordenação de instrumentos militares e não militares para explorar ambiguidades, intensificar incertezas e pressionar vulnerabilidades estrategicamente significativas sem necessariamente desencadear uma guerra interestatal aberta e em larga escala. A questão analítica central, portanto, não é apenas quais ferramentas são utilizadas, mas como essas ferramentas são integradas em torno de um propósito político.

Essa linha de análise é consistente com a visão clássica de que o conflito armado permanece subordinado ao propósito político, mesmo quando suas formas, ritmo e tecnologias mudam ao longo do tempo (Clausewitz, 1976). Ela também ressoa com a compreensão de Hoffman da guerra híbrida como a fusão de diferentes modos de conflito e com esforços mais recentes para identificar a ambiguidade como uma das características centrais do conceito (Hoffman, 2007; Mumford e Carlucci, 2023). Neste artigo, a ambiguidade não é tratada como a única característica definidora da guerra híbrida, mas como a condição estratégica que permite que instrumentos combinados dificultem a atribuição, tornem os limiares menos nítidos, fragmentem o consenso político e atrasem ou restrinjam as respostas (Mumford e Carlucci, 2023).

A tecnologia amplifica essa lógica, mas não a substitui. Sua importância está menos em criar uma nova lógica política do conflito do que em expandir a escala, a velocidade, o alcance, a opacidade e a persistên-

cia da ação coercitiva em múltiplos domínios. Infraestruturas digitais, comunicações em rede, capacidades cibernéticas, plataformas de informação, sensores comerciais e sistemas habilitados por IA tornam mais fácil, barato e, em alguns casos, mais plausivelmente negável perturbar sistemas, manipular percepções e pressionar vulnerabilidades que não podem ser reduzidas apenas a alvos no campo de batalha (Mumford e Carlucci, 2023). A tecnologia, portanto, funciona principalmente como facilitadora e multiplicadora da coerção híbrida, especialmente quando vulnerabilidades estratégicas estão localizadas na credibilidade informacional, coesão institucional, infraestrutura crítica e confiança pública.

O artigo está organizado em quatro seções. A primeira esclarece o conceito de guerra híbrida e identifica as principais tensões em torno de seu uso. A segunda examina o propósito político e explica por que a ambiguidade é estrategicamente útil na gestão da atribuição, retaliação e escalada. A terceira analisa como a mudança tecnológica intensifica a incerteza e o atrito em múltiplos domínios. A quarta desloca o foco dos instrumentos para as vulnerabilidades, argumentando que a guerra híbrida deve ser melhor entendida como a exploração coordenada de vulnerabilidades informacionais, institucionais, sociais e de infraestrutura.

1. Guerra híbrida em debate

A guerra híbrida continua sendo difícil de definir porque o termo tem sido usado para descrever diferentes fenômenos. As primeiras definições focaram na combinação de métodos militares convencionais e irregulares dentro de uma mesma campanha (Hoffman, 2007; Glenn, 2009). Abordagens doutrinárias e políticas posteriores ampliaram o conceito para incluir o uso coordenado de instrumentos militares e não militares em múltiplos domínios (OTAN, 2024).

A literatura mais recente tem enfatizado a ambiguidade, as operações cibernéticas, a desinformação, os atores por procuração (proxy) e a gestão de limiares como elementos centrais da coerção híbrida (Mumford e Carlucci, 2023). À medida que o termo se espalhou pelo

campo dos estudos estratégicos, doutrina de defesa e debate político, ele também se entrelaçou com conceitos adjacentes como ameaças híbridas, conflito de zona cinzenta, guerra cognitiva, guerra política e guerra societal virtual (Mazarr et al., 2019; Steen, 2025). O resultado é um debate marcado tanto pela relevância analítica quanto pela confusão conceitual (Solmaz, 2022; Libiseller, 2023).

Em uma das primeiras formulações do termo, Hoffman definiu ameaças híbridas como adversários que empregam simultaneamente e de forma adaptativa uma mistura combinada de armas convencionais, táticas irregulares, terrorismo e criminalidade (Hoffman, 2007). O ponto central não era listar os métodos em si, mas a afirmação de que esses métodos poderiam ser usados juntos dentro de um mesmo espaço de batalha e campanha. Hoffman, portanto, mudou o debate das distinções binárias entre guerra "regular" e "irregular" para a ideia de que adversários contemporâneos cada vez mais combinam o uso de modalidades que muitas vezes eram tratadas separadamente. Neste sentido, Glenn reconheceu que as categorias de guerra estavam se tornando menos estanques, mas questionou se o "conflito híbrido" merecia reconhecimento como uma categoria genuinamente nova, e não como um subconjunto ou variante da guerra irregular (Glenn, 2009). Esse ceticismo inicial é importante porque demonstra que a contestação sobre o conceito esteve presente desde o início do debate.

O conceito posteriormente se ampliou. O que inicialmente se referia principalmente à violência mista em ambientes operacionais passou a incluir operações cibernéticas, campanhas de desinformação, pressão econômica, interferência eleitoral, manipulação jurídica, uso coercitivo da migração, guerra por procuração e ataques à infraestrutura crítica. Essa ampliação explica a crescente relevância do conceito, mas também a preocupação de que ele se torne excessivamente elástico caso toda forma de hostilidade abaixo do limiar da guerra aberta seja simplesmente incorporada ao rótulo de guerra híbrida (Solmaz, 2022; Mumford e Carlucci, 2023). Essa ampliação do escopo foi reforçada à medida que o conceito migrou dos debates acadêmicos e militares para o campo das

políticas públicas de defesa e da doutrina. Os marcos da OTAN tratam ameaças híbridas como características centrais do ambiente de segurança contemporâneo, especialmente após 2014, quando o termo passou a estar intimamente associado ao comportamento russo na Crimeia e no leste da Ucrânia (Libiseller, 2023; OTAN, 2024). Essa adoção doutrinária teve um efeito ambivalente. Por um lado, reconheceu corretamente a complexidade multidomínio da coerção contemporânea, mas por outro, também incentivou o uso da guerra híbrida como uma categoria ampla de planejamento ao invés de um conceito analítico preciso.

Nesse sentido, a literatura crítica é essencial. Solmaz argumenta que o termo guerra híbrida foi levado além de seu contexto original e aplicado a casos que carecem de suas características essenciais (Solmaz, 2022). Almäng aborda o problema de forma diferente, examinando a natureza vaga do termo "guerra híbrida" como uma categoria situada entre paz e guerra (Almäng, 2019). Stoker e Whiteside vão além, argumentando que tanto o "conflito em zona cinzenta" quanto a "guerra híbrida" frequentemente prejudicam, em vez de aprimorar, o pensamento estratégico ao borrar as distinções entre guerra, paz e competição geopolítica (Stoker e Whiteside, 2020). Libiseller acrescenta que a difusão do conceito foi impulsionada não apenas pelo valor explicativo, mas também pela moda acadêmica e política após a popularização do termo pela OTAN em 2014 (Libiseller, 2023).

Essas críticas não devem ser descartadas. Um conceito que se expande demais acaba explicando muito pouco. No entanto, seria igualmente errado concluir que a guerra híbrida é analiticamente inútil. Interpretações mais contidas preservam o termo ao restringir seu escopo. Caliskan, por exemplo, argumenta que a guerra híbrida é mais útil quando tratada por meio da teoria estratégica do que como prova de uma forma radicalmente nova de guerra (Caliskan, 2019). Mumford e Carlucci desenvolvem essa linha de pensamento argumentando que a essência da guerra híbrida reside na ambiguidade, e não na mera combinação de instrumentos. Sua contribuição desloca o debate dos inventários de ferramentas para a lógica estratégica que torna essas ferramentas

eficazes em combinação: incerteza sobre atribuição, intenção, limiar e resposta (Mumford e Carlucci, 2023).

Em conjunto, o debate sugere que o conceito de guerra híbrida permanece útil apenas se for definido de modo suficientemente restrito para não se converter em sinônimo de qualquer conflito complexo ou não convencional. Na literatura, um conjunto limitado de elementos aparece repetidamente: a combinação de diferentes instrumentos de poder; a integração de meios militares e não militares; coordenação entre domínios; ambiguidade deliberada; direcionamento político, psicológico e social; e um esforço, ao menos inicialmente, para permanecer abaixo do limiar de uma guerra aberta e em larga escala (Hoffman, 2007; Solmaz, 2022; Mumford e Carlucci, 2023). Visto sob essa perspectiva, este artigo trata a guerra híbrida não como um novo tipo de guerra, mas como um modo contemporâneo de coerção integrada no qual atores estatais ou não estatais coordenam instrumentos militares e não militares para explorar a ambiguidade, aplicar pressão gradual e enfraquecer a capacidade do adversário de responder efetivamente. Cinco dimensões são especialmente importantes: integração instrumental, ambiguidade, gradualismo, direcionamento psicológico e social, e exploração sistêmica da vulnerabilidade. Definida dessa forma, a guerra híbrida permanece um conceito útil não porque nomeia tudo de novo sobre conflitos contemporâneos, mas porque captura uma lógica estratégica específica por meio da qual instrumentos mistos geram efeitos coercitivos cumulativos sob condições de ambiguidade (Caliskan, 2019; Hoffman, 2007; Mumford e Carlucci, 2023).

2. Propósito político e ambiguidade

O debate conceitual se torna mais claro quando a guerra híbrida é abordada a partir do propósito político, e não da sua suposta novidade. Clausewitz permanece indispensável aqui porque trata a guerra como um instrumento político e não como uma esfera autônoma de violência. Para ele, o objeto político é o motivo original da guerra e mol-

da tanto o objetivo militar quanto o grau de esforço a ser despendido (Clausewitz, 1976). Aplicado à guerra híbrida, isso significa que a questão analítica decisiva não é se operações cibernéticas, desinformação, proxies, sabotagem, pressão econômica, medidas legais ou força limitada estão presentes. É o efeito político que esses instrumentos pretendem produzir quando usados em conjunto. O argumento de Caliskan é útil precisamente por essa razão: a guerra híbrida é melhor abordada por meio da teoria estratégica do que tratada como uma nova categoria doutrinária (Caliskan, 2019). Mumford e Carlucci fazem um movimento semelhante ao argumentar que sua essência não está na novidade, mas na função política da ambiguidade (Mumford e Carlucci, 2023). Uma leitura clausewitziana, portanto, trata a guerra híbrida como uma configuração historicamente específica de coerção politicamente dirigida, em vez de uma ruptura com a teoria estratégica clássica. Guerra e coerção podem mudar em forma, ritmo e mediação tecnológica, mas permanecem subordinadas ao propósito político. Isso está alinhado com a afirmação de Caliskan de que a guerra híbrida não deve ser entendida como uma doutrina nova, e com a visão de Mumford e Carlucci de que ela é melhor vista como uma escolha operacional adequada à competição estratégica contemporânea do que como uma "nova guerra" (Caliskan, 2019; Mumford e Carlucci, 2023). A implicação chave é simples: a prioridade analítica deve ser o propósito, não a novidade.

Uma vez que o propósito político é priorizado, a atração estratégica dos métodos híbridos torna-se mais clara. Campanhas híbridas são frequentemente projetadas para garantir ganhos políticos limitados, mas significativos, sem incorrer nos custos de uma guerra aberta e em larga escala. Esses ganhos podem incluir enfraquecer a coesão do adversário, alterar gradualmente fatos no terreno, criar poder de barganha, moldar o ambiente político antes que um confronto armado mais amplo se torne necessário ou dividir internamente um país ou uma coalizão adversária. A discussão de Clausewitz sobre guerra limitada é relevante porque mostra que objetivos políticos menores podem exigir esforços menores. Isso também significa que o sucesso pode, em certos casos,

ser buscado por meio de efeitos políticos, e não apenas militares, como desarticular alianças ou paralisar a vontade do oponente (Clausewitz, 1976). A pesquisa contemporânea aponta na mesma direção: Mazarr define estratégias de zona cinzenta como campanhas graduais abaixo dos limiares que causariam uma escalada; Wigell conceitua a interferência híbrida como uma estratégia divisória; e Chivvis enfatiza que a guerra híbrida russa atua dentro dos marcos políticos e sociais existentes para avançar objetivos estratégicos, em vez de simplesmente destruir alvos militares (Mazarr, 2015; Wigell, 2019; Chivvis, 2017). Portanto, o conceito de guerra híbrida é mais útil quando visto como uma forma de coerção ajustada a propósitos políticos limitados e cuidadosamente calibrados.

Central para essa lógica política está a ambiguidade. Ambiguidade não é simplesmente vagueza ou ocultação; é uma condição estratégica em que o alvo enfrenta múltiplas interpretações plausíveis sobre atribuição, intenção, limiares e resposta adequada (Mumford e Carlucci, 2023). Para Mumford e Carlucci, esse é o elemento definidor da guerra híbrida porque força os defensores a agir sob incerteza, dispersando atenção e recursos entre cenários concorrentes. Sua utilidade não está apenas em obscurecer a responsabilidade, mas também em atrasar a tomada de decisões, complicar a retaliação, fragmentar o consenso interno e aliado, e permitir que atores revisionistas modulem a escalada. O conceito de negação plausível de Wigell aponta para o mesmo mecanismo, enquanto o trabalho de Mazarr sobre a zona cinzenta enfatiza a tentativa deliberada de permanecer abaixo das linhas vermelhas que possam desencadear uma resposta convencional (Wigell, 2019; Mazarr, 2015). Ao mesmo tempo, trabalhos recentes que distinguem a guerra híbrida da interferência híbrida abaixo do limiar do conflito armado são um lembrete útil de que nem toda coerção ambígua é guerra no sentido estrito (Bergaust e Sellevåg, 2024).

Clausewitz também ajuda a explicar por que a ambiguidade é eficaz. Sua teoria da guerra é estruturada em torno de atrito, incerteza, probabilidade, paixão e a dificuldade do julgamento em conflitos reais.

Uma leitura clausewitziana da guerra híbrida, portanto, não ficaria especialmente impressionada com a novidade das ferramentas cibernéticas, operações de informação, atores por procuração ou manipulação legal-política em si. O que importa é como esses instrumentos geram atrito dentro do sistema político e societal do oponente. Nesse sentido, a guerra híbrida pode ser entendida como uma forma de coerção que atua simultaneamente sobre as três tendências da notável trindade de Clausewitz. Primeiro, ela pressiona a esfera da razão e do governo ao complicar a atribuição, classificação legal, avaliações de proporcionalidade e gestão de escalada. Os tomadores de decisão são forçados a agir sob incerteza, muitas vezes sem evidências suficientes para construir consenso interno ou aliado para a resposta. Segundo, explora o acaso e a probabilidade multiplicando incidentes ambíguos, sinais incertos, atores cuja vinculação pode ser plausivelmente negada e interações contingentes entre os domínios cibernético, informacional, político, econômico e militar. O defensor deve interpretar se os eventos são isolados, coordenados, acidentais, criminosos, políticos ou militares, e esse ônus interpretativo aumenta a possibilidade de erro de cálculo. Terceiro, mobiliza a paixão ao atacar emoções públicas, desconfiança social, medo, humilhação, ressentimento e polarização. Campanhas de desinformação, sabotagem simbólica, sinalização coercitiva e violência por procuração podem inflamar divisões existentes e tornar as comunidades políticas menos capazes de julgamento coletivo. Como resultado, a guerra híbrida não é simplesmente uma mistura de instrumentos. É um modo de coerção que busca perturbar a relação entre razão política, incerteza e paixão social. Seu valor estratégico está em tornar o sistema político do adversário menos capaz de decidir, coordenar e responder de forma coerente. Nesse sentido, a ambiguidade não é apenas um véu que esconde a ação; é um mecanismo para converter a incerteza em instrumento de coerção sobre toda a comunidade política.

Ao mesmo tempo, uma análise clausewitziana alerta contra o excesso de extensão da linguagem da guerra. Nem todo ato hostil encoberto, plausivelmente negável ou situado abaixo do limiar da guerra aberta

deve ser classificado como guerra. Algumas atividades agrupadas sob o rótulo híbrido são melhor compreendidas como ação coercitiva de Estado, guerra política ou interferência híbrida conduzida abaixo do limiar do conflito armado (Wigell, 2019; Bergaust, e Sellevåg, 2024). Essa distinção não enfraquece o conceito; ela o aperfeiçoa. A guerra híbrida deve ser reservada para campanhas politicamente dirigidas nas quais instrumentos militares e não militares são coordenados para explorar ambiguidades, impor pressão gradual e enfraquecer a capacidade do adversário de resposta coerente sem necessariamente desencadear uma guerra aberta.

3. Tecnologia, incerteza e atrito

A combinação de métodos coercitivos associada à guerra híbrida não é nova. O que distingue o momento atual é o ambiente tecnológico no qual esses métodos são articulados, sincronizados e empregados. Redes digitais, capacidades cibernéticas, ecossistemas de informação plataformados, sistemas de IA, satélites comerciais e drones de baixo custo não alteram a natureza política do conflito. Em vez disso, alteram algumas de suas características operacionais, como velocidade, escala, alcance, precisão, opacidade e persistência. Em termos clausewitzianos, a tecnologia muda os meios e, portanto, o caráter prático do conflito, sem alterar o fato de que guerra e coerção permanecem subordinadas ao propósito político (Clausewitz, 1976). Assim, as tecnologias contemporâneas não inventam conflitos híbridos, mas expandem o repertório disponível de instrumentos, ampliam a possibilidade de explorar vulnerabilidades em sociedades complexas e possibilitam efeitos em múltiplos domínios com velocidade e persistência incomuns (Beyerchen, 1992; Thiele, 2020; Romansky et al., 2024).

É útil distinguir entre coerção híbrida dependente de tecnologia e coerção híbrida intensificada por tecnologia. A primeira refere-se a práticas hostis que dependem de infraestrutura digital ou sistemas técnicos avançados para existirem como táticas viáveis, como implantes

de malware, botnets de redes sociais, mídias sintéticas, personificação assistida por IA, intrusões cibernéticas em sistemas industriais de controle e falsificação de GPS. A segunda refere-se a práticas coercitivas mais antigas cuja eficácia é amplificada pelas tecnologias contemporâneas. A propaganda torna-se algoritmicamente direcionada e escalável; a vigilância torna-se automatizada e intensiva em dados; a sabotagem torna-se mais precisa; a coordenação de atores por procuração se torna mais rápida; e funções de reconhecimento e ataque se difundem por drones e sensores em rede comercialmente disponíveis. Essa distinção é importante porque a tecnologia reduz os custos de entrada para novos atores, aumenta a superfície de ataque e tanto cria novas formas de coerção quanto aprimora práticas antigas de subversão, engano, intimidação e disrupção.

Operações cibernéticas estão entre os exemplos mais claros de coerção híbrida habilitada pela tecnologia. Sua atração não reside apenas no potencial disruptivo, mas também na ambiguidade. A atribuição raramente é um fato puramente técnico; é um processo político pelo qual a incerteza é reduzida o suficiente para justificar a ação e atribuir significado a um incidente (Egloff e Dunn, Cavelty, 2021). É por isso que operações cibernéticas são úteis em campanhas híbridas: podem criar disrupções ao mesmo tempo em que permitem negação plausível, atraso e contestação sobre responsabilidade e intenção. No entanto, é importante evitar determinismo tecnológico. Borghard e Lonergan argumentam que efeitos cibernéticos ofensivos sofisticados são frequentemente ferramentas imperfeitas de coerção e escalada porque exigem acesso prévio, reconhecimento, exploits personalizados e condições favoráveis de direcionamento; mesmo assim, os efeitos permanecem incertos e frequentemente limitados (Borghard e Lonergan, 2017; Borghard e Lonergan, 2019). Essa advertência também ressoa com o argumento de Rid de que muitas atividades descritas como guerra cibernética são melhor entendidas como sabotagem, espionagem ou subversão do que como guerra no sentido estrito (Rid, 2012). Lindsay mostra de forma semelhante que a arquitetura interdependente do ciberespaço cria incentivos para

a contenção, mesmo enquanto permite uma competição persistente de baixo nível (Lindsay, 2017). Operações cibernéticas, portanto, são politicamente atraentes, mas seus efeitos estratégicos permanecem contingentes, incertos e frequentemente mais limitados do que relatos populares sugerem.

A inteligência artificial intensifica essa lógica ao acelerar a produção, o direcionamento, a circulação e a interpretação de efeitos coercitivos. Sua relevância para a guerra híbrida é especialmente visível no domínio informacional, em que sistemas generativos podem ampliar a escala, a velocidade, a personalização e a adaptabilidade linguística das operações de influência. Deepfakes, materiais audiovisuais manipulados, personas sintéticas e geração de conteúdo assistida por IA tornam a confiança em evidências digitais mais contestável e o engano mais escalável (Candolin et al., 2021; Hanhijärvi, 2026). No entanto, operações militares recentes também sugerem que a relevância da IA já não se limita à desinformação, às mídias sintéticas ou às operações de influência. Ela se torna cada vez mais visível na fusão de inteligência, no desenvolvimento de alvos e na aceleração dos ciclos de seleção de alvos. A Reuters relatou que o Pentágono utilizou ferramentas Claude, da Anthropic, durante ataques dos Estados Unidos ao Irã, embora não tenha conseguido determinar com precisão como essas ferramentas foram integradas ao esforço de guerra (Reuters 2026). A Chatham House também observou que o Almirante Brad Cooper confirmou o uso de ferramentas avançadas de IA para filtrar grandes volumes de dados e acelerar a tomada de decisão no conflito, ao mesmo tempo em que ressaltou que o grau de envolvimento da IA em decisões específicas de seleção de alvos permanecia sem confirmação (Amaral, 2026). Isso é importante porque a IA pode comprimir o tempo entre detecção, interpretação, designação de alvos, revisão jurídica e execução do ataque. Ela pode reduzir algumas formas de atrito operacional, mas desloca esse atrito para a qualidade dos dados, a supervisão humana, a revisão jurídica, a responsabilização e a compressão decisória. Sistemas de aprendizado de máquina são moldados por dados de treinamento, desenho de modelos e processos

inferenciais opacos; podem produzir inferências úteis, erros ou manipulações com igual velocidade (Thiele, 2020). Pesquisas sobre análise de campo de batalha habilitada por IA também indicam vulnerabilidade a dados enviesados, falsificações, interferências e envenenamento de dados, o que significa que tais sistemas podem automatizar erros tão facilmente quanto automatizam inferências úteis (Gardner, 2024). Portanto, a IA reduz o custo marginal de alguns efeitos coercitivos, mas não abole a incerteza. Ela a redistribui.

Sistemas autônomos e semiautônomos de baixo custo reproduzem esse mesmo padrão de forma mais concreta. A guerra na Ucrânia demonstrou que pequenos drones comerciais podem desempenhar funções de reconhecimento, aquisição de alvos e ataque de precisão por uma fração do custo e do ônus organizacional associados ao poder aéreo tradicional (Kunertova, 2023). Sua importância reside menos na sofisticação em si do que na difusão e na compressão de custos. Capacidades antes associadas a forças armadas avançadas agora podem ser improvisadas, adaptadas e empregadas em escala por Estados e, em alguns contextos, por atores por procuração ou grupos não estatais. Em ambientes híbridos, isso amplia a gama de atores capazes de realizar vigilância, intimidação, sabotagem e ataques de autoria plausivelmente negável contra alvos militares e civis. Ao mesmo tempo, a expansão desses sistemas impõe novos encargos defensivos, pois mais sinais precisam ser interpretados, mais plataformas de baixo custo precisam ser interceptadas e mais incidentes ambíguos precisam ser distinguidos do ruído rotineiro de fundo (Kunertova, 2023; Romansky et al., 2024).

O ponto central é melhor compreendido através do conceito de atrito. Novas tecnologias frequentemente prometem clareza, controle e velocidade. No entanto, como argumenta Gardner, elas reduzem algumas formas de atrito ao mesmo tempo em que amplificam outras ou introduzem atritos inteiramente novos (Gardner, 2024). A dependência da rede cria pontos ocultos de falha; a complexidade do software produz comportamento opaco do sistema; a rápida circulação de informações fortalece o engano; e líderes políticos que operam sob pressão da mídia

podem ser pressionados a responder antes que atribuição, intenção e proporcionalidade estejam adequadamente estabelecidas (Turell, Su e Boulanin, 2020). A implicação é que a tecnologia é central para a guerra híbrida não porque transcende a lógica política do conflito, mas porque fornece novas formas de fabricar confusão, explorar dependência, reduzir alguns custos operacionais e aumentar o ônus de decisão do adversário.

4. Vulnerabilidades estratégicas e instrumentos mistos

Com base na mudança analítica desenvolvida acima, esta seção desloca a análise da pergunta sobre quais ferramentas são utilizadas para a questão mais estratégica de quais vulnerabilidades são tomadas como alvo, por que elas importam politicamente e como instrumentos mistos são coordenados para explorá-las. Atores que conduzem campanhas híbridas geralmente não buscam a decisão imediata no campo de batalha ou a conquista territorial direta como seu primeiro objetivo. Mais frequentemente, eles buscam efeitos políticos limitados: enfraquecimento da governabilidade, atraso na resposta, fragmentação de alianças, erosão da legitimidade, alteração de cálculos custo-benefício ou remodelação do ambiente em que a coerção posterior pode ocorrer. O conceito de centro de gravidade de Clausewitz permanece útil aqui porque direciona a atenção para as fontes de poder e de coesão do oponente (Clausewitz, 1976). Em campanhas híbridas contemporâneas, essas fontes frequentemente estão não apenas nas forças armadas, mas também na coesão política, integridade informacional, confiabilidade infraestrutural e capacidade institucional. A guerra híbrida, portanto, visa tanto o funcionamento de uma comunidade política quanto seu aparato militar (Mumford e Carlucci, 2023; Jungwirth et al., 2023; Wrange, 2026).

Isso ajuda a explicar por que o direcionamento psicológico, político e social é central para a guerra híbrida. O objetivo muitas vezes é menos persuadir populações inteiras do que aprofundar divisões já existentes, amplificar a desconfiança e reduzir a capacidade de ação política cole-

tiva. O conceito de Wigell de interferência híbrida como uma "estratégia de divisão" (*wedge strategy*) captura essa dinâmica: atores externos exploram a abertura liberal por meio da diplomacia clandestina, geoeconomia e desinformação para dividir sociedades-alvo e enfraquecer a governabilidade (Wigell, 2019). A análise de Paul e Matthews sobre a "mangueira de incêndio da falsidade" russa mostra de forma semelhante que volume, repetição e inconsistência podem ser eficazes não porque produzem crenças coerentes, mas porque sobrecarregam a atenção, corroem a confiança na verificação e confundem julgamentos (Paul e Matthews, 2016). Mazarr et al. estendem esse argumento sugerindo que a "guerra societal virtual" tem como alvo a confiança, a estabilidade social e o funcionamento das sociedades democráticas, e não apenas as capacidades militares (Mazarr et al., 2019). Trabalhos empíricos recentes reforçam o ponto: operações de influência frequentemente buscam alcance entre comunidades já polarizadas ou marginais, explorando divisões que já existiam antes do próprio ataque (Okholm, 2025).

Essas dinâmicas importam porque as sociedades contemporâneas funcionam cada vez mais como sistemas densamente conectados em rede. Infraestrutura crítica, plataformas digitais, cadeias logísticas, sistemas de mensagens financeiras, serviços em nuvem, redes de comunicação e ambientes de informação eleitoral são profundamente interdependentes. Essa interdependência é relevante porque a densidade dos fluxos transnacionais pode amplificar a sensibilidade e a vulnerabilidade dos sistemas sociais, econômicos, logísticos e institucionais, produzindo efeitos em cascata que ultrapassam rapidamente o setor inicialmente afetado (Lasmar e Santa Rita, 2021). O conceito de interdependência instrumentalizada como arma, desenvolvido por Farrell e Newman, mostra como os atores podem explorar posições centrais nessas redes para vigilância, coerção e disrupção (Farrell e Newman, 2019). Uma lógica semelhante aparece nos marcos de resiliência da União Europeia, que tratam ameaças híbridas como pressões sistêmicas capazes de explorar dependências e gerar efeitos em cascata entre domínios cívicos, de governança e de serviços (Jungwirth et al., 2023). Vulnerabilidade estratégica, portanto, não

significa mais apenas exposição militar na fronteira. Ela também inclui dependência digital, fragilidade institucional, concentração de infraestrutura, desconfiança pública, dependência da cadeia de suprimentos, assimetrias legais e polarização política. Muitos desses elementos pertencem a sistemas civis com relevância militar direta, razão pela qual os debates contemporâneos sobre resiliência enfatizam cada vez mais a colaboração civil-militar e a preparação para toda a sociedade, em vez de apenas a defesa militar estrita (Willmer, 2023; Wrange, 2026).

O valor estratégico dos instrumentos mistos reside em sua capacidade de operar sobre essas vulnerabilidades. Campanhas híbridas raramente dependem de um único ato decisivo. Elas combinam intrusões cibernéticas, operações de influência, proxies, sabotagem, pressão econômica, manipulação legal e sinalização militar calibrada de maneiras que se reforçam mutuamente ao longo do tempo. Robinson et al. definem tais campanhas como usos deliberados de múltiplos instrumentos de poder para afetar a tomada de decisão sem recorrer à guerra convencional aberta (Robinson et al., 2018). Na interferência híbrida, a desinformação frequentemente é acompanhada de pressão geoeconômica e influência política encoberta ou semi-encoberta (Wigell, 2019). Operações cibernéticas também podem contribuir para essa orquestração, não apenas por meio de efeitos técnicos diretos, mas também por consequências de segunda ordem para instituições, alinhamentos de elite e atitudes públicas. Nesse sentido, influência eficaz requer moldar o ambiente informacional, não apenas hackear sistemas ou contas (Whyte, 2020; Whyte e Etudo, 2025). A guerra híbrida opera por meio de sequenciamento, reforço e acumulação: o que importa não são as ferramentas em si, mas sua integração estratégica em torno de vulnerabilidades exploráveis.

Isso também ajuda a explicar por que métodos híbridos contemporâneos podem oferecer alavancagem estratégica seletiva para estados mais fracos, proxies e alguns atores não estatais. A digitalização reduz os custos de certas capacidades disruptivas. Ferramentas cibernéticas, comportamento inautêntico coordenado, sabotagem remota e operações de

influência baseadas em plataformas podem impor sérios encargos sem exigir paridade nas forças convencionais (Willmer, 2023). No entanto, esses métodos não eliminam a hierarquia da política internacional. Sua eficácia depende do acesso, preparação, capacidade organizacional e das vulnerabilidades subjacentes ao alvo. Maschmeyer está certo ao alertar que operações cibernéticas enfrentam trade-offs entre velocidade, intensidade e controle, que limitam sua utilidade estratégica independente (Maschmeyer 2021). É por isso que campanhas híbridas dependem de combinações em vez de substituições. Operações de sabotagem, interrupção cibernética e influência tornam-se mais consequentes quando combinadas com outros instrumentos que exploram a confusão, desconfiança e desempenho degradado que criam dentro de sistemas complexos (Rovner, Cormac e Maschmeyer 2025). Métodos híbridos não tornam atores mais fracos iguais aos mais fortes, mas podem permitir efeitos desproporcionalmente disruptivos sob condições favoráveis.

Definida dessa forma mais restrita, a guerra híbrida permanece útil porque captura uma lógica estratégica específica. Essa lógica começa com a identificação de vulnerabilidades politicamente relevantes, como confiança, legitimidade, coesão, interoperabilidade, infraestrutura crítica e ciclos de decisão, e prossegue por meio do uso coordenado de instrumentos mistos para explorá-los cumulativamente sob condições de ambiguidade. Nem todo ciberataque, campanha de desinformação ou episódio de diplomacia coercitiva constitui guerra híbrida. O termo é valioso analiticamente apenas quando tais ações são integradas a uma campanha politicamente direcionada, projetada para enfraquecer a capacidade de resposta do adversário, mantendo a escalada incerta e contestada, e a atribuição de responsabilidade difícil de estabelecer claramente (Mumford e Carlucci, 2023; Jungwirth et al., 2023).

Conclusão

A guerra híbrida é melhor compreendida como uma forma de coerção historicamente específica, mediada tecnologicamente e politi-

camente dirigida, e não como uma essência totalmente nova da guerra. Sua importância contemporânea não reside na mera combinação de ferramentas militares e não militares, já que métodos mistos de coerção são historicamente recorrentes. Tampouco está apenas na novidade das operações cibernéticas, da inteligência artificial, dos drones, da desinformação ou dos atores por procuração. Esses instrumentos importam, mas não definem sozinhos a guerra híbrida. O que dá valor analítico ao conceito é a lógica estratégica pela qual diferentes instrumentos são coordenados para buscar efeitos políticos sob condições de ambiguidade.

Essa lógica possui três componentes centrais. Primeiro, a guerra híbrida permanece subordinada ao propósito político. Seus métodos são atraentes porque permitem que os atores busquem ganhos políticos limitados, porém significativos, enquanto gerenciam os riscos de atribuição, retaliação e escalada. Segundo, a ambiguidade não é incidental à guerra híbrida. É um de seus principais mecanismos. Ao obscurecer responsabilidade, intenção, limiares e resposta proporcional, a ambiguidade atrasa a tomada de decisão, fragmenta o consenso e aumenta o ônus de interpretação do defensor. Terceiro, a tecnologia intensifica essa lógica ao expandir a velocidade, escala, alcance, opacidade e persistência da ação coercitiva. Infraestruturas digitais, manipulação habilitada por IA, operações cibernéticas, sensores comerciais e drones de baixo custo não aboliram a incerteza; antes, a redistribuem e frequentemente criam novas formas de atrito.

A implicação mais importante é que a guerra híbrida deve ser analisada menos como um catálogo de ferramentas e mais como uma estratégia de exploração de vulnerabilidades. Comunidades políticas contemporâneas dependem de redes densas de confiança, informação, infraestrutura, logística, finanças e coordenação institucional. Esses sistemas são frequentemente civis em sua forma, mas estrategicamente decisivos em sua função. Campanhas híbridas exploram precisamente essas interdependências. Seus efeitos são cumulativos, e não necessariamente decisivos: um incidente cibernético pode reforçar uma operação

de influência; sabotagem pode aprofundar a desconfiança pública; manipulação legal pode atrasar a resposta; pressão econômica pode dividir coalizões; sinalização militar calibrada pode fazer a retaliação parecer custosa demais ou incerta.

Essa definição mais rígida também protege o conceito do uso excessivo. Nem toda operação cibernética hostil, campanha de desinformação, ação encoberta ou medida diplomática coercitiva deve ser chamada de guerra híbrida. O termo é mais útil quando se refere a campanhas politicamente direcionadas que coordenam instrumentos mistos para explorar a ambiguidade e enfraquecer a capacidade do adversário de responder de forma coerente. Nesse sentido, a guerra híbrida não substitui a teoria estratégica clássica. Ela confirma uma das percepções centrais da teoria estratégica clássica: o conflito pode mudar em forma, ritmo e tecnologia, mas continua organizado em torno do propósito político, da incerteza e do esforço de impor a própria vontade a um adversário.

Referências

ALMÄNG, Jan. War, Vagueness and Hybrid War. **Defence Studies** 19 (2), p. 189–204, 2019.

AMARAL, Nilza. **The Iran War Highlights the Creeping Use of AI in Warfare**. Chatham House, March 27, 2026.

BERGAUST, Julie Celine, and SELLEVÅG, Stig Rune. Improved Conceptualising of Hybrid Interference below the Threshold of Armed Conflict. **European Security** 33 (2), p. 169–195, 2024.

BEYERCHEN, Alan. 1992. Clausewitz, Nonlinearity, and the Unpredictability of War. **International Security** 17 (3), p. 59–90, 1992.

BORGHARD, Erica D., and LONERGAN, Shawn W.. The Logic of Coercion in Cyberspace. **Security Studies** 26 (3), p. 452–481, 2017.

BORGHARD, Erica D., and LONERGAN, Shawn W.. 2019. Cyber Operations as Imperfect Tools of Escalation. **Strategic Studies Quarterly** 13 (3), p. 122–145, 2019.

CALISKAN, Murat. Hybrid Warfare through the Lens of Strategic Theory. **Defense & Security Analysis** 35 (1), p. 40–58, 2019.

CANDOLIN, Catharina; CARVIN, Stephanie; CUSUMANO, Eugenio; LASCONJARIAS, Guillaume; LINDSTRÖM, Lauri; MYATT, Madeleine; SAVOLA, Reijo; WIJERMARS, Mariëlle; SMITH, Hanna; SCHROEFL, Josef; LAPPALAINEN, Emma, and VÄLIMÄKI, Jarno. The Future of Cyberspace and Hybrid Threats. **Hybrid CoE Trend Report** 6. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2021.

CHIVVIS, Christopher S. **Understanding Russian "Hybrid Warfare":** And What Can Be Done About It: Addendum. Santa Monica, CA: RAND Corporation, 2017.

CLAUSEWITZ, Carl von. **On War**. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press,1976.

EGLOFF, Florian J., and Myriam Dunn CAVELTY. 2021. Attribution and Knowledge Creation Assemblages in Cybersecurity Politics. **Journal of Cybersecurity** 7 (1), 2021.

FARRELL, Henry, and Abraham L. NEWMAN. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. **International Security** 44 (1), p. 42–79, 2019.

GARDNER, Nikolas. Clausewitzian Friction and Twenty-First-Century War—The Paradox of Technology. **Naval War College Review** 77 (1), 2024.

GLENN, Russell W. Thoughts on 'Hybrid' Conflict. **Small Wars Journal**, March 3, 2009.

HANHIJÄRVI, Heidi. Artificial Intelligence and Foreign Information Manipulation: Chinese and Russian Approaches. **Hybrid CoE Paper** 29. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2026.

HOFFMAN, Frank G. **Conflict in the 21st Century:** The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 2007.

JUNGWIRTH, Rainer, SMITH, Hanna; WILLKOMM, Etienne; SAVOLAINEN, Jukka; VILLOTA, Marina Alonso; LEBRUN, Maxime; AHO, Aleksi; and GIANNOPOULOS, Georgios. **Hybrid Threats:** A Comprehensive Resilience Ecosystem. Luxembourg: Publications Office of the European Union, 2023.

KUNERTOVA, Dominika. Drones Have Boots: Learning from Russia's War in Ukraine. **Contemporary Security Policy** 44 (4), p. 576–591, 2023.

LASMAr, Jorge M., and SANTA RITA, Leonardo Coelho Assunção. Coronavirus, Global Risk and The New International Crisis Management Model. **Conjuntura Internacional** 17 (3), p. 47–61, 2021.

LIBISELLER, Chiara. Hybrid Warfare as an Academic Fashion. **Journal of Strategic** *Studies* 46 (4), p. 858–880, 2023.

LINDSAY, Jon R. Restrained by Design: The Political Economy of Cybersecurity. **Digital Policy, Regulation and Governance** 19 (6), p. 493–514, 2017.

MASCHMEYER, Lennart. The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. **International Security** 46 (2), p. 51–90, 2021.

MAZARR, Michael J. **Mastering the Gray Zone:** Understanding a Changing Era of Conflict. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press. https://press.armywarcollege.edu/monographs/428/, 2015.

MAZARR, Michael J.; BAUER, Ryan M.; CASEY, Abigail; HEINTZ, Sarah A.; MATTHEWS, Luke J. **The Emerging Risk of Virtual Societal Warfare:** Social Manipulation in a Changing Information Environment. Rand: Santa Monica, 2019.

MUMFORD, Andrew, and Pascal CARLUCCI. Hybrid Warfare: The Continuation of Ambiguity by Other Means. **European Journal of International Security** 8 (2), p. 192–206, 2023.

NATO. **Hybrid Threats and Hybrid Warfare Reference Curriculum**. Brussels: NATO / Partnership for Peace Consortium, 2024.

OKHOLM, Christiern Santos. Conditions of Subversive Reach: Comparing Societal and Strategic Factors for Russian Propaganda Outlets' Reach among Western European Fringe Communities. **European Journal of International Security**, First View, p. 1–23, 2025.

PAUL, Christopher, and MATTHEWS, Miriam. **The Russian "Firehose of Falsehood" Propaganda Model:** Why It Might Work and Options to Counter It. Santa Monica, CA: RAND Corporation, 2016.

REUTERS. **US Uses Anthropic AI, B-2 Bombers and Suicide Drones in Iran Strikes**. March 2, 2026.

RID, Thomas. Cyber War Will Not Take Place. **The Journal of Strategic Studies** 35 (1), p. 5–32, 2012.

ROBINSON, Linda, HELMUS, Todd C.; COHEN, Raphael S.; NADER, Alireza; RADIN, Andrew; MAGNUSON, Madeline; and MIGACHEVA, Katya. **Modern Political Warfare:** Current Practices and Possible Responses. Santa Monica, CA: RAND Corporation, 2018.

ROMANSKY, Sofia, HOENIG, Alisa; MEESSEN, Rick; and KRUIJVER, Kimberley. **New Technologies, Changing Strategies:** Five Trends in the Hybrid Threat Landscape. The Hague: The Hague Centre for Strategic Studies and TNO, 2024.

ROVNER, Joshua; CORMAC, Rory, and MASCHMEYER, Lennart. Sand in the Gears: Sabotage in World Politics. **European Journal of International Security**, p. 1–20, 2025.

SOLMAZ, Tarık. 'Hybrid Warfare': A Dramatic Example of Conceptual Stretching. National Security and the Future 23 (1), p. 9–30, 2022.

STEEN, B. J. M. Søndergaard. **Cognitive Warfare**, 2025.

STOKER, Donald, and WHITESIDE, Craig. Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking. **Naval War College Review** 73 (1), p. 12–48, 2020.

THIELE, Ralph. **Artificial Intelligence – A Key Enabler of Hybrid Warfare**. Hybrid CoE Working Paper 6. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2020.

TURELL, Johan; SU, Fei, and BOULANIN, Vincent. Cyber-Incident Management: Identifying and Dealing with the Risk of Escalation. **SIPRI Policy Paper** 55. Stockholm: Stockholm International Peace Research Institute, 2020.

WHYTE, Christopher, and ETUDO, Ugochukwu. Finding the Thieves amongst the Liars: Thinking Clearly about Cyber-Enabled Influence Operations. **European Journal of International Security**, p. 1–19, 2025.

WHYTE, Christopher. Beyond Tit-for-Tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online. **European Journal of International Security** 5 (2), p. 195–214, 2020.

WIGELL, Mikael. 2019. Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy. **International Affairs** 95 (2), p. 255–275.

WILLMER, Lukas. Does Digitalization Reshape the Principle of Non-Intervention? **German Law Journal** 24 (Special Issue 3), p. 508–521, 2023.

WRANGE, Jana. Strategic Autonomy: A 'Quantum Leap Forward on' European Total Defence? **European Journal of International Security**, First View, p. 1–22, 2026.

Jorge M. Lasmar é Coordenador do Programa de Pós-Graduação em Relações Internacionais da PUC Minas e Professor Colaborador do Mestrado em Ciências Policiais e Tecnologias Inovadoras da Academia da Polícia Militar de MG. É doutor em Relações Internacionais pela London School of Economics, LSE, e atua como consultor para diversas organizações internacionais, com ampla experiência na capacitação de forças policiais, militares, de inteligência e instituições públicas.

Cenários de tecnologia, defesa e democracia no Brasil até 2050: autonomia militar interna, heteronomia externa e dependência epistêmica[1]

Jonathan de Araujo de Assis
Raquel Gontijo
Samuel Alves Soares

Resumo

Neste artigo, propomos que os impactos das tecnologias de segurança sobre a democracia e a autonomia estratégica do Brasil até 2050 devem ser compreendidos a partir de uma perspectiva sociotécnica crítica que articula tecnologia, poder e produção de conhecimento. Sustenta-se que o país opera sob uma tensão estrutural entre autonomia militar interna (expressa na capacidade ampliada das Forças Armadas de definir meios e, em larga medida, os próprios fins da defesa) e heteronomia externa, caracterizada por dependência tecnológica e por dependência epistêmica. Em diálogo com a literatura crítica e com os Estudos de Defesa no Brasil, indicamos que o desenvolvimento tecnológico não constitui variável autônoma, mas sim um processo politicamente orientado e con-

1 Este artigo é extensamente baseado no livro ***Tecnologia, Defesa e Democracia no Brasil de 2025***: cenários para a construção do futuro (Gontijo et al., 2025). Gostaríamos de agradecer aos demais membros da equipe de pesquisa, que contribuíram para as reflexões propostas aqui: David P. Succi Junior, Kimberly Alves Digolin, Lívia Peres Milani, Luiza Elena Januário, Mariana da Gama Janot, e Patricia Capelini Borelli.

dicionado por estruturas internacionais de poder. A partir da construção de cenários, argumentamos que a autonomia estratégica depende da articulação entre a autonomia epistêmica, o fortalecimento do controle civil e a definição situada de ameaças.

Abstract

In this article, we propose that the impacts of security technologies on Brazil's democracy and strategic autonomy through 2050 should be understood from a critical socio-technical perspective that links technology, power, and knowledge production. We argue that the country operates under a structural tension between internal military autonomy (expressed in the Armed Forces' expanded capacity to define the means and, to a large extent, the very ends of defense) and external heteronomy, characterized by technological dependence and epistemic dependence. In dialogue with critical literature and Defense Studies in Brazil, we indicate that technological development is not an autonomous variable, but rather a politically oriented process conditioned by international power structures. Based on scenario building, we argue that strategic autonomy depends on the articulation between epistemic autonomy, the strengthening of civilian control, and the situated definition of threats.

1. Introdução

A condução da defesa nacional é uma das atividades primordiais do Estado, sendo, em sua essência, condição para a sobrevivência do Estado e, portanto, para a realização de todas as demais atividades coletivas de um país. As atividades de defesa, em qualquer país, estão em constante processo de transformação, respondendo a pressões externas e a mudanças domésticas. Por isso, é fundamental um olhar atento aos futuros possíveis, para que o planejamento seja feito de forma proativa e propositiva, e não apenas reativa.

Atualmente, o recrudescimento dos conflitos internacionais entre Estados, no contexto da intensificação das rivalidades entre grandes potências e da crise da hegemonia internacional, tem recolocado a dimensão militar no centro dos debates sobre a inserção internacional do Brasil e de outros países do Sul Global. A percepção de instabilidade sistêmica, associada à guerra interestatal como possibilidade concreta, tende a produzir respostas orientadas pela lógica da urgência, nas quais a ampliação das capacidades materiais de defesa aparece como solução imediata. No caso brasileiro, esse movimento articula demandas internas por fortalecimento das Forças Armadas com pressões externas decorrentes da reorganização do sistema internacional, resultando na demanda pela ampliação dos gastos em defesa.

Nesse contexto, a tecnologia emerge como elemento estruturante do debate estratégico. A incorporação de sistemas avançados, o investimento em inovação e a busca por autonomia tecnológica passam a ser apresentados como condições necessárias – e até suficientes – para a inserção internacional do país. Essa associação entre tecnologia, poder e autonomia, embora amplamente difundida, é analiticamente problemática, na medida em que obscurece dimensões centrais da relação entre tecnologia, defesa e democracia.

O Brasil convive com uma tensão estrutural entre duas dinâmicas contraditórias: de um lado, uma autonomia militar interna significativa; de outro, uma condição de heteronomia externa, marcada por dependência tecnológica e, de forma mais profunda, por dependência epistêmica. Essa dinâmica desloca o foco da definição de objetivos estratégicos para a acumulação de capacidades, fazendo com que a tecnologia deixe de ser um instrumento subordinado à estratégia e passe a condicioná-la, invertendo a relação entre meios e fins.

Partimos, portanto, de uma perspectiva que articula tecnologia, poder e produção de conhecimento, compreendendo o desenvolvimento tecnológico como fenômeno inserido em estruturas de poder. Nesse quadro, as tecnologias de segurança não apenas respondem a ameaças, mas também moldam sua definição, organizando práticas institucio-

nais e decisões estratégicas. Do mesmo modo, os futuros são concebidos como construções que orientam a ação e a demanda presentes; em outras palavras, a elaboração de cenários estrutura prioridades materiais, tecnológicas e institucionais, ao delimitar horizontes do que é possível e desejável.

Assim, buscando contribuir para o diálogo sobre o tema, neste artigo buscamos analisar como a incorporação de tecnologias de segurança no Brasil se relaciona com a dependência epistêmica e os limites da autonomia estratégica e propomos uma breve reflexão a partir de três cenários de futuro: tendencial, desejável e indesejável. A discussão proposta aqui é fruto de pesquisas conduzidas pela equipe do Grupo de Elaboração de Cenários e Estudos de Futuro (GECEF) desde 2019[2].

A discussão aqui proposta é relevante para situar o pensamento sistemático sobre o futuro e sobre a incerteza como orientador para o planejamento e as decisões em torno da política de defesa. Esta é uma área que opera, necessariamente, com horizontes temporais alargados, devido ao tempo necessário ao desenvolvimento e à aquisição de equipamentos, bem como a preparação das forças[3]. Sem o olhar para o futuro, o país estaria restrito a se preparar para problemas que já passaram. De

---

2 Este artigo traz contribuições de pesquisa já concluída sobre o futuro da defesa e da democracia no Brasil, que contou com financiamento do Programa de Cooperação Acadêmica em Defesa Nacional (PROCAD-DEFESA), edital nº 15/2019, processo 23038.004236/2019-10, da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, à qual expressamos nossos agradecimentos. Este artigo também traz contribuições de pesquisa em andamento sobre o futuro da governança internacional em paz e segurança, que conta com financiamento do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), via chamada Universal (chamada CNPq/MCTI nº 10/2023; processo nº 408946/2023-7), ao qual também expressamos nosso agradecimento.

3 O Programa de Submarinos (PROSUB) do Brasil, por exemplo, foi iniciado em 2008, tendo como um de seus objetivos a produção do primeiro submarino a propulsão nuclear do Brasil, cuja previsão de lançamento é (atualmente) 2033 (Marinha do Brasil, 2025). Isso significa que os recursos em que o governo brasileiro escolheu investir quando o PROSUB foi iniciado não deveriam ser pensados para lidar com as ameaças existentes em 2008, mas sim com as ameaças que se imaginava que existiriam décadas adiante.

fato, é comum o dizer de que as forças armadas estão sempre preparadas para lutar a última guerra que lutaram, e não a próxima (Soutou, 2012, p. 43). Assim, para o planejamento da defesa e para a incorporação qualificada de novas tecnologias no setor, o olhar para a História é necessário, já que é preciso aprender as lições do passado; mas também é necessário o pensamento rigoroso sobre o futuro, sobre aquilo que não é apenas repetição, mas mudança e incerteza.

Este artigo é organizado em cinco seções, incluindo esta introdução. Na próxima seção, discutimos a relação entre a incorporação de tecnologias às atividades de defesa e as dinâmicas de dependência internacional. Em seguida, mobilizamos a discussão sobre imaginários para problematizar como as visões de futuro moldam e são moldadas pelas tecnologias características do setor. Na seção 4, apresentamos a construção de três cenários de futuro sobre a incorporação de tecnologias à defesa nacional. E o artigo se encerra com algumas reflexões finais.

2. Tecnologia, poder e produção de dependência

A tecnologia, particularmente no campo da defesa, não pode ser compreendida como um instrumento neutro ou como uma variável autônoma. Seu desenvolvimento deve ser analisado como fenômeno sociotécnico, isto é, como resultado de processos historicamente situados que articulam conhecimento, poder e instituições (Jasanoff, 2004). Essa perspectiva permite deslocar a análise da dimensão técnica para as condições políticas e estruturais que orientam a produção, a circulação e o uso das tecnologias de segurança. A associação recorrente entre sofisticação tecnológica e autonomia estratégica repousa em uma construção ideológica que naturaliza a centralidade da tecnologia, operando sob uma lógica cumulativa segundo a qual capacidades avançadas conduziriam automaticamente à ampliação do poder e da autonomia. Tal interpretação, contudo, ignora que o desenvolvimento tecnológico ocorre em estruturas internacionais assimétricas, nas quais as capacidades produtivas e cognitivas são concentradas (Neuman, 2006, 2010).

Nesse sentido, conforme argumentam Saint-Pierre e Assis (2025), a centralidade atribuída à tecnologia pode operar como forma de fetichização, ao deslocar a atenção para os meios e obscurecer a dimensão política da autonomia estratégica. Esse deslocamento contribui para a inversão da relação entre meios e fins, fazendo com que a estratégia passe a ser orientada pelas capacidades disponíveis e desejadas, e não o contrário. Tal dinâmica insere-se em processos mais amplos de produção de dependência, na medida em que a incorporação tecnológica por países periféricos ocorre por meio de cadeias globais estruturadas por atores centrais, que definem padrões técnicos, protocolos e modelos organizacionais, reproduzindo condições que limitam a ação autônoma (Kaldor, 1986).

A dimensão mais profunda dessa dependência é epistêmica. A colonialidade do poder permite compreender como as hierarquias globais se reproduzem por meio da imposição de padrões de conhecimento, manifestando-se na internalização de categorias analíticas e de modelos estratégicos produzidos em outros contextos (Quijano, 2000). No campo da defesa, isso se expressa na adoção de paradigmas exógenos, sem mediação crítica, de modo que são incorporados não apenas instrumentos técnicos, mas igualmente em categorias que orientam sua interpretação e emprego. Como argumenta Wulf (1979),

> a importação de armas modernas dos países industrializados não interessa apenas aos produtores das metrópoles ou a seus coprodutores na periferia, mas as forças armadas também desejam ser equipadas com os mais recentes artefatos produzidos pelos laboratórios de pesquisa e desenvolvimento dos países industrializados. **A oposição à importação de equipamentos modernos seria inconsistente com seu profissionalismo**. Portanto, a demanda por armas e a exigência de colaboração estrangeira se reforçam mutuamente; ao importar doutrinas e tecnologias militares, não apenas o modo de produção do país fornecedor é importado, **mas também a dependência dos militares na periferia é perpetuada simultaneamente**. (Wulf 1979, 253, tradução nossa, grifo nosso).

A segurança pode ser compreendida como tecnologia política, o que permite problematizar a ideia de que as tecnologias respondem a ameaças previamente dadas. Ao contrário, participam da produção dessas ameaças, estruturando práticas institucionais e definindo os termos em que determinados fenômenos são enquadrados como problemas de segurança. Nesse sentido, sistemas de vigilância, inteligência artificial e plataformas de análise de dados não constituem apenas ferramentas operacionais, senão também dispositivos que reconfiguram o exercício do poder e ampliam a capacidade de intervenção estatal. Tal leitura permite compreender a segurança como forma historicamente situada de organização do poder, orientada pela produção e gestão de ameaças, e não apenas como resposta a elas (Neocleous, 2008).

A superação da dependência epistêmica constitui condição indispensável para qualquer forma consistente de autonomia estratégica, implicando a produção de conhecimento situado e a capacidade de dialogar criticamente com paradigmas dominantes. As implicações desse argumento para a relação entre tecnologia, decisão política e democracia serão exploradas na seção seguinte.

Por fim, sustenta-se que o principal desafio para países como o Brasil não reside na ausência de acesso a tecnologias avançadas, mas na dificuldade de articulá-las a um projeto estratégico coerente. Na ausência dessa articulação, a incorporação tecnológica tende a reproduzir dependências e a limitar a capacidade de ação autônoma, reforçando a heteronomia externa mesmo em contextos de relativa autonomia institucional.

A autonomia estratégica não se reduz à dimensão material das capacidades militares. Seu caráter eminentemente político envolve a capacidade de decidir sobre o emprego dos meios disponíveis e sobre a definição dos fins da defesa, deslocando o foco da acumulação de capacidades para a articulação entre meios, objetivos e interpretações do ambiente internacional. Tem sido recorrente, inclusive em setores progressistas (Amorim, 2026), associar autonomia estratégica à aquisição de tecnologias avançadas, reduzindo-a a uma questão técnica. Tal leitura dissocia

os meios de seus contextos de uso e desconsidera as condições políticas e institucionais que orientam sua mobilização, tornando-se ainda mais limitada quando baseada exclusivamente em comparações materiais.

A autonomia estratégica depende da capacidade de formular interpretações próprias sobre o sistema internacional, envolvendo a definição de ameaças, interesses e estratégias coerentes com a posição do país. Na ausência dessa dimensão interpretativa, a posse de capacidades tecnológicas pode reforçar padrões de dependência, em vez de ampliar a autonomia. Nesse sentido, a dependência epistêmica constitui um obstáculo central. A internalização de categorias analíticas e de modelos estratégicos produzidos em outros contextos se materializa não apenas no plano das ideias, como também em práticas institucionais, modelos de planejamento e processos decisórios, resultando em referenciais desalinhados às condições nacionais. Esse deslocamento compromete a coerência das políticas de defesa, dificultando a articulação entre as capacidades e os objetivos.

A construção da autonomia estratégica exige a institucionalização de processos de reflexão crítica sobre modelos externos. No caso brasileiro, a autonomia militar interna apresenta caráter ambivalente: embora possa favorecer certa independência decisória, permanece atravessada por concepções colonizadas e por uma retórica pouco ancorada às condições do país. Ao mesmo tempo, a concentração da definição de prioridades estratégicas nesses atores ocorre sem a devida condução política. Como argumentam Soares e Mathias (2002, p. 86), após o término do regime autoritário, as forças armadas brasileiras conservaram relativo grau de autonomia sobre certos temas, ainda que formalmente subordinadas ao novo governo. Sob essa perspectiva, definições sobre a demanda por tecnologias tendem a ser compreendidas como "meramente técnicas" e de competência exclusiva dos militares.

A ausência de coordenação interinstitucional e de direção política limita a articulação entre a autonomia militar interna e um projeto estratégico mais amplo, resultando em uma definição fragmentada das capacidades. Essa fragmentação reforça a dependência epistêmica ao

favorecer a adoção de modelos externos como compensação pela falta de integração analítica. Nesse contexto, a relação entre tecnologia e autonomia permanece dissociada de um projeto político, o que separa os fins da defesa das escolhas relativas ao desenvolvimento, à inserção internacional e aos interesses da sociedade brasileira. A construção da autonomia estratégica exige, portanto, a articulação entre três dimensões: material, epistêmica e institucional. A ausência de qualquer uma delas compromete a capacidade de formular uma estratégia coerente.

3. Tecnologia e imaginários de futuro

Uma dimensão ainda pouco valorizada é que a relação entre tecnologia e estratégia não pode ser compreendida sem considerar os modos pelos quais os futuros são imaginados, construídos e institucionalizados. As tecnologias de defesa não são desenvolvidas apenas em resposta a ameaças previamente identificadas, e sim produzidas no interior de regimes de antecipação que estruturam sua própria concepção. Essa perspectiva desloca a análise da tecnologia como variável autônoma para sua inserção em processos mais amplos de produção de sentido. Ao antecipar possíveis formas de conflito, os cenários delimitam os horizontes de inteligibilidade da ação estratégica, de modo que os futuros não são apenas previstos, mas produzidos, influenciando a alocação de recursos e a definição de capacidades. Conforme argumentam Succi Junior, Castro e Soares (2024), a construção de cenários no campo da defesa não constitui um exercício meramente especulativo, mas sim um dispositivo central de produção de sentido estratégico, por meio do qual possíveis formas de conflito são antecipadas, encenadas e, desse modo, tornadas operativas para a tomada de decisão.

Essa dinâmica é central para compreender a dependência epistêmica no campo da defesa. Quando cenários são construídos com base em referenciais externos, as tecnologias desenvolvidas para enfrentá-los tendem a reproduzir esses referenciais. Nesse processo, não apenas os meios técnicos são importados, como também as formas de ima-

ginar o futuro, reforçando padrões de dependência e limitando a formulação de alternativas. A relação entre tecnologia e futuro é constitutiva: tecnologias disponíveis influenciam os cenários considerados críveis, enquanto estes orientam o desenvolvimento tecnológico. Essa circularidade tende a produzir um fechamento analítico, privilegiando determinadas possibilidades. Assim, a definição do que constitui um cenário plausível não é neutra, mas resulta de processos atravessados por relações de poder e por estruturas de conhecimento. Essa relação é capturada pelo conceito de imaginários sociotécnicos, definido como definido como

> […] visões de futuro desejáveis, mantidas coletivamente, estabilizadas institucionalmente e publicamente performadas, animadas por entendimentos compartilhados sobre formas de vida e ordens sociais alcançáveis por meio de, e que suportam, avanços na ciência e na tecnologia. (Jasanoff, 2015, p. 4, tradução nossa).

Os imaginários não apenas codificam visões sobre o que é possível nos campos científico e tecnológico, mas também apontam formas sociais teleológicas, de como a vida deve, ou não, ser; portanto, expressam o entendimento compartilhado pela sociedade do que é bom e ruim (Jasanoff, 2015, p. 4). Como argumenta Sismondo (2020, p. 505), a utilidade analítica do conceito de imaginários sociotécnicos é a forma como certas visões podem ser compreendidas como infraestruturas de futuros imaginados e planejados. Nesse sentido, a possibilidade de delinear o espaço da escolha vincula os imaginários sociotécnicos diretamente ao campo da ação política. Dessa forma, ainda que temporal e culturalmente situados, os imaginários constituem visões de futuro coletivas, duráveis e performáveis; e, conforme sugere sua qualidade "sociotécnica", são tanto produtos quanto instrumentos da coprodução entre ciência, tecnologia e sociedade.

No campo da defesa, essa dinâmica se expressa na centralidade atribuída a conflitos de alta intensidade, disputas tecnológicas entre gran-

des potências e operações baseadas em sistemas avançados, que passam a orientar o desenvolvimento tecnológico. Esse processo de constituição imaginária da demanda militar é ainda amplificado pelo que Rossiter (2025) denomina *hype* tecnológico, definido como

> [...] condição de expectativas excessivas entre atores sociais sobre tecnologias emergentes [...] expectativas podem ser consideradas excessivas quando uma tecnologia emergente gera um otimismo generalizado sobre seu impacto revolucionário no curto prazo, antes que seu verdadeiro potencial possa ser conhecido. (Rossiter, 2025, p. 614, tradução nossa).

Rossiter (2025) demonstra que contextos de rivalidade estratégica intensa – como a atual competição sino-americana no campo da inteligência artificial – são catalisadores sistemáticos do *hype*, na medida em que a pressão contínua para produzir e implantar novos sistemas amplifica as expectativas quanto ao seu potencial transformador. Para países periféricos à margem dessa rivalidade, o *hype* tecnológico gerado pelos atores centrais funciona como um mecanismo adicional de naturalização da dependência. Isto é, ao difundir ideias sobre determinadas tecnologias como necessidades estratégicas urgentes e inexoráveis, estreita o horizonte de escolhas tecnopolíticas disponíveis e reforça a demanda por sistemas cujo desenvolvimento permanece concentrado nos países do núcleo orgânico do sistema capitalista internacional. Tal orientação frequentemente não corresponde às condições dos países periféricos, o que acarreta uma deturpação que compromete a autonomia estratégica.

A incorporação de tecnologias de segurança deve, portanto, ser analisada no âmbito desses regimes de imaginários e de antecipação. Tais tecnologias emergem em resposta a expectativas sobre formas futuras de conflito e de organização social, participando da construção desses futuros. A autonomia estratégica depende, assim, não apenas da capacidade de desenvolver ou adquirir tecnologias, mas também de definir os futuros a partir dos quais essas tecnologias são concebidas. Quando ce-

nários são reproduzidos de forma acrítica, a tecnologia tende a reforçar a dependência epistêmica, mesmo diante de avanços materiais.

Em consonância com essa leitura, Pretorius (2008) argumenta que o isomorfismo militar – a tendência de forças armadas ao redor do mundo a assemelharem-se em doutrina, armamentos e organização – não resulta de imposição direta por parte das potências centrais ou dominantes, mas de um processo dialético pelo qual o imaginário de segurança da sociedade receptora é constituído por discursos que naturalizam os modelos tecnológico-militares difundidos pelas potências hegemônicas. Nesses termos, entendemos que a dependência epistêmica das forças armadas brasileiras não resulta de pressão externa direta, mas de um processo histórico de socialização pelo qual os imaginários militares são constituídos por expectativas normativas oriundas de países centrais do sistema internacional.

A construção de cenários constitui, portanto, uma dimensão central da política de defesa e não pode ser tratada como uma atividade técnica isolada. Sua definição exige reflexão crítica sobre as condições do país, sua inserção internacional e suas prioridades estratégicas. Além disso, a articulação entre tecnologia e imaginários de futuro tensiona a relação entre a defesa e a democracia. Cenários que enfatizam ameaças internas ou riscos difusos tendem a legitimar tecnologias de vigilância e controle, ampliando a intervenção estatal e tensionando os limites democráticos.

Em contextos em que a distinção entre defesa e segurança interna é difusa, tecnologias de uso dual ampliam essa sobreposição ao serem aplicadas em contextos domésticos. Nesses casos, os cenários futuros influenciam diretamente a organização das relações entre o Estado e a sociedade. Ao explicitar diferentes formas de articulação entre tecnologia, poder e autonomia, os cenários permitem problematizar trajetórias possíveis e seus efeitos sobre a relação entre defesa e democracia, preparando a apresentação dos cenários – desejável, indesejável e tendencial – na seção seguinte.

4. Cenários de futuros, tecnologias de segurança e trajetórias de autonomia

Cenários não são previsões, e sim configurações analíticas que explicitam diferentes articulações entre capacidades materiais, estruturas institucionais e produção de conhecimento (Januário, Gontijo, Soares, 2024). Eles evidenciam que o futuro da tecnologia na defesa não está determinado, e sim condicionado por escolhas políticas e institucionais. Operam, assim, como instrumento analítico para explicitar as condições em que diferentes trajetórias podem se consolidar, contribuindo para qualificar o debate sobre defesa no Brasil. A formulação de cenários desejável, indesejável e tendencial, que sintetizamos a seguir, torna visíveis os efeitos políticos e epistêmicos de distintas formas de incorporação tecnológica na defesa. O elemento decisivo não reside na disponibilidade de tecnologias, e sim nas formas de sua interpretação, apropriação e mediação institucional. A variável crítica corresponde ao conjunto de relações sociais e políticas que orienta a sua utilização. Assim, a análise estrutura-se em três dimensões: definição autônoma de ameaças, grau de dependência epistêmica e articulação entre tecnologia e projeto estratégico.

A abordagem metodológica que adotamos para a elaboração dos cenários articula análise qualitativa de caráter sociotécnico e instrumentos prospectivos, compreendendo tecnologia, defesa e autonomia como dimensões interdependentes (Gontijo et al., 2025). A discussão sobre futuros possíveis que dá origem aos cenários baseia-se em uma análise sistemática do tema, com a identificação de atores relevantes e temas centrais, a partir do estudo do passado e do presente. Isso permite uma reflexão sobre os possíveis elementos de continuidade e mudança, com a identificação de processos e dinâmicas já em curso e a problematização das potencialidades decorrentes da incerteza.

Após esse trabalho de pesquisa, identificamos perguntas centrais para pensar o futuro da defesa no Brasil, como as indicadas a seguir:

- Como será a interação do Sul Global com as grandes potências?
- Haverá transformações no regime de controle de armas nucleares?
- Como será construída a governança global digital?
- Como será o uso de sistemas autônomos no Brasil?
- Como será o acesso de diferentes países às atividades espaciais?
- Como será estruturada a política industrial de defesa do Brasil?
- Como serão os mecanismos de controle político sobre as atividades de defesa e a segurança pública?

Para cada pergunta, elaboramos hipóteses sobre os possíveis desdobramentos. A partir disso, diferentes combinações dessas hipóteses nos permitem explorar mais detidamente alguns cenários de futuro, com foco em um horizonte de 25 anos[4]. Adotamos três vias para orientar os cenários: identificação dos processos tendenciais, visão sobre o que seria desejável e visão sobre o que seria indesejável[5]. Aqui, cabe uma observação de que essas demarcações são inerentemente subjetivas, e refletem as percepções e valores dos pesquisadores que participaram da construção dos cenários. Evidentemente, outros grupos poderiam trazer visões diferentes sobre o que seria desejável ou não.

O cenário tendencial expressa a continuidade das dinâmicas atuais, combinando avanços pontuais em capacidades com persistência da dependência epistêmica. Podemos visualizar um processo marcado por iniciativas políticas fragmentadas e pela ausência de um projeto estratégico integrado. A definição de ameaças permaneceria influenciada por referenciais externos, enquanto as tecnologias incorporadas refletiriam

4 Deve-se notar que este é um horizonte relativamente longo, no qual podem ocorrer muitas rupturas em comparação com a realidade atual. Essa escolha se justifica pelo longo período que, muitas vezes, é necessário para desenvolver, produzir e incorporar novos sistemas tecnológicos às atividades de defesa. Paralelamente, esse tipo de horizonte longo nos permite explorar, com alguma liberdade, as possibilidades de futuros para além de meras projeções das tendências atuais.

5 Os cenários sintetizados aqui são apresentados de forma mais detalhada em Gontijo et al. (2025).

ambivalência entre reprodução e tentativa de autonomia, resultando no uso limitado das capacidades disponíveis. Trata-se de uma inércia estruturada, na qual a ausência de decisões estratégicas explícitas restringe a transformação, mantendo a tecnologia como vetor simultâneo de capacitação e de dependência.

O cenário indesejável caracteriza-se pela intensificação da heteronomia externa e da dependência epistêmica. A incorporação tecnológica ocorreria de forma desarticulada e orientada por paradigmas exógenos, cuja centralidade produziria fetichização e obscureceria a dimensão política da autonomia. A definição de ameaças seria influenciada por referenciais externos, o que geraria processos e capacidades desalinhados às condições nacionais e reproduziria um ciclo de dependência. O cenário inclui a expansão do uso de tecnologias de segurança em contextos domésticos, ampliando práticas de vigilância e controle, açulando formas de violência, e reforçando a adoção de modelos externos diante da ausência de condução política.

Por fim, o cenário desejável supõe a ampliação da autonomia decisória, com a definição soberana de meios e fins. A incorporação tecnológica ocorreria no âmbito de um projeto estratégico coerente, sustentado por um campo analítico próprio e orientado pelos interesses da sociedade brasileira. A dependência epistêmica seria reduzida, permitindo que a tecnologia deixasse de operar como vetor de dependência e passasse a integrar um processo de construção de autonomia. Nesse contexto, a tecnologia seria subordinada à estratégia, com critérios de seleção de capacidades definidos por objetivos políticos, reduzindo o descolamento entre meios e fins. Esse cenário envolve o fortalecimento da condução política e da coordenação institucional, integrando tecnologia a políticas de inovação, desenvolvimento e inserção internacional.

A análise comparada indica que a autonomia estratégica não depende primariamente da disponibilidade tecnológica, e sim da capacidade de articulá-la a um projeto político coerente, no qual a dimensão epistêmica ocupa posição central e é a condição indispensável para a superação da dependência estratégica. Os cenários trazem a

provocação de que o futuro da incorporação de tecnologias na defesa não está determinado, sendo condicionado por escolhas políticas e institucionais.

5. Considerações Finais

A análise desenvolvida aponta que a relação entre tecnologia, defesa e democracia no Brasil não pode ser compreendida a partir de uma perspectiva centrada exclusivamente na dimensão material das capacidades. Como proposto, a tecnologia insere-se em estruturas de poder e em processos de produção de conhecimento que condicionam sua direção, seus usos e seus efeitos.

A tensão entre autonomia militar interna e heteronomia externa constitui um elemento estruturante dessa problemática. De um lado, observa-se a ampliação da capacidade das instituições militares de definir meios e prioridades no âmbito doméstico e de estabelecer os marcos dos documentos normativos de Defesa. De outro, verifica-se a persistência de uma inserção internacional marcada por dependência tecnológica e, sobretudo, epistêmica. A dependência incide diretamente sobre a capacidade de formular os termos do debate estratégico, orientando a definição de ameaças, a seleção de capacidades e a construção de cenários de futuro.

A partir da síntese dos três cenários mobilizados (desejável, indesejável e tendencial) sustentamos que o elemento decisivo para a definição das trajetórias possíveis não reside na disponibilidade de tecnologias, mas nas formas pelas quais essas tecnologias são interpretadas e articuladas a projetos estratégicos, o que depende da articulação entre as dimensões material, epistêmica e institucional. A fragilização de qualquer uma dessas dimensões compromete a capacidade de formular estratégias coerentes e consistentes.

Decolonizar as formas de compreender a realidade é tarefa essencial para a superação da dependência epistêmica e constitui, portanto, condição indispensável para a construção da autonomia estratégica. Este

processo articula-se diretamente com a relação entre tecnologia e imaginários de futuro, que desempenham papel decisivo na organização das práticas de defesa. Os riscos de imaginários colonizados agravam ainda mais o quadro e até impedem a concretização da autonomia. A capacidade de definir os futuros a partir dos quais a estratégia é concebida constitui uma dimensão central da autonomia, na medida em que condiciona a forma como as ameaças são interpretadas e enfrentadas.

O desafio central para o Brasil – e para os países do entorno – não reside simplesmente na ampliação das capacidades tecnológicas, mas na construção de um projeto estratégico capaz de articular tecnologia, defesa e democracia de forma coerente com os interesses da sociedade. Isso implica rearticular a relação entre meios e fins, fortalecer os mecanismos de controle civil e promover a produção de conhecimento decolonizado, capaz de orientar a formulação de políticas públicas. A autonomia estratégica deve ser compreendida como um processo em construção, dependente de escolhas políticas e institucionais que definem os caminhos possíveis para o futuro.

Referências bibliográficas

AMORIM, Celso. A estratégia da paz. **Carta Capital**, 27 jan. 2026. Disponível em: https://www.cartacapital.com.br/opiniao/a-estrategia-da-paz/. Acesso em 20 abr. 2026.

GONTIJO, R. et al (orgs.). **Tecnologia, Defesa e Democracia no Brasil de 2025:** cenários para a construção do futuro. São Paulo: Cultura Acadêmica Editora, 2025.

JANUÁRIO, Luiza Elena; GONTIJO, Raquel; SOARES, Samuel Alves (Orgs.). **A consciência de Janus e o futuro na política internacional:** Ferramentas para elaboração de cenários, análise e ação. São Paulo: Cultura Acadêmica, 2024.

JASANOFF, Sheila. **States of Knowledge:** The Co-production of Science and Social Order. London: Routledge, 2004.

JASANOFF, S. Future Imperfect: Science, Technology, and the Imaginations of Modernity. In: JASANOFF, S. KIM, S. H. (Orgs.) **Dreamscapes of Modernity**. Chicago, London: University of Chicago Press, 2015.

KALDOR, M. **El arsenal barroco**. Madrid: Siglo XXI de España Editores, 1986.

MARINHA DO BRASIL. **PROSUB**. Publicado em 17/08/2020, atualizado em 14/01/2025. Disponível em: https://www.marinha.mil.br/programas-estrategicos/prosub. Acesso em 20 abr. 2026.

NEOCLEOUS, Mark. **Critique of Security**. Edinburgh: Edinburgh University Press, 2008.

NEUMAN, Stephanie. Defense Industries and Global Dependency. **Orbis**, v. 50, n. 3, p. 429-451, 2006.

NEUMAN, Stephanie. Power, influence, and hierarchy: defense industries in a unipolar world. **Defence and Peace Economics**, v. 21, n. 1, p. 105-134, 2010.

PRETORIUS, J. The Security Imaginary: Explaining Military Isomorphism. **Security Dialogue**, v. 39, n. 1, p. 99–120, 2008. DOI: 10.1177/0967010607086825.

QUIJANO, Aníbal. Colonialidad del poder, eurocentrismo y América Latina. In: LANDER, Edgardo (org.). **La colonialidad del saber**: eurocentrismo y ciencias sociales. Buenos Aires: CLACSO, 2000. p. 201-246.

ROSSITER, A. Hyping emerging military technology: probing the causes and consequences of excessive expectations. **International Relations**, v. 39, n. 4, p. 612–631, 2025. DOI: 10.1177/00471178231186256.

SAINT-PIERRE, Héctor Luis; ASSIS, Jonathan de Araujo de. Da essência da tecnologia à dependência estratégica: uma agenda para os Estudos de Defesa. **Revista Brasileira de Estudos de Defesa**, v. 12, n. 1, p. 1-23, 2025.

SISMONDO, S. Sociotechnical imaginaries: An accidental themed issue. **Social Studies of Science**, v. 50, n. 4, 2020.

SOARES, S.; MATHIAS, S. Forças Armadas, orçamento e autonomia militar. **Perspectivas**, v. 24/25, 2002.

SOUTOU, Georges-Henri. "How history shapes war". In: BOYER, Y.; LINDLEY-FRENCH, J. (eds.). **The Oxford Handbook of War**. New York: Oxford University Press, 2012.

SUCCI JUNIOR, D. P.; CASTRO, H. S.; SOARES, S. A. Staging the Conflicts to Come: Visions of the Future-Tracing Security Practices. In: GRUSZCZAK, A.; KAEMPF, S. (ed.). **Routledge Handbook of the Future of Warfare**. London and New York: Routledge, 2024.

WULF, Herbert. "Dependent militarism in the periphery and possible alternative concepts". In Neuman, Stephanie and Harkavy, Robert (eds.). **Arms transfers in the modern world**. New York: Praeger Publishers, 1979.

Raquel Gontijo · Professora do Departamento de Relações Internacionais na PUC Minas. Doutora em Relações Internacionais pelo PPGRI San Tiago Dantas (UNESP, UNICAMP, PUC-SP). Vice-coordenadora do Grupo de Elaboração de Cenários e Estudos de Futuro (GECEF), pesquisadora do Grupo de Estudos de Defesa e Segurança Internacional (GEDES).

Jonathan de Araujo de Assis · Pesquisador de pós-doutorado no Instituto de Políticas Públicas e Relações Internacionais (IPPRI-Unesp), projeto "Defesa, Tecnologia e Estudos de Futuro" – Pro-Defesa V (nº 88887.310637/2026-00). Doutor em Relações Internacionais pelo PPGRI San Tiago Dantas (UNESP, UNICAMP, PUC-SP). Pesquisador do Grupo de Estudos de Defesa e Segurança Internacional (GEDES) e do Instituto Nacional de Ciência e Tecnologia para Estudos sobre os Estados Unidos (INCT-INEU).

Samuel Alves Soares · Professor da Unesp e do PPGRI San Tiago Dantas (UNESP, UNICAMP, PUC-SP). Pesquisador do Grupo de Estudos de Defesa e Segurança Internacional, Coordenador do Grupo de Elaboração de Cenários e Estudos de Futuro e vice-coordenador do Instituto Nacional de Ciência e Tecnologia para Estudos sobre os Estados Unidos (INCT-INEU). Coordenador da Área de Ciência Política e Relações Internacionais da CAPES. Pesquisador do CNPq.

A Fundação Konrad Adenauer é uma fundação política da República Federal da Alemanha que, naquele país e no plano internacional, vem trabalhando em prol dos direitos humanos, da democracia representativa, do Estado de Direito, da economia social de mercado, da justiça social e do desenvolvimento sustentável.

Os principais campos de atuação da Fundação Konrad Adenauer são a formação política, o desenvolvimento de pesquisas aplicadas, o incentivo à participação política e social e a colaboração com as organizações civis e os meios de comunicação.

A Fundação Konrad Adenauer está no Brasil desde 1969 e atualmente realiza seu programa de cooperação internacional por meio da Representação no Brasil, no Rio de Janeiro, trabalhando em iniciativas próprias e em cooperação com parceiros locais. Com suas publicações, a Fundação Konrad Adenauer pretende contribuir para a ampliação do debate público sobre temas de importância nacional e internacional.

Os *Cadernos Adenauer* versam sobre temas de interesse público, relacionados ao desenvolvimento de uma sociedade democrática.

Privilegiam-se artigos que abarcam temas variados nos campos da política, da situação social, da economia, das relações internacionais e do direito.

As opiniões externadas nas contribuições desta série são de exclusiva responsabilidade de seus autores.

KONRAD ADENAUER STIFTUNG

adenauer-brasil@kas.de
www.kas.de/brasil