UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 2, e96728, p. 1-27, jun. 2026 • https://dx.doi.org/10.5902/2357797596728
Submissão: 14/05/2026 • Aprovação: 14/05/2026 • Publicação: 1º/06/2026

Artigos Dossiê

Da lição estratégica à capacidade nacional: governança em defesa, capital humano tecnológico e Base Industrial de Defesa no Brasil

From strategic lessons to national capability: defence governance, technological human capital, and the Defence Industrial Base in Brazil

Marcelo Carvalho Ribeiro[I]
Mauro Beirão[II]

[I]Universidade Federal de Santa Maria, Santa Maria, RS, Brasil
[II]AEL Sistemas S.A., Porto Alegre, RS, Brasil

Resumo

Este artigo examina como a governança em defesa pode contribuir para transformar lições estratégicas contemporâneas e demandas tecnológicas emergentes em capacidades nacionais sustentáveis para o Brasil. O argumento central é que o desafio brasileiro não consiste apenas em identificar capacidades críticas, como sistemas não tripulados, inteligência artificial, ciberdefesa, logística resiliente, defesa antiaérea, defesa costeira e dissuasão estratégica. O desafio decisivo está em institucionalizar mecanismos de governança capazes de priorizar, financiar, monitorar e coordenar essas capacidades por meio do Ministério da Defesa, das Forças Armadas, da Base Industrial de Defesa, das universidades, dos centros de pesquisa e do setor produtivo. O artigo adota uma perspectiva de governança em defesa baseada em liderança, estratégia e controle, com ênfase em governança de portfólio, gestão de riscos, *assurance*, indicadores de desempenho, coordenação interagências e interface civil qualificada. Metodologicamente, combina análise documental, revisão bibliográfica seletiva e interpretação institucional de tendências contemporâneas em defesa, tecnologia e inovação. A contribuição principal consiste em propor uma matriz de governança de capacidades tecnológicas em defesa para o Brasil, conectando diagnóstico estratégico, capital humano tecnológico, inovação industrial, gestão de riscos, coordenação institucional e accountability. Conclui-se que a autonomia em defesa depende não apenas da aquisição de sistemas avançados, mas da existência de rotinas institucionais estáveis capazes de converter alertas estratégicos em capacidades efetivas, sustentáveis e verificáveis.

Palavras-chave: Governança em defesa; Desenvolvimento de capacidades; Base Industrial de Defesa; Autonomia tecnológica; Brasil

Abstract

This article examines how defence governance can contribute to transforming contemporary strategic lessons and emerging technological demands into sustainable national defence capabilities in Brazil. The central argument is that the Brazilian challenge is not merely to identify critical capabilities, such as unmanned systems, artificial intelligence, cyber defence, resilient logistics, air defence, coastal defence and strategic deterrence. Rather, the decisive challenge lies in institutionalising governance mechanisms capable of prioritising, funding, monitoring and coordinating these capabilities through the Ministry of Defence, the Armed Forces, the Defence Industrial Base, universities, research centres and the productive sector. The article adopts a defence governance perspective based on leadership, strategy and control, with emphasis on portfolio governance, risk management, *assurance*, performance indicators, interagency coordination and qualified civil engagement. Methodologically, it combines documentary analysis, selective literature review and institutional interpretation of contemporary trends in defence, technology and innovation. Its main contribution is to propose a governance-of-technological-capabilities framework for Brazil, connecting strategic diagnosis, technological human capital, industrial innovation, risk management, institutional coordination and accountability. The article concludes that defence autonomy depends not only on the acquisition of advanced systems, but also on stable institutional routines capable of converting strategic warnings into effective, sustainable and verifiable defence capabilities.

Keywords: Defence governance; Capability development; Defence Industrial Base; Technological autonomy; Brazil

INTRODUÇÃO

As transformações recentes do ambiente estratégico internacional têm recolocado no centro do debate a relação entre defesa, tecnologia, autonomia industrial e capacidade estatal de coordenação. A guerra entre Rússia e Ucrânia evidenciou o retorno da guerra convencional de alta intensidade ao continente europeu e ofereceu um campo de observação privilegiado sobre o emprego combinado de sistemas não tripulados, inteligência artificial, guerra eletrônica, ciberdefesa, defesa antiaérea, fogos de precisão, estoques, logística resiliente e adaptação doutrinária. Relatórios especializados, como os produzidos pelo Royal United Services Institute, indicam que a invasão russa de 2022 permitiu avaliar, em condições reais, a interação entre capacidades militares, planejamento operacional, inteligência, defesa aérea, fogos, logística e adaptação no campo de batalha (ZABRODSKYI et al., 2022).

Para o Brasil, essas lições possuem relevância particular. A dimensão continental do território, a extensão das fronteiras terrestres, a centralidade estratégica da Amazônia, a proteção da Amazônia Azul, a segurança de infraestruturas críticas e as responsabilidades no Atlântico Sul impõem ao país o desafio de estruturar capacidades compatíveis com sua estatura geopolítica. A Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, aprovados pelo Decreto nº 12.725, de 18 de novembro de 2025, reafirmam a necessidade de que os órgãos e entidades da administração pública federal considerem, em seus planejamentos, ações voltadas ao fortalecimento da defesa nacional (BRASIL, 2025).

Entretanto, a identificação de capacidades críticas não resolve, por si só, o problema da defesa nacional. Drones, inteligência artificial, ciberdefesa, sensores, defesa antiaérea, defesa costeira, sistemas autônomos, munições de precisão, logística resiliente e capacidades de dissuasão só se convertem em poder efetivo quando integrados a processos institucionais de priorização, financiamento, desenvolvimento, aquisição, monitoramento e avaliação. O desafio central, portanto, não consiste apenas em definir quais capacidades o Brasil deve desenvolver, mas em compreender como o Estado brasileiro pode governar a geração dessas capacidades de modo coordenado, sustentável e verificável.

É nesse ponto que o debate sobre governança em defesa se torna decisivo. A governança pública, nos termos do Decreto nº 9.203/2017, envolve mecanismos de liderança, estratégia e controle voltados a avaliar, direcionar e monitorar a gestão pública, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade (BRASIL, 2017). O Referencial Básico de Governança Organizacional do Tribunal de Contas da União aprofunda essa concepção ao associar a governança à capacidade de orientar organizações públicas para resultados, accountability, transparência, integridade e controle (TCU, 2020).

Aplicada ao setor de defesa, essa noção exige adaptações. Políticas de defesa envolvem ciclos longos de planejamento, programas intensivos em recursos, decisões de

elevado impacto estratégico, coordenação interorganizacional, informações sensíveis e permanente tensão entre sigilo, efetividade, transparência e prestação de contas. A governança em defesa, portanto, não se confunde com gestão operacional. Ela diz respeito ao arranjo institucional que organiza prioridades, define responsabilidades, estrutura portfólios, monitora riscos, produz evidências, coordena atores e estabelece mecanismos de accountability compatíveis com as especificidades do setor.

A geração de capacidades tecnológicas também depende da articulação entre defesa, indústria, ciência, tecnologia e capital humano. Estudos sobre a Base Industrial de Defesa brasileira indicam que o setor envolve dimensões científicas, tecnológicas, industriais, infraestruturais e logísticas, além de desempenhar papel relevante na inovação militar e no desenvolvimento de tecnologias de alto valor agregado (AMARANTE, 2012; NEGRETE et al., 2016). Essa constatação aproxima o debate de defesa da literatura sobre inovação orientada por missão, segundo a qual o Estado não deve atuar apenas como regulador ou comprador, mas como indutor, coordenador e financiador de trajetórias tecnológicas estratégicas (MAZZUCATO, 2018).

Nesse contexto, universidades, centros de pesquisa, empresas, Forças Armadas, agências de fomento e órgãos de governo precisam ser integrados em uma arquitetura de governança capaz de produzir capacidades e não apenas projetos isolados. A abordagem da hélice tríplice, ao enfatizar as interações entre universidade, indústria e governo em economias baseadas no conhecimento, oferece uma chave útil para pensar a defesa como ecossistema de inovação e não apenas como setor comprador de equipamentos (ETZKOWITZ; LEYDESDORFF, 2000).

O problema de pesquisa que orienta este artigo pode ser formulado nos seguintes termos: como a governança em defesa pode contribuir para transformar lições estratégicas contemporâneas e demandas tecnológicas emergentes em capacidades nacionais sustentáveis para o Brasil? A hipótese sustentada é que o principal desafio brasileiro não está apenas na identificação de capacidades críticas, mas na construção de mecanismos de governança capazes de priorizar, financiar,

monitorar e articular essas capacidades com a Base Industrial de Defesa, a academia, os centros tecnológicos, o setor produtivo e os órgãos de controle.

Metodologicamente, o artigo adota abordagem qualitativa, exploratória e propositiva, combinando análise documental, revisão bibliográfica seletiva e interpretação institucional de tendências contemporâneas em defesa, tecnologia e inovação. A análise documental apoia-se em documentos oficiais brasileiros de defesa, referenciais de governança pública, estudos sobre Base Industrial de Defesa e relatórios especializados sobre conflitos contemporâneos. A contribuição principal consiste em propor uma matriz de governança de capacidades tecnológicas em defesa, conectando diagnóstico estratégico, priorização de portfólio, capital humano, inovação industrial, gestão de riscos, coordenação interagências e accountability compatível com as especificidades do setor.

O artigo está organizado em quatro seções, além desta introdução e das considerações finais. A primeira apresenta o referencial de governança em defesa e sua relação com a geração de capacidades. A segunda examina lições estratégicas contemporâneas relevantes para o Brasil, com ênfase em tecnologia, logística, ciberdefesa, dissuasão e resiliência. A terceira discute o papel do capital humano tecnológico e da Base Industrial de Defesa na sustentação dessas capacidades. A quarta propõe uma matriz de governança de capacidades para o Brasil, estruturada em direção estratégica e portfólio, *assurance* e gestão de riscos, indicadores e monitoramento, coordenação interagências e interface qualificada com academia, indústria e centros tecnológicos.

GOVERNANÇA EM DEFESA E GERAÇÃO DE CAPACIDADES

A governança em defesa deve ser compreendida como o conjunto de mecanismos institucionais que permite ao Estado transformar objetivos políticos, diagnósticos estratégicos e recursos disponíveis em capacidades militares e não militares efetivamente mobilizáveis. No caso brasileiro, essa compreensão dialoga

diretamente com a política de governança da administração pública federal, segundo a qual governança pública corresponde aos mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade (BRASIL, 2017).

No setor de defesa, contudo, a aplicação desses referenciais exige uma adaptação conceitual. Diferentemente de políticas públicas de execução mais imediata, a defesa nacional envolve ciclos longos de planejamento, programas de grande complexidade tecnológica, elevada dependência de recursos orçamentários plurianuais, integração interforças, coordenação com a Base Industrial de Defesa e níveis variáveis de sigilo. Por essa razão, a governança em defesa não pode ser reduzida à gestão administrativa cotidiana. Ela diz respeito à arquitetura decisória que define prioridades, estabelece responsabilidades, estrutura portfólios, acompanha riscos, monitora resultados e produz formas de prestação de contas compatíveis com a proteção de informações sensíveis.

Essa distinção entre governança e gestão é central para evitar dois equívocos recorrentes. O primeiro consiste em imaginar que a existência de documentos estratégicos, conselhos, portarias e instâncias formais seja suficiente para assegurar a geração de capacidades. O segundo consiste em tratar capacidades de defesa como simples resultado de aquisições de equipamentos. Em ambos os casos, perde-se de vista que capacidades dependem de doutrina, organização, treinamento, material, liderança, pessoal, infraestrutura, interoperabilidade, financiamento, sustentação logística e mecanismos de aprendizado institucional.

Essa concepção permite deslocar o debate brasileiro de uma lógica predominantemente aquisitiva para uma lógica de geração, sustentação e avaliação de capacidades. A questão não é apenas adquirir drones, radares, sistemas de comando e controle, plataformas navais, meios blindados, capacidades cibernéticas ou sistemas de defesa antiaérea. A questão central é construir um processo institucional capaz

de definir por que determinada capacidade é prioritária, qual efeito estratégico ela deve produzir, que lacuna pretende mitigar, quais riscos reduz, quais atores devem participar de seu desenvolvimento, como será financiada, quais indicadores permitirão monitorá-la e como sua efetividade será avaliada ao longo do tempo.

O planejamento baseado em capacidades oferece uma chave metodológica relevante para esse debate. Em termos gerais, essa abordagem busca orientar o planejamento de defesa sob condições de incerteza, identificando necessidades, alocando recursos e acompanhando atividades e resultados. A RAND Corporation descreve o planejamento baseado em capacidades como instrumento para que organizações militares identifiquem necessidades programáticas, aloquem recursos e acompanhem atividades e resultados (RAND CORPORATION, s.d.). Davis (2002) acrescenta que essa abordagem é particularmente adequada para contextos de transformação e incerteza, nos quais escolhas de força devem considerar efeitos, missões e alternativas de alocação de recursos.

Entretanto, o planejamento baseado em capacidades somente produz efeitos institucionais consistentes quando inserido em uma governança mais ampla. Sem mecanismos de direção estratégica, priorização de portfólio, gestão de riscos, *assurance*, monitoramento e revisão periódica, o planejamento tende a se fragmentar em projetos dispersos ou em listas de intenções. A governança, nesse sentido, é o elo que conecta objetivos políticos, análise estratégica, requisitos militares, recursos orçamentários, Base Industrial de Defesa, ciência e tecnologia, capital humano e prestação de contas.

Essa perspectiva é particularmente importante no caso brasileiro. A Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, aprovados pelo Decreto nº 12.725/2025, reafirmam a necessidade de que os órgãos e entidades da administração pública federal considerem, em seus planejamentos, ações que concorram para o fortalecimento da defesa nacional (BRASIL, 2025). Isso significa que a defesa não pode ser entendida como responsabilidade exclusiva

das Forças Armadas ou do Ministério da Defesa. A geração de capacidades envolve também órgãos de ciência e tecnologia, agências de fomento, universidades, empresas estratégicas, instituições de controle, diplomacia, indústria e infraestrutura nacional.

A literatura de relações civis-militares contribui para essa discussão ao demonstrar que a defesa democrática exige mediação permanente entre expertise militar, direção política e controle civil. Huntington (1957) distingue a função militar profissional, a função fiscal-administrativa e a função político-estratégica, ressaltando que a política de defesa requer articulação entre necessidades militares, restrições de recursos e objetivos políticos. Feaver (2003), por sua vez, enfatiza a supervisão civil como mecanismo indispensável para assegurar que as instituições militares atuem em conformidade com os objetivos definidos pelo poder político.

A esse argumento soma-se uma leitura institucional do processo decisório. A governança em defesa não ocorre em um espaço neutro. Ela se desenvolve em um campo marcado por disputas por autoridade legítima, controle de informações, expertise técnica, precedência orçamentária e definição de prioridades. A incorporação de uma leitura inspirada em Bourdieu (2002) permite compreender que mecanismos de governança não são apenas instrumentos administrativos: eles reorganizam posições, distribuem autoridade, definem quem participa da decisão e estabelecem quais critérios serão reconhecidos como tecnicamente válidos.

Por essa razão, o aprimoramento da governança em defesa não exige necessariamente a criação de estruturas inteiramente novas. Em muitos casos, o desafio está em conferir maior densidade funcional a estruturas já existentes, mediante rotinas estáveis de coordenação, indicadores, responsáveis institucionais, trilhas de escalonamento, avaliação de riscos, ciclos de revisão e mecanismos de prestação de contas. Essa lógica se aproxima da literatura do institucionalismo histórico sobre mudança incremental, especialmente das noções de layering e conversion, segundo as quais instituições podem ser transformadas pela adição de novas regras, novos usos e novas funções a arranjos preexistentes (CONRAN; THELEN, 2016).

A partir dessa base, este artigo propõe o conceito de governança de capacidades tecnológicas em defesa. Por essa expressão, entende-se o arranjo institucional voltado a converter diagnósticos estratégicos e demandas tecnológicas em capacidades priorizadas, financiadas, desenvolvidas, monitoradas e avaliadas, mediante coordenação entre Ministério da Defesa, Forças Armadas, Base Industrial de Defesa, universidades, centros de pesquisa, setor produtivo, agências de fomento e órgãos de controle. Trata-se, portanto, de uma governança orientada não apenas à conformidade normativa, mas à produção de efeitos estratégicos verificáveis.

LIÇÕES ESTRATÉGICAS CONTEMPORÂNEAS: TECNOLOGIA, LOGÍSTICA E DISSUASÃO NA GUERRA RÚSSIA-UCRÂNIA

A guerra entre Rússia e Ucrânia tem sido amplamente interpretada como um laboratório estratégico da guerra contemporânea. Seu significado, entretanto, não reside apenas na identificação de novas tecnologias empregadas em combate, mas na demonstração de que a efetividade militar depende da capacidade de integrar tecnologia, logística, inteligência, adaptação doutrinária, mobilização industrial e sustentação política em ciclos prolongados de conflito. Relatórios especializados do Royal United Services Institute indicam que a invasão russa de 2022 ofereceu oportunidade rara para avaliar, em condições reais, a interação entre capacidades militares, planejamento operacional, inteligência, defesa aérea, fogos, logística e adaptação no campo de batalha (ZABRODSKYI et al., 2022).

Para os fins deste artigo, o conflito não é tratado como modelo a ser transposto automaticamente ao Brasil, mas como fonte de problemas de governança. A pergunta relevante não é apenas quais capacidades se mostraram decisivas na guerra, mas como um Estado transforma lições estratégicas em prioridades, programas, orçamento, indicadores, capital humano, base industrial e mecanismos de coordenação. Essa distinção é essencial para evitar uma leitura meramente tecnológica do conflito.

Uma das lições mais evidentes do conflito é a centralidade dos sistemas não tripulados. Drones têm sido empregados para reconhecimento, aquisição de alvos, ajuste de fogos, ataques de precisão, saturação de defesas, apoio à logística e ações de interdição. Slusher (2025) observa que a guerra da Ucrânia evidenciou cinco domínios transformadores: sistemas autônomos, operações de informação, guerra eletrônica, logística contestada e defesa aérea em evolução. O impacto desses sistemas não decorre apenas de sua sofisticação tecnológica, mas de sua relação custo-efeito, de sua capacidade de produção em escala e da velocidade de adaptação.

No caso brasileiro, a lição não deve ser lida apenas como necessidade de adquirir drones. O problema é mais amplo: trata-se de construir uma governança de sistemas não tripulados que envolva requisitos operacionais, certificação, doutrina, interoperabilidade, produção nacional, proteção de enlaces, contramedidas eletrônicas, integração com sensores e formação de operadores e engenheiros. Sem essa arquitetura, o país corre o risco de adquirir plataformas sem desenvolver capacidade efetiva, sustentável e adaptável.

A inteligência artificial acrescenta outra camada ao problema. Aplicações de IA no campo de batalha tendem a impactar análise de dados, priorização de alvos, fusão de sensores, detecção de ameaças, apoio à decisão, manutenção preditiva e gestão logística. A incorporação dessas tecnologias exige governança específica. Não basta incluir inteligência artificial como prioridade genérica em documentos estratégicos. É necessário definir missões, casos de uso, limites éticos e jurídicos, padrões de segurança, proteção de dados, requisitos de auditoria algorítmica, cadeia de suprimento digital, centros responsáveis, interoperabilidade e mecanismos de avaliação de desempenho.

A guerra Rússia-Ucrânia também demonstrou que o espaço cibernético e o espectro eletromagnético são dimensões permanentes da competição militar. Ainda que os efeitos cibernéticos iniciais tenham sido, em alguns momentos, menos decisivos do que certas previsões antecipavam, o conflito evidenciou a vulnerabilidade de redes de energia, comunicações, finanças, comando e controle, satélites, sistemas

logísticos e bases de dados. O guia da OTAN sobre lições aprendidas da guerra foi estruturado para tratar de temas de guerra geral e warfighting específicos, incluindo domínios operacionais e tecnológicos relevantes para instituições de educação militar (NATO, 2023).

Para o Brasil, a questão é particularmente sensível. A proteção de infraestruturas críticas envolve sistemas energéticos, comunicações, portos, aeroportos, redes financeiras, infraestrutura espacial, plataformas offshore, cadeias logísticas e sistemas governamentais. Esses ativos não pertencem exclusivamente ao Ministério da Defesa ou às Forças Armadas. Sua segurança depende de coordenação entre Defesa, Gabinete de Segurança Institucional, órgãos de inteligência, agências reguladoras, empresas públicas e privadas, setor financeiro, operadores de infraestrutura, universidades e centros tecnológicos.

Outra lição central do conflito é a importância da logística. A guerra demonstrou que capacidades tecnologicamente avançadas perdem valor se não forem sustentadas por estoques, manutenção, reposição, transporte, proteção de rotas, munições, peças, combustíveis, comunicações e capacidade industrial de recomposição. Em ambiente de atrito prolongado, a logística deixa de ser mera função de apoio e passa a constituir dimensão central da dissuasão e da prontidão.

Para o Brasil, essa lição tem implicações diretas. Um país de dimensões continentais, com fronteiras extensas, áreas de baixa densidade demográfica, grandes distâncias logísticas e responsabilidades simultâneas na Amazônia e no Atlântico Sul, não pode tratar logística como dimensão secundária do planejamento de defesa. Estoques, mobilidade estratégica, manutenção, transporte, pré-posicionamento, infraestrutura dual, capacidade de reparo e integração com a indústria nacional devem ser considerados parte da capacidade de dissuasão.

A guerra também recolocou a defesa antiaérea no centro do planejamento militar. A experiência ucraniana indicou que defesas antiaéreas em camadas, integradas a sensores, radares, mísseis, artilharia antiaérea, guerra eletrônica e sistemas de

comando e controle, podem negar superioridade aérea e impor custos elevados ao adversário. Stoll, Hoehn e Courtney (2024) observam que as defesas antiaéreas terrestres ucranianas demonstraram alcance suficiente para negar superioridade aérea geral à Rússia, sugerindo que a defesa aérea passou a moldar a forma de combate na Ucrânia.

A defesa costeira também assume relevância particular. A guerra no Mar Negro mostrou que meios relativamente baratos, como drones navais e mísseis antinavio, podem desafiar frotas convencionais e modificar a dinâmica de controle marítimo. Para o Brasil, cuja dimensão marítima envolve Amazônia Azul, pré-sal, linhas de comunicação marítima, portos e projeção no Atlântico Sul, a defesa costeira deve ser tratada como capacidade integrada, envolvendo Marinha, Força Aérea, sensores, satélites, sistemas antinavio, vigilância marítima, guerra eletrônica, ciberdefesa e indústria nacional.

Por fim, a guerra Rússia-Ucrânia reabriu o debate sobre dissuasão. O conflito demonstrou que garantias políticas, acordos internacionais e expectativas normativas não substituem integralmente capacidades nacionais de defesa. A dissuasão contemporânea depende de uma combinação de prontidão militar, resiliência econômica, capacidade industrial, mobilização social, alianças, comunicação estratégica, inteligência e credibilidade política. Em ambientes de incerteza, autonomia estratégica não significa isolamento, mas capacidade de reduzir vulnerabilidades críticas e preservar liberdade de ação.

As lições extraídas da guerra convergem para um ponto central: conflitos contemporâneos exigem capacidade estatal de aprendizado rápido, integração tecnológica e sustentação prolongada. Drones, IA, ciberdefesa, defesa antiaérea, guerra eletrônica, logística e dissuasão não devem ser tratados como recomendações isoladas, mas como componentes de um sistema de capacidades. A principal contribuição analítica para o caso brasileiro está em transformar esses temas em problemas de governança: quem prioriza, quem financia, quem desenvolve, quem integra, quem monitora e quem responde pela geração de capacidades nacionais sustentáveis.

CAPITAL HUMANO TECNOLÓGICO, BASE INDUSTRIAL DE DEFESA E INOVAÇÃO ORIENTADA À AUTONOMIA

A transformação de lições estratégicas em capacidades nacionais depende de uma dimensão frequentemente subestimada no debate de defesa: a existência de capital humano, base científica, infraestrutura tecnológica e capacidade industrial para desenvolver, absorver, adaptar, produzir, manter e evoluir sistemas complexos. Em conflitos tecnologicamente intensivos, a vantagem estratégica não deriva apenas da posse de meios militares, mas da capacidade de sustentar ciclos de inovação, manutenção, atualização, reposição e aprendizado institucional.

A Base Industrial de Defesa deve ser compreendida como componente estrutural da autonomia nacional. Amarante (2012) define a BID brasileira como integrada por cinco pilares fundamentais: científico, tecnológico, infraestrutural, industrial e logístico. Essa formulação é particularmente útil porque desloca a análise da indústria de defesa de uma visão restrita à produção de equipamentos para uma concepção sistêmica, na qual conhecimento, tecnologia, infraestrutura, capacidade fabril e logística formam uma arquitetura interdependente.

Do ponto de vista da governança, isso significa que a BID não pode ser tratada apenas como fornecedora eventual de bens e serviços. Ela deve ser incorporada como parte do processo de geração de capacidades. Projetos de defesa que envolvem drones, sensores, sistemas de comando e controle, ciberdefesa, defesa antiaérea, comunicações seguras, munições inteligentes, guerra eletrônica ou plataformas complexas exigem cadeias produtivas, fornecedores qualificados, domínio de propriedade intelectual, certificação, capacidade de integração, manutenção e atualização.

A literatura aplicada à BID brasileira reforça esse ponto. O Mapeamento da Base Industrial de Defesa, produzido pelo IPEA, oferece uma visão sistêmica da competitividade, da capacidade produtiva, tecnológica e de inovação das empresas da BID, com vistas a subsidiar medidas mais eficientes e baseadas em evidências

(NEGRETE et al., 2016). A relevância desse tipo de diagnóstico está justamente em permitir que a defesa deixe de operar com percepções fragmentadas sobre sua base produtiva e passe a articular políticas orientadas por informação, indicadores e planejamento de longo prazo.

A autonomia tecnológica não se sustenta sem capital humano qualificado. Sistemas de defesa contemporâneos dependem de engenheiros de sistemas, especialistas em software crítico, profissionais de cibersegurança, cientistas de dados, integradores de sensores, projetistas, especialistas em materiais, eletrônica, comunicações, inteligência artificial, automação, manutenção preditiva, manufatura avançada, custos e gestão de projetos complexos. A defesa contemporânea é, portanto, intensiva em conhecimento.

Essa constatação tem duas implicações. A primeira é que a formação de recursos humanos deve ser tratada como parte da política de defesa, não como externalidade do sistema educacional. A segunda é que a governança de capacidades precisa prever mecanismos de atração, formação, retenção e mobilização de talentos, especialmente em áreas nas quais o setor de defesa compete com empresas de tecnologia, mercado financeiro, indústria aeroespacial, setor de energia, telecomunicações e empresas globais de software.

No Brasil, esse problema ganha relevância adicional porque muitas competências críticas estão fora das organizações militares. Universidades, institutos federais, centros tecnológicos, empresas de base tecnológica e startups concentram parte significativa do conhecimento necessário para IA, sistemas autônomos, cibersegurança, sensores, materiais avançados e análise de dados. Assim, a governança em defesa precisa construir canais institucionais estáveis para acessar esse conhecimento, sem depender apenas de contatos informais ou projetos isolados.

A abordagem da hélice tríplice, formulada por Etzkowitz e Leydesdorff (2000), oferece uma chave teórica relevante para esse ponto. Os autores interpretam a inovação como resultado de interações entre universidade, indústria e governo

em economias baseadas no conhecimento, nas quais comunicação, negociação e sobreposição institucional reorganizam os arranjos tradicionais de produção científica e tecnológica. Aplicada à defesa, essa abordagem permite compreender que capacidades tecnológicas não emergem apenas de laboratórios militares ou de empresas contratadas, mas de ecossistemas que combinam pesquisa, demanda pública, financiamento, produção, certificação e emprego operacional.

A defesa é também um campo típico de inovação orientada por missão. Tecnologias como radar, internet, GPS, materiais avançados, sistemas aeroespaciais e cibernética foram historicamente impulsionadas por demandas estratégicas do Estado e por investimentos públicos de longo prazo. A literatura de inovação orientada por missão sustenta que políticas públicas inovadoras não devem limitar-se a corrigir falhas de mercado, mas podem criar e moldar mercados, definindo direções estratégicas, mobilizando atores e coordenando investimentos em torno de desafios complexos (MAZZUCATO, 2018).

Esse argumento é particularmente relevante para a defesa brasileira. A geração de capacidades em áreas como sistemas não tripulados, defesa cibernética, IA aplicada à defesa, sensores, guerra eletrônica, satélites, comunicações seguras, munições de precisão e defesa antiaérea exige política pública orientada por missão, com metas claras, financiamento estável, encomendas tecnológicas, interação com universidades, incentivos à indústria, avaliação de riscos e mecanismos de monitoramento. Sem direção estratégica, o sistema tende a produzir iniciativas dispersas, incapazes de gerar escala, continuidade e domínio tecnológico.

A política de inovação em defesa também deve ser compreendida como política industrial. Andrade e Leite (2017) analisam a indústria de defesa no contexto da política de inovação brasileira, destacando a relação entre inovação, desenvolvimento tecnológico militar, conhecimento, gestão e sistema de inovação. Essa perspectiva reforça que defesa não é apenas consumo público de equipamentos, mas instrumento de desenvolvimento tecnológico, capacitação produtiva e geração de competências de alto valor agregado.

Um dos principais desafios da BID é conciliar autonomia estratégica com sustentabilidade econômica. Empresas de defesa operam em mercados de demanda restrita, ciclos longos, alta regulação, dependência de compras governamentais e forte sensibilidade a oscilações orçamentárias. Por isso, a governança de capacidades deve considerar não apenas o desenvolvimento tecnológico, mas também a viabilidade produtiva, a inserção em cadeias globais, o potencial dual, as exportações, a manutenção de competências críticas e a previsibilidade de demanda.

O BNDES, em estudo sobre a indústria de defesa e segurança no Brasil, identifica o setor como marcado por transformações decorrentes de políticas públicas recentes e discute possibilidades de atuação do banco no apoio à indústria (CORREA FILHO et al., 2013). Essa dimensão financeira é decisiva: sem instrumentos adequados de crédito, garantias, financiamento à inovação e suporte a projetos de longo prazo, a BID dificilmente conseguirá sustentar capacidades tecnológicas sensíveis.

A conexão entre capital humano, BID e governança de capacidades pode ser sintetizada em uma premissa: não há capacidade militar sustentável sem ecossistema tecnológico capaz de desenvolvê-la, mantê-la e atualizá-la. Essa premissa altera o modo como programas de defesa devem ser avaliados. Um projeto estratégico não deve ser examinado apenas pelo produto entregue, mas também por sua contribuição para formação de engenheiros, domínio de tecnologias críticas, fortalecimento de fornecedores, nacionalização de componentes, geração de propriedade intelectual, ampliação de infraestrutura laboratorial, criação de empregos qualificados e redução de vulnerabilidades externas.

5. Matriz de governança de capacidades tecnológicas em defesa para o Brasil

As seções anteriores demonstraram que a geração de capacidades tecnológicas em defesa não pode ser reduzida à aquisição de equipamentos, à formulação de documentos estratégicos ou à execução isolada de projetos de pesquisa e desenvolvimento. Capacidades como sistemas não tripulados, inteligência artificial, ciberdefesa, sensores, guerra eletrônica, defesa antiaérea,

defesa costeira, logística resiliente e sistemas autônomos exigem integração entre estratégia, orçamento, doutrina, capital humano, indústria, ciência, tecnologia, infraestrutura e mecanismos de controle. Em razão disso, o desafio brasileiro consiste em construir uma governança capaz de transformar alertas estratégicos em capacidades efetivas, sustentáveis e verificáveis.

A proposta desta seção é apresentar uma matriz de governança de capacidades tecnológicas em defesa, concebida como instrumento analítico e operacional para organizar a relação entre diagnóstico estratégico, priorização de portfólio, desenvolvimento tecnológico, mobilização industrial, formação de capital humano, gestão de riscos, coordenação interagências e accountability. A matriz parte da premissa de que o Brasil já dispõe de estruturas formais relevantes, mas ainda enfrenta dificuldades para convertê-las em rotinas estáveis de direção, monitoramento, *assurance*, participação qualificada e reporte sanitizado.

A matriz proposta apoia-se em cinco premissas. A primeira é que capacidades tecnológicas de defesa devem ser tratadas como portfólios estratégicos, e não como projetos isolados. A segunda é que a governança deve articular direção política, expertise militar e competência civil especializada. A terceira é que a autonomia estratégica depende de continuidade institucional. A quarta é que sigilo e *accountability* não são categorias incompatíveis. A quinta é que a governança deve produzir entregas verificáveis.

A primeira premissa é particularmente importante. Um sistema não tripulado, por exemplo, não é apenas uma plataforma; envolve sensores, enlaces, doutrina, operadores, engenheiros, manutenção, proteção cibernética, guerra eletrônica, interoperabilidade, logística, indústria e atualização tecnológica. O mesmo se aplica à ciberdefesa, à inteligência artificial, à defesa antiaérea e à logística resiliente. Por isso, capacidades devem ser tratadas como sistemas integrados e não como produtos isolados.

A segunda premissa enfatiza a necessidade de integrar expertise militar e conhecimento civil especializado. A defesa nacional não pode prescindir do conhecimento militar, mas também não pode ser concebida apenas como assunto interno das Forças Armadas. Universidades, centros tecnológicos, empresas, agências de fomento, órgãos de controle, diplomacia, indústria e operadores de infraestrutura crítica possuem competências indispensáveis à geração de capacidades.

A terceira premissa diz respeito à continuidade. Capacidades de defesa exigem ciclos longos de desenvolvimento, orçamentos plurianuais, estabilidade de requisitos, aprendizagem acumulada e preservação de capital humano. Sem governança, programas estratégicos ficam vulneráveis a descontinuidade, dispersão, sobreposição, atraso e perda de competências.

A quarta premissa trata da tensão entre sigilo e *accountability*. A governança de defesa deve proteger informações sensíveis, mas pode produzir formas sanitizadas de reporte, indicadores agregados, mecanismos de controle interno, auditoria, avaliação de riscos e prestação de contas compatíveis com as especificidades do setor. A solução não está na transparência absoluta nem na opacidade integral, mas em mecanismos proporcionais de prestação de contas.

A quinta premissa ressalta a necessidade de entregas verificáveis. Não basta afirmar prioridades. É necessário definir responsáveis, prazos, indicadores, produtos mínimos, ciclos decisórios, mecanismos de acompanhamento e procedimentos de revisão. A proposta, portanto, deve evitar o risco da governança de papel, isto é, a criação de normas e documentos sem tração organizacional, sem calendarização e sem instrumentos de cobrança e aprendizagem.

Essa matriz não deve ser entendida como novo órgão ou nova estrutura burocrática. Trata-se de um modelo de funcionamento. Seu objetivo é organizar ritos, responsabilidades e entregas a partir de estruturas já existentes, conferindo maior densidade operacional a instrumentos de governança que, em muitos casos, já estão formalmente previstos, mas ainda carecem de rotinização.

Quadro 1 - Matriz de governança de capacidades tecnológicas em defesa

Dimensão	Instrumentos de governança	Atores principais	Produtos verificáveis
Direção estratégica e portfólio	Portfólio nacional de capacidades tecnológicas; critérios de priorização; owners institucionais; trilha decisória.	MD; Forças Armadas; CONSUG/MD; EMCFA; secretarias setoriais.	Portfólio priorizado; mapa de lacunas; matriz de capacidades críticas; atas decisórias.
Assurance, riscos e controles	Matriz de riscos tecnológicos; avaliação de dependência externa; auditoria de ciclo de vida; controles internos.	MD; Forças; CGU; TCU; órgãos de controle interno; BID.	Matriz de riscos; relatório de *assurance*; plano de mitigação; follow-up de riscos críticos.
Indicadores, monitoramento e reporte	KPIs de capacidades; painel de monitoramento; dicionário de indicadores; reporte sanitizado.	MD; Forças; ASPLAN; centros tecnológicos; BID; academia.	Painel de indicadores; relatório anual sanitizado; séries históricas; metas de maturidade.
Coordenação interagências	Comitês temáticos; protocolos de acionamento; exercícios interagências; after-action review.	MD; MCTI; MDIC; BNDES; FINEP; GSI; MRE; universidades; empresas.	Protocolos interagências; planos temáticos; relatórios pós-ação; agenda de projetos críticos.
Interface civil qualificada e conhecimento	Conselhos consultivos temáticos; consultas sanitizadas; briefs de evidência; redes de pesquisa.	Universidades; centros de pesquisa; ABIMDE; empresas; especialistas; escolas militares.	Briefs técnicos; agenda de pesquisa; chamadas de P&D; banco de especialistas.

Fonte: Autores (2026)

A primeira dimensão da matriz é a direção estratégica e a governança de portfólio. Seu objetivo é responder a uma pergunta fundamental: quais capacidades tecnológicas são prioritárias para o Brasil e por quê? Sem essa resposta, a política de defesa tende a acumular projetos sem hierarquia clara, muitas vezes pressionada por oportunidades industriais, demandas específicas das Forças ou disponibilidade episódica de recursos.

A governança de portfólio deve estabelecer critérios transparentes, ainda que nem todos publicamente detalhados, para ordenar capacidades segundo sua contribuição para os Objetivos Nacionais de Defesa, sua relevância para a dissuasão, sua capacidade de reduzir vulnerabilidades, seu impacto na autonomia tecnológica, seu potencial de integração interforças, sua viabilidade industrial e sua sustentabilidade orçamentária. Essa lógica é compatível com o planejamento baseado em capacidades, que busca orientar escolhas em ambientes de incerteza e organizar recursos em função de efeitos desejados, e não apenas de meios disponíveis (DAVIS, 2002).

A segunda dimensão é *assurance*, riscos e controles. Em defesa, riscos não são apenas financeiros ou administrativos. São também tecnológicos, industriais, logísticos, cibernéticos, regulatórios, geopolíticos e operacionais. Uma capacidade pode fracassar não porque o equipamento não foi adquirido, mas porque depende de componentes importados, não possui manutenção nacional, carece de pessoal qualificado, não se integra a sistemas existentes ou não dispõe de orçamento para sustentação.

A terceira dimensão é a criação de indicadores, monitoramento e reporte sanitizado. Sem indicadores, não há governança efetiva; há apenas intenção estratégica. O desafio, contudo, é construir indicadores adequados à defesa, evitando métricas simplistas ou excessivamente burocráticas. Indicadores de capacidades tecnológicas devem medir maturidade, prontidão, autonomia, integração e sustentabilidade.

Entre os indicadores possíveis, destacam-se: nível de maturidade tecnológica; percentual de nacionalização; número de engenheiros formados ou retidos; disponibilidade operacional; tempo de recomposição logística; grau de interoperabilidade; dependência de componentes importados; volume de P&D contratado; número de empresas nacionais envolvidas; propriedade intelectual gerada; capacidade de manutenção nacional; participação de universidades; e redução de vulnerabilidades críticas.

A quarta dimensão é a coordenação interagências. Capacidades tecnológicas de defesa não podem ser produzidas apenas pelo Ministério da Defesa. Elas dependem de

órgãos de ciência e tecnologia, política industrial, financiamento público, diplomacia, controle de exportações, infraestrutura crítica, inteligência, segurança cibernética, universidades e empresas. Nesse sentido, protocolos temáticos de coordenação interagências poderiam ser organizados por capacidades críticas, como ciberdefesa, sistemas não tripulados, defesa antiaérea, sensores, IA aplicada à defesa, logística resiliente e proteção de infraestruturas críticas.

A quinta dimensão é a interface civil qualificada e a governança do conhecimento. A defesa contemporânea depende de conhecimentos que muitas vezes se encontram fora das organizações militares. Inteligência artificial, ciência de dados, materiais avançados, robótica, cibersegurança, manufatura aditiva, sensores, autonomia, propulsão, comunicações e análise de sistemas complexos são campos nos quais universidades, startups, empresas e centros civis de pesquisa possuem competências essenciais.

A implementação da matriz deve ser incremental. Na fase inicial, o objetivo seria criar a infraestrutura mínima de governança: definir capacidades-piloto, instituir owners, organizar o primeiro portfólio, construir matriz inicial de riscos, selecionar indicadores mínimos e estabelecer ritos decisórios. Na fase intermediária, o objetivo seria ampliar o portfólio, estabilizar indicadores, implantar trilhas formais de escalonamento, produzir relatórios sanitizados, consolidar protocolos interagências e envolver universidades, empresas e órgãos de fomento. Na fase de maturidade, a matriz deveria ser incorporada como rotina institucional, com séries históricas de indicadores, metas de maturidade tecnológica, avaliações periódicas de risco, integração com planejamento orçamentário e revisões pós-ação após exercícios, crises ou eventos críticos.

A implementação envolve riscos. O primeiro é a formalização sem prática, quando novos instrumentos são criados sem alteração real das rotinas decisórias. O segundo é a inflação de indicadores, quando se mede muito, mas se decide pouco. O terceiro é a resistência organizacional, especialmente se os mecanismos forem

percebidos como perda de autonomia das Forças ou aumento de controle burocrático. O quarto é a tensão entre sigilo e transparência, que pode levar tanto à exposição indevida quanto à opacidade excessiva. O quinto é a descontinuidade orçamentária, capaz de comprometer programas tecnológicos de longo prazo.

Esses riscos podem ser mitigados por desenho institucional cuidadoso. A matriz deve ser enxuta, vinculada a decisões reais, orientada por produtos verificáveis e apoiada pela alta administração do Ministério da Defesa. Os indicadores devem ser poucos, estáveis e relevantes. Os relatórios sanitizados devem proteger informações sensíveis, mas comunicar resultados agregados. A participação civil deve ser qualificada por tema, com regras claras de confidencialidade quando necessário. E a governança do portfólio deve estar conectada ao planejamento orçamentário, evitando que capacidades prioritárias sejam tratadas como intenções sem financiamento.

A matriz de governança de capacidades tecnológicas em defesa procura responder ao problema central deste artigo: como transformar lições estratégicas contemporâneas e demandas tecnológicas emergentes em capacidades nacionais sustentáveis. Sua contribuição está em deslocar o debate da simples identificação de tecnologias críticas para o desenho de mecanismos institucionais capazes de priorizá-las, financiá-las, desenvolvê-las, monitorá-las e avaliá-las.

CONSIDERAÇÕES FINAIS

Este artigo partiu do pressuposto de que os conflitos contemporâneos, em especial a guerra Rússia-Ucrânia, evidenciam uma transformação relevante na relação entre defesa, tecnologia, indústria e capacidade estatal. Drones, inteligência artificial, ciberdefesa, guerra eletrônica, sensores, defesa antiaérea, defesa costeira, logística resiliente e dissuasão passaram a ocupar posição central no debate estratégico. Entretanto, o argumento desenvolvido ao longo do texto foi que a simples identificação dessas capacidades não é suficiente para fortalecer a defesa nacional. O desafio decisivo está em construir mecanismos de governança capazes de transformar

alertas estratégicos em capacidades sustentáveis, financiáveis, monitoráveis e institucionalmente coordenadas.

A pergunta que orientou o artigo foi: como a governança em defesa pode contribuir para transformar lições estratégicas contemporâneas e demandas tecnológicas emergentes em capacidades nacionais sustentáveis para o Brasil? A hipótese sustentada foi confirmada em termos analíticos: o principal problema brasileiro não reside apenas em saber quais tecnologias ou sistemas devem ser priorizados, mas em desenvolver uma arquitetura institucional capaz de priorizar, financiar, coordenar, acompanhar e avaliar essas capacidades em articulação com o Ministério da Defesa, as Forças Armadas, a Base Industrial de Defesa, universidades, centros tecnológicos, agências de fomento, setor produtivo e órgãos de controle.

A discussão demonstrou que a governança em defesa deve ser compreendida como mediação entre estratégia, recursos e capacidades. Nesse sentido, ela não se confunde com gestão operacional nem com mera conformidade normativa. Trata-se de um conjunto de mecanismos de liderança, estratégia e controle voltados à definição de prioridades, à organização de portfólios, à gestão de riscos, ao monitoramento de resultados, à coordenação interinstitucional e à prestação de contas compatível com as especificidades do setor.

A análise das lições estratégicas contemporâneas mostrou que a guerra Rússia-Ucrânia deve ser lida menos como modelo a ser transposto e mais como alerta sobre a necessidade de integração. A vantagem tecnológica e operacional deriva da combinação entre sensores, fogos de precisão, sistemas não tripulados, guerra eletrônica, ciberdefesa, estoques, logística e capacidade de adaptação. Para o Brasil, isso implica tratar capacidades como sistemas integrados, e não como aquisições isoladas.

O artigo também destacou que não há autonomia estratégica sem capital humano tecnológico e Base Industrial de Defesa. A sofisticação dos sistemas militares contemporâneos exige engenheiros, especialistas em software crítico, profissionais de cibersegurança, cientistas de dados, integradores de sistemas, técnicos de manutenção,

pesquisadores e gestores de projetos complexos. A defesa, nesse sentido, é cada vez mais intensiva em conhecimento. O fortalecimento da BID, da pesquisa aplicada, das universidades e das empresas tecnológicas deve ser tratado como componente da geração de capacidades, e não apenas como política industrial acessória.

A contribuição principal do artigo foi propor uma matriz de governança de capacidades tecnológicas em defesa estruturada em cinco dimensões: direção estratégica e portfólio; *assurance*, riscos e controles; indicadores, monitoramento e reporte sanitizado; coordenação interagências; e interface civil qualificada e governança do conhecimento. Essa matriz busca deslocar o debate da modernização tecnológica como lista de equipamentos para uma abordagem institucional, orientada por prioridades, responsáveis, indicadores, riscos, ciclos decisórios e entregas verificáveis.

Do ponto de vista político-institucional, o artigo sustentou que sigilo e *accountability* não são categorias excludentes. A defesa nacional exige proteção de informações sensíveis, mas também demanda legitimidade pública, controle democrático e capacidade de demonstrar resultados. A solução não está na transparência absoluta nem na opacidade integral, mas em mecanismos de reporte sanitizado, indicadores agregados, auditoria compatível com o setor, controle interno qualificado e participação civil estruturada.

A conclusão central é que a autonomia estratégica brasileira depende da institucionalização de uma governança de capacidades. O Brasil pode reconhecer corretamente as lições da guerra contemporânea, identificar tecnologias críticas, dispor de documentos estratégicos, possuir empresas relevantes e contar com universidades qualificadas. Ainda assim, esses elementos permanecerão dispersos se não forem integrados por uma arquitetura de governança capaz de estabelecer prioridades, mobilizar recursos, coordenar atores, medir resultados, controlar riscos e preservar continuidade institucional.

Assim, a principal agenda de pesquisa e de política pública que emerge deste artigo é a necessidade de conectar defesa, ciência, tecnologia, indústria e governança

em um mesmo ciclo estratégico. O desafio brasileiro não é apenas modernizar meios militares, mas criar condições institucionais para que tecnologia, capital humano e Base Industrial de Defesa sejam convertidos em capacidades reais, sustentáveis e orientadas à dissuasão. Em última instância, a defesa nacional não se fortalece apenas pela aquisição de sistemas avançados, mas pela capacidade do Estado de aprender, coordenar, priorizar e transformar conhecimento em poder nacional efetivo.

REFERÊNCIAS

AMARANTE, José Carlos Albano do. **A base industrial de defesa brasileira**. Texto para Discussão, n. 1758. Rio de Janeiro: IPEA, 2012. Disponível em: https://repositorio.ipea.gov.br/handle/11058/1091. Acesso em: 14 maio 2026.

ANDRADE, Israel de Oliveira; LEITE, Alixandro Werneck. A indústria de defesa no contexto da política de inovação. *In*: TURCHI, Lenita Maria; MORAIS, José Mauro de (org.). **Políticas de apoio à inovação tecnológica no Brasil**: avanços recentes, limitações e propostas de ações. Brasília: IPEA, 2017.

BEVIR, Mark. **A theory of governance**. Berkeley: University of California Press, 2013.

BOURDIEU, Pierre. **O poder simbólico**. Rio de Janeiro: Bertrand Brasil, 2002.

BRASIL. **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Brasília, DF: Presidência da República, 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm. Acesso em: 14 maio 2026.

BRASIL. **Decreto nº 12.725, de 18 de novembro de 2025**. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12725.htm. Acesso em: 14 maio 2026.

CONRAN, James; THELEN, Kathleen. Institutional change. *In*: FIORETOS, Orfeo; FALLETI, Tulia G.; SHEINGATE, Adam (ed.). **The Oxford handbook of historical institutionalism**. Oxford: Oxford University Press, 2016.

CORREA FILHO, Sérgio Leite Schmitt et al. Panorama sobre a indústria de defesa e segurança no Brasil. **BNDES Setorial**, Rio de Janeiro, n. 38, p. 373-408, set. 2013. Disponível em: https://web.bndes.gov.br/bib/jspui/handle/1408/2684. Acesso em: 14 maio 2026.

DAVIS, Paul K. **Analytic architecture for capabilities-based planning, mission-system analysis, and transformation**. Santa Monica: RAND Corporation, 2002. Disponível em: https://www.rand.org/pubs/monograph_reports/MR1513.html. Acesso em: 14 maio 2026.

ETZKOWITZ, Henry; LEYDESDORFF, Loet. The dynamics of innovation: from National Systems and 'Mode 2' to a Triple Helix of university-industry-government relations. **Research Policy**, v. 29, n. 2, p. 109-123, 2000.

FEAVER, Peter D. **Armed servants**: agency, oversight, and civil-military relations. Cambridge: Harvard University Press, 2003.

HUNTINGTON, Samuel P. **The soldier and the state**: the theory and politics of civil-military relations. Cambridge: Harvard University Press, 1957.

MAZZUCATO, Mariana. Mission-oriented innovation policies: challenges and opportunities. **Industrial and Corporate Change**, v. 27, n. 5, p. 803-815, 2018.

NATO. **Russian war against Ukraine**: lessons learned curriculum guide. Brussels: NATO, 2023. Disponível em: https://www.nato.int/content/dam/nato/webready/documents/deep/231208-RusWar-Ukraine-Lessons-Curriculum-Guide-en.pdf. Acesso em: 14 maio 2026.

NEGRETE, Ana Carolina Aguilera et al. **Mapeamento da base industrial de defesa**. Brasília: IPEA, 2016. Disponível em: https://repositorio.ipea.gov.br/items/cd247fb9-ec27-434d-b7e4-948ccee16de3. Acesso em: 14 maio 2026.

RAND CORPORATION. **Capabilities-based planning**. Santa Monica: RAND Corporation, s.d. Disponível em: https://www.rand.org/topics/capabilities-based-planning.html. Acesso em: 14 maio 2026.

SLUSHER, Matthew. **Lessons from the Ukraine conflict**: modern warfare in the age of autonomy, information, and resilience. Washington, DC: Center for Strategic and International Studies, 2025. Disponível em: https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience. Acesso em: 14 maio 2026.

STOLL, Hunter; HOEHN, John; COURTNEY, William. **Air defense shapes warfighting in Ukraine**. Santa Monica: RAND Corporation, 2024. Disponível em: https://www.rand.org/pubs/commentary/2024/02/air-defense-shapes-warfighting-in-ukraine.html. Acesso em: 14 maio 2026.

TRIBUNAL DE CONTAS DA UNIÃO. **Referencial básico de governança aplicável a organizações públicas e outros entes jurisdicionados ao TCU**. 3. ed. Brasília: TCU, 2020. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-publica-a-3%C2%AA-edicao-do-referencial-basico-de-governanca-organizacional. Acesso em: 14 maio 2026.

ZABRODSKYI, Mykhaylo; WATLING, Jack; DANYLYUK, Oleksandr V.; REYNOLDS, Nick. **Preliminary lessons in conventional warfighting from Russia's invasion of Ukraine**: February-July 2022. London: Royal United Services Institute, 2022. Disponível em: https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022. Acesso em: 14 maio 2026.

Autoria

1 Marcelo Carvalho Ribeiro

Bacharel em Direito, Mestre em Operações Militares, Doutor em Ciências Militares pela Universidade Federal do Rio de Janeiro; Graduado em Ciências Militares pela Academia Militar das Agulhas Negras; General de Brigada da reserva do Exército Brasileiro; Mestrando em Relações Internacionais

https://orcid.org/0000-0002-5413-3015 • marcelo.ribeiro@acad.ufsm.br

2 Mauro Beirão

Graduado em Engenharia Mecânica; Gerente de Marketing

https://orcid.org/0009-0002-6911-579X • mbeirao@ael.com.br

Como citar este artigo

RIBEIRO, M. C.; BEIRÃO, M. Da lição estratégica à capacidade nacional: governança em defesa, capital humano tecnológico e Base Industrial de Defesa no Brasil. **InterAção**, Santa Maria, v. 17, n. 2, e96728, p. 1-27, jun. 2026. DOI 10.5902/1980509896728. Disponível em: https://dx.doi.org/10.5902/2357797596728. Acesso em: dia mês abreviado. ano.