UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 2, e95275, p. 1-24, jun. 2026 • https://dx.doi.org/10.5902/2357797595275
Submissão: 30/01/2026 • Aprovação: 18/05/2026 • Publicação: 08/06/2026

Artigos Dossiê

Operações Multidomínio (MDO) no Sul Global: modelo mínimo viável para C2 e dados

MDO in the Global South: minimum viable Model for C2 and data

Ali Kamel Issmael Júnior[I]

[I]Centro Tecnológico da Marinha, Rio de Janeiro, RJ, Brasil

Resumo

Operações Multidomínio (*Multidomain Operations*, MDO) e agendas correlatas, como *Joint All-Domain Operations* (JADO) e *Joint All-Domain Command and Control* (JADC2), oriundas dos Estados Unidos da América (EUA) e da Organização do Tratado do Atlântico Norte (OTAN), reposicionam a vantagem operacional na integração de dados, conectividade e comando e controle (C2) sob contestação (EUA, 2018; 2022; OTAN, 2015; 2018). Países do Sul Global enfrentam, contudo, restrições fiscais, heterogeneidade de sistemas, dependência tecnológica e vulnerabilidades cibernéticas que dificultam a adoção de arquiteturas complexas e proprietárias. Este artigo propõe um modelo mínimo viável para MDO, entendendo-o como um conjunto incremental de capacidades materiais e não materiais capaz de gerar ganhos mensuráveis sem pressupor convergência plena a ecossistemas de alto custo. A pesquisa é qualitativa, analítica e propositiva, baseada em revisão bibliográfica e documental de documentos doutrinários e estratégicos. Como síntese, o artigo apresenta um framework em camadas (dados, integração, decisão e efeitos), uma escala de maturidade em cinco níveis, uma matriz de riscos (espectro eletromagnético, cibernético e cognitivo) com mitigação prioritária e um roteiro por fases para implementação. Para reforçar aderência institucional sem recorte de Força, utiliza-se evidência documental brasileira sobre autonomia tecnológica, continuidade de capacidades e resiliência de serviços essenciais e infraestruturas críticas (Brasil, 2020a; 2020b; 2025a; 2025b; 2025c). Conclui-se que a abordagem mínima viável reduz *lock-in*, favorece resiliência sob degradação e oferece um caminho realista para países do Sul Global ampliarem coordenação conjunta, interoperabilidade incremental e capacidade de resposta em ambientes contestados.

Palavras-chave: Operações multidomínio; Comando e controle; Integração de dados; Resiliência; Sul Global

ABSTRACT

Multidomain Operations (MDO) and related agendas, such as Joint All-Domain Operations (JADO) and Joint All-Domain Command and Control (JADC2), originating from the United States of America (USA) and the North Atlantic Treaty Organization (NATO), shift operational advantage toward integrating data, connectivity, and command and control (C2) under contestation (EUA, 2018; 2022; OTAN, 2015; 2018). Global South countries, however, face fiscal constraints, heterogeneous legacy systems, technology dependence, and cyber vulnerabilities that complicate the adoption of complex proprietary architectures. This article proposes a minimum viable model for MDO as an incremental set of material and non-material capabilities that delivers measurable gains without requiring full convergence to high-cost ecosystems. The study is qualitative, analytical, and propositional, based on a literature and document review of doctrinal and strategic sources. It synthesizes findings into a layered framework (data, integration, decision, and effects), a five-level maturity scale, a risk matrix (electromagnetic spectrum, cybernetic and cognitive) with prioritized mitigations, and a phased implementation roadmap. To reinforce institutional alignment without a service-specific focus, the paper draws on Brazilian official documents addressing technological autonomy, capability continuity, and resilience of essential services and critical infrastructures (Brasil, 2020a; 2020b; 2025a; 2025b; 2025c). The paper concludes that a minimum viable approach reduces lock-in, improves resilience under degradation, and provides a realistic pathway for Global South countries to strengthen joint coordination, incremental interoperability, and responsiveness in contested environments.

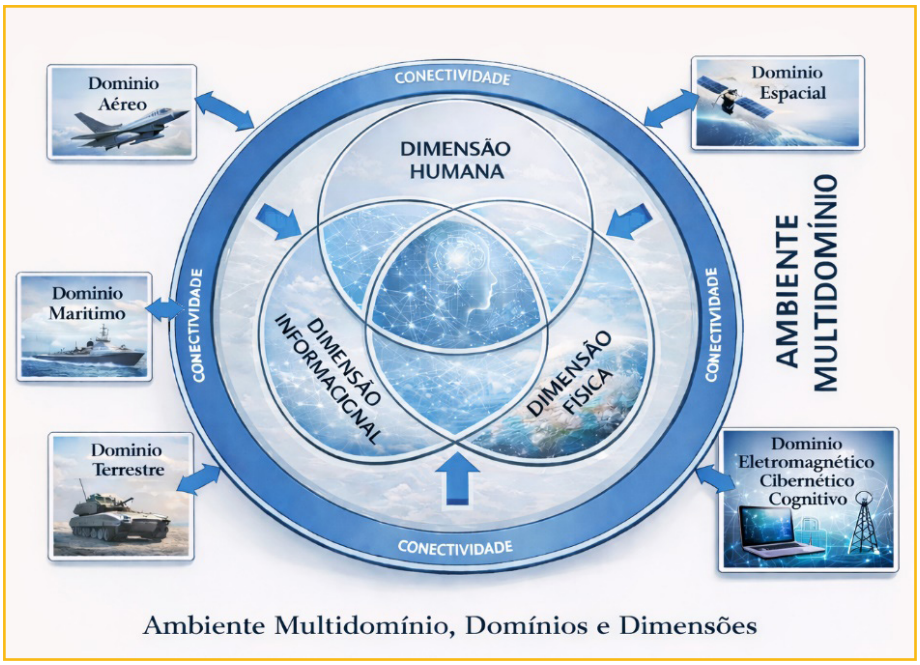
Keywords: Multi-domain operations; Command and control; Data integration; Resilience; Global South

INTRODUÇÃO

A literatura doutrinária e estratégica contemporânea tem convergido para a ideia de que a vantagem operacional, em disputas entre Estados e em cenários híbridos, decorre cada vez menos do desempenho isolado de plataformas e cada vez mais da capacidade de coordenar sensores, decisores e atuadores (efetores) em redes resilientes e informadas por dados. É nesse contexto que emergem as Operações Multidomínio (*Multidomain Operations*, MDO) e formulações correlatas, como *Joint All-Domain Operations* (JADO) e *Joint All-Domain Command and Control* (JADC2), que consolidam o Comando e Controle (C2) como função integradora, orientada por dados e capaz de operar sob contestação (EUA, 2018; 2022). Em paralelo, documentos da OTAN reforçam dimensões transversais indispensáveis a esse tipo de coordenação, como a guerra eletrônica e as operações no ciberespaço, ambas essenciais para sustentar conectividade, confiança e continuidade de comando em ambiente degradado (OTAN,

2015; 2018). No plano nacional, a Doutrina Militar de Defesa (DMiD) reconhece que as ameaças e disputas contemporâneas se manifestam em múltiplos, especialmente nos campos intensivos em tecnologia e informação, e define o Domínio Eletromagnético-Cibernético-Cognitivo como transversal, ligado ao trâmite de informações em redes, sistemas interconectados e à própria mente humana (Brasil, 2025c). A Figura 1 ilustra a visão da DMiD do ambiente multidomínio, com seus domínios e dimensões.

Figura 1 – Ambiente Multidomínio, Domínios e Dimensões



Fonte: Adaptado de DMiD (Brasil, 2025c)

Embora o conceito de MDO seja frequentemente associado a arquiteturas sofisticadas, alto grau de interoperabilidade e infraestrutura digital robusta, o desafio central para o Sul Global é que grande parte desse "pacote completo" exige investimentos prolongados, capacidade industrial e tecnológica avançada, e acesso contínuo a cadeias de suprimentos críticas. Além disso, sistemas legados heterogêneos, fragmentação institucional e assimetrias de conectividade tendem a elevar custo de integração e aumentar a vulnerabilidade a interrupções, coerção tecnológica e *lock-in*[I]

[I] *Lock-in* (aprisionamento tecnológico) é a dependência estrutural de um fornecedor, padrão proprietário ou ecossistema fechado que eleva custos de migração, reduz poder de barganha e limita interoperabilidade; em defesa, pode ampliar vulnerabilidades de suprimento, atualizações e continuidade operacional.

(aprisionamento tecnológico). Assim, para esse conjunto de países, o problema não é apenas "adotar MDO", mas definir qual porção do conceito é essencial, qual porção é incremental e qual porção é, no curto prazo, aspiracional.

Este artigo formula, portanto, a seguinte questão: como viabilizar ganhos multidomínio no Sul Global sem pressupor aquisições de alto custo e convergência plena a ecossistemas proprietários, preservando resiliência e soberania funcional. A hipótese adotada é que uma estratégia incremental, baseada em governança de dados, integração por camadas e desenho para degradação, permite capturar benefícios relevantes do paradigma multidomínio com custo controlado e risco reduzido. Em outras palavras, propõe-se um "mínimo viável" que privilegia continuidade de comando, integridade informacional e interoperabilidade pragmática, antes de perseguir a integração total.

O objetivo geral é propor um modelo mínimo viável para MDO orientado a C2 e integração de dados com resiliência. Como objetivos específicos: (i) sistematizar fundamentos e implicações tecnológicas de MDO, JADO e JADC2; (ii) estruturar um framework em camadas com requisitos mínimos; (iii) propor uma escala de maturidade aplicável a trajetórias incrementais; (iv) organizar uma matriz de riscos e medidas prioritárias de mitigação; e (v) apresentar um roteiro por fases para implementação. Para reforçar aderência institucional e evitar recorte por Força, o texto ancora a discussão também em evidências documentais brasileiras sobre autonomia tecnológica e continuidade de capacidades, além de diretrizes recentes de cibersegurança voltadas à resiliência de serviços essenciais e infraestruturas críticas.

DESENVOLVIMENTO

MDO, JADO e a centralidade do C2 orientado a dados

No núcleo das formulações de MDO está a premissa de que a coordenação entre domínios permite criar janelas de vantagem temporária, explorando assimetrias

e acelerando ciclos de decisão. A doutrina norte-americana explicita essa lógica ao enfatizar que a integração entre sensores, redes e atuadores (efetores) deve permitir identificar oportunidades, orientar efeitos e reorientar esforços com velocidade superior à do oponente (EUA, 2018). Nessa perspectiva, plataformas continuam importantes, mas sua contribuição passa a depender mais do "ecossistema" em que operam do que de suas características isoladas. Para tornar essa lógica mais intuitiva, a Figura 2 sintetiza o princípio operacional de MDO: múltiplos domínios interagindo sob uma função integradora de C2, em que a vantagem emerge menos da plataforma isolada e mais do encadeamento sensor-decisor-efetor em rede.

Figura 2 – Operações Multidomínio (MDO) centradas em C2

Fonte: Autor (2026)

A estratégia JADC2 reforça esse deslocamento ao propor, como direção de modernização, a conexão de capacidades conjuntas por meio de dados e interoperabilidade. O eixo prático, aqui, é transformar informação dispersa em consciência situacional compartilhada, garantindo rastreabilidade, integridade e disponibilidade para apoiar decisões em tempo oportuno (EUA, 2022). Trata-se de uma lógica de C2 em que o valor é produzido pela integração contínua de dados e pelo desenho de redes capazes de operar mesmo sob contestação.

Para o Sul Global, a principal implicação é que a adoção de MDO não deve ser compreendida como uma "compra" de sistemas avançados, mas como uma trajetória institucional e tecnológica. Nessa trajetória, o essencial inclui padrões mínimos de dados, procedimentos de coordenação, segurança por padrão e operação degradada. O desejável, por sua vez, tende a incluir automação avançada, integração total e ecossistemas proprietários de alto custo. O risco, se a trajetória não for bem desenhada, é a produção de um arranjo que falha justamente quando mais precisa funcionar: sob pressão, degradação de redes e ataque a infraestruturas digitais.

Evidências contemporâneas: como a lógica multidomínio tem se manifestado em conflitos recentes

Embora MDO e agendas correlatas, como JADO e JADC2, tenham nascido como formulações doutrinárias e de modernização em países centrais, seus pressupostos tecnológicos já aparecem, de modo explícito ou implícito, em episódios recentes de segurança internacional. O ponto comum é que a vantagem operacional passa a depender de três fatores combinados: (i) integração de dados entre sensores, decisores e atuadores (efetores); (ii) conectividade resiliente, inclusive em condições degradadas; e (iii) capacidade de manter o ciclo decisório e a coordenação conjunta apesar de ataques cibernéticos, contestação do espectro eletromagnético e operações de influência. Essa orientação é coerente com a ênfase de MDO em sincronização e exploração de janelas de oportunidade entre domínios, e com a lógica de JADC2 de conectar capacidades distribuídas em rede, mesmo sob interferência e degradação (EUA, 2018; 2022).

No teatro Rússia-Ucrânia, a "industrialização" de efeitos por sistemas não tripulados, a disputa permanente do espectro eletromagnético e a dependência de serviços digitais e espaciais tornaram-se elementos estruturantes do combate contemporâneo. Análises recentes apontam o conflito como um "laboratório" aberto de observação de como tecnologias são rapidamente adaptadas e militarizadas,

pressionando rotinas, doutrina e integração de capacidades em escala (Schmidt, 2024). Em termos práticos, o que se observa é um ambiente em que sensores e enlaces são continuamente contestados, com necessidade de operar com informação incompleta, atrasos e degradação deliberada. Em termos de lições operacionais, análises sobre as operações ofensivas ucranianas em 2022–2023 destacam fricções de coordenação, adaptação sob contestação e a importância de integrar reconhecimento, fogos e manobra com ciclos de aprendizagem rápidos (Watling; Danylyuk; Reynolds, 2024). A contestação do espectro eletromagnético, em particular, deixa de ser um problema "de nicho" e passa a ser requisito de coordenação de toda a força: quando o espectro é disputado, a própria coesão do C2 pode colapsar se não houver disciplina de emissões, coordenação e mecanismos de redundância (Watling; Sylvia, 2025). Isso se conecta diretamente ao "mínimo viável" proposto no artigo: sem requisitos básicos de integração, rastreabilidade e operação degradada, a promessa de MDO tende a converter-se em fragilidade sistêmica.

Ainda no caso ucraniano, a experiência com serviços espaciais e sua negação mostra que a "camada de integração" (redes, sincronização, compartilhamento) não é neutra. O emprego de comunicações por satélite, PNT[II] (*Positioning, Navigation and Timing* - Posicionamento, Navegação e Sincronização Temporal) e ISR[III] (*Intelligence, Surveillance and Reconnaissance* - Inteligência, Vigilância e Reconhecimento) comercial ampliou a capacidade de coordenação e consciência situacional, ao mesmo tempo em que expôs vulnerabilidades relevantes, como ataques cibernéticos a provedores e interferência (*jamming*[IV]) em sinais de navegação, com efeitos diretos sobre comunicações e precisão (Radin et al., 2025). Para o Sul Global, essa vulnerabilidade tende a ser agravada por restrições orçamentárias, dependência tecnológica e pela adoção de arquiteturas de "mínimo viável", nas quais mecanismos de redundância, proteção cibernética e resiliência eletromagnética podem ser menos sofisticados.

[II] *Positioning, Navigation and Timing - PNT* (posicionamento, navegação e sincronização temporal), conjunto de serviços essenciais para navegação, sincronismo e guiamento.

[III] *Intelligence, Surveillance and Reconnaissance – ISR* (inteligência, vigilância e reconhecimento), é a cadeia de coleta e processamento de informações para apoio ao comando e controle (C2).

[IV] *Jamming* é a interferência deliberada (por emissão de energia eletromagnética) para degradar ou negar o funcionamento de comunicações, enlaces de dados, radares ou sinais de navegação; pode ser pontual ou em larga área, contínuo ou intermitente, e costuma exigir contramedidas (redundância de enlaces, salto de frequência, controle de potência, modos alternativos).

Assim, a contestação no espectro eletromagnético e no ciberespaço pode criar ou explorar pontos críticos de falha, neutralizando a conectividade e comprometendo a integração dos sistemas multidomínio. Portanto, o núcleo de MDO aplicável a restrições fiscais e tecnológicas não é "ter mais plataformas", mas desenhar um arranjo mínimo de continuidade, redundâncias e governança técnica que sustente o ciclo decisório mesmo quando parte dos enlaces e serviços falhar (EUA, 2022; Radin et al., 2025).

No Sul da Ásia, os episódios de escalada e gestão de crise entre Índia e Paquistão reforçam outra faceta do problema: a integração sob contestação não é apenas um desafio tecnológico, mas também um desafio de controle, sinalização e prevenção de escalada inadvertida. Em maio de 2025, ataques e respostas na região evidenciaram como decisões são tomadas sob pressão de tempo e sob forte assimetria informacional, com riscos elevados de erro de atribuição, narrativa e cálculo político (India, 2025; Clary, 2025). Em paralelo, relatos posteriores associam a fricção do ambiente informacional e o uso crescente de sistemas não tripulados e intrusões com drones como parte de um repertório que tensiona fronteiras e rotinas de vigilância, ampliando a demanda por integração de dados e por procedimentos consistentes de reporte e validação (Arab News, 2026). Nesse tipo de cenário, um "mínimo viável" para MDO tem valor precisamente por separar o essencial do desejável: mecanismos simples, auditáveis e repetíveis de compartilhamento de informação crítica, confirmação de eventos e coordenação interagências podem reduzir ruído informacional e acelerar respostas sem exigir arquiteturas proprietárias complexas.

No Oriente Médio, os episódios envolvendo ações de EUA e Israel contra alvos relacionados ao programa nuclear do Irã, bem como o ambiente de ameaças híbridas associado a ataques, represálias e riscos de escalada, reforçam a centralidade de resiliência e integração como "capacidade de continuidade". Cobertura jornalística de referência descreve a dinâmica de advertências e pressões para negociações sob a sombra de emprego de força e de possíveis novos ataques, o que evidencia como decisões estratégicas são condicionadas por inteligência, tempo e capacidade de manter

conectividade e confiança em dados (Reuters, 2025; 2026a). Para o Sul Global, a lição não é replicar o pacote tecnológico de grandes potências, mas internalizar a lógica: quando há contestação deliberada, o valor operacional migra para (i) integridade de dados (evitar manipulação), (ii) continuidade de comunicações (rotas alternativas e modos degradados) e (iii) coordenação interdomínios com *"deconfliction"*[V] mínimo, reduzindo fratricídio e erro de engajamento. Essa orientação dialoga com doutrinas aliadas de guerra eletrônica e operações cibernéticas, que tratam o espectro eletromagnético e o ciberespaço como ambientes de manobra e disputa permanentes (OTAN 2015; 2018).

Por fim, nas Américas, a captura do presidente venezuelano Nicolás Maduro por forças dos EUA, amplamente noticiada, mostra como operações contemporâneas envolvem simultaneamente dimensões cinéticas, jurídicas, informacionais e de legitimação pública, em que narrativa e percepção influenciam custos e consequências estratégicas (Reuters, 2026b). Mesmo sem detalhar juízos de valor, esse tipo de episódio explicita uma camada frequentemente subestimada no debate tecnológico: a dimensão cognitiva, isto é, a disputa por credibilidade, confiança e adesão, que afeta coordenação e continuidade. Nesse sentido, trabalhos institucionais sobre guerra cognitiva[VI] (*cognitive warfare*) chamam atenção para como a competição se estende à percepção e à confiança social e organizacional, com implicações diretas para o processo decisório (OTAN, 2020). Para um modelo mínimo viável, isso significa estabelecer protocolos de integridade informacional, compreendendo validação de fontes, rastreabilidade, auditoria de automação e comunicação. Esses protocolos podem ser articulados à Metodologia de Produção de Conhecimento de Inteligência, que oferece uma abordagem sistemática e científica (sistemática, crítica e metodologicamente orientada) para a avaliação de dados, fontes e evidências, permitindo qualificar a confiabilidade da informação antes de sua incorporação ao processo decisório. Afinal, a integração de dados só produz vantagem se os decisores confiarem no dado e se houver mecanismos para detectar e corrigir enganos, manipulações e vieses cognitivos.

[V] *Deconfliction* (coordenação para evitar interferência/choques) é o conjunto de medidas de coordenação para evitar conflitos entre meios e efeitos (por exemplo, interferência mútua no espectro, sobreposição de frequências, rotas/altitudes, janelas de emprego), reduzindo risco de incidentes e perdas de eficácia.

[VI] Guerra cognitiva (*cognitive warfare*) refere-se a ações e operações destinadas a influenciar, degradar ou capturar processos cognitivos de indivíduos e grupos (percepção, atenção, confiança, julgamento e tomada de decisão), por meio de técnicas informacionais e psicossociais que exploram vieses, emoções e dinâmicas sociais. Diferentemente da "propaganda" clássica, opera de forma persistente e adaptativa (inclusive com plataformas digitais), buscando efeitos estratégicos como erosão de coesão, perda de credibilidade institucional e distorção do ciclo decisório.

Em síntese, esses episódios recentes convergem para uma conclusão operacional: MDO, no que importa ao Sul Global, pode ser entendido como capacidade de integrar informação e coordenar efeitos em ambiente contestado, sustentando o C2 apesar de ataques ao ciber, interferência no espectro e operações cognitivas. A consequência metodológica para o artigo é direta: o "mínimo viável" deve ser concebido desde a origem como desenho para degradação e continuidade, isto é, como um conjunto incremental de requisitos de governança de dados, integração interoperável e rotinas de decisão que permaneçam funcionais quando a arquitetura ideal falha (EUA, 2022; Watling; Sylvia, 2025).

Em termos de síntese comparativa, a Figura 3 organiza os episódios discutidos nesta seção, explicitando (i) onde a cadeia sensor–decisor–efetor foi ampliada ou degradada, (ii) como ciber e espectro afetaram conectividade e confiança, e (iii) quais vulnerabilidades recorrentes aparecem quando se tenta coordenar efeitos sob contestação — precisamente o tipo de pressão que um 'mínimo viável' precisa absorver.

Figura 3 – Casos contemporâneos e "lições MDO"

Fonte: Autor (2026)

Dimensões transversais e riscos sistêmicos

A adoção de um conceito multidomínio expõe riscos que podem comprometer o C2 e colapsar a integração de dados. Este artigo organiza esses riscos nas três classes pertencentes ao Domínio Eletromagnético-Cibernético-Cognitivo, por seu potencial sistêmico de impactar todos os demais (terrestre, marítimo aéreo e espacial), sendo essa opção é consistente com a DMiD, que explicita este domínio como transversal e relacionado ao trâmite de informações em redes/sistemas e à dimensão cognitiva humana, justamente por afetar integração, confiança e decisão ao longo de todos os demais domínios (Brasil, 2025c).

Os riscos cibernéticos incidem diretamente sobre confidencialidade, integridade e disponibilidade. Em ambientes multidomínio, a integridade do dado torna-se tão crítica quanto a disponibilidade do enlace: manipulação de dados, comprometimento de credenciais e ataques a cadeias de software podem produzir decisões erradas com aparência de normalidade. A doutrina de operações no ciberespaço ressalta a natureza persistente, escalável e transversal desse vetor, reforçando a necessidade de controles de acesso, monitoramento e resiliência (OTAN, 2018). No Brasil, a Estratégia Nacional de Cibersegurança reforça a prioridade de resiliência de serviços essenciais e infraestruturas críticas, alinhando-se ao requisito de continuidade do C2 e dos serviços digitais de apoio (Brasil, 2025a; 2025b; 2025c).

Os riscos no espectro eletromagnético incluem interferência, *jamming, spoofing*[VII] e "fratricídio" eletromagnético[VIII]. Em termos práticos, a degradação do espectro pode reduzir drasticamente a eficácia de sensores e comunicações, fragmentando o quadro situacional e dificultando a coordenação. A doutrina de guerra eletrônica da OTAN e a doutrina norte-americana de operações no espectro detalham a centralidade desse ambiente como condição para o emprego de capacidades modernas (OTAN, 2015; EUA, 2023). Para um "mínimo viável", isso implica que procedimentos de coordenação e alternativas de enlace devem ser projetados desde o início.

[VII] *Spoofing* é a falsificação de sinais ou dados (por exemplo, de navegação por satélite ou de identificação/telemetria) para induzir o sistema a 'acreditar' em informações falsas, produzindo erro de posicionamento, identificação ou decisão; diferencia-se de *jamming* porque não apenas nega o sinal, mas o substitui por um sinal enganoso.

[VIII] Fratricídio eletromagnético é a degradação involuntária de sistemas 'amigos' causada por interferências geradas pela própria força (emissões, contramedidas, saturação de espectro), resultando em perda de comunicações, degradação de sensores ou falhas de enlace sem ação direta do adversário; é mitigado por coordenação e disciplina de emissões.

Por fim, os riscos cognitivos e informacionais incluem desinformação, manipulação de narrativas e engenharia social[IX], com potencial de corroer confiança e induzir decisões enviesadas. A discussão sobre guerra cognitiva destaca que a disputa pode buscar afetar percepção, credibilidade de fontes e coesão decisória, gerando efeito estratégico sem engajamento cinético (OTAN, 2020). Em um arranjo multidomínio, o risco cognitivo se agrava quando a integração produz excesso de informação sem governança, ou quando automações não são auditáveis.

A consequência é direta: o modelo mínimo viável precisa incorporar mitigação desses riscos como requisitos de projeto e não como "camadas adicionadas" posteriormente.

Evidências documentais brasileiras relevantes ao modelo mínimo viável

No Brasil, documentos estruturantes de defesa e de política pública destacam autonomia tecnológica e continuidade de capacidades como componentes de soberania e de efetividade estratégica (Brasil, 2020a; 2020b). Embora não sejam documentos específicos sobre MDO, eles oferecem base conceitual para uma abordagem incremental: preservar capacidades essenciais, reduzir dependências críticas e sustentar continuidade operacional em cenários adversos.

Adicionalmente, ao estabelecer diretrizes para a cibersegurança nacional, o país enfatiza resiliência de serviços essenciais e de infraestruturas críticas, o que se conecta diretamente à necessidade de continuidade do C2 e dos serviços de integração de dados em ambiente contestado (Brasil, 2025a; 2025b). Assim, a proposta de "mínimo viável" apresentada neste artigo dialoga com esses fundamentos ao priorizar resiliência, governança e continuidade como critérios de implementação.

[IX] Engenharia social são técnicas de manipulação psicológica e exploração de confiança para induzir usuários a revelar credenciais, executar ações inseguras ou legitimar informações falsas; em MDO, afeta diretamente o vetor cognitivo e a integridade do processo decisório.

METODOLOGIA

A pesquisa é qualitativa, analítica e propositiva. O procedimento central foi uma revisão bibliográfica e documental de referências doutrinárias e estratégicas associadas a MDO/JADO/JADC2 dos EUA e da OTAN, por já virem estudando o assunto há bastante tempo e também por já, em algum nível, concretizando as MDO, e às dimensões transversais que condicionam sua operacionalização: operações no ciberespaço, guerra eletrônica e operações no espectro eletromagnético, bem como aspectos cognitivo-informacionais (EUA, 2018; 2022; 2023; OTAN, 2015; 2018; 2020). Complementarmente, foram mobilizados documentos brasileiros que fornecem fundamentos de autonomia tecnológica e de resiliência cibernética, permitindo ancoragem institucional sem recorte por Força (Brasil, 2020a; 2020b; 2025a; 2025b;).

A síntese foi estruturada em quatro artefatos de saída: (i) um framework em camadas para organizar requisitos mínimos; (ii) uma escala de maturidade em cinco níveis para orientar progressão incremental; (iii) uma matriz de riscos com mitigação prioritária; e (iv) um roteiro por fases para implementação. O método não pretende "provar" superioridade de um arranjo específico, mas oferecer um modelo de referência e um caminho de adoção compatível com restrições típicas do Sul Global.

RESULTADOS E DISCUSSÃO

Framework mínimo viável em camadas

A proposta central deste artigo é que as MDO, no Sul Global, podem ser operacionalizadas por uma arquitetura em camadas que separa claramente fundamentos de integração, mecanismos decisórios e produção de efeitos. Essa separação reduz complexidade, melhora governança e facilita investimentos incrementais, evitando a dependência de uma "integração total" como condição de funcionamento. Como visão de conjunto, a Figura 4 explicita as dependências entre

camadas e a lógica de construção incremental do modelo mínimo viável, deixando claro o que precisa existir ‘antes’ para que as camadas superiores funcionem sob degradação.

Figura 4 – Framework do modelo mínimo viável (camadas e dependências)

Fonte: Adaptado de (EUA, 2022) e (Brasil, 2020a)

A Camada 1 (Dados) define o que é essencial para produzir confiança: taxonomias mínimas, metadados, classificação e trilha de auditoria. Sem esses elementos, o sistema pode até transmitir informação, mas não garante integridade, rastreabilidade nem priorização. A Camada 2 (Integração) trata da interoperabilidade pragmática: padrões mínimos de mensagem e *gateways*[X] para sistemas legados, com redundância e procedimentos de *fallback*[XI]. A Camada 3 (Decisão) formaliza rotinas de C2, regras de coordenação e *playbooks*[XII], buscando assegurar consistência e continuidade mesmo

[X] Um *gateway* é um dispositivo ou serviço que funciona como uma “porta de entrada” e “saída”, conectando duas redes ou sistemas diferentes, permitindo a comunicação e troca de dados entre eles, mesmo que usem protocolos ou arquiteturas distintas, atuando como um tradutor de protocolos e um ponto de controle de tráfego, como um roteador doméstico ou um processador de pagamentos online.

[XI] *Fallback* é um mecanismo de segurança, plano de contingência ou alternativa que entra em ação quando o sistema, processo ou opção primária falha ou não está disponível. Em tecnologia, garante a continuidade, revertendo para uma funcionalidade mais simples ou um método de backup (ex: tarja magnética quando o chip falha).

[XII] Um *playbook* é um guia prático e abrangente que documenta as melhores práticas, estratégias, processos e fluxos de trabalho

sob degradação. Por fim, a Camada 4 (Efeitos) organiza coordenação de tarefas, *deconfliction* e avaliação de efeitos, reduzindo risco operacional e promovendo aprendizagem institucional.

A Tabela 1 consolida esse framework, detalhando objetivo operacional, requisitos mínimos e entregáveis verificáveis por camada, de modo a transformar 'integração' em critérios auditáveis de progresso.

Tabela 1 – Camadas do modelo mínimo viável e requisitos mínimos por camada

Camada	Objetivo operacional	Requisitos mínimos (tecnologia e processo)	Entregáveis verificáveis
1. Dados	Disponibilizar dados confiáveis e rastreáveis para C2	Taxonomias mínimas; metadados; níveis de classificação; trilha de auditoria; qualidade de dados (validação básica); catálogo de dados essenciais	Catálogo de dados; dicionário de dados; política de classificação; logs de ingestão e acesso; indicadores de qualidade
2. Integração	Trocar informação crítica em redes heterogêneas, inclusive degradadas	Padrões mínimos de mensagem; *gateways* para sistemas legados; sincronização temporal básica; redundância de enlace; procedimentos de *fallback*; gestão de identidades e chaves	Conjunto de mensagens padronizadas; gateway operacional; plano de comunicações degradadas; matriz de interoperabilidade mínima
3. Decisão (C2)	Coordenar e priorizar efeitos com consistência e velocidade	Rotinas de C2; regras de coordenação; *playbooks*; gestão de incidentes; apoio analítico governado; exercícios regulares	Procedimentos operacionais padrão; *playbooks* de decisão; registro de decisões; indicadores de tempo de ciclo
4. Efeitos	Executar e avaliar efeitos evitando conflito e fratricídio	Coordenação de tarefas e prioridades; *deconfliction* no espectro; confirmação e avaliação de efeito; lições aprendidas; regras de segurança operacional	Checklist de coordenação; protocolo de confirmação; registro de avaliação; relatório de lições aprendidas

Fonte: Adaptado de (EUA, 2022) e (Brasil, 2020a)

A principal vantagem analítica do modelo em camadas é que ele permite medir progresso: cada camada possui entregáveis verificáveis e pode evoluir por incrementos. Isso reduz risco de projetos "tudo ou nada", em que a integração total é prometida, mas a governança e a resiliência ficam para depois.

Escala de maturidade

Para orientar trajetórias realistas, a escala de maturidade define cinco níveis:

– O Nível 1 caracteriza integração *ad hoc*[XIII], com baixa rastreabilidade e predominância de trocas manuais;

– O Nível 2 introduz *gateways* operacionais e controles básicos de identidade;

– O Nível 3 institucionaliza governança de dados e operação degradada, com exercícios e métricas;

– O Nível 4 amplia coordenação com apoio analítico governado e práticas de validação;

– O Nível 5 busca orquestração resiliente e avaliação contínua, mantendo desempenho sob contestação.

A progressão não pressupõe aquisição de um "sistema mágico". Ela pressupõe evolução combinada de tecnologia, processos e treinamento, coerente com a lógica de JADC2 (integração e resiliência) e com diretrizes nacionais de continuidade e resiliência de serviços essenciais (EUA, 2022; Brasil, 2025a; 2025b).

Para evitar descrições apenas qualitativas, a Tabela 2 traduz os cinco níveis em capacidades mínimas e critérios objetivos de passagem, permitindo diagnóstico e planejamento por incrementos (do *ad hoc* à orquestração resiliente).

[XIII] Integração *ad hoc* (para este fim) refere-se a um método de conexão entre sistemas, aplicações ou fontes de dados criado especificamente para atender a um propósito pontual, necessidade imediata ou situação única.

Tabela 2 – Níveis de maturidade do modelo mínimo viável e critérios de progressão

Nível	Caracterização	Capacidades mínimas presentes	Critério de passagem
1	Integração *ad hoc* e fragmentada	Catálogo inicial de dados e mensagens; troca predominantemente manual; baixa rastreabilidade	Mensagens mínimas definidas e usadas de modo consistente em rotinas críticas
2	Integração assistida por *gateways*	*Gateways* operacionais; controles básicos de identidade; logs mínimos; procedimentos de *fallback*	Troca de informação crítica em tempo operacional entre pelo menos dois sistemas heterogêneos
3	Governança de dados e operação degradada	Metadados e auditoria; qualidade de dados; exercícios de degradação; plano de continuidade	Execução de rotinas de C2 em modo degradado com métricas de desempenho e lições aprendidas
4	Coordenação ampliada com apoio analítico governado	Análises para triagem e priorização; validação e monitoramento; *red teaming* básico[XIV]	Redução sustentada do tempo de ciclo sem aumento de incidentes e com auditoria
5	Orquestração resiliente e avaliação contínua	Integração ampla; coordenação de espectro; avaliação de efeito sistemática; melhoria contínua	Manutenção de C2 sob contestação com degradação graciosa e indicadores estáveis

Fonte: Adaptado de (EUA, 2022), (Brasil, 2020a) e (Brasil, 2025a; 2025b)

Matriz de riscos e mitigação prioritária

A Tabela 3 organiza riscos por vetores com potencial sistêmico. O objetivo não é "esgotar" o conjunto de ameaças, mas orientar priorização: em ambientes com restrição fiscal e tecnológica, a escolha de mitigação precisa privilegiar medidas com alto impacto de resiliência e baixo risco de *lock-in*.

A leitura recomendada é por componente do domínio eletromagnético-ciber-cognitivo, pois cada um pode degradar simultaneamente dados, integração e decisão, impactando também os outros domínios. Por isso, o modelo mínimo viável deverá enfatizar a gestão de identidades e acessos, o registro sistemático de eventos, a manutenção de cópias de segurança protegidas contra alterações, a gestão de

[XIV] *Red Teaming* (Equipe Vermelha) básico consiste na simulação de ataques cibernéticos e físicos do mundo real para testar as defesas de uma organização (pessoas, processos e tecnologias). Diferente de um teste de penetração (*pen test*) convencional, que busca vulnerabilidades técnicas, o *Red Teaming* foca em um objetivo específico (como roubar dados sensíveis) agindo como um "adversário ético" para avaliar a capacidade de detecção e resposta (*Blue Team*).

vulnerabilidades no domínio cibernético, a coordenação e disciplina de emissões eletromagnéticas, a adoção de protocolos de integridade informacional e a capacitação contra ações cognitivas, dentre outras (OTAN, 2015; 2018; 2020; Brasil, 2020a; 2020b; Brasil, 2025a; 2025b; 2025c).

Tabela 3 – Matriz de riscos (domínio eletromagnético-ciber-cognitivo) e mitigação prioritária

Vetor de risco	**Ameaças típicas**	**Impacto no C2 e na integração**	**Mitigações prioritárias (mínimo viável)**	**Indicadores de controle**
Espectro eletromagnético (EEltmg)	Interferência; *jamming; spoofing*; fratricídio eletromagnético; degradação de enlaces	Perda de sensores e comunicações; falha de coordenação; aumento de risco operacional	Coordenação e *deconfliction*; procedimentos de reporte; redundâncias de enlace; modos alternativos; disciplina de emissões	Taxa de interrupção; tempo de restabelecimento; incidentes de fratricídio; disponibilidade de enlace
Ciber	Comprometimento de credenciais; *exfiltração*[XV]; manipulação de dados; *ransomware*[XVI]; vulnerabilidades de cadeia de software (*supply chain*)[XVII]	Perda de confiança no dado; indisponibilidade; decisões incorretas; interrupção operacional	Gestão de identidades e acessos; segmentação; criptografia de mensagens críticas; backup imutável; *logging* centralizado; gestão de vulnerabilidades	Tempo de detecção; taxa de incidentes; tempo de recuperação; cobertura de logs; conformidade de acesso
Cognitivo e informacional	Desinformação; campanhas de influência; manipulação de narrativas; engenharia social	Erosão de confiança; decisões enviesadas; ruptura de coordenação	Protocolos de integridade informacional; treinamento; validação de fontes; governança de comunicação; auditoria de automação	Incidentes de engenharia social; tempo de correção; aderência a protocolos; confiança percebida em canais

Fonte: Adaptado de (Brasil, 2025a; 2025b), (Brasil, 2020b) e (OTAN, 2015; 2018; 2020; EUA, 2023)

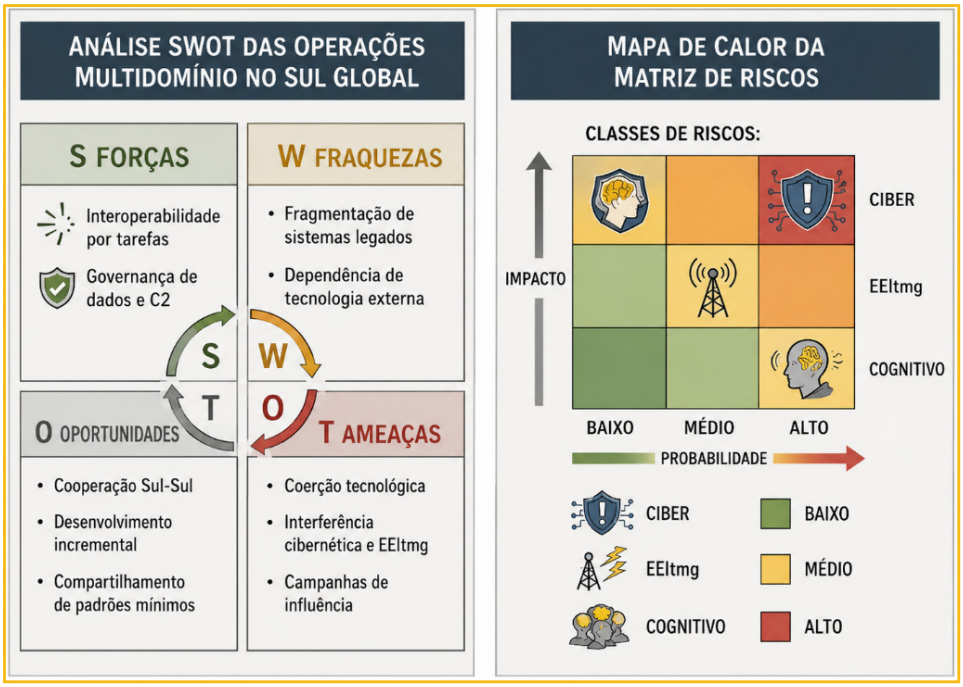
[XV] Exfiltração é a extração não autorizada de dados para fora do ambiente protegido, com potencial de comprometer operações, inteligência e confiança na integridade/segurança do C2.

[XVI] *Ransomware* é um tipo de malware que cifra ou bloqueia sistemas/dados e exige resgate, frequentemente combinado com exfiltração e ameaça de vazamento ('double extortion'), afetando diretamente a disponibilidade e continuidade de serviços.

[XVII] Ataques à cadeia de software (supply-chian) exploram dependências e etapas do ciclo de desenvolvimento/distribuição (bibliotecas, atualizações, assinaturas, fornecedores) para inserir código malicioso de forma 'legítima', com alto potencial de impacto sistêmico.

Para facilitar a priorização executiva (o que mitigar primeiro, com maior retorno de resiliência), a Figura 5 resume a Tabela 3 em duas leituras complementares: uma visão SWOT (pressões internas/externas – Forças, Fraquezas, Oportunidades e Ameaças) e um mapa de calor de criticidade, útil para decisão de investimento incremental.

Figura 5 – Síntese estratégica dos riscos: matriz SWOT e mapa de calor da Tabela 3



Fonte: Autor (2026)

Roteiro por fases para implementação

A operacionalização do mínimo viável exige uma sequência por fases que compatibilize entregas com aprendizado institucional. Na fase inicial, o foco deve recair sobre padronização mínima de dados, catálogo e mensagens essenciais, além de *gateways* para reduzir fragmentação. Na fase seguinte, a prioridade é consolidar governança, controles de identidade e rotinas de C2, acompanhadas de exercícios de degradação e continuidade. Em fases mais avançadas, amplia-se interoperabilidade, coordenação do espectro e apoio analítico governado, sempre com auditoria e métricas de desempenho, coerentes com diretrizes de modernização de C2 orientado a dados (EUA, 2022) e com diretrizes de resiliência de serviços essenciais (Brasil, 2025a; 2025b).

A Figura 6 consolida esse roteiro por fases, vinculando marcos de governança, integração e resiliência a entregas progressivas, de modo que o leitor visualize uma trajetória realista (do essencial ao avançado) sem pressupor convergência imediata a ecossistemas proprietários.

Figura 6 – Roteiro por fases do modelo mínimo viável

Fonte: Adaptado de (EUA, 2022) e (Brasil, 2025a; 2025b)

CONCLUSÃO

Este artigo propôs um modelo mínimo viável para Operações Multidomínio no Sul Global, estruturando o problema como uma trajetória incremental de capacidades e não como adoção imediata de arquiteturas completas. A proposta organiza-se em quatro camadas e busca tornar explícito o que é essencial para obter ganhos mensuráveis: governança de dados, integração pragmática, rotinas consistentes de C2 e coordenação de efeitos com avaliação. Ao introduzir uma escala de maturidade, o texto oferece um instrumento para planejar progressão verificável e reduzir risco de projetos maximalistas.

A matriz de riscos, por sua vez, evidencia que a operacionalização de MDO depende de mitigação integrada no domínio ciber, espectro eletromagnético (EEltmg) e cognitivo. Para o Sul Global, onde recursos e infraestrutura podem ser limitados, a prioridade deve ser resiliência sob degradação, integridade informacional e continuidade do comando. Essa orientação está alinhada tanto com diretrizes internacionais sobre C2 orientado a dados e contestação (EUA, 2018; 2022; OTAN, 2015; 2018) quanto com diretrizes brasileiras de autonomia e de resiliência de serviços essenciais e infraestruturas críticas (Brasil, 2020a; 2020b; 2025a; 2025b).

Em termos de contribuição, o modelo mínimo viável proposto oferece um arcabouço operacionalizável, com camadas, maturidade, matriz de riscos e roteiro por fases, para orientar decisões de investimento e priorização sob restrições típicas do Sul Global, com ênfase em ganhos mensuráveis e resiliência sob degradação. Reconhece-se, como limitação, a necessidade de validação empírica sistemática em diferentes arranjos organizacionais e perfis de ameaça. Ainda assim, ao deslocar o foco de arquiteturas ideais para progresso verificável e governança, o artigo fornece um caminho replicável para elevar interoperabilidade incremental e continuidade do C2 em ambientes contestados, em alinhamento com diretrizes internacionais e nacionais correlatas mais atuais, uma vez que o status desse tema avança de forma intensa e rápida, conforme os casos de conflitos mencionados neste artigo.

Como agenda futura, recomenda-se: (i) operacionalizar indicadores quantitativos por nível de maturidade; (ii) testar a abordagem em exercícios com degradação controlada de enlaces e serviços; (iii) avaliar custo-benefício de medidas de resiliência frente a investimentos em desempenho “em condições ideais”; e (iv) investigar mecanismos de governança interorganizacional capazes de reduzir fragmentação e melhorar interoperabilidade incremental.

REFERÊNCIAS

ARAB NEWS. **India has told Pakistan to control 'drone intrusions,' Indian army chief says.** 13 jan. 2026. Disponível em: https://www.arabnews.com/node/2629161/pakistan. Acesso em: 29 jan. 2026.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF: Ministério da Defesa, 2020a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congressonacional_22_07_2020.pdf. Acesso em: 27 jan. 2026.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Brasília, DF: Ministério da Defesa, 2020b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf. Acesso em: 27 jan. 2026.

BRASIL. **Decreto nº 12.573, de 4 de agosto de 2025**. Institui a Estratégia Nacional de Cibersegurança. Diário Oficial da União, Brasília, DF, 5 ago. 2025a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Acesso em: 27 jan. 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, 2025b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12725.htm. Acesso em: 27 jan. 2026.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa: DMiD (MD51-M-04). 3. ed.** Brasília, DF: Ministério da Defesa, 2025. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/md51-m-04-doutrina-militar-de-defesa-dmid-3a-ed-2025.pdf. Acesso em: 30 jan. 2026.

CLARY, Christopher. **Four Days in May: Understanding India and Pakistan's 2025 Crisis.** Washington, DC: Stimson Center, 2025. Disponível em: https://www.stimson.org/2025/four-days-in-may-the-india-pakistan-crisis-of-2025/. Acesso em: 29 jan. 2026.

ESTADOS UNIDOS (EUA). Department of the Army. U.S. Army Training and Doctrine Command. **TRADOC Pamphlet 525-3-1: The U.S. Army in Multi-Domain Operations 2028**. Fort Eustis, VA: TRADOC, 2018. Disponível em: https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf. Acesso em: 27 jan. 2026.

ESTADOS UNIDOS (EUA). Department of Defense. **Summary of the Joint All-Domain Command and Control (JADC2) Strategy**. Washington, DC: DoD, 2022. Disponível em: https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF. Acesso em: 27 jan. 2026.

ESTADOS UNIDOS (EUA). Department of the Air Force. **Air Force Doctrine Publication (AFDP) 3-85: Electromagnetic Spectrum Operations**. Washington, DC: DAF, 2023. Disponível em: https://img.antpedia.com/standard/files/pdfs_ora/20240203/Air%20Force%20Doctrine%20Publication%20AFDP%203-85%20%EF%BC%882023%EF%BC%89.pdf . Acesso em: 27 jan. 2026.

INDIA. Ministry of External Affairs. **Special briefing on OPERATION SINDOOR (May 08, 2025).** New Delhi: MEA, 2025. Disponível em: https://www.mea.gov.in/Speeches-Statements.htm?dtl/39478. Acesso em: 29 jan. 2026.

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE (OTAN). **AJP-3.10: Allied Joint Doctrine for Electronic Warfare**. Bruxelas: OTAN, 2015. Disponível em: https://mpsotc.army.gr/wp-content/uploads/2024/03/2.-AJP-3.10-EDA-V1-E.pdf. Acesso em: 27 jan. 2026.

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE (OTAN). **AJP-3.20: Allied Joint Doctrine for Cyberspace Operations**. Bruxelas: OTAN, 2018. Disponível em: https://iwar.org.uk/wp-content/uploads/2021/06/AJP-3.20-EDA-V1-E.pdf. Acesso em: 27 jan. 2026.

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE (OTAN). **Cognitive Warfare**. Norfolk, VA: Allied Command Transformation, 2020. Disponível em: https://innovationhub-act.org/wp-content/uploads/2023/12/20210122_CW-Final.pdf. Acesso em: 27 jan. 2026.

RADIN, Andrew; HOLYNSKA, Khrystyna; TRETTER, Cheyenne; VAN BIBBER, Thomas. **Lessons from the War in Ukraine for Space: Challenges and Opportunities for Future Conflicts.** Santa Monica, CA: RAND Corporation, 2025. Disponível em: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2900/RRA2950-1/RAND_RRA2950-1.pdf. Acesso em: 29 jan. 2026.

REUTERS. **US warns against Iran retaliation as Trump raises 'regime change'.** 23 jun. 2025. Reuters. Disponível em: https://www.reuters.com/world/middle-east/us-strikes-against-iran-nuclear-facilities-incredible-overwhelming-success-2025-06-22/. Acesso em: 29 jan. 2026.

REUTERS. Trump tells Iran to make nuclear deal or next attack will be far worse. Reuters, 28 jan. 2026a. Disponível em: https://www.reuters.com/world/middle-east/trump-tells-iran-make-nuclear-deal-or-next-attack-will-be-far-worse-2026-01-28/. Acesso em: 29 jan. 2026.

REUTERS. Condemnation and applause in Latin America after US seizes Venezuela's Maduro. *Reuters*, 3 jan. 2026b. Disponível em: https://www.reuters.com/world/americas/condemnation-applause-latin-america-after-us-seizes-venezuelas-maduro-2026-01-03. Acesso em: 29 jan. 2026.

SCHMIDT, Todd A. **The Russia-Ukraine Conflict Laboratory: Observations Informing IAMD.** Military Review, Space & Missile Defense Special Edition, 2024. Disponível em: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/March-2024/Russia-Ukraine-Conflict-Laboratory/Russia-Ukraine-Conflict-Laboratory-UA.pdf. Acesso em: 29 jan. 2026.

WATLING, Jack; DANYLYUK, Oleksandr V.; REYNOLDS, Nick. *Preliminary Lessons from Ukraine's Offensive Operations, 2022–23*. London: Royal United Services Institute, 2024. Disponível em: https://static.rusi.org/lessons-learned-ukraine-offensive-2022-23.pdf. Acesso em: 29 jan. 2026.

WATLING, Jack; SYLVIA, Noah. *Competitive Electronic Warfare in Modern Land Operations*. London: Royal United Services Institute, 2025. Disponível em: https://static.rusi.org/competitive-electronic-warfare-in-land-operations_1.pdf. Acesso em: 29 jan. 2026.

Autoria

1 Ali Kamel Issmael Júnior

Bacharel em Engenharia Elétrica com ênfase em Sistemas Eletrônicos pela Universidade do Estado do Rio de Janeiro; MSc. em Engenharia Elétrica pelo Centro Federal de Educação Tecnológica Celso Suckow da Fonseca; Doutor em Ciências Navais pela Escola de Guerra Naval; Oficial Superior do Corpo de Engenheiros da Marinha no posto de Capitão de Mar e Guerra (EN); Superintendente Técnico
https://orcid.org/0000-0001-8846-400X • alikamel1974@gmail.com

Como citar este artigo

ISSMAEL JÚNIOR, A. K. Operações Multidomínio (MDO) no Sul Global: modelo mínimo viável para C2 e dados. **InterAção**, Santa Maria, v. 17, n. 2, e95275, p. 1-24, jun. 2026. DOI 10.5902/1980509895275. Disponível em: https://dx.doi.org/10.5902/2357797595275. Acesso em: dia mês abreviado. ano.