ARTIGO DOI 10.52781/cmm.a202

Uma nova visão para a Rede Operacional de Defesa (ROD): Integração a Níveis de Pessoas, Processos e Tecnologias

A new vision for the Defense Operational Network (DON): Integration at the Levels of People, Processes and Technologies

Resumo: O atual cenário mundial, marcado por forte interdependência entre países e rápidas transformações políticas, econômicas e tecnológicas, tem acentuado a instabilidade em diversas regiões. Disputas comerciais, informacionais e cibernéticas ocorrem constantemente, e as Forças de Defesa Internacionais repensam suas estratégias: ou intensificam sua cooperação para superar desafios comuns, ou adotam uma reestruturação profunda, adequando-se às exigências do presente. A doutrina brasileira prevê integrações periódicas em operações conjuntas, enquanto, diariamente, cada Força Singular tem seus próprios objetivos, planejamentos e ações, que, de forma autônoma, coordenam internamente sua infraestrutura de Tecnologia da Informação e Comunicações. Este artigo propõe uma nova visão para a Rede Operacional de Defesa (ROD), capaz de agregar capacidades conjuntas e integrar continuamente pessoas, processos e tecnologias. Nesse quadro tão dinâmico, caro e com escassez de investimentos, a união de esforços no planejamento e na construção de uma infraestrutura única e flexível pode acelerar o desenvolvimento e o poder de defesa nacional.

Palavras-chave: Ciências Militares; Defesa; Integração; Rede Operacional de Defesa; SD-WAN.

Abstract: The current global scenario, marked by strong interdependence between countries and rapid political, economic, and technological transformations, has exacerbated instability in several regions. Trade, information, and cyber disputes are constantly occurring, and the International Defense Forces are rethinking their strategies: either intensifying cooperation to overcome common challenges or adopting a profound restructuring to adapt to current demands. Brazilian doctrine provides for periodic integrations in joint operations, while each Singular Force has its own daily objectives, plans, and actions, which coordinate their Information and Communications Technology infrastructure internally. This article proposes a new vision for the Defense Operational Network, capable of aggregating joint capabilities and continuously integrating people, processes, and technologies. In such a dynamic, costly, and underinvested environment, joint efforts in planning and building a single, flexible infrastructure can accelerate the development and power of national defense.

Keywords: Military Science; Defense; Defense Operational Network; Integration; SD-WAN

Igor David Brito Caldeira
Exército Brasileiro. Instituto Militar de Engenharia (IME). Programa de Pós-Graduação em Engenharia de Defesa (PGED).
Rio de Janeiro, RJ, Brasil.
caldeira.igor@ime.eb.br

Ronaldo Moreira Salles
Exército Brasileiro. Instituto Militar de Engenharia (IME). Programa de Pós-Graduação em Engenharia de Defesa (PGED).
Rio de Janeiro, RJ, Brasil.
salles@ime.eb.br

Recebido: 30 jul. 2025
Aprovado: 09 abr. 2026

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 INTRODUÇÃO

Na história militar mundial, as ações integradas entre as Forças Armadas (FFAA) são comuns. Entretanto, a grande e rápida evolução tecnológica, acelerada e potencializada pelo desenvolvimento da Inteligência Artificial (IA), tem impulsionado a reformulação de conceitos e doutrinas que impactam na arte da guerra na atualidade.

No início da década de 2020, lideranças americanas agiram em prol da ampliação e do desenvolvimento de sistemas conjuntos nos Estados Unidos, sinalizando requisitos de evolução de sistemas e integração de capacidades conjuntas (Estados Unidos da América, 2021). Ainda mais detalhadamente, desenvolveu-se uma estratégia específica para a integração completa de Comando e Controle (C^2) Conjunto e Integrado, chamada de "*Joint All-Domain Command and Control (JADC2) Strategy*" (Estados Unidos da América, 2022).

Outros países perceberam as mudanças no modelo dos confrontos recentes globais, como os observados na guerra entre Rússia e Ucrânia, na qual os atacados desenvolveram rapidamente as "*Unmanned Systems Forces*", uma nova força armada não tripulada com capacidade de atuar por terra, mar e ar na linha de frente da batalha, com mais de 2.000 km de alcance (Ucrânia, 2025). De forma alinhada e ainda mais ampla, o Reino Unido divulgou recentemente uma política integrada que coordena sua jornada de migração de operação conjunta para integrada nos próximos dez anos, sinalizando, inclusive, para a criação de uma nova Força Integrada (Reino Unido, 2025), responsável pela sustentação da base digital comum e pela gestão dos dados compartilhados, tão essenciais para o novo modelo de guerra definida por software.

Apesar dos avanços doutrinários, a Rede Operacional de Defesa (ROD) brasileira ainda enfrenta o desafio da fragmentação, operando como um arranjo de sistemas independentes (Recim, EBNet e Intraer) com gestões isoladas. A lacuna identificada reside na ausência de um modelo que integre essas infraestruturas, não apenas tecnologicamente, mas também de forma articulada com pessoas e processos organizacionais. Diante disso, este artigo responde à seguinte pergunta de pesquisa: como viabilizar uma infraestrutura de conectividade única e flexível que atenda aos requisitos de soberania e interoperabilidade das Forças Armadas? O objetivo deste trabalho é propor uma nova visão para a ROD, fundamentada na tecnologia *Software-Defined Wide Area Network* (SD-WAN), que funcione como um sistema de sistemas integrado sob uma governança compartilhada.

A contribuição principal deste manuscrito é a proposição de um modelo organizacional e conceitual de integração da ROD. Este estudo não se limita ao diagnóstico, mas projeta uma arquitetura de rede de longa distância definida por software (SD-WAN) como o motor para a evolução da base digital comum da Defesa. Nesse sentido, o mundo caminha para fomentar uma evolução doutrinária de aproximação entre as FFAA e consolidar a infraestrutura de operações conjuntas, desde seu planejamento até o cumprimento da missão finalística. A seguir, será apresentada uma nova visão para a ROD, buscando maior integração da infraestrutura de conectividade e de dados nos níveis de pessoas, processos e tecnologias, em colaboração com o crescimento do compartilhamento de força de trabalho, conhecimento e investimentos. Assim, será possível uma completa integração informacional, bem como uma maior segurança cibernética aliando potenciais da IA na solução e no enfrentamento de vulnerabilidades e ameaças, provendo, também, a demonstração de evolução na obtenção dos objetivos nacionais permanentes.

2 REVISÃO TEÓRICA, DESENVOLVIMENTO E METODOLOGIA

No final da última década, o Brasil atualizou e estabeleceu novos procedimentos para nortear as operações conjuntas no país. A Doutrina para o Sistema Militar de Comando e Controle (SisMC²) estabelece os princípios de C² básicos no seu planejamento e na sua execução: unidade de comando, simplicidade, segurança, flexibilidade, confiabilidade, continuidade, rapidez, amplitude e integração (Brasil, 2015). A Doutrina de Operações Conjuntas orienta que os planejamentos conjuntos considerem como premissas a universalidade, a unidade, a objetividade, a flexibilidade, a coordenação e a interoperabilidade (Brasil, 2020). Pode-se observar que apenas "unidade" e "flexibilidade" constam em comum nas demandas de ambas as doutrinas.

Recentemente, foi aprovada a atualização da Estratégia Nacional de Defesa (END), ratificando que o estado de prontidão desejado resulta da evolução contínua no processo de transformação e na busca de novas capacidades, guiadas por características doutrinárias de flexibilidade, adaptabilidade, modularidade, elasticidade e sustentabilidade (Brasil, 2025a). Em consequência, foi desenvolvido o Planejamento Estratégico Setorial de Defesa (PESD) para os próximos 12 anos (2024-2035), com a intenção de proporcionar diretrizes para a obtenção de novas capacidades que respondam aos desafios da defesa com a rapidez e a eficácia necessárias, visando o grau de maturidade para a realização do almejado salto estratégico (Brasil, 2025b). Comparando essa evolução com as demandas anteriores, destaca-se que a flexibilidade é o único fator comum em todos eles.

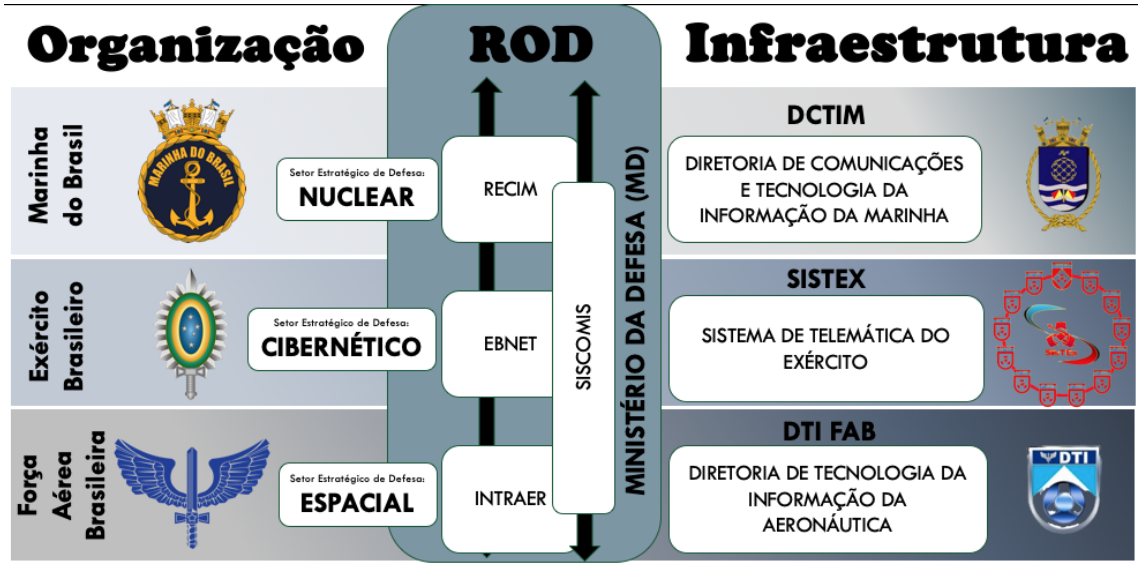
O Conceito Operacional do Sistema de Informação de Apoio à Decisão para Comando e Controle (SIADC²) relaciona os principais Sistemas de Informação/Sistemas de Apoio à Decisão (SI/SAD) do Estado-Maior Conjunto das Forças Armadas (EMCFA) e das FFAA, organizando-os em uma estrutura de Sistema de Sistemas (SdS). Ou seja, é um conjunto ou arranjo de sistemas independentes, reunidos para prover uma capacidade que não é possível de ser obtida com aqueles sistemas individualmente (Brasil, 2019). Entretanto, a integração de uma série de sistemas independentes não é equivalente a um sistema único, em que cada dado é compartilhado e estruturado logicamente e todas as suas informações são conhecidas por uma inteligência lógica central.

Dessa forma, diante de cenários mundiais dinâmicos, a flexibilidade doutrinária é proporcionalmente maior quanto maior for a flexibilidade da sua infraestrutura, desenvolvendo a capacidade de refletir as mudanças rapidamente em seus níveis estratégico, operacional e tático. Na busca por maior visibilidade e sinergia de redes e sistemas, é desejável pensar na jornada para ampliar o compartilhamento de uma única rede e infraestrutura de dados para todas as FFAA, caminhando para desenvolver e agregar capacidades conjuntas.

2.1 Desenvolvimento

A ROD é a rede que integra e fornece serviços ao SisMC² (BRASIL, 2023a), sendo constituída por um conjunto de enlaces de comunicação de dados militares operacionais do tipo *Wide Area Network* (WAN). Ela consiste na infraestrutura por onde transitam os dados e informações da defesa, possuindo conectividades segregadas e diversificadas no segmento espacial e terrestre. Compreende, também, as redes de dados das FFAA (Recim, EBNet e Intraer) e, em casos específicos, a internet com segurança (Brasil, 2019), conforme a Figura 1.

Figura 1 – Organização e Estruturação da ROD atual



Fonte: Elaborado pelo autor.

A Recim é a Rede de Comunicações Integradas da Marinha, que conecta suas diversas Organizações Militares (OM) e estende sua abrangência aos navios em missão no exterior e à Estação Antártica Comandante Ferraz (EACF). Dessa forma, ela proporciona a troca de informações entre os nove distritos navais, responsáveis por coordenar e controlar operações em suas respectivas áreas de jurisdição, consolidando-se, desse modo, como uma peça fundamental para a eficácia das comunicações navais (Marinha do Brasil, 2025). Cabe, então, ao Departamento de Comunicações e Tecnologia da Informação da Marinha (DCTIM):

> [...] assegurar a eficiência e a eficácia do Sistema de Comunicações da Marinha (SISCOM) e das atividades de prevenção e proteção do Espaço Cibernético de interesse da MB (ECiber-MB), a fim de contribuir para o preparo e emprego do Poder Naval, do Sistema Naval de Guerra Cibernética (SisNavGCiber) e do Sistema Militar de Defesa Cibernética (SMDC). [...] prover serviços flexíveis, integrados e interoperáveis de Tecnologia da Informação e Comunicações (TIC), com confiança, segurança e rapidez (Marinha do Brasil, 2025, p. 2).

A EBNet é a Rede de Dados Corporativa do Exército, constituindo-se como uma intranet corporativa e privativa, cuja finalidade é interligar as redes metropolitanas e locais do Exército Brasileiro (EB) para a tramitação de dados, voz e imagens entre as OM (Exército Brasileiro, 2013). Cabe ao Sistema de Telemática do Exército (SisTEx) prover a infraestrutura de conectividade (TIC) para os demais sistemas e meios integrantes do Sistema de Comando e Controle (SC^2Ex), sob a liderança do Centro Integrado de Telemática do Exército (CITEx) (Exército Brasileiro, 2024a, p. 2). O SisTEx possui, ainda, em sua composição, 12 Centros de Telemática, elementos

operacionais distribuídos geograficamente pelo Brasil e que atuam em apoio às OM em todo o território nacional.

Já a Intraer é a rede interna do Comando da Aeronáutica (Comaer), responsável por prover as comunicações internas e o acesso aos sistemas da Força Aérea Brasileira (FAB). A Divisão de Tecnologia da Informação (DTI) da Aeronáutica é encarregada pelo desenvolvimento e pelo suporte de sistemas corporativos, de simuladores de voo e de segurança da informação, atuando na direção administrativa e operacional, além de realizar atividades de ensino e de gestão de recursos humanos em todas as suas áreas de responsabilidade (Força Aérea Brasileira, 2023).

Como redundância entre níveis de comando mais elevados, existe uma integração complementar de telefonia e de dados composta por sistemas satelitais, permitindo maior coordenação e cooperação entre as três FFAA brasileiras (Neto, 2023). O Sistema de Comunicações Militares por Satélite (Siscomis) é capaz de proporcionar a sobrevivência de comunicações críticas, mesmo em cenários de inoperância das redes comerciais, e garantir a continuidade do C^2.

2.2 Metodologia

Esta pesquisa possui natureza qualitativa e exploratória. O procedimento metodológico consistiu em uma revisão bibliográfica e uma análise documental de diretrizes estratégicas e doutrinas militares nacionais e internacionais (EUA, Reino Unido e Ucrânia). Complementarmente, aplicou-se uma reflexão analítica sobre a experiência institucional de implementação da tecnologia SD-WAN em ambientes de crise, especificamente durante a Operação Taquari II no Rio Grande do Sul, a fim de validar as premissas do modelo proposto.

No âmbito do Ministério da Defesa (MD), observa-se que cada uma das FFAA possui uma infraestrutura de TIC com gestão própria e independente, alinhada às diretrizes do Escalão Superior e integrada em pontos estratégicos. Entretanto, este estudo busca apresentar a oportunidade de integrar as redes corporativas desde seu planejamento até sua implementação, desenvolvendo uma infraestrutura de rede única, totalmente integrada, com gestão compartilhada e capaz de atender a todas as exigências normativas.

De acordo com a END (Brasil, 2025a), o setor estratégico mais relacionado ao tema de conectividade é o cibernético, que possui é liderado pelo EB, mas que também conta com a participação da Marinha do Brasil (MB) e da FAB na capacitação, proteção, resposta e coordenação de suas atividades de resposta a incidentes de rede interna (Força Aérea Brasileira, 2025). Tais esforços ocorrem também de forma conjunta com a atuação do Comando de Defesa Cibernética (ComDCiber), com a missão de planejar, orientar, coordenar e controlar as atividades operativas, doutrinárias, de desenvolvimento e de capacitação no âmbito do Sistema Militar de Defesa Cibernética (SMDC) (Brasil, 2017), que assumiu o papel de órgão central, com o objetivo de assegurar o uso efetivo do espaço cibernético pelas FFAA e impedir ou dificultar sua utilização contra interesses da Defesa Nacional. Entretanto, cabe ao CITEx a missão de implantar e manter o SC^2Ex, integrado ao Sistema de Comando e Controle da Força Terrestre (SC^2FTer), a fim de permitir o fluxo seguro e oportuno de informações aos comandantes em todos os níveis, contribuindo para o incremento do poder de combate do Exército e para o desenvolvimento nacional (Exército Brasileiro, 2024b).

No campo pessoal, processual e tecnológico, a Doutrina Operacional do Exército exige que o seu SC²Ex sofra o mínimo de alterações em suas bases física e lógica, devendo adequar-se rapidamente às mudanças situacionais, empregando múltiplas possibilidades de ligação e flexibilidade, propiciando continuidade, confiabilidade e segurança (Exército Brasileiro, 2021). O EB regulamentou a organização e o funcionamento do SC²Ex, emitindo premissas, orientações e atribuições:

> "No contexto das operações de convergência, o C² é indispensável para assegurar a interoperabilidade conjunta, combinada e interagências, contribuindo para a atuação do Exército em todos os domínios (terrestre, marítimo, aéreo, cibernético, eletromagnético e espacial) e em todas as dimensões do combate (física, humana e informacional)" (Exército Brasileiro, 2024a, p. 2).

A governança do SEC²Ex é exercida pelo Estado-Maior do Exército (EME) e a gestão desses sistemas é realizada pelo Departamento de Ciência e Tecnologia (DCT). Dessa forma, ocorre coordenadamente uma colaboração integrada dentro do EB, com a responsabilidade do CITEx de gerenciar os projetos e a operação da infraestrutura da EBNet. Isto posto, pode ser interessante aumentar a sinergia e a integração entre as redes de todas as FFAA, sendo que o caminho mais lógico pela maior cobertura e distribuição em território nacional caberia ao SisTEx. Nesse mesmo sentido, seria facilitado o acesso da MB e da FAB aos *data centers* do Exército, integrando de forma complementar os dados e as informações e proporcionando: uma melhor gestão de pessoal interinstitucional, com a ampliação da capacidade da gestão operacional da rede e da resposta a incidentes, além de economicidade nas capacitações e multiplicação do conhecimento; uma melhor gestão de processos, mediante o compartilhando de recursos em investimentos centralizados, a consolidação das melhores práticas e a unificação das elaborações regulatórias; e uma melhor gestão tecnológica, por meio da aplicação de efetivos combinados nos controles das políticas e nas operações de rede totalmente integradas em conectividade e hospedagem de sites e sistemas críticos, o que colabora para os serviços de inteligência, operações conjuntas e desenvolvimento tecnológico integrado.

3 DESAFIOS DE PESQUISA IDENTIFICADOS

Como consequência da Política Cibernética de Defesa, o Ministério da Defesa criou o SMDC e regulamentou que:

> "A capacidade interagências do órgão central do SMDC caracteriza-se pela atuação colaborativa com representantes de órgãos da administração pública federal, de infraestruturas críticas e de outros órgãos, instituições e empresas, públicos ou privados, de interesse da Defesa" (Ministério da Defesa, 2020, p. 1).

Nesse contexto, é comum que, no campo pessoal, a coordenação do Ministério da Defesa e de seu EMCFA se relacione com os Estados-Maiores das Forças Singulares. Quanto aos processos, a obtenção e a aplicação da capacidade de Defesa Cibernética, bem como o tratamento de incidentes de redes, permanecem sob a responsabilidade independente da MB, do EB e da FAB,

com autonomia para planejar, implementar e controlar sua infraestrutura e seu modo de operação, além da elaboração e da fiscalização das normas internas.

Desafios no campo tecnológico são guiados por uma questão paradoxal, conforme a Doutrina Militar de Defesa Cibernética:

> "Paradoxo Tecnológico – quanto maior é o desenvolvimento tecnológico, maior é a dependência da TI e, consequentemente, maior a vulnerabilidade às ações cibernéticas. Contudo, paradoxalmente, melhores são as condições de defesa face a ataques cibernéticos em virtude do alto grau de desenvolvimento tecnológico" (Brasil, 2023b, p. 22).

Entretanto, a IA tem se apresentado como um fator-chave para os conflitos militares da atualidade, sendo capaz de obter dados de diversas fontes, processar um volume imenso de informações e analisar situações em alta velocidade para a tomada de decisão das Forças Armadas (Pederneiras, 2024). Dessa forma, com o crescente emprego da IA no controle da automação robótica demonstrado em âmbito global, torna-se essencial a busca pelo desenvolvimento e pela independência no ramo tecnológico de defesa.

Os desafios de governança e gestão da EBNet estão ligados ao binômio "necessidade versus possibilidade" (Santos; Oliveira; Belderrain, 2022). A migração de serviços para a nuvem digital aumenta a demanda de banda na conectividade entre as OM e os *data centers*. A economicidade proporcionada pela concentração de investimentos em centros de dados está relacionada à necessidade de recursos para suprir o aumento da demanda de capacidade e dimensionamento de cada enlace da EBNet, esbarrando nas diferenças de visões e interesses dos vários stakeholders.

Uma grande dificuldade tecnológica evidenciada é o desafio de padronização dos equipamentos empregados. Desde o início das comunicações por rádio analógicas até modelos recentes de complexas redes digitais, as comunicações seguem vinculadas às diferentes tecnologias proprietárias e, por isso, apresentam limitações de integração entre diferentes fabricantes. É inerente à indústria utilizar padrões proprietários e fechados para forçar o emprego de suas famílias produtivas em toda a organização. Os problemas de despadronização são mais evidentes no comando, controle e comunicações (C^3) do que em qualquer outra área (Medeiros, 2024).

Um dos principais desafios das redes atuais é a interconexão de tecnologias de enlaces utilizados em tempo de operação, sem perda de capacidade, alcance e mobilidade. Consequentemente, um sistema de comunicações militar "deve ser uma única estrutura lógica integrada por múltiplas tecnologias de enlace" (Camilo; Moura; Salles, 2020, p. 6). Realmente, dentre as redes de comunicações atualmente empregadas nas subredes componentes da ROD – Recim, EBNet e Intraer – que utilizam as tecnologias de mercado, não existe a possibilidade de integração automática e sem intervenção humana por terem sido planejadas, implementadas e desenvolvidas organicamente e de forma independente entre si. Isso faz com que estejam conectadas por ligações específicas e adaptações limitadas a redes legadas disjuntas, com restrições de interoperabilidade e integração incompleta, além de demandarem a tradução de endereços IP e portas de rede (NAT/PAT).

A ROD, como integrante do SMDC, é um dos pilares da proteção cibernética, que é uma atividade de caráter permanente e busca manter a operação segura e oportuna de equipamentos e

sistemas computacionais, bem como promover a proteção contra ações de exploração e ataque do oponente (Brasil, 2023b). Isto posto, realizar a gestão de tamanha infraestrutura sem uma única liderança e ações combinadas e alinhadas – no sentido de convergir para uma infraestrutura singular – constitui um grande desafio.

4 UMA NOVA VISÃO PARA INTEGRAÇÃO DA REDE OPERACIONAL DE DEFESA (ROD)

A Doutrina Militar de Defesa Cibernética afirma que:

> O SMDC é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional, bem como impedir ou dificultar ações hostis contra seus interesses. Cabe também ao SMDC assegurar a proteção cibernética do SisMC^2, possibilitando a capacidade de atuar em rede com segurança, bem como de maneira integrada e colaborativa na gestão de riscos que envolvam a proteção de infraestruturas críticas, conforme previsto no Plano Nacional de Segurança de Infraestruturas Críticas (Brasil, 2023b, p. 27)

Nesse sentido, a segurança cibernética já caminha para uma gestão integrada entre a MB, o EB e a FAB, mas ainda não se reflete, na prática, em uma infraestrutura de conectividade e compartilhamento de dados conjuntos, monitorados por um único *Network Operation Center* (NOC) e por um *Security Operation Center* (SOC) –Centro de Operações de Rede e de Segurança, respectivamente –, o que seria capaz de consolidar todo esse sistema.

4.1 Integração a níveis de pessoas, processos e tecnologias

A Estratégia Nacional de Defesa afirma que:

> [...] tornam-se imperiosas a criação e a ampliação de polos tecnológicos integradores, com o objetivo de conquistar a autossuficiência em projetos de desenvolvimento e na fabricação de sistemas de C^{3}I (Comando, Controle, Comunicação e Inteligência), com vistas a eliminar, progressivamente, a dependência externa (Brasil, 2025a, p. 14).

Dessa forma, esta proposta tem como objetivo apresentar um modelo de inovação para a ROD, coordenando e integrando pessoas, processos e tecnologias.

4.1.1 Proposta de integração pessoal

As medidas de proteção cibernética são mais efetivas quando alinham outras duas variáveis que compõem o sistema de C^2 em ação: pessoal e doutrina, que, quando fracos, tornam-se

vulnerabilidades em potencial (Cordeiro, 2014). Portanto, cabe às FFAA desenvolver uma doutrina conjunta para que seu efetivo seja capacitado e tenha condições de disseminar conhecimento, proteger as informações críticas, enfrentar as ações cibernéticas do oponente e permanecer em condições de responder aos ataques.

No campo de integração pessoal, podem ser adotadas medidas drásticas e disruptivas, como a criação de uma nova Força, ou medidas mais suaves e integradoras, similares à de criação do ComDCiber (Ministério da Defesa, 2016), na qual o MD e seu EMCFA têm expertise em estabelecer projetos e grupos de trabalho, estudar e emitir diretrizes e coordenar continuamente. Tendo em vista que os efetivos das Forças não são proporcionais e que o EB está designado como responsável pela segurança cibernética, uma alternativa nesse campo seria a criação de um novo Centro de Operações de Rede e Segurança Conjuntos, com atuação continuada e integrada que, além de monitorar e operar a infraestrutura da ROD, atuaria ativamente no projeto, desenvolvimento, implementação e suporte da infraestrutura de rede única e comum para desenvolver novas capacidades integradas.

A implementação de uma infraestrutura baseada em redes definidas por software (SD-WAN) e orquestração cognitiva exige uma reestruturação profunda nas competências do corpo técnico das Forças Singulares. A transição do paradigma de configuração estática de ativos para a gestão de fluxos dinâmicos requer a formação de militares com perfil de "Orquestradores de Redes" (paradigma NetOps). Neste cenário, o letramento em Inteligência Artificial Explicável (XAI) torna-se um requisito crítico, capacitando o operador a interpretar e validar as decisões autônomas dos agentes de roteamento, garantindo que a automação tecnológica permaneça sob o controle e a supervisão ética do decisor humano em contextos de crise.

Para além da aptidão técnica, a "Nova Visão" da ROD pressupõe uma evolução na cultura organizacional, migrando de silos informacionais específicos de cada Força para um mindset de interoperabilidade plena (*joint* mindset). Esta mudança cultural é o alicerce para que a soberania digital seja percebida como um ativo coletivo. A confiança mútua nos protocolos de segurança e o compartilhamento de infraestruturas críticas sob a coordenação do EMCFA permitem que a rede atue como um multiplicador de poder de combate, no qual a resiliência do sistema transcende as fronteiras administrativas de cada Força Singular.

A principal necessidade de aumentar a compatibilidade é suprida por um órgão conjunto de elaboração e mediação de requisitos operacionais (Medeiros, 2024), que seria um ponto de controle único para a ROD, com viés de gestão e supervisão da rede. Esse grupo poderia ser uma subseção do ComDCiber, voltada à proteção de comunicações, dados e informações; porém, uma solução mais lógica e menos traumática seria a expansão do NOC/SOC do SisTEx em Brasília/DF, que já administra quase mil sites nacionalmente. Assim, seria possível a integração e absorção da Recim e da Intraer pela EBNet, transformando-se na nova ROD, com a colaboração de pessoal e recursos financeiros da MB e da FAB, integrando completamente as OM de todas as Forças Singulares. Não coincidentemente, o CITEx tem buscado uma atualização tecnológica da EBNet em nível nacional desde 2024 e, inclusive, já validou o emprego de suas facilidades no contexto das enchentes do Rio Grande do Sul – conforme será exposto na Seção 4.2 deste artigo – e, desde então, possui o maior efetivo de militares capacitados nessa tecnologia.

4.1.2 Proposta de integração processual

A integração e a padronização de processos entre as FFAA tendem a ser assertivas, permitindo a combinação e a atualização das melhores práticas e a uniformização das regulamentações entre as Forças Singulares, o que reduz as diferenças inerentes entre a MB, o EB e a FAB. Tal dinâmica colabora para a aproximação das pessoas e para a igualdade nas rotinas militares, permitindo planejamentos e aquisições conjuntas, bem como o desenvolvimento de capacidades e sistemas para a nova ROD.

Em nível normativo, uma atualização combinada poderia não apenas otimizar os processos em vigor, mas também encaminhar novas ações estratégicas integradoras em níveis de rede e de sistemas, expandindo o SMDC e alinhando as gestões, práticas e possibilidades em todos os níveis estratégicos, táticos e operacionais. Além disso, a concentração de dados militares pode gerar a capacidade de ampliar as identificações das informações de inteligência, correlacionar bases de dados e eventos de rede, bem como agregar repositórios de conhecimento e informações conjuntas.

No âmbito da FAB, por exemplo, a DTI é o órgão que centraliza a governança, a legislação, a capacitação e o aprimoramento do sistema, a segurança da informação e a defesa cibernética de todas as suas OM. Realiza, ainda, o apoio de TI nos eventos oficiais e nas operações militares, em projetos estratégicos do Estado-Maior da Aeronáutica (EMAER), em simuladores, no planejamento e na gestão orçamentária, entre outros (Força Aérea Brasileira, 2015). Se o MD preferir expandir as atribuições desse órgão central de rede e agregar atribuições, isso pode ser estabelecido por meio de uma nova Doutrina.

Outro processo favorecido seria a aquisição centralizada. Em 2024, o CITEx realizou uma compra de mais de 800 equipamentos para implementação em todo o território nacional, com uma grande economicidade por interesse direto dos grandes fabricantes e pela economia de escala inerente. A centralização das aquisições é capaz de gerar ganhos de eficácia e eficiência para a Administração Pública Federal (APF), desde que conte com a ampliação da integração dos processos de planejamento das três Forças, com a realização de compras conjuntas, com a maior padronização do material e com o incremento da interoperabilidade entre elas (Medeiros, 2024).

A própria orientação para a hospedagem de sites e sistemas da MB e da FAB nos *data centers* do EB pode aumentar a eficácia do emprego de recursos públicos, compartilhando recursos militares e equipes de tratamento de incidentes de rede, entre outros. Essa solução seria ainda mais simplificada e facilitada com a nova ROD, que proveria o acesso aos sistemas de C^3I nacionais e conjuntos subordinados ao MD.

No âmbito da governança, a arquitetura proposta otimiza a relação entre o nível estratégico (EMCFA) e o operativo (Forças Singulares) através do modelo de Redes Baseadas em Intenção (–IBN, na sigla em inglês). Esse processo permite que o comando superior estabeleça políticas de alto nível, como a priorização de tráfego de Comando e Controle em áreas de conflito, enquanto a orquestração automatizada traduz essas intenções em configurações técnicas em tempo real. Tal fluxo de governança preserva a autonomia operativa das Forças na ponta, ao mesmo tempo em que garante a conformidade sistêmica e a agilidade na resposta a incidentes jurisdicionais.

Doutrinariamente, a integração de processos de *Zero Trust Architecture* (ZTA) redefine o fluxo de acesso a dados estratégicos, substituindo a confiança baseada em perímetro por uma verificação contínua de identidade e integridade. Este rigor processual é potencializado pelo fatiamento

de rede (*network slicing*), que viabiliza o provisionamento *on demand* de redes lógicas isoladas para missões específicas. Dessa forma, a ROD evolui de uma infraestrutura rígida para um serviço flexível e resiliente, capaz de instanciar corredores seguros de comunicação em teatros de operações dinâmicos, com agilidade superior à dos processos tradicionais de engenharia de tráfego.

4.1.3 Proposta de integração tecnológica

No campo tecnológico, são estudadas redes empresariais atrativas (Navarro; Canonico; Botta, 2023), mais autônomas e inteligentes, que podem se adaptar e se autorrecuperar com menor interação humana (Waseem *et al.*, 2022), agregando maior resiliência, reduzindo custos e permitindo a adoção de alternativas de mercado completas para a nova ROD. Entre elas, algumas podem oferecer um novo modelo de arquitetura de rede definida por software, programável e flexível (Aggarwal, 2020) para ambientes locais (*Local Area Networ*k – LAN), por meio de *Software Defined Networks* (SDN), ou de longa distância (*Wide Area Network* – WAN), via SD-WAN. Essa evolução desenvolve capacidades computacionais (Khalifa *et al.*, 2025) e inovações continuadas por ampla pesquisa (Belgaum *et al.*, 2020).

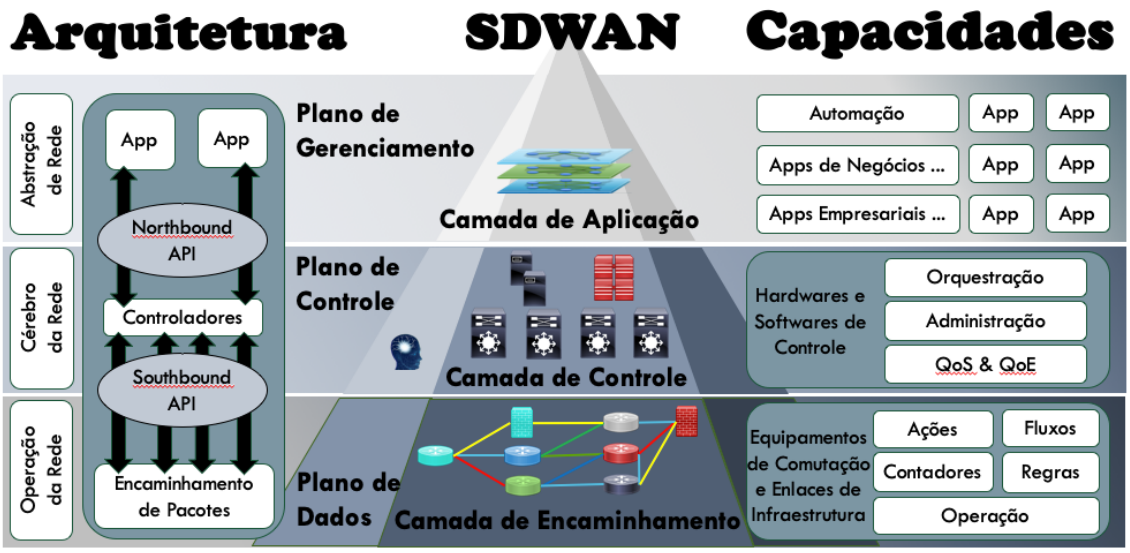
Devido à dimensão continental do Brasil e à ampla área de atuação das FFAA, a arquitetura de redes de comunicações SD-WAN é capaz de operar em escala global, como uma tecnologia de rede flexível amplamente empregada na atualidade (Fu; Wang; Wang, 2024). Ela consiste em uma solução baseada em um conjunto programável de hardware e software com vantagens como: baixo custo , pela redução de requisitos de hardware e despesas operacionais (Diaz *et al*., 2022); maior velocidade de gerenciamento simplificado; mais segurança e visibilidade, com análises aprofundadas e automação na solução de problemas; melhor disponibilidade, por meio de *failover* simplificado e rápido; e melhor desempenho total da rede, com otimização da largura de banda (Yalda; Hamad; Tapus, 2022). Essa tecnologia se apresenta como meio capaz de prover os requisitos necessários à obtenção dos objetivos nacionais de defesa.

A engenharia inovadora agregada permite reduzir os custos recorrentes dos sistemas, oferecer amplo controle e visibilidade e aprimorar a inovação na organização da infraestrutura de forma automatizada por intermédio de uma administração integrada (Badotra; Panda, 2020). Vale destacar que o EB já possui experiência com a tecnologia SD-WAN. Atualmente, o CITEx emprega recursos do Programa Defesa Cibernética com o objetivo de dotar o EB de capacidades para atuar no espaço cibernético nos níveis estratégico, operacional e tático (Estado-Maior do Exército, 2022). Entre as próximas entregas, consta a reestruturação da proteção cibernética da EBNet (Oliveira; Teixeira, 2021), com boa parte dos recursos empregados nessa solução. Projetos paralelos, como o Sistema Integrado de Monitoramento de Fronteiras (Sisfron), também visam à aquisição de equipamentos de TI para os centros de operações localizados na faixa de fronteira (Exército Brasileiro, 2024c) e colaboram para a execução das aquisições e o alinhamento das entregas.

Dentre os pilares estratégicos dos projetos futuros, registrados nas inúmeras doutrinas atualizadas recentemente e citadas neste artigo, destacaram-se como premissas a flexibilidade e a unidade. A tecnologia de redes que mais apresenta condições de entregar tais requisitos em âmbito nacional, podendo ser expandida para o global, é o SD-WAN, cuja arquitetura e capacidades são

expostas conforme a Figura 2. Essa tecnologia utiliza a flexibilidade e a programabilidade de uma SDN (Abderrahman *et al.*, 2023), agregando, ainda, uma visão global de todos os sites e integrando a rede em todos os níveis. Essa solução também permite que todas as políticas de gestão e controle da rede em vigor sejam implementadas simultaneamente (Ouamri *et al.*, 2025), bem como torna possível uma segregação e uma migração para a implementação gradual supervisionada por site ou OM.

Figura 2 – Arquitetura Geral da Tecnologia SD-WAN e Capacidades.



Fonte: Elaborada pelo autor.

O Plano de Gerenciamento do SD-WAN mantém as aplicações de SDN (Kaur; Krishna; Patil, 2025) e agrega novas, voltadas aos objetivos de negócio, organizacionais ou empresariais, permitindo uma gestão simplificada da rede e dos dispositivos a ela atrelados (Mahar *et al.*, 2024) e aumentando o nível de gerência e controle das filiais e sites remotos vinculados. De forma similar, coordena as configurações e políticas de rede que o plano de controle deve implementar no ambiente de produção empresarial (Ali *et al.*, 2015).

O Plano de Controle também faz a administração do Plano de Dados (Bahashwan *et al.*, 2023), porém necessita de maior resiliência devido a questões de distância e métricas relacionadas que podem interromper a comunicação com um único controlador remoto. Desta forma, a latência ou o atraso podem prejudicar a gerência e a instalação de fluxos e regras, bem como falhas nos links podem prejudicar o controle e deixar a rede inoperante (Ayodele; Buttigieg, 2024). Por esse motivo, é comum a implementação de mais de um controlador distribuído para maior resiliência do controle e melhor eficiência no encaminhamento (Kanwal *et al.*, 2024). Para viabilizar isso, se faz necessária uma orquestração adicional entre os controladores, mantendo-os sempre coordenados e sincronizados, provendo, assim, a conectividade com o QoS (Qualidade do Serviço) e o QoE (Qualidade da Experiência) previstos (Rahouti *et al.*, 2022).

O Plano de Dados do SD-WAN realiza os encaminhamentos da solução sobre uma infraestrutura complexa e distribuída, com diversos, simultâneos e redundantes enlaces de rede entre os nós e sites, por meio das mais diversas tecnologias (Rahouti; Xiong; Xin, 2020). Isso posto, há uma subdivisão na Camada de Encaminhamento entre a rede de infraestrutura e uma malha lógica em plano superior, que constrói túneis específicos e alternativos com regras de encaminhamento granularizadas e criptografadas ponto a ponto na organização (Abdi *et al.*, 2024).

A solução SD-WAN é considerada flexível e única por utilizar camadas de abstração e elementos otimizados para WAN para entregar tais facilidades, que constituem um único sistema (Jiménez *et al.*, 2021). O seu gerenciamento é executado pelo Orquestrador de Serviços da solução, que atua como uma camada superior, gerenciando múltiplos controladores SD-WAN e aplicativos de negócios (Jain; Khondoker, 2018). Ele é responsável por simplificar a configuração e o gerenciamento de políticas em uma rede geograficamente distribuída. Os equipamentos de comutação distribuídos são os *Customer Premises Equipment* (CPEs), dispositivos de borda físicos ou virtuais implantados nas filiais, *data centers* e nuvens. Eles são os pontos de início e fim dos túneis SD-WAN e são responsáveis por encapsular o tráfego e aplicar políticas. Os Túneis de Sobreposição (*overlay*) são túneis seguros – como o *Internet Protocol Security* (IPSec) ou o *Virtual Extensible LAN* (VXLAN) – sobre redes físicas subjacentes (*underlay*) para criar uma rede virtual e privada. Isso permite o uso de diversas opções de conectividade e garante segurança sobre redes públicas (Kytomäki, 2021).

Portanto, o SD-WAN foi concebido para gerenciar WANs que conectam múltiplos sites geograficamente dispersos, como filiais de empresas, *data centers* e infraestruturas de nuvem pública ou privada. Seu objetivo é otimizar a conectividade através de múltiplas redes subjacentes (MPLS, internet, 4G/5G, satélites) a fim de garantir alta qualidade de serviço (QoS) e experiência (QoE), além de segurança e redução de custos (Badotra; Panda, 2020). Em resumo, enquanto o SDN estabelece as bases de uma rede programável e centralizada, o SD-WAN a estende e a otimiza para as complexidades e exigências das redes de longa distância modernas, incorporando camadas adicionais de funcionalidade e inteligência (Rahman; Hasan; Jeong, 2022). Neste momento de posse de uma inteligência e de uma visão centralizada da rede, a associação com soluções de IA aumenta sua relevância (Sahran; Altarturi; Anuar, 2024).

Atualmente, a Recim realiza a criptografia de dados e a redundância de enlaces, além do monitoramento constante de sistemas críticos (Marinha do Brasil, 2025). O SD-WAN pode garantir a continuidade dessas facilidades, pois permite a seleção de múltiplos enlaces automaticamente, criptografando os sites de forma automatizada e coordenada, com filtros de controle específicos por fluxos, caso estejam autorizados pelas políticas em vigor. Assim, ele agrega robustez para além da infraestrutura singular das FFAA, com o emprego de medidas avançadas de segurança e recursos para prevenir e reagir a ameaças cibernéticas, preparando a maximização da resiliência frente aos desafios da guerra cibernética moderna.

Embora a tecnologia SD-WAN ofereça alto potencial de automação e redução de custos operacionais, sua implementação na ROD impõe desafios significativos. A transição de redes legadas e disjuntas para uma estrutura única exige uma governança interinstitucional robusta para evitar conflitos de gestão entre as Forças Singulares. Além disso, a interoperabilidade entre diferentes fabricantes – evitando o *vendor lock-in* – e a necessidade de capacitação contínua de pessoal técnico

para lidar com redes programáveis são barreiras que demandam um planejamento de transição gradual e supervisionado.

Por fim, a superação dos desafios de implementação e a mitigação das limitações citadas passam, necessariamente, pelo fomento à autonomia tecnológica e à soberania digital. Nesse contexto, a transição para uma ROD moderna e integrada exige o estímulo ao desenvolvimento de soluções de SD-WAN de soberania nacional, articuladas sob o modelo de inovação da Tripla Hélice (Estado, Academia e Indústria). A convergência de esforços entre os institutos de pesquisa das Forças, as universidades e a Base Industrial de Defesa (BID) é essencial para reduzir a dependência estratégica de tecnologias e protocolos estrangeiros. Tal alinhamento não apenas fortalece a inovação no setor de defesa, mas também garante que o controle e a governança da infraestrutura crítica de comunicações do país permaneçam sob estrita jurisdição e domínio tecnológico nacional.

4.2 Validação do SD-WAN nas Enchentes do RS e Evolução Tecnológica da EBNet

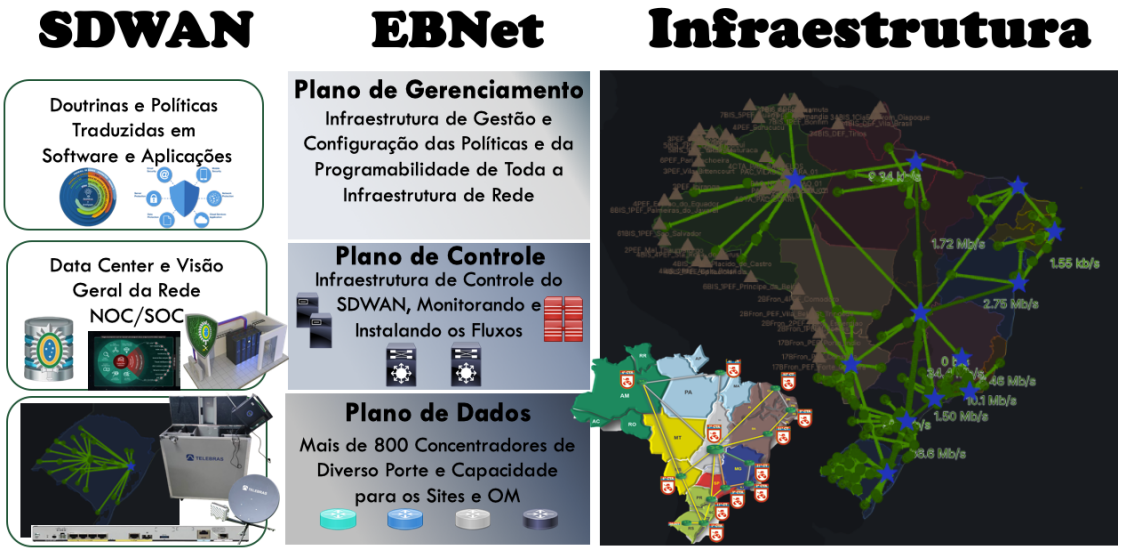
Por ocasião das fortes enchentes no Sul do Brasil em 2024 que desencadearam a Operação Taquari II, a infraestrutura de C^2 passou por muita instabilidade. Diante de interrupções consecutivas, simultâneas e duradouras dos meios convencionais de rede e conectividade, faltaram militares técnicos qualificados para atuar nas mudanças necessárias à sobrevivência da rede. As adaptações nas configurações dos equipamentos eram necessárias na criptografia dos enlaces convencionais, que apresentavam intermitência, bem como no ajuste dos túneis para sites distintos, feito manualmente e em uma situação com baixa disponibilidade de recursos, como transporte e energia elétrica.

Como alternativa, foram convertidos enlaces Metro Ethernet em internet, o que aumentou a sua disponibilidade. Ademais, foram recebidos e distribuídos no estado mais de 480 terminais satelitais de diferentes tecnologias para as OM e os postos táticos, provendo o acesso remoto à EBNet aos usuários mediante o uso de cliente VPN nos dispositivos. Para garantir respostas mais rápidas e independentes de interação humana, foi realizada emergencialmente a implementação virtual do software integrador de SD-WAN, que concentrou as políticas de encaminhamento responsáveis por coordenar e controlar os fluxos de rede entre os equipamentos empregados nessa arquitetura em três sites críticos da EBNet, os quais operaram paralelamente e concentraram todos os enlaces disponíveis nessa OM (Metro Ethernet, rádio, fibra, internet e satélite). A nova solução foi capaz de monitorar, selecionar e encaminhar os pacotes de rede com os recursos existentes, fazendo o balanceamento automatizado entre os enlaces disponíveis e a seleção do caminho recomendado pelas políticas vigentes pré-configuradas, o que aumentou a resiliência das redes e viabilizou o fluxo contínuo de informações. Assim, com a implementação rápida, eficaz e parcialmente virtualizada da infraestrutura SD-WAN em sites estratégicos (Figura 3), foi possível obter a integração completa e segura das redes internas das OM, o que validou grande parte das facilidades expostas neste artigo.

Na Figura 3, é possível identificar a composição das camadas SD-WAN integradas à EBNet no Piloto, o que traduz doutrinas e políticas em softwares. Estes são voltados a uma inteligência computacional que concentra informações de toda a rede e as conecta de forma conveniente aos

melhores enlaces disponíveis, incluindo meios provisórios e dinâmicos, como no caso dos recursos emergenciais dos enlaces satelitais. As OM do Sul foram precursoras na jornada de migração de todo o Exército, durante a execução do Projeto Proteção do Ambiente Cibernético. O SisTEx segue projetando, implementando e operando em todo o território nacional, com apoio regional dos Centros de Telemática.

Figura 3 – Infraestrutura de validação do SD-WAN nas Enchentes do Sul



Fonte: Elaborada pelo autor.

Dessa forma, pode-se afirmar que o SD-WAN foi eficiente na integração das OM com flexibilidade e resiliência à EBNet, o que garantiu sucesso na gestão automatizada dos enlaces via software e permitiu concluir que essa era a melhor solução tecnológica para momentos de incerteza. Essa ferramenta proporcionou conectividade e segurança com a programabilidade de políticas, fato que expandiu a autonomia da rede, viabilizou o *self-healing* (autocura), automatizou os fluxos de dados e exigiu menor atenção da equipe técnica especializada frente a intermitências nos enlaces de infraestrutura.

Uma rede como essa, mais autônoma e flexível, já estava sendo projetada pelo CITEx; porém, não foi implementada antes da ocorrência desse desastre, que acabou sendo uma prova da eficiência da tecnologia SD-WAN mesmo em redes amplas como as do EB, com mais de 860 pontos de conexão. Tal fato foi essencial para as aquisições decorrentes, já planejadas em nível nacional e com pregão de aquisições padronizadas e centralizadas, o qual está válido no âmbito nacional e é capaz de proporcionar uma visão global e integrada para a nova EBNet. Nos meses que se sucederam, foi possível ao EB acelerar as fases do projeto de evolução tecnológica da EBNet e redirecionar os equipamentos fabricados inicialmente para a região Sul, permitindo a implementação e a operação dessa tecnologia nos 108 quartéis regionais em alguns meses, o que agregou capacidades de sobrevivência na região. Nesse contexto, pode-se inferir que tal infraestrutura é capaz de se

expandir organicamente e absorver mais sites, incluindo os da MB e da FAB, de modo a constituir a nova ROD e integrar pessoas, processos e serviços.

5 CONSIDERAÇÕES FINAIS

O EME definiu a Força 40 para guiar a evolução da Concepção de Transformação do EB no período de 2024 a 2039, alicerçada e fundamentada nos seguintes eixos de esforço: Concepção Estratégica voltada para 2040; novas capacidades; nova doutrina; e pessoal. (Exército Brasileiro, 2024d). Nesse cenário, a proposta desenvolvida para a nova ROD surge de maneira oportuna, pois agrega capacidades de Proteção e Defesa Cibernéticas e proporciona ao EB o protagonismo de assumir o papel de coordenador da infraestrutura conjunta das FFAA.

Em um cenário de recursos financeiros escassos e dependência tecnológica, no qual ocorre a demanda por aquisição imediata de tecnologia estrangeira, não há nada mais desejável do que adotar um único modelo de infraestrutura flexível e capaz de aumentar a articulação das redes e sistemas em todos os níveis, proporcionando o desenvolvimento de capacidades conjuntas. Além disso, quanto antes se estabelecerem parcerias estratégicas, com um país aliado de interesses comuns, mais brevemente o Brasil será capaz de desenvolver sua própria tecnologia de SD-WAN. Essa solução agrega programabilidade e flexibilidade gerenciadas por software, estando totalmente potencializadas por evoluções paralelas e capacidades agregadas pela IA (Cifuentes *et al.*, 2024).

Nesse sentido, a Estratégia Brasileira de Inteligência Artificial (EBIA) (Brasil, 2021) afirma que a integração de sistemas de IA à estrutura produtiva é uma realidade, e que ela terá um papel fundamental para proporcionar eficácia, reduzir custos e minimizar erros operacionais, além de automatizar uma série de processos e tornar as rotinas mais flexíveis e ágeis. De forma completamente alinhada, foi confeccionada para o EB uma diretriz estratégica que recomenda implantar e integrar sistemas de IA, o que gera a capacidade de tratar informações de diversas fontes existentes, bem como estruturar e relacionar dados fornecidos por novos sensores e sistemas, com o objetivo de compor uma consciência situacional oportuna, antecipar eventos e apoiar a tomada de decisão (Exército Brasileiro, 2024e). De forma conjunta, surge também a oportunidade de expandir, otimizar e compartilhar os investimentos na infraestrutura de IA das FFAA e do MD.

REFERÊNCIAS

ABDERRAHMAN, R. *et al*. Software Defined Networking Concept (SDN) Based on Artificial Intelligence: Taxonomy of Methods and Future Directions. **Springer Nature**, Switzerland, 2023.

ABDI, A. H. *et al*. Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI, and MTD Approaches to Security Solutions. **IEEE Access**, 2024.

AGGARWAL, A. Artificial Intelligence in Software Defined Networking. **International Journal of Advance Research, Ideas and Innovations in Technology**, v. 6, n. 2, 2020.

ALI, S. T. *et al*. A Survey of Securing Networks Using Software Defined Networking. **IEEE Transactions on Reliability**, v. 64, n. 3, 2015.

AYODELE, B.; BUTTLGLEG, V. SDN as a defence mechanism: a comprehensive survey. **International Journal of Information Security**, v. 23, p. 141-185, 2024.

BADOTRA, S.; PANDA, S. N. A Survey on Software Defined Wide Area Network. **International Journal of Applied Science and Engineering**, 2020.

BAHASHWAN, A. A. *et al*. A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking. **Sensors**, v. 23, n. 9, p. 4441, 2023.

BELGAUM, M. R. *et al*. A Systematic Review of Load Balancing Techniques in Software-Defined Networking. **IEEE Access**, 2020.

BRASIL. Ministério da Defesa. **Doutrina para o Sistema Militar de Comando e Controle (MD31-M-03)**. Brasília, DF: Ministério da Defesa, 2015. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/doutrina_militar/lista_de_publicacoes/md31a_ma_03a_douta_sismca_3a_eda_2015.pdf. Acesso em: 22 jul. 2025.

BRASIL. **Comando Conjunto na Defesa Cibernética**. Agência Gov Br, 2017. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/comando-conjunto-na-defesa-cibernetica. Acesso em: 25 jul. 2025.

BRASIL. Ministério da Defesa. **Conceito Operacional (CONOPS) do Sistema de Informação e de Apoio à Decisão para Comando e Controle (SIADC²) – MD31-S-04**. 1. ed. Brasília, DF: Ministério da Defesa, 2019. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/File/doutrinamilitar/listadepublicacoesEMD/md31a_sa_04a_finala_20a_nova_2019a_1a_edicao.pdf. Acesso em: 21 jul. 2025.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas (MD30-M-01)**. Brasília, DF: Ministério da Defesa, 2020. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/legislacao/emcfa/publicacoes/doutrina/md30-m-01-vol-1-2a-edicao-2020-dou-178-de-15-set.pdf. Acesso em: 22 jul. 2025.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. **Estratégia Brasileira de Inteligência Artificial (EBIA)**. Brasília, DF: MCTI, 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/copy2_of_RelatoriofinalEBIA_Eixo6V2.4.pdf. Acesso em: 8 jul. 2026.

BRASIL. Ministério da Defesa. **Política de Segurança da Informação para o Sistema Militar de Comando e Controle**. . Brasília, DF: Ministério da Defesa, 2023a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31P03PolticadeSeguranadaInformaoparaoSistemaMilitardeComandoeControle3Ed2023.pdf. Acesso em: 21 jul. 2025.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética (MD31-M-07)**. Brasília, DF: Ministério da Defesa, 2023b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 27 jul. 2025.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa (END)**. Brasília, DF: Ministério da Defesa, 2025a. Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/governanca/governanca-do-setor-de-defesa/decreto-no-12-725-de-18-de-novembro-de-2025-dou_lbdn.pdf. Acesso em: 24 jul. 2025.

BRASIL. Ministério da Defesa. **Planejamento Estratégico Setorial de Defesa (PESD) 2024-2035**. Brasília, DF: Assessoria Especial de Planejamento, 2025b. Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/governanca/governanca-do-setor-de-defesa/planejamento-estrategico-1/arquivos/2025/web_planejamento-estrategico-setorial-de-defesa.pdf. Acesso em: 24 jul. 2025.

CAMILO, J. M.; MOURA, D. F. C.; SALLES, R. M. Redes de comunicações militares: desafios tecnológicos e propostas para atendimento dos requisitos operacionais do Exército Brasileiro. **Revista Militar de Ciência e Tecnologia (RMCT)**, v. 37, n. 3, 2020.

CIFUENTES, B. J. O. *et al*. Analysis of the Use of Artificial Intelligence in Software-Defined Intelligent Networks: A Survey. **Technologies**, v. 12, n. 7, p. 99, 2024.

CORDEIRO, S. S. **A influência da Guerra Cibernética nos sistemas de Comando e Controle (C2) nas Operações Militares**. [*s. l.*]: Escola de Comando e Estado-Maior do Exército, 2014.

DIAZ, C. J. M. *et al*. Analysis about Benefits of Software-Defined Wide Area Network: A New Alternative for WAN Connectivity. **International Journal of Advanced Computer Science and Applications (IJACSA)**, v. 13, n. 1, 2022.

ESTADO MAIOR DO EXÉRCITO. **Os projetos/programas estratégicos do EB**: importância, situação atual e perspectivas. Brasília, DF: Escritório de Projetos do Exército, 2022. Disponível em: https://epex.eb.mil.br/index.php/programas-estrategicos-do-exercito. Acesso em: 27 jul. /2025.

ESTADOS UNIDOS DA AMÉRICA. Joint Staff. **Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System**. Washington, DC: Joint Staff, 2021. Disponível em: https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%205123.01J.pdf. Acesso em: 22 jul. 2025.

ESTADOS UNIDOS DA AMÉRICA. Department of Defense. **Summary of TI-IE Joint All-Domain Command & Control (JADC2) Strategy**. Washington, DC: Department of Defense, 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: 22 jul. 2025.

EXÉRCITO BRASILEIRO. Secretaria Geral do Exército. **Instruções Gerais para Estruturação e Emprego Sistêmico da Base de Dados Corporativa do Exército Brasileiro (EBCORP), - EB10-IG-01.005**. 1. ed. Brasília, DF: SGEx, 2013. Disponível em: https://www.sgex.eb.mil.br/sg8/002_instrucoes_gerais_reguladoras/01_gerais/port_n_578_cmdo_eb_10jul2013.html. Acesso em: 25 jul. 2025.

EXÉRCITO BRASILEIRO. Secretaria Geral do Exército. **Diretriz Estratégica Organizadora do Sistema de Comando e Controle do Exército (EB10-D-01.013)**. 2. ed. Brasília, DF: Secretaria Geral do Exército, 2021. Disponível em: https://www.sgex.eb.mil.br/sg8/002_instrucoes_gerais_reguladoras/01_gerais/port_n_578_cmdo_eb_10jul2013.html. Acesso em: 8 jul. 2026.

EXÉRCITO BRASILEIRO. Secretaria Geral do Exército. **Diretriz Organizadora do Sistema Estratégico de Comando e Controle do Exército (EB20-D-02.037)**. 1. ed. **Secretaria Geral do Exército**, 2024a. Disponível em: https://www.sgex.eb.mil.br/sistemas/boletim_do_exercito/copiar.php?codarquivo=181261862&act=sep. Acesso em: 27 jul. 2025.

EXÉRCITO BRASILEIRO. Centro Integrado de Telemática do Exército (CITEx). **Missão, visão e valores**. Brasília, DF: CITEx, 2024b. Disponível em: https://citex.eb.mil.br/index.php/institucional/missao-visao-e-valores.html. Acesso em: 25 jul. 2025.

EXÉRCITO BRASILEIRO. Escritório de Projetos. **SISFRON**. Brasília, DF: Escritório de Projetos, 2024c. Disponível em: https://epex.eb.mil.br/. Acesso em: 27 jul. 2025.

EXÉRCITO BRASILEIRO. Comando do Exército. **Concepção de Transformação do Exército e do Desenho da Força 40 – 2024-2039 (EB10-P- 01.025)**. 1. ed. Brasília, DF: Comando do Exército, 2024d. Disponível em: https://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/07_publicacoes_diversas/01_comando_do_exercito/port_n_2300_cmdo_eb_12agosto2024.html. Acesso em: 27 jul. 2025.

EXÉRCITO BRASILEIRO. Estado-Maior do Exército (EME). **Diretriz Estratégica de Inteligência Artificial para o Exército Brasileiro**. Brasília, DF: EME, 2024e. Disponível em: https://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/01_diretrizes/04_estado-maior_do_exercito/port_n_1318_eme_14mai2024.html. Acesso em: 8 jul. 2026.

FORÇA AÉREA BRASILEIRA. Organização se prepara para proteger redes corporativas da instituição. **Tecnologia da Informação**, 2015. Disponível em: https://www.fab.mil.br/noticias/tag/DTI. Acesso em: 27 jul. /2025.

FORÇA AÉREA BRASILEIRA. Diretoria de Tecnologia da Informação completa 13 anos. **O Portal da FAB**, 2023. Disponível em: https://forcaaerea.fab.mil.br/noticias/mostra/40280/ANIVERS%C3%81RIO%20-%20Diretoria%20de%20Tecnologia%20da%20Informa%C3%A7%C3%A3o%20completa%2013%20anos. Acesso em: 21 jul. 2025.

FORÇA AÉREA BRASILEIRA. Centro de Defesa Cibernética encerra intercâmbio com expectativas superadas. **Agência da Força Aérea**, 2025. Disponível em: https://www.fab.mil.br/noticias/mostra/44014/DEFESA%20CIBERN%C3%89TICA%20-%20Centro%20de%20Defesa%20Cibern%C3%A9tica%20encerra%20interc%C3%A2mbio%20com%20expectativas%20superadas. Acesso em: 25 jul. /2025.

FU, C.; WANG, B.; WANG, W. Software-Defined Wide Area Networks (SD-WANs): A Survey. School of Computer Science and Technology, **Harbin Institute of Technology**, v. 13, n. 15, p. 3011, 2024.

JAIN, R.; KHONDOKER, R. Security Analysis of SDN WAN Applications - B4 and IWAN. *In*: KHONDOKER, R. SDN and NFV Security. [*s. l.*]: **Springer Lecture Notes in Networks and Systems**, v. 30, p. 111-127, 2018.

JIMÉNEZ, M. B. *et al*. A Survey of the Main Security Issues and Solutions for the SDN Architecture. **IEEE Access**, v. 9, p. 122016-122038, 2021.

KANWAL, A. *et al*. Exploring Security Dynamics in SDN Controller Architectures: Threat Landscape and Implications. **IEEE Access**, 2024.

KAUR, A.; KRISHNA, C. R.; PATIL, N. V. A comprehensive review on Software-Defined Networking (SDN) and DDoS attacks: Ecosystem, taxonomy, traffic engineering, challenges and research directions. **Computer Science Review**, v. 55, n. 9, p. 100692, 2025.

KHALIFA, E. H. *et al*. Brief Review of Using Machine Learning for Traffic Engineering in Software-Defined Networks. **Pakistan Journal of Life and Social Sciences**, v. 3, n. 1, p. 1738-1758, 2025.

KYTOMÄKI, J. **Artificial Intelligence and Machine Learning with SD-WAN**. 2021. Dissertação (Mestrado em Inteligência Artificial e Aprendizado de Máquina com SD-WAN) – [*s. l.*], 2021.

MAHAR, I. A. *et al*. A Comprehensive Survey of Software Defined Networking and its Security Threats. *In*: IEEE 1ST KARACHI SECTION HUMANITARIAN TECHNOLOGY CONFERENCE (KHI-HTC), 2024. **Anais** [...]. IEEE, 2024.

MARINHA DO BRASIL. Diretoria de Comunicação e Tecnologia da Informação da Marinha. **Acervo Arquivístico da Matinha do Brasil**, 2012. Disponível em: https://arquivodamarinha.marinha.mil.br/index.php/diretoria-de-comunicacao-e-tecnologia-da-informacao-da-marinha. Acesso em: 25 jul. 2025.

MARINHA DO BRASIL. Comunicações Navais: conheça a rede invisível que conecta e protege a Amazônia Azul. **Agência Marinha de Notícias**, 2025. Disponível em: https://www.agencia.marinha.mil.br/index.php/ciencia-e-tecnologia/comunicacoes-navais-conheca-rede-invisivel-que-conecta-e-protege-amazonia-azul. Acesso em: 21 jul. 2025.

MEDEIROS, F. A. R. **Organizações Conjuntas de Aquisição de Material de Defesa**: Uma alternativa para o Brasil? Rio de Janeiro: Biblioteca Digital do Exército, 2024. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/13200. Acesso em: 8 jul. 2026.

MINISTÉRIO DA DEFESA. **Diretriz de Implantação do Projeto de Criação do Comando de Defesa Cibernética**. Brasília, DF: Exército Brasileiro, 2016. Disponível em: https://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/01_diretrizes/04_estado-maior_do_exercito/port_n_004_eme_08jan2016.html. Acesso em: 27 jul. 2025.

MINISTÉRIO DA DEFESA. **Cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências**. Portaria nº 3.781/GM-MD, de 2020. Brasília, DF: Gabinete do Ministro, 2020. Disponível em: https://mdlegis.defesa.gov.br/norma_pdf/?NUM=3781&ANO=2020&SER=A. Acesso em: 27 jul. 2025.

NAVARRO, A.; CANONICO, R.; BOTTA, A. Software Defined Wide Area Networks: Current Challenges and Future Perspectives. *In*: INTERNATIONAL CONFERENCE ON NETWORK SOFTWARIZATION (NETSOFT), 9., 2023. **Anais** [...]. IEEE, 2023.

NETO, E. P. O Sistema de Comunicações Militares por Satélite do Brasil: breves considerações. **Panorâmico**, Rio de Janeiro, v. 2, n. 6, p. 61-64, 2023.

OLIVEIRA, M. M.; TEIXEIRA, L. **A defesa cibernética, o EB e a gestão de projetos**. Trabalho de Conclusão de Curso (Especialização em Gestão, Assessoramento e Estado-Maior) – Escola de Formação Complementar do Exército, Salvador, 2021.

OUAMRI, R. A. *et al*. A comprehensive survey on software-defined wide area network (SD-WAN): principles, opportunities and future challenges. **The Journal of Supercomputing**, v. 81, n. 291, 2025.

PEDERNEIRAS, L. C. **A guerra em transformação:** inteligência artificial sob a teoria de Clausewitz. Dissertação (Mestrado em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2024. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/13882. Acesso em: 8 jul. 2026.

RAHMAN, A.; HASAN, K.; JEONG, S. H. An Enhanced Security Architecture for Industry 4.0 Applications based on Software-Defined Networking. *In*: INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATION TECHNOLOGY CONVERGENCE (ICTC), 13., 2022. **Anais** [...]. IEEE, 2022.

RAHOUTI, M. *et al*. SDN Security Review: Threat Taxonomy, Implications, and Open Challenges. **IEEE Access**, 2022.

RAHOUTI, M.; XIONG, K.; XIN, Y. Secure Software-Defined Networking Communication Systems for Smart Cities: Current Status, Challenges, and Trends. **IEEE Access**, 2020.

REINO UNIDO. Ministry of Defence. **Strategic Defence Review**: Making Britain Safer: secure at home, strong abroad. Londres: Ministry of Defense, 2025. Disponível em: https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad. Acesso em: 8 jul. 2026.

SAHRAN, F.; ALTARTURI, H. H. M.; ANUAR, N. B. Exploring the Landscape of AI-SDN: A Comprehensive Bibliometric Analysis and Future Perspectives. **Eletronics**, v. 13, n. 1, p. 26, 2024.

SANTOS, M. G.; OLIVEIRA, J. M. P.; BELDERRAIN, M. C. N. Estruturação do Problema de Dimensionamento de Enlaces EBNet com Value-Focused Thinking e Strategic Choice Approach. *In*: SIMPÓSIO DE GUERRA ELETRÔNICA (SIGE), 2022. Disponível em: https://www.sige.ita.br/aiovg_videos/estruturacao-do-problema-de-dimensionamento-de-enlaces-ebnet-com-value-focused-thinking-e-strategic-choice-approach/. Acesso em: 21 jul. 2025.

UCRÂNIA. Unmanned Systems Force. **Unmanned Systems Force**, 2025. Disponível em: https://usforces.army/en/. Acesso em: 21 jul. 2025.

WASEEM, Q. *et al*. Software-Defined Networking (SDN): A Review. In: INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICOIACT), 5., 2022. **Anais** [...]. IEEE, 2022.

YALDA, K. G.; HAMAD, D. J.; TAPUS, N. A survey on Software-defined Wide Area Network (SD-WAN) architectures. In: INTERNATIONAL CONGRESS ON HUMAN-COMPUTER INTERACTION, OPTIMIZATION AND ROBOTIC APPLICATIONS (HORA), 2022. **Anais** [...]. IEEE, 2022.