ARTICLE DOI 10.52781/cmm.a202

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

Una nueva perspectiva para la Red Operativa de Defensa (ROD): Integración a nivel de Personas, Procesos y Tecnologías

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.

Resumen: El panorama mundial actual, caracterizado por una fuerte interdependencia entre los países y por rápidas transformaciones políticas, económicas y tecnológicas, ha acentuado la inestabilidad en diversas regiones. Las disputas comerciales, informáticas y cibernéticas ocurren constantemente, y las Fuerzas de Defensa Internacionales están replanteándose sus estrategias: o bien intensifican su cooperación para superar los desafíos comunes, o bien adoptan una reestructuración profunda, adaptándose a las exigencias del presente. La doctrina brasileña prevé integraciones periódicas en operaciones conjuntas, mientras que, a diario, cada Fuerza Individual tiene sus propios objetivos, planes y acciones, y coordina de manera autónoma y a nivel interno su infraestructura de Tecnología de la Información y de las Comunicaciones. Este artículo propone una nueva visión para la Red Operativa de Defensa (ROD), capaz de reunir capacidades conjuntas e integrar de manera continua a las personas, los procesos y las tecnologías. En este contexto tan dinámico, costoso y con escasez de inversiones, la unión de esfuerzos en la planificación y la construcción de una infraestructura única y flexible puede acelerar el desarrollo y la capacidad de defensa nacional.

Palabras clave: Ciencias Militares; Defensa; Integración; Red Operativa de Defensa; 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

Received: Jul. 30, 2025
Accepted: Apr. 09, 2026

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

1 INTRODUCTION

In global military history, integrated actions among the Armed Forces are common. However, rapid technological evolution, accelerated and bolstered by the development of Artificial Intelligence (AI), has driven the reformulation of concepts and doctrines that shape the modern art of war.

In the early 2020s, U.S. leadership moved to expand and develop joint systems within the United States, signaling requirements for system evolution and the integration of joint capabilities (Estados Unidos da América, 2021). More specifically, a strategy was developed for the full integration of Joint and Integrated Command and Control (C^2), known as the Joint All-Domain Command and Control (JADC2) Strategy (Estados Unidos da América, 2022).

Other nations have recognized shifts in the nature of recent global conflicts, such as the war between Russia and Ukraine, where the defending side rapidly developed Unmanned Systems Forces, a new unmanned military branch capable of operating across land, sea, and air on the battlefront with a range exceeding 2,000 km (Ucrânia, 2025). In a similarly aligned and even broader move, the United Kingdom recently released an integrated policy coordinating its transition from joint to integrated operations over the next decade. This includes the creation of a new Integrated Force (Reino Unido, 2025), responsible for maintaining a common digital foundation and managing shared data, elements essential to the new model of software-defined warfare.

Despite these doctrinal advances, the Brazilian Defense Operational Network (DON) still faces the challenge of fragmentation, operating as an arrangement of independent systems (RECIM, EBNet, and INTRAER) with isolated management structures. The identified gap is the absence of a model that integrates these infrastructures, not merely technologically, but also in ways aligned with people and organizational processes. Given this, this article addresses the following research question: how can a unified and flexible connectivity infrastructure be enabled to meet the Armed Forces' requirements for sovereignty and interoperability? The objective of this work is to propose a new vision for the DON, based on Software-Defined Wide Area Network (SD-WAN) technology, functioning as a system-of-systems integrated under shared governance.

The manuscript's primary contribution is the proposal of an organizational and conceptual model for integrating the DON. This study goes beyond mere diagnosis: it designs a Software-Defined Wide Area Network (SD-WAN) architecture to serve as the engine for the evolution of Defense's common digital foundation. In this context, the global trend is moving toward fostering a doctrinal evolution that brings the FFAA closer together and consolidates the infrastructure for joint operations, spanning everything from planning to the execution of core missions. A new vision for the DON is presented below, aiming to deepen the integration of connectivity and data infrastructure across people, processes, and technologies, while fostering greater sharing of workforce, knowledge, and investments. This approach enables complete information integration and enhanced cybersecurity by leveraging AI capabilities to address vulnerabilities and threats, while also demonstrating progress toward achieving permanent national objectives.

2 THEORETICAL REVIEW, DEVELOPMENT, AND METHODOLOGY

At the end of the last decade, Brazil updated and established new procedures to guide joint operations within the country. The Doctrine for the Military Command and Control System (SisMC²) establishes the fundamental C² principles for planning and execution: unity of command, simplicity, security, flexibility, reliability, continuity, speed, scope, and integration (Brasil, 2015). Joint Operations Doctrine dictates that joint planning must be grounded in the principles of universality, unity, objectivity, flexibility, coordination, and interoperability (Brasil, 2020). It is worth noting that only "unity" and "flexibility" appear as common requirements in both doctrines.

An update to the National Defense Strategy (END – *Estratégia Nacional de Defesa*) was recently approved, reaffirming that the desired state of readiness stems from continuous evolution in the transformation process and the pursuit of new capabilities, guided by doctrinal characteristics such as flexibility, adaptability, modularity, elasticity, and sustainability (Brasil, 2025a). Consequently, the Sectoral Defense Strategic Planning (PESD –*Planejamento Estratégico Setorial de Defesa*) was developed for the upcoming 12-year period (2024-2035). It aims to provide guidelines for acquiring new capabilities to address defense challenges with the necessary speed and effectiveness, targeting the maturity level required to achieve the desired strategic leap (Brasil, 2025b). When comparing this evolution with previous requirements, flexibility stands out as the only common factor.

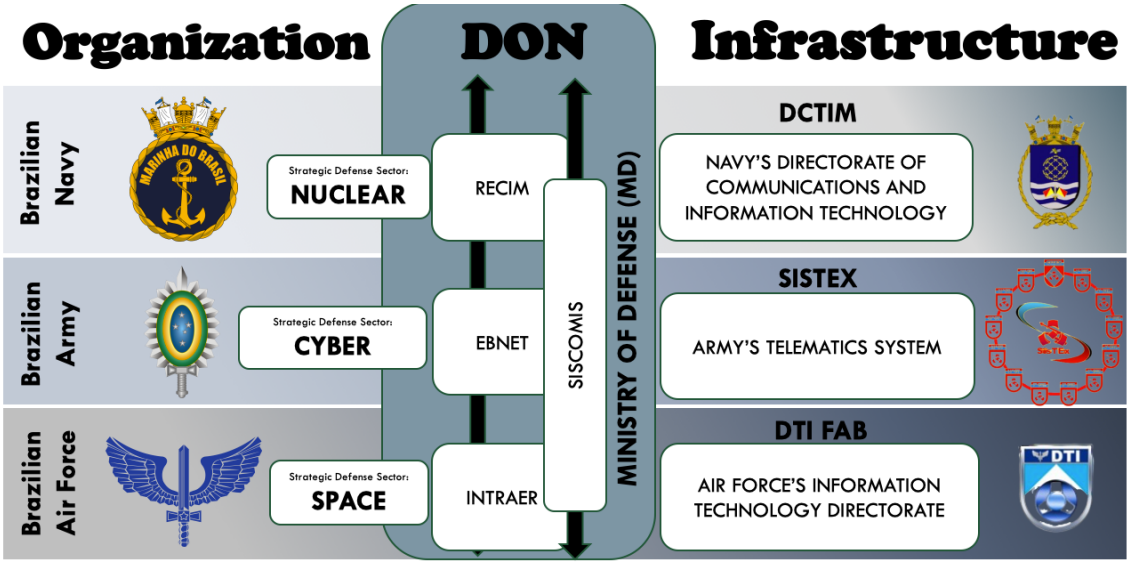
The Operational Concept for the Command and Control Decision Support Information System (SIADC²) links the key Information Systems/Decision Support Systems (SI/SAD) of the Joint Staff of the Armed Forces (EMCFA) and the individual Armed Forces, organizing them into a System of Systems structure. In other words, it is a set or arrangement of independent systems brought together to provide a capability that could not be achieved by those systems individually (Brasil, 2019). However, integrating a series of independent systems is not equivalent to a single, unified system in which every piece of data is shared and logically structured, and all information is known to a central logical intelligence.

Thus, in the face of dynamic global scenarios, doctrinal flexibility is directly proportional to infrastructure flexibility, enabling rapid reflection of changes across strategic, operational, and tactical levels. In the pursuit of greater visibility and synergy among networks and systems, it is desirable to consider expanding the sharing of a single network and data infrastructure across all FFAA, with a move toward developing and integrating joint capabilities.

2.1 Development

The DON is the network that integrates and provides services to the SisMC² (BRASIL, 2023a). It consists of a set of operational military data communication links configured as a Wide Area Network (WAN). It consists of the infrastructure through which defense data and information flow, featuring segregated and diversified connectivity across space and ground segments. It also encompasses the FFAA's data networks (RECIM, EBNet, and INTRAER) and, in specific cases, secure internet (Brasil, 2019), as shown in Figure 1.

Figure 1 – Organization and Structure of the current DON



Source: Prepared by the author.

The RECIM is the Navy's Integrated Communications Network, which connects the Navy's various Military Organizations (MO) and extends its reach to ships on missions abroad and to the Comandante Ferraz Antarctic Station (EACF – *Estação Antártica Comandante Ferraz*). In this way, it enables information exchange among the nine naval districts, which are responsible for coordinating and controlling operations within their respective areas of jurisdiction, thereby establishing itself as a fundamental component for the effectiveness of naval communications (Marinha do Brasil, 2025). It is, therefore, the responsibility of the Navy's Directorate of Communications and Information Technology (DCTIM) to:

> [...] ensure the efficiency and effectiveness of the Navy's Communications System (SISCOM) and of activities regarding the prevention and protection of the Cyberspace of Interest to the Brazilian Navy (ECiber-MB), to contribute to the readiness and employment of Naval Power, the Naval Cyber Warfare System (SisNavGCiber), and the Military Cyber Defense System (SMDC). [...] provide flexible, integrated, and interoperable Information and Communication Technology (TIC) services, with reliability, security, and speed (Marinha do Brasil, 2025, p. 2, our translation).

The EBNet is the Army's Corporate Communications Network, which functions as a private corporate intranet that interconnects the Brazilian Army's (EB) metropolitan and local networks to transmit data, voice, and images among MO (Exército Brasileiro, 2013). The Army's Telematics System (SisTEx) is responsible for providing the connectivity infrastructure (TIC) for the other systems and assets comprising the Army's Command and Control System (SC^2Ex), under the leadership of the Army's Integrated Telematics Center (CITEx) (Exército Brasileiro,

2024a, p. 2). SisTEx also comprises 12 Telematics Centers, operational elements geographically distributed across Brazil that support MO nationwide.

INTRAER is the internal network of the Air Force Command (COMAER), responsible for providing internal communications and access to Brazilian Air Force (FAB) systems. The Air Force's Information Technology Directorate (DTI) is tasked with developing and supporting corporate systems, flight simulators, and information security measures. It handles administrative and operational management, as well as training and human resources management, across its areas of responsibility (Força Aérea Brasileira, 2023).

To ensure redundancy between higher command levels, there is a complementary telephony and data integration system based on satellite technology, enabling greater coordination and cooperation among the three Brazilian FFAA (Neto, 2023). The Military Satellite Communications System (SISCOMIS) ensures the survivability of critical communications, even when commercial networks are inoperative, and guarantees the continuity of C^2.

2.2 Methodology

This research is qualitative and exploratory in nature. The methodological procedure consisted of a literature review and a document analysis of strategic guidelines and military doctrines from both Brazil and other nations (USA, UK, and Ukraine). Additionally, an analytical reflection was conducted regarding the institutional experience of implementing SD-WAN technology in crisis environments, specifically during Operation Taquari II in Rio Grande do Sul, to validate the premises of the proposed model.

Within the Ministry of Defense (MD), each of the FFAA maintains its own independent TIC infrastructure, which is aligned with high-level directives and integrated at strategic points. However, this study aims to present an opportunity to integrate corporate networks from planning through implementation, developing a unified, fully integrated network infrastructure with shared management that meets all regulatory requirements.

According to END (Brasil, 2025a), the strategic sector most closely linked to connectivity is the cyber domain. While led by the EB, this sector also involves the Brazilian Navy (MB) and the FAB in training, protection, response, and coordination of internal network incident response activities (Força Aérea Brasileira, 2025). These efforts are conducted jointly with the Cyber Defense Command (ComDCiber), which is tasked with planning, guiding, coordinating, and controlling operational, doctrinal, developmental, and training activities within the Military Cyber Defense System (SMDC – *Sistema Militar de Defesa Cibernética*) (Brasil, 2017), which acts as the central body, aiming to ensure the effective use of cyberspace by the FFAA while preventing or hindering its use against national defense interests. However, the CITEx is responsible for implementing and maintaining the SC^2Ex, integrated into the Land Force Command and Control System (SC^2FTer), to enable the secure and timely flow of information to commanders at all levels, thereby contributing to the enhancement of the Army's combat power and to national development (Exército Brasileiro, 2024b).

Regarding personnel, processes, and technology, the Army's Operational Doctrine requires the SC²Ex to undergo minimal changes to its physical and logical foundations while rapidly adapting to situational changes. It must employ diverse connectivity options and maintain flexibility to ensure continuity, reliability, and security (Exército Brasileiro, 2021). The EB has regulated the organization and operation of the SC²Ex, establishing premises, guidelines, and responsibilities:

> "In the context of convergence operations, C² is indispensable for ensuring joint, combined, and interagency interoperability, contributing to the Army's performance across all domains (land, maritime, air, cyber, electromagnetic, and space) and all dimensions of combat (physical, human, and informational)" (Exército Brasileiro, 2024a, p. 2, our translation).

Governance of the SEC²Ex is exercised by the Army's General Staff (EME – *Estado-Maior do Exército*), while the management of these systems is carried out by the Department of Science and Technology (DCT). Thus, collaboration is integrated within the EB, with CITEx responsible for managing projects and operating the EBNet infrastructure. Given this, increasing synergy and integration among the networks of all the FFAA could be beneficial. The most logical path, given SisTEx's extensive coverage and distribution across national territory, would be through it. Along these same lines, access for MB and FAB to Army data centers would be facilitated, integrating data and information in a complementary way and providing: better inter-institutional personnel management, expanding network operational management and incident response capabilities, while also achieving cost-efficiency in training and knowledge multiplication; better process management through resource sharing in centralized investments, the consolidation of best practices, and the unification of regulatory development; and better technological management through the application of combined personnel to policy controls and network operations, fully integrated in terms of connectivity and the hosting of critical sites and systems, thereby supporting intelligence services, joint operations, and integrated technological development.

3 IDENTIFIED RESEARCH CHALLENGES

As a result of the Cyber Defense Policy, the Ministry of Defense established the SMDC and mandated that:

> "The interagency capability of the SMDC's central body is characterized by collaborative action with representatives from federal public administration agencies, critical infrastructure sectors, and other public or private bodies, institutions, and companies of interest to Defense" (Ministério da Defesa, 2020, p. 1, our translation).

In this context, regarding personnel, the coordination involving the Ministry of Defense and its EMCFA typically interfaces with the General Staffs of the Singular Forces. Regarding processes, the acquisition and application of Cyber Defense capabilities, as well as the handling of network incidents, remain the independent responsibility of the MB, EB, and FAB, with autonomy to

plan, implement, and control their own infrastructure and operational methods, as well as to draft and oversee internal regulations.

Challenges in the technological realm are driven by a paradox, as outlined in the Cyber Defense Military Doctrine:

> "Technological Paradox – the greater the technological development, the greater the reliance on IT and, consequently, the greater the vulnerability to cyber actions. However, paradoxically, the conditions for defense against cyberattacks are also improved due to that high level of technological development" (Brasil, 2023b, p. 22, our translation).

However, AI has emerged as a key factor in modern military conflicts, capable of gathering data from diverse sources, processing vast amounts of information, and analyzing situations at high speed to support the Armed Forces' decision-making (Pederneiras, 2024). Thus, given the growing global use of AI in controlling robotic automation, pursuing development and independence in the defense technology sector has become essential.

The governance and management challenges faced by EBNet are linked to the "need versus possibility" dynamic (Santos, Oliveira & Belderrain, 2022). Migrating services to the digital cloud increases bandwidth demand for connectivity between MO and data centers. The cost-efficiency gained by concentrating investments in data centers is tied to the resources required to meet rising capacity demands and to scale each EBNet link, a process complicated by the differing visions and interests of various stakeholders.

A major technological hurdle is standardizing the equipment used. From early analog radio communications to modern, complex digital networks, communications have remained tied to proprietary technologies, resulting in integration limitations across manufacturers. It is inherent in the industry to use proprietary, closed standards to compel adoption of specific product lines across an entire organization. Issues regarding a lack of standardization are more pronounced in command, control, and communications (C^3) than in any other area (Medeiros, 2024).

One of the primary challenges for current networks is interconnecting link technologies used in operation without compromising capacity, range, or mobility. Consequently, a military communications system "must be a single logical structure integrated by multiple link technologies" (Camilo, Moura & Salles, 2020, p. 6). Indeed, among the communication networks currently employed within the DON's component sub-networks—RECIM, EBNet, and INTRAER—that utilize commercial technologies, there is no possibility for automatic integration without human intervention, as they were planned, implemented, and developed organically and independently of one another. Consequently, they are connected via specific links and limited adaptations to disjointed legacy networks, facing interoperability constraints and incomplete integration, and requiring IP address and port translation (NAT/PAT).

As part of the SMDC, the DON is a pillar of cyber defense, a permanent activity that seeks to maintain the secure and timely operation of computing equipment and systems, as well

as to promote protection against adversary exploitation and attack actions (Brasil, 2023b). Given this context, managing such an extensive infrastructure without unified leadership and combined, aligned actions—aimed at converging toward a single infrastructure—poses a major challenge.

4 A NEW VISION FOR THE INTEGRATION OF THE OPERATIONAL DEFENSE NETWORK (DON)

The Cyber Defense Military Doctrine states that:

> The SMDC is a set of facilities, equipment, doctrine, procedures, technologies, services, and personnel essential for carrying out actions to ensure the effective use of cyberspace by National Defense and to prevent or hinder hostile actions against its interests. It is also the responsibility of the SMDC to ensure the cyber protection of the SisMC², enabling secure networked operations as well as an integrated and collaborative approach to risk management regarding the protection of critical infrastructure, as outlined in the National Policy for Critical Infrastructure Security (Brasil, 2023b, p. 27, our translation)

In this regard, cybersecurity is already moving toward integrated management among the MB, EB, and FAB. However, this has not yet translated into a practical infrastructure for connectivity and joint data sharing, with a unified Network Operation Center (NOC) and Security Operation Center (SOC) capable of consolidating the entire system.

4.1 Integration at the levels of people, processes, and technologies

The National Defense Strategy states that:

> [...] the creation and expansion of integrating technology hubs are imperative to achieve self-sufficiency in the design and manufacture of C³I (Command, Control, Communication, and Intelligence) systems, to progressively eliminate external dependency (Brasil, 2025a, p. 14, our translation).

Thus, this proposal aims to present an innovation model for the DON that coordinates and integrates people, processes, and technologies.

4.1.1 Personnel integration proposal

Cyber protection measures are most effective when two other variables that comprise the C² system in action are aligned: personnel and doctrine. When these are weak, they become

potential vulnerabilities (Cordeiro, 2014). Therefore, it is incumbent on the FFAA to develop a joint doctrine to ensure that its personnel are trained and capable of disseminating knowledge, protecting critical information, countering an opponent's cyber actions, and remaining ready to respond to attacks.

Regarding personnel integration, measures could range from drastic and disruptive actions, such as creating a new Force, to more moderate, integrative steps, such as establishing ComDCiber (Ministério da Defesa, 2016). In the latter model, the MD and its EMCFA leverage their expertise to establish projects and working groups, formulate and issue guidelines, and ensure continuous coordination. Given the disparity in force sizes and the EB's designation as responsible for cybersecurity, one option is to establish a new Joint Network Operations and Security Center. Operating continuously and in an integrated manner, this center would not only monitor and operate the DON infrastructure but also actively design, develop, implement, and support a unified, common network infrastructure to foster new integrated capabilities.

Implementing an infrastructure based on software-defined networking (SD-WAN) and cognitive orchestration requires a profound restructuring of personnel technical skills across the Singular Forces. Transitioning from the paradigm of static asset configuration to dynamic flow management requires training military personnel to act as "Network Orchestrators" (the NetOps paradigm). In this scenario, literacy in Explainable Artificial Intelligence (XAI) is critical, enabling the operator to interpret and validate the autonomous decisions made by routing agents, thereby ensuring that technological automation remains under the control and ethical supervision of the human decision-maker during crises.

Beyond technical aptitude, the "New Vision" for the DON presupposes an evolution in organizational culture, shifting from information silos specific to each branch toward a mindset of full interoperability (a joint mindset). This cultural shift serves as the foundation for viewing digital sovereignty as a collective asset. Mutual trust in security protocols and the sharing of critical infrastructure, coordinated by the EMCFA, enable the network to act as a combat power multiplier, in which system resilience transcends the administrative boundaries of each Singular Force.

The primary need to enhance compatibility is addressed by a joint body responsible for developing and mediating operational requirements (Medeiros, 2024). This body would serve as a single control point for the DON, focusing on network management and oversight. While this group could function as a subsection of ComDCiber dedicated to protecting communications, data, and information, a more logical and less disruptive solution would be to expand the SisTEx NOC/SOC in Brasília, Federal District, which already manages nearly a thousand sites nationwide. Thus, it would be possible to integrate and absorb RECIM and INTRAER into EBNet, transforming it into the new DON with the collaboration of personnel and financial resources from the MB and FAB, thereby fully integrating the MO of all the Singular Forces. Not coincidentally, CITEx has been pursuing a nationwide technological upgrade of EBNet since 2024, having already validated its capabilities during the Rio Grande do Sul floods, as detailed in Section 4.2 of this article, and currently possesses the largest workforce of military personnel trained in this technology.

4.1.2 Proposal for procedural integration

Integrating and standardizing processes across the FFAA tends to be highly effective, enabling the consolidation and updating of best practices and the harmonization of regulations among the Singular Forces, thereby reducing inherent differences among the MB, EB, and FAB. Such dynamics foster closer ties among personnel and greater uniformity in military routines, facilitating joint planning and procurement, as well as the development of capabilities and systems for the new DON.

At a normative level, a combined update could not only optimize existing processes but also drive new, integrative strategic actions at the network and system levels, expanding the SMDC and aligning management, practices, and capabilities across strategic, tactical, and operational tiers. Furthermore, consolidating military data could enable enhanced intelligence identification, the correlation of databases and network events, and the aggregation of knowledge repositories and joint information.

Within the FAB, for instance, the DTI is the body that centralizes governance, legislation, system training and enhancement, information security, and cyber defense for all its MO. It also provides IT support for official events and military operations, strategic projects of the Air Force's General Staff (EMAER – *Estado-Maior da Aeronáutica*), simulators, and budget planning and management, among other areas (Força Aérea Brasileira, 2015). Should the MD choose to expand the mandate of this central network body and add new responsibilities, this could be established through a new Doctrine.

Centralized procurement is another process that would benefit from this approach. In 2024, CITEx purchased over 800 pieces of equipment for nationwide deployment, achieving significant cost savings driven by the direct interest of major manufacturers and inherent economies of scale. Centralizing procurement can generate gains in effectiveness and efficiency for the Federal Public Administration, provided there is greater integration of planning processes across the three Armed Forces, joint purchasing, increased equipment standardization, and enhanced interoperability among them (Medeiros, 2024).

Hosting MB and FAB websites and systems within EB data centers can itself enhance the efficiency of public resource utilization by sharing military assets and network incident response teams, among other resources. This solution would be further streamlined and facilitated by the new DON, which would provide access to national and joint C^3I systems subordinate to the MD.

Regarding governance, the proposed architecture optimizes the relationship between the strategic level (EMCFA) and the operational level (Singular Forces) through the Intent-Based Networking (IBN) model. This process allows higher command to establish high-level policies, such as prioritizing Command and Control traffic in conflict zones. At the same time, automated orchestration translates these intentions into technical configurations in real time. Such a governance flow preserves the operational autonomy of the Forces in the field while ensuring systemic compliance and agility in responding to jurisdictional incidents.

From a doctrinal standpoint, the integration of Zero Trust Architecture (ZTA) processes redefines the flow of access to strategic data, replacing perimeter-based trust with continuous verification of identity and integrity. This procedural rigor is enhanced by network slicing, which

enables the on-demand provisioning of isolated logical networks for specific missions. Thus, the DON evolves from a rigid infrastructure into a flexible, resilient service capable of instantiating secure communication corridors in dynamic theaters of operations with greater agility than traditional traffic engineering processes.

4.1.3 Technological integration proposal

In the technological realm, research focuses on attractive enterprise networks (Navarro, Canonico & Botta, 2023), autonomous and intelligent systems capable of adaptation and self-recovery with minimal human intervention (Waseem *et al.*, 2022). These networks enhance resilience, reduce costs, and enable the adoption of comprehensive market alternatives for the new DON. Among these options, some offer a new, flexible, and programmable software-defined networking architecture (Aggarwal, 2020), whether for Local Area Networks (LANs) via Software-Defined Networks (SDN), or Wide Area Networks (WANs) via SD-WAN. This evolution fosters computational capabilities (Khalifa *et al.*, 2025) and drives innovations sustained by extensive research (Belgaum *et al.*, 2020).

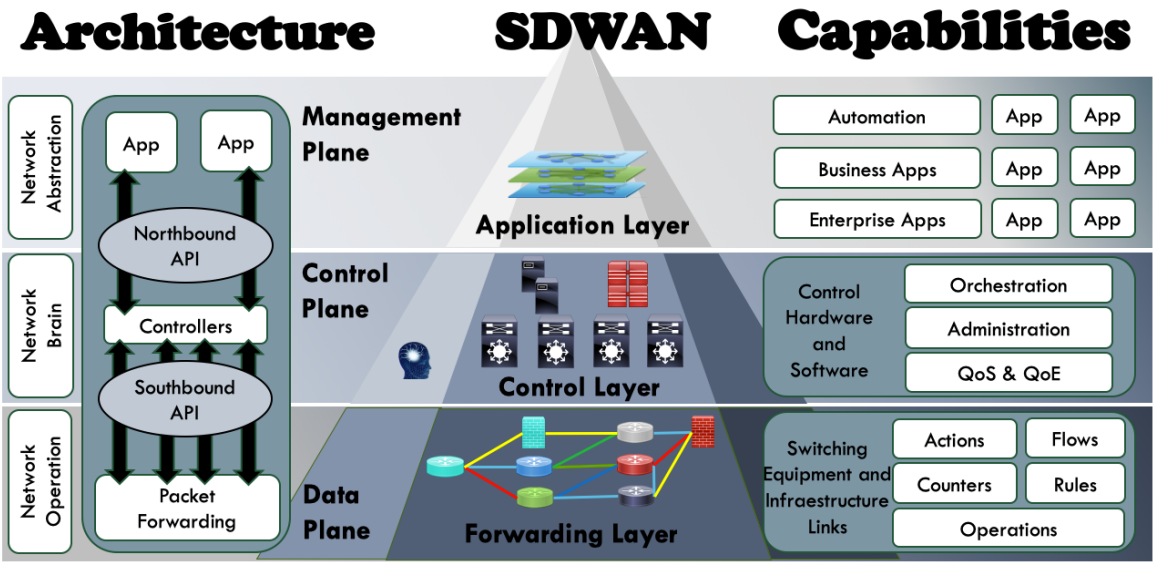
Given Brazil's continental dimensions and the FFAA's vast operational scope, SD-WAN communication network architecture, a flexible networking technology widely deployed today (Fu, Wang & Wang, 2024), is capable of operating on a global scale. It comprises a solution based on a programmable combination of hardware and software, offering advantages such as: low costs resulting from reduced hardware requirements and operating expenses (Diaz *et al*., 2022); faster, simplified management; enhanced security and visibility, featuring in-depth analytics and automated troubleshooting; improved availability through rapid, simplified failover; and superior overall network performance via bandwidth optimization (Yalda, Hamad & Tapus, 2022). This technology meets the requirements for achieving national defense objectives.

The integrated, innovative engineering approach enables reduced recurring system costs, extensive control and visibility, and enhanced innovation in infrastructure organization through automated, integrated management (Badotra; Panda, 2020). It is worth noting that the EB already possesses experience with SD-WAN technology. Currently, CITEx draws on resources from the Cyber Defense Program to equip the EB with capabilities to operate in cyberspace at the strategic, operational, and tactical levels (Estado-Maior do Exército, 2022). Upcoming deliverables include the restructuring of EBNet's cyber protection (Oliveira; Teixeira, 2021), with a significant portion of resources allocated to this solution. Parallel projects, such as the Integrated Border Monitoring System (SISFRON), also aim to acquire IT equipment for operations centers in the border zone (Exército Brasileiro, 2024c), thereby supporting acquisition execution and the alignment of deliverables.

Among the strategic pillars of future projects, documented in the numerous recently updated doctrines cited in this article, flexibility and unity stand out as key premises. The networking technology best suited to deliver these requirements on a national scale (with the potential for global expansion) is SD-WAN. Figure 2 illustrates its architecture and capabilities. This

technology leverages the flexibility and programmability of SDN (Abderrahman *et al.*, 2023) while providing a global view of all sites and integrating the network at all levels. Furthermore, this solution enables the simultaneous implementation of all active network management and control policies (Ouamri *et al.*, 2025). It facilitates segregation and migration for a gradual, supervised rollout at the site or OM level.

Figure 2 – General Architecture and Capabilities of SD-WAN Technology.



Source: Prepared by the author.

The SD-WAN Management Plane retains SDN applications (Kaur, Krishna & Patil, 2025) and incorporates new ones aligned with business, organizational, or enterprise objectives, enabling simplified management of the network and its associated devices (Mahar *et al.*, 2024) while enhancing the level of management and control over linked branches and remote sites. Similarly, it coordinates the network configurations and policies that the control plane is to implement within the enterprise production environment (Ali *et al.*, 2015).

While the Control Plane also manages the Data Plane (Bahashwan *et al.*, 2023), it requires greater resilience due to distance-related issues and associated metrics that can disrupt communication with a single remote controller. Consequently, latency or delays can hinder the management and installation of flows and rules, while link failures can compromise control and render the network inoperative (Ayodele; Buttigieg, 2024). For this reason, it is common to implement multiple distributed controllers to enhance control resilience and improve forwarding efficiency (Kanwal *et al.*, 2024). Enabling this requires additional orchestration among the controllers to keep them coordinated and synchronized, thereby ensuring connectivity that meets the expected Quality of Service (QoS) and Quality of Experience (QoE) standards (Rahouti *et al.*, 2022).

The SD-WAN Data Plane handles the solution's forwarding operations across a complex, distributed infrastructure featuring diverse, simultaneous, and redundant network links between nodes and sites, utilizing a wide range of Technologies (Rahouti, Xiong & Xin, 2020). Within this context, the Forwarding Layer is subdivided into the underlying infrastructure network and an overlay logical mesh. The latter establishes specific, alternative tunnels with granular, encrypted, point-to-point forwarding rules across the organization (Abdi *et al.*, 2024).

The SD-WAN solution is considered flexible and unique because it employs abstraction layers and WAN-optimized elements to deliver these capabilities, forming a unified system (Jiménez *et al.*, 2021). Its management is handled by the solution's Service Orchestrator, which serves as an upper-layer entity that manages multiple SD-WAN controllers and business applications (Jain; Khondoker, 2018). It is responsible for simplifying policy configuration and management across a geographically distributed network. The distributed switching components are Customer Premises Equipment (CPEs), physical or virtual edge devices deployed at branch offices, data centers, and cloud sites. They serve as endpoints for SD-WAN tunnels, encapsulating traffic and enforcing policies. Overlay tunnels, such as Internet Protocol Security (IPSec) or Virtual Extensible LAN (VXLAN), run over underlying physical networks (underlay) to create a private virtual network. This enables the use of diverse connectivity options and ensures security over public networks (Kytomäki, 2021).

Therefore, SD-WAN was designed to manage WANs connecting multiple geographically dispersed sites, such as corporate branches, data centers, and public or private cloud infrastructures. Its goal is to optimize connectivity across multiple underlying networks (MPLS, Internet, 4G/5G, and satellite) to ensure high QoS and QoE, as well as security and cost reduction (Badotra; Panda, 2020). In summary, while SDN lays the foundation for a programmable, centralized network, SD-WAN extends and optimizes it to meet the complexities and demands of modern wide-area networks by incorporating additional layers of functionality and intelligence (Rahman, Hasan & Jeong, 2022). Given this centralized network intelligence and visibility, integrating AI solutions further enhances its relevance (Sahran, Altarturi & Anuar, 2024).

Currently, RECIM handles data encryption and link redundancy, as well as the constant monitoring of critical systems (Marinha do Brasil, 2025). SD-WAN can ensure the continuity of these capabilities by enabling automatic multi-link selection and automated, coordinated site encryption, including flow-specific control filters, provided they comply with established policies. Thus, it bolsters robustness beyond the FFAA's individual infrastructures by employing advanced security measures and resources to prevent and respond to cyber threats, thereby maximizing resilience to the challenges of modern cyber warfare.

While SD-WAN technology offers significant potential for automation and operational cost reduction, its implementation within the DON presents substantial challenges. Transitioning from disjointed legacy networks to a unified structure requires robust inter-institutional governance to prevent management conflicts among the Singular Forces. Furthermore, ensuring interoperability across different vendors—thereby avoiding vendor lock-in—and the need for

continuous technical staff training to manage programmable networks constitute barriers that necessitate a gradual, supervised transition plan.

Ultimately, overcoming implementation challenges and mitigating the aforementioned limitations necessarily requires fostering technological autonomy and digital sovereignty. In this context, the transition to a modern, integrated DON requires promoting domestically developed SD-WAN solutions, coordinated through the Triple Helix innovation model (State, Academia, and Industry). The convergence of efforts among the Armed Forces' research institutes, universities, and the Defense Industrial Base (BID) is essential to reduce strategic dependence on foreign technologies and protocols. Such alignment not only strengthens innovation within the defense sector but also ensures that control and governance of the country's critical communications infrastructure remain under strict national jurisdiction and technological sovereignty.

4.2 SD-WAN Validation During the RS Floods and the Technological Evolution of EBNet

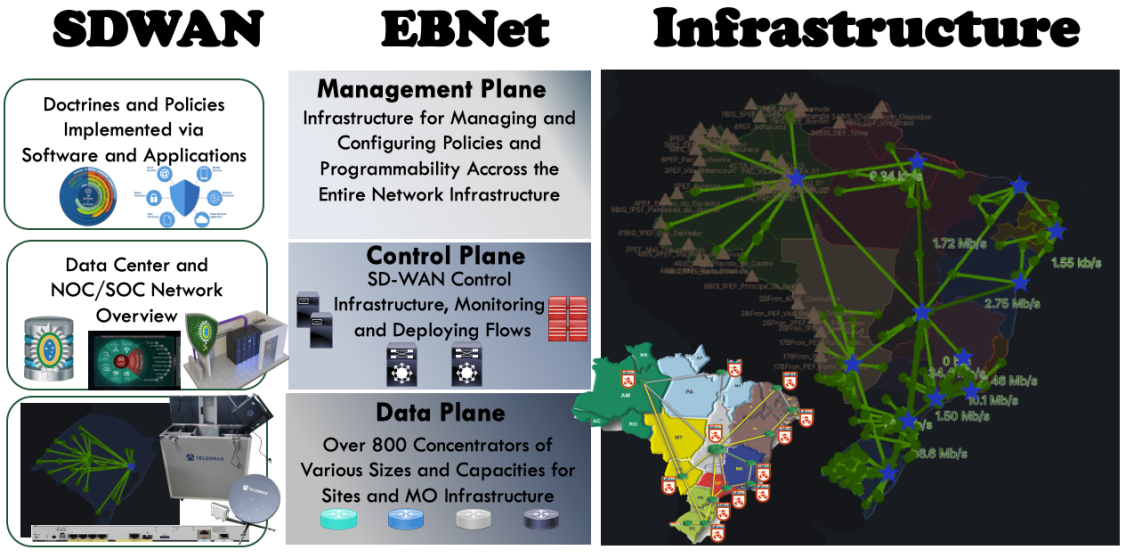
During the severe floods in southern Brazil in 2024, which triggered Operation Taquari II, the C^2 infrastructure experienced significant instability. Faced with consecutive, simultaneous, and prolonged outages of conventional network and connectivity systems, there was a shortage of qualified technical personnel to implement the changes needed to keep the network operational. Adjustments to equipment configurations were required, specifically regarding encryption for conventional links (which were experiencing intermittent connectivity) and the manual reconfiguration of tunnels across various sites, all under limited resources, such as transport and electricity.

As an alternative, Metro Ethernet links were converted to internet access, thereby increasing availability. Furthermore, over 480 satellite terminals utilizing various technologies were received and distributed across the state to OM and tactical posts, providing users with remote access to EBNet via VPN clients on their devices. To ensure faster responses without human intervention, SD-WAN integration software was rapidly deployed in a virtualized environment. This software centralized the forwarding policies that coordinated and controlled network traffic among the equipment in this architecture across three critical EBNet sites. These sites operated in parallel and aggregated all available links at the MO (Metro Ethernet, radio, fiber, internet, and satellite). The new solution was capable of monitoring, selecting, and forwarding network packets using existing resources, performing automated load balancing across available links and selecting paths based on pre-configured policies, thereby increasing network resilience and enabling continuous information flow. Thus, the rapid, effective, and partially virtualized implementation of the SD-WAN infrastructure at strategic sites (Figure 3) achieved complete and secure integration of the OM's internal networks, validating many of the capabilities described in this article.

Figure 3 illustrates the composition of the SD-WAN layers integrated into the EBNet during the pilot project, translating doctrines and policies into software. This software leverages computational intelligence to aggregate network-wide information and efficiently route it via the

best available links, including temporary and dynamic options, such as emergency satellite links. MO in the South pioneered the Army-wide migration process during the Cyber Environment Protection Project. SisTEx continues to design, implement, and operate systems across the national territory, with regional support from the Telematics Centers.

Figure 3 – SD-WAN validation infrastructure during the Southern Floods



Source: Prepared by the author.

Thus, SD-WAN can be considered efficient at integrating MO into the EBNet, offering flexibility and resilience. This ensured successful automated, software-based link management and led to the conclusion that it was the best technological solution for times of uncertainty. This tool provided connectivity and security through policy programmability. This feature expanded network autonomy, enabled self-healing capabilities, automated data flows, and reduced the need for specialized technical staff intervention during intermittent infrastructure outages.

A network of this nature, more autonomous and flexible, was already being designed by CITEx. However, it had not yet been implemented by the time of the disaster. The event ultimately demonstrated the efficiency of SD-WAN technology, even within the EB's extensive network, which comprises over 860 connection points. This proved crucial for subsequent acquisitions, which were already planned at the national level through a centralized, standardized procurement process, thereby providing a comprehensive, integrated view of the new EBNet. In the months that followed, the EB was able to accelerate the EBNet technological evolution project and redirect equipment originally intended for the Southern region, enabling the implementation and operation of this technology across 108 regional barracks within a few months and thereby enhancing the region's operational resilience. In this context, it can be inferred that this infrastructure is capable

of organic expansion and of incorporating additional sites, including those of the MB and FAB, to form the new DON and to integrate personnel, processes, and services.

5 FINAL CONSIDERATIONS

EME defined Force 40 to guide the evolution of EB's Transformation Concept for the 2024–2039 period, grounded in the following pillars of effort: a Strategic Concept oriented toward 2040; new capabilities; new doctrine; and personnel (Exército Brasileiro, 2024d). In this context, the proposal developed for the new DON is timely, as it incorporates Cyber Protection and Defense capabilities and positions the EB to lead coordination of the FFAA's joint infrastructure.

In a context of scarce financial resources and technological dependence, where there is a demand for the immediate acquisition of foreign technology, nothing is more desirable than adopting a unified, flexible infrastructure model that enhances network and system integration at all levels, thereby fostering the development of joint capabilities. Furthermore, the sooner strategic partnerships are established with an ally sharing common interests, the sooner Brazil will be able to develop its own SD-WAN technology. This solution incorporates software-managed programmability and flexibility, fully enabled by parallel advancements and AI-enhanced capabilities (Cifuentes *et al.*, 2024).

In this context, the Brazilian Artificial Intelligence Strategy (Brasil, 2021) states that the integration of AI systems into the productive structure is a reality and will play a fundamental role in enhancing efficiency, reducing costs, and minimizing operational errors, in addition to automating various processes and making routines more flexible and agile. Fully aligned with this, a strategic guideline was developed for the EB recommending the implementation and integration of AI systems. This enables the processing of information from diverse existing sources, as well as the structuring and correlation of data from new sensors and systems, to establish timely situational awareness, anticipate events, and support decision-making (Exército Brasileiro, 2024e). Concurrently, an opportunity arises to expand, optimize, and share investments in the AI infrastructure of the FFAA and the MD.

REFERENCES

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. Available at: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/doutrina_militar/lista_de_publicacoes/md31a_ma_03a_douta_sismca_3a_eda_2015.pdf. Access on: July 22, 2025.

BRASIL. **Comando Conjunto na Defesa Cibernética**. Agência Gov Br, 2017. Available at: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/comando-conjunto-na-defesa-cibernetica. Access on: July 25, 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. Available at: https://www.gov.br/defesa/pt-br/arquivos/File/doutrinamilitar/listadepublicacoesEMD/md31a_sa_04a_finala_20a_nova_2019a_1a_edicao.pdf. Access on: July 21, 2025.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas (MD30-M-01)**. Brasília, DF: Ministério da Defesa, 2020. Available at: 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. Access on: July 22, 2025.

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

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

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

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa (END).** Brasília, DF: Ministério da Defesa, 2025a. Available at: 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. Access on: July 24, 2025.

BRASIL. Ministério da Defesa. **Planejamento Estratégico Setorial de Defesa (PESD) 2024-2035**. Brasília, DF: Assessoria Especial de Planejamento, 2025b. Available at: 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. Access on: July 24, 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. Available at: https://epex.eb.mil.br/index.php/programas-estrategicos-do-exercito. Access on: July 27, 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. Available at: https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%205123.01J.pdf. Access on: July 22, 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. Available at: https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf. Access on :July 22, 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. Available at: https://www.sgex.eb.mil.br/sg8/002_instrucoes_gerais_reguladoras/01_gerais/port_n_578_cmdo_eb_10jul2013.html. Access on: July 25, 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. Available at: https://www.sgex.eb.mil.br/sg8/002_instrucoes_gerais_reguladoras/01_gerais/port_n_578_cmdo_eb_10jul2013.html. Access on: July 8, 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. Available at: https://www.sgex.eb.mil.br/sistemas/boletim_do_exercito/copiar.php?codarquivo=181261862&act=sep. Access on: July 27, 2025.

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

EXÉRCITO BRASILEIRO. Escritório de Projetos. **SISFRON**. Brasília, DF: Escritório de Projetos, 2024c. Available at: https://epex.eb.mil.br/. Access on: July 27, 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. Available at: https://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/07_publicacoes_diversas/01_comando_do_exercito/port_n_2300_cmdo_eb_12agosto2024.html. Access on: July 27, 2025.

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

FORÇA AÉREA BRASILEIRA. Organização se prepara para proteger redes corporativas da instituição. **Tecnologia da Informação**, 2015. Available at: https://www.fab.mil.br/noticias/tag/DTI. Access on: July 27, 2025.

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

FORÇA AÉREA BRASILEIRA. Centro de Defesa Cibernética encerra intercâmbio com expectativas superadas. **Agência da Força Aérea**, 2025. Available at: 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. Available at: https://arquivodamarinha.marinha.mil.br/index.php/diretoria-de-comunicacao-e-tecnologia-da-informacao-da-marinha. Access on: July 25, 2025.

MARINHA DO BRASIL. Comunicações Navais: conheça a rede invisível que conecta e protege a Amazônia Azul. **Agência Marinha de Notícias**, 2025. Available at: https://www.agencia.marinha.mil.br/index.php/ciencia-e-tecnologia/comunicacoes-navais-conheca-rede-invisivel-que-conecta-e-protege-amazonia-azul. Access on: July 21, 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. Available at: https://bdex.eb.mil.br/jspui/handle/123456789/13200. Access on: July 8, 2026.

MINISTÉRIO DA DEFESA. **Diretriz de Implantação do Projeto de Criação do Comando de Defesa Cibernética**. Brasília, DF: Exército Brasileiro, 2016. Available at: https://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/01_diretrizes/04_estado-maior_do_exercito/port_n_004_eme_08jan2016.html. Access on: July 27, 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. Available at: https://mdlegis.defesa.gov.br/norma_pdf/?NUM=3781&ANO=2020&SER=A. Access on: July 27, 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. Available at: https://bdex.eb.mil.br/jspui/handle/123456789/13882. Access on: July 8, 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. Available at: https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad. Access on: July 8, 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. Available at: https://www.sige.ita.br/aiovg_videos/estruturacao-do-problema-de-dimensionamento-de-enlaces-ebnet-com-value-focused-thinking-e-strategic-choice-approach/. Access on: July 21, 2025.

UCRÂNIA. Unmanned Systems Force. **Unmanned Systems Force**, 2025. Available at: https://usforces.army/en/. Access on: July 21, 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.