MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

# An Indigenous Unified Defence Cloud: Securing India's Digital Sovereignty

*Mohit Walia*

November 10, 2025

## Summary

A self-reliant Armed Forces Cloud will safeguard India's military communication systems while strengthening strategic independence. A unified, secure digital backbone will enable faster decision-making and protect vital information.

The age of purely conventional warfare is receding. Warfare has irrevocably shifted to the digital, cyber and information domains. Modern wars decisively hinge on information, speed and resilient digital infrastructure, the foundation of which is the Cloud. Secure communication, real-time data management, seamless intelligence sharing and the rapidity of the command decision cycle are all crucial elements that give an upper hand in the modern battlefield.

Today’s battlespace relies heavily on acronyms like Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). There is the proliferation of Cyber Warfare, reliance on Artificial Intelligence (AI) assisted decision-making and the conduct of complex Multi-Domain Operations (MDOs). Every modern capability, from processing satellite imagery to guiding hypersonic missiles, relies fundamentally on the robustness, security and scalability of the cloud infrastructure that supports it.

The Indian Armed Forces are positioned at a critical crossroads where cloud technology, cyber defence and data sovereignty intersect. Developing a self-reliant and sovereign Defence Cloud has become a strategic imperative rather than an option.[1] Reliance on foreign systems for vital military communications exposes the nation to significant dangers such as data breaches, supply chain risks and operational vulnerabilities, particularly in crises or conflict. In today’s digital age, data has become the ‘new gold’ and a unified Data Cloud functions as its secure ‘vault’—offering reliable protection against theft, intrusion or irretrievable loss. Ensuring true digital sovereignty requires absolute national control over these essential data assets.

## Current Landscape: Fragmented and Nascent Capabilities

Developing a robust and specialised Armed Forces Cloud requires an in-depth evaluation of the current cloud frameworks that serve the government, defence and research domains. While India has established several key initiatives that perform effectively for civilian use, they are not yet adequately strengthened to withstand the rigorous requirements of real-time, high-intensity military operations in wartime scenarios. At the core of the government’s cloud initiative lies the MeghRaj National Cloud (GI Cloud), developed mainly for the National Informatics Centre (NIC) and various government departments to support e-governance and public service delivery. It provides Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) services. It strongly promotes the adoption of Open-Source Software (OSS),

[1] **“Atmanirbhar, Agrani, and Atulya Bharat 2047: India's Defence Industrial Sector Vision 2047”**, KPMG, May 2025.

thereby serving as a benchmark for secure and transparent technology implementation.[2]

**Table 1. India's Cloud Initiatives**

| Name | Purpose / User Base | Key Features |
|---|---|---|
| **MeghRaj National Cloud** ("GI Cloud") | Government/NIC's departments, e-public governance, services[3] | It offers IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) and SaaS (Software-as-a-Service), multiple locations, guidelines/policies for security, and data locality.[4] |
| **NICSI-Jio Government Cloud under Megh Raj 2.0** | To enhance the national cloud infrastructure for government entities[5] | Secure, scalable cloud services; multi-cloud options; dedicated government cloud offerings. |
| **RailTel / DRDO on-premises cloud/data centre enhancements** | DRDO's research, testbeds, data storage/processing under defence R&D | Projects for enhancing data centres' networks and infrastructure; cloud services orders to RailTel for DRDO. |

These existing clouds, however, are primarily designed for administrative functions and basic research rather than active military deployment. They often fall short of the stringent military-grade requirements for security classification, air-gapping, advanced encryption and redundancy essential for combat readiness.

India's armed forces have also undoubtedly embarked on developing exclusive, mission-specific digital platforms. The Army Cloud, the Indian Army's Private Cloud, is an exclusive internal network established to securely store personnel and operational information within a strongly encrypted framework, operating as an Infrastructure-as-a-Service (IaaS) system with centralised, near-line and disaster recovery facilities. ARPAN 3.0 (Army Record Office Process Automation) is a dedicated Software-as-a-Service (SaaS) solution operating on the Army Data Network/Cloud

[2] **"Policy on Adoption of Open Source Software for Government of India"**, Ministry of Electronics and Information Technology (MeitY), Government of India, 2014.

[3] **"About MeghRaj"**, NIC.

[4] **"Annual Report 2021-22"**, Ministry of Defence, Government of India, 2022.

[5] **"AMBUD: Adoption of MeghRaj By User Departments"**, Ministry of Electronics and Information Technology (MeitY), Government of India.

that digitises personnel records, enabling secure, instant access for administrative management.[6]

There are also integrated initiatives such as the Defence Information Infrastructure (DII), which seeks to establish a unified information network linking the three armed services. The Naval Network Centric Operation (NNCO) functions as the Navy's cloud-based platform for real-time data exchange, supported by the tri-service Defence Communication Network that unifies communication systems. A limited Armed Forces Cloud is also being developed to provide secure computing and storage capabilities.

Though progressing, India's defence cloud ecosystem remains underdeveloped and compartmentalised compared to global military benchmarks. Key constraints include:

- **Fragmented Structure**: Different protocols restrict data sharing across services, hindering the seamless coordination and integration required for effective multi-domain operations.[7]
- **Foreign Dependence**: Reliance on overseas hardware and essential software components heightens vulnerability to cyber intrusions and potential disruptions within the supply chain.
- **Scalability Limitations**: The existing infrastructure is inadequate for managing the massive data volumes, analytics demands and computational intensity required for advanced tasks such as sensor fusion and real-time C4ISR coordination.
- **Limited Integration with Emerging Technologies**: Present infrastructures cannot seamlessly incorporate advanced tools like AI, machine learning and quantum-secure encryption, all critical for future warfare environments.

These deficiencies underscore the urgent need for a unified, fully indigenous defence cloud architecture to close current gaps and strengthen long-term strategic resilience.

## The Global Cloud Arms Race: Setting the Benchmark for Sovereignty

The necessity for a unified military cloud is driven by a fierce global 'cloud arms race' in which major military powers—the United States and China—have achieved

[6] Huma Siddiqui, **"Indian Army Gets Cloud Cover"**, *Express Computer*, 16 November 2015.

[7] **"Breaking Silos: Why India's Armed Forces Must Embrace a Joint Culture"**, *India Today*, 2 October 2025.

significant operationalised maturity. This competition is not about capacity alone but about establishing strategic advantage through digital superiority and data control.

**Table 2. Defence/Government Digital Cloud Structures: India, China and the US**

| Description | India | China | USA |
|---|---|---|---|
| **Scale / Investment** | Growing, multiple governmental and DRDO/data clouds, centre upgrades, but less publicly known capacity for a fully hardened combat cloud. | Large state-controlled cloud providers (e.g., Alibaba Cloud, Tencent Cloud, Baidu), strict legal mandates to store data locally; rapid build-out in defence and dual-use infrastructure.[8] | The United States has mature defence clouds, such as milCloud 2.0, JWCC (Joint Warfighting Cloud Capability), DISA, and the Department of Defense Information Network (formerly GIG). It also has massive budgets for secure, hybrid, air-gapped and edge computing integration.[9] |
| **Legal / Jurisdictional Control** | There is high potential via local laws and policy, but empirical public documentation is weaker for some military-grade clouds on dependent private providers. | Very strong-Chinese law mandates data localisation, government oversight and state control over critical infrastructure. | Strong regulations also apply, but some providers are global; federal contract vehicles and high-classification cloud segments ensure control. |

[8] X. Chen and W. Li, **"**PLA Cloud Computing and Military Modernization**"**, *Journal of Strategic Studies*, Vol. 46, No. 3, pp. 412–438.

[9] "Joint Warfighting Cloud Capability: Implementation Report", U.S. Department of Defense, 2022.

| | | | |
|---|---|---|---|
| **Edge / Theatre Command Cloud** | There are large signs of movement, but it is not fully operational. In India, edge cloud/theatre command cloud is still more conceptual. | China invests heavily in distributed cloud infrastructure, edge cloud across regions and dual-use infrastructure. | The USA is pushing "battlefield cloud", edge computing, mesh architectures, and secure nodes in contested environments. |
| **Resilience, Security, Encryption Standards** | India is catching up, with examples like the DRDO Cloud and RailTel enhancements, but there is relatively less public information on hardened, air-gapped military cloud infrastructure. | China is likely ahead in deploying a large-scale secure defence cloud: many internal cloud providers are under tight government oversight. | The USA has explicit programs, multi-level certifications, secure multi-level clouds, formal assurance levels, and ongoing R&D. |

The Chinese People’s Liberation Army (PLA) has rapidly advanced its cloud infrastructure, driven by a state policy that tightly integrates military and civilian innovation. Its architecture supports MDOs by merging cyber, space and electronic warfare assets under a unified data environment. China’s reliance on state-owned providers, governed by strict data localisation and oversight laws, ensures complete national control.[10] Significant investments in distributed cloud networks and edge computing allow the PLA to sustain high-speed processing at the tactical level, strengthening the fusion between military and civilian systems.

The US Department of Defense (DoD) operates an extensive, globally interconnected network of secure cloud systems. Programmes such as the Joint Warfighting Cloud Capability (JWCC) utilise commercial hyperscale platforms fortified to military-grade standards (Impact Level 6).[11] This hybrid–multi-cloud model underpins

[10] **“Military and Security Developments Involving the People's Republic of China 2024”**, Annual Report to Congress, U.S. Department of Defense.

[11] **“Military Cloud Computing Market Size, Share, Industry Report, Revenue Trends and Growth Drivers”**, Markets and Markets, September 2023.

the Joint All-Domain Command and Control (JADC2) concept—linking every sensor and shooter across land, sea, air, space and cyber into a single, real-time data grid described as the “battlefield cloud”.[12]

As noted above, progress is visible in India, but the defence cloud remains fragmented and limited in scale.[13] While domestic laws provide a framework for sovereign data control, dependence on private and foreign technologies dilutes this authority. The Edge or Theatre Command Cloud remains more in concept than deployment, lagging major powers' operational models. The takeaway is evident: a robust combat cloud must become the core nervous system of India’s future warfare architecture. Guided by Atmanirbhar Bharat, sustained and accelerated development is essential to achieve full strategic autonomy and effectively support the emerging Tri-Service Commands.

## National Policy and Emerging Architecture: The Road to Atmanirbharta

Major national policy initiatives, notably the Atmanirbhar Bharat (Self-Reliant India) mission, propel the strategic shift towards a unified military cloud. This policy creates a unified framework consistent with the MeghRaj (GI Cloud) initiative and MeitY’s Cloud First Policy, advancing India’s goal of achieving digital sovereignty and maintaining secure control over its critical data assets.[14]

Key programmes shaping this foundation include:

- **Defence Cloud Initiative (DRDO)**: Focused on building a specialised, secure, scalable cloud infrastructure to manage classified defence information and support mission-critical operations.
- **Cyber Security and Native Grid (CSNG)**: This initiative by the Ministry of Defence aims to establish a self-reliant and robust cyber infrastructure.
- **Collaborations and Investments**: Strategic funding and partnerships include agreements with RailTel to modernise data centres, provide on-premise cloud services for DRDO, and leverage government community cloud platforms operated by NICSI and Jio Platforms.

[12] "Department of Defense Cloud Strategy", U.S. Department of Defense, 2022.

[13] P. Rao and M. Singh, “Cloud Computing in Indian Armed Forces: Current Status and Future Directions”, *Defence Science Journal*, Vol. 73, No. 5, 2023, pp. 567–584.

[14] **“Atmanirbhar, Agrani, and Atulya Bharat 2047: India's Defence Industrial Sector Vision 2047”**, no. 1.

The primary catalyst for cloud integration is restructuring India's armed forces into Tri-Service Theatre Commands, guided by the Chief of Defence Staff (CDS).[15] Creating these unified commands necessitates a theatre-level cloud framework that connects the Army, Navy and Air Force within a single operational ecosystem, ensuring smooth multi-domain collaboration and coordinated decision-making.[16]

Current efforts are establishing the necessary ecosystem for AI and true network-centricity:

- **Tri-Service Agencies**: Agencies for Cyber, Space and Special Operations have been established under the Integrated Defence Staff, acknowledging these new domains and their requirement for unified digital infrastructure.[17]
- **Defence AI Council (DAIC) and Defence AI Project Agency (DAIPA)**: Tasked with marshalling resources for the R&D and implementation of AI in the armed forces. An enhanced cloud platform is explicitly recognised as the critical ICT backbone required to power AI applications for C4ISR and predictive analytics.
- **Scaling MeghRaj-like Solutions**: Experts advocate for significantly scaling up the National Cloud MeghRaj or an equivalent indigenous platform to facilitate the secure exchange of voluminous data, integrating indigenous 5G/6G technology to expedite AI deployment at the tactical edge.
- **Private–Public Partnership in Tech**: An increased push for collaboration with the private sector, led by DRDO, to develop cutting-edge C4I2SR systems foundational to military cloud infrastructure.

## Case Study: Securing the Human Layer with Indigenous Communication

India's operational and logistical data security faces significant vulnerabilities through the communication practices of defence personnel. The widespread and often casual use of commercial messaging platforms like WhatsApp—even for non-classified but operationally sensitive communications—creates a substantial yet frequently ignored security gap, exposing critical metadata to foreign legal frameworks and intelligence oversight.[18] Moving towards genuine digital

[15] "Tri-Service Commands: The Way Forward for Indian Armed Forces", Centre for Land Warfare Studies, 2022.

[16] **"Theatre Command: How India is Looking to Integrate Air Force, Navy and Army Operations Under a New Strategy"**, *The Economic Times*, 2 October 2025.

[17] **"Indian Armed Forces: Building a Future-Ready Military"**, *NEXT IAS*, 3 October 2025.

[18] **"Zoho Fasttracks End-to-end Encryption for its WhatsApp Rival Arattai"**, *The Economic Times*, 8 October 2025.

independence requires the strategic adoption of indigenous communication platforms. For instance, the SAI and Zoho's Arattai apps represent a viable, immediately deployable Indian alternative that could address these security concerns while supporting domestic technological capabilities.[19]

**Table 3. Indigenous App Features**

| Feature | Indigenous App Advantage | Strategic Impact |
|---|---|---|
| **Data Residency** | All user data is warehoused at servers located in India. | Data Sovereignty: Disconnects data from foreign legal /intelligence jurisdiction, maintaining control under Indian law. |
| **Indigenous Development** | Sai, developed by Col Sai Shankar of the Indian Army.<br>Arattai, developed by an Indian company, Zoho Corporation. | Trust and Transparency: Aligns with the indigenous policy of Atmanirbhar Bharat and ensures accountability under Indian law to minimise foreign supply chain risk. |
| **Functionality** | Provides one-on-one and group chats, audio/video calls, and end-to-end encryption features exactly like WhatsApp. | Gives necessary secure communication functionality without compromising operational security, even for non-classified exchanges. |

The SAI (Secure Application for Internet) app is a messaging/multimedia communication app developed for Army use and launched in 2020 by Raksha Mantri Rajnath Singh. The SAI app can be customised for defence requirements, aligning with operational and intelligence military environments, not just generic chat. Arattai (meaning 'chat' in Tamil) enhances communication security by ensuring all data remains within India's borders, with servers hosted entirely domestically. Although its end-to-end encryption framework is still evolving, the platform's strong emphasis on privacy, data protection and full compliance with national regulations makes it a timely and suitable substitute for existing foreign applications. While a

[19] **"**Arattai: Enterprise Secure Communication Platform – Technical Specifications**"**, Zoho Corporation, 2023.

customised, hardened version would eventually be necessary for mission-critical and highly secure communications, establishing SAI/Arattai as the medium for routine, human-level exchanges represents a crucial first step towards reinforcing the nation's broader digital security framework and reducing the dependence on foreign commercial apps, viz. WhatsApp.[20]

## Defining the Strategic Imperatives of a Unified Defence Cloud Architecture

Moving beyond India's fragmented digital infrastructure towards a comprehensive Armed Forces Cloud requires adherence to several fundamental strategic principles.

### *Secure, Classified Infrastructure with Tiered Access*

Armed Forces Cloud must operate on a physically hardened, classified digital backbone completely isolated from public internet domains. Establishing Tri-Service Classified Data Centres (TSDCs) at strategic command locations equipped with air-gapped connectivity, Faraday shielding, and defence-grade electromagnetic protection is required. Tiered access control across Strategic (HQ), Operational (Command) and Tactical (Unit) levels through multi-factor authentication combining biometrics and cryptographic keys needs to be implemented. Ensuring trusted supply chain verification for all semiconductor and hardware components, using only NAC- or DRDO-certified vendors, is essential.

### *Absolute Data Sovereignty*

All operational, intelligence and mission-critical data should be hosted exclusively within MoD-controlled sovereign cloud clusters at Naval HQ, Army Data Centre and AFNET nodes. Any foreign-origin technology deployment should undergo mandatory security clearance, source code inspection and vulnerability testing before induction. Formulation of a Defence Data Protection Framework (DDPF) aligned with the Defence Cyber Security Policy to enforce legal, physical and jurisdictional sovereignty across all data ecosystems is crucial.

### *Embedded Edge Computing Capabilities*

Ruggedised edge servers at Forward Operating Bases (FOBs), Air Defence Nodes and Naval Tactical Centres to enable local AI-driven analytics and mission autonomy need to be deployed. Combat Edge Nodes for naval and air assets capable

[20] R. Singh and K. Patel, **"**Secure Communication Platforms for Defence: An Assessment of Indigenous Alternatives**"**, *Cyber Security Review*, Vol. 8, No. 1, 2024, pp. 45–67.

of executing real-time threat analytics and autonomous decision-support must be developed when disconnected from central networks.

***Interoperability and Unified Standards***

A joint digital battlespace requires unified protocols, encryption suites and access control mechanisms across all services. A Defence Digital Interoperability Protocol (DDIP) standardising data formats, APIs and encryption algorithms is required. Integrated Command Dashboards to fuse sensor feeds and ISR data from all services into a single operating picture need to be developed. A unified Identity and Access Management (IAM) framework must be adopted for seamless cross-service collaboration under future Theatre Commands.

***Engineered Resilience***

Geographically distributed, tri-service data centres must be built to provide redundancy and load balancing during crises. Hybrid deployment models must also be deployed that combine on-premise military clouds with portable tactical clouds for deployed formations.

***Secure Communication Platforms***

Deploy a Tri-Service Secure Communication Suite (e.g., Sangraha 2.0) as the standard messaging, conferencing and collaboration tool. Enforce quantum-ready end-to-end encryption and multi-factor authentication for all command communication channels. Replace all foreign-hosted applications with MoD-managed platforms running within classified networks.

***Strong Policy, Funding and Governance Mechanisms***

A Defence Cloud Authority (DCA) under IDS must be created to manage architecture evolution, certification and oversight. A dedicated capital allocation within the Defence Budget for Digital Sovereignty and Cloud Infrastructure Development needs to be given. Quarterly Security Evaluation Boards with DRDO, NTRO and CERT-In must be instituted to ensure compliance and threat adaptability.

***Strategic Human Capital Development***

A Tri-Service Cyber and Cloud Warfare Academy under MILIT (Pune) needs to be established to train officers and technical personnel in AI, cloud and quantum systems. Defence Digital Fellowship Programmes with IITs/IISc and select private R&D institutions need to be initiated. A Digital Warfare Specialist (DWS) cadre must be built and embedded within operational commands for field-level integration.

***Future Battlespace Design***

Quantum-resistant encryption and zero-trust security architectures must be integrated across all cloud layers. AI-enabled autonomous defence modules must be deployed for predictive threat detection and self-healing network defence. A multi-domain cloud environment integrating space, cyber and electromagnetic domain data into a unified operational picture for real-time command advantage needs to be developed.

## Conclusion: The Mandate for Strategic Autonomy

India’s military effectiveness in future conflicts will be determined as much by its kinetic strength as by its resilience in cyberspace and the integrity of its digital command architecture. Therefore, creating a homegrown Armed Forces Cloud has emerged as a strategic necessity—crucial for protecting national security, enhancing operational readiness and preserving technological independence.

Existing projects like MeghRaj, the DRDO–RailTel Defence Cloud and indigenous communication tools like SAI/Arattai represent significant groundwork. Yet, these elements must mature into an integrated, scalable and resilient structure supporting a unified digital defence ecosystem. Realising this objective demands clear policy guidance, consistent financial support and coordinated collaboration between defence organisations, industry partners and academic bodies.

A self-reliant Armed Forces Cloud will safeguard India’s military communication systems while strengthening strategic independence by keeping command and control entirely under national authority. Establishing a unified, secure digital backbone will enable faster decision-making, protect vital information and empower India to exercise full autonomy across physical and digital battlefields.

## About the Author

**Cdr. Cdr Mohit Walia** is with the Naval War College, Goa

**Manohar Parrikar Institute for Defence Studies and Analyses** is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.



Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses