



CENJOWS

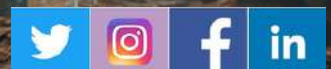
WEB ARTICLE
WA/24/26

BEYOND TACTICS: RECASTING LEADERSHIP AND TECHNOLOGY INTEGRATION IN THE INDIAN ARMED FORCES

LT GEN MU NAIR (RETD)



www.cenjows.in



CENTRE FOR JOINT WARFARE STUDIES



CENJOWS

Beyond Tactics: Recasting Leadership and Technology Integration in the Indian Armed Forces



Lt Gen MU Nair, PVSM, AVSM, SM (Retd) is a former Signal Officer-in-Chief of the Indian Army

Abstract

Operation Sindoor (May 2025) validated a shift long anticipated in military thought. Advantage accrues not to the force with superior numbers, but to the force best able to integrate and govern complex technological systems across domains. Warfare has transitioned from platform centric operations to fully networked, multi domain conflicts.

This article argues that the Indian Armed Forces must undertake a structural recalibration of leadership pathways, by developing technologically enabled decision makers and operationally grounded technologists, to effectively negotiate future conflicts. As the Indian Army designates 2026 as the Year of Networking and Data Centricity, the imperative is not to replace traditional strengths, but to expand leadership to match the demands of the system driven warfare of the future.

Introduction

Military institutions evolve through operational experience. Tactical proficiency, command acumen, and operational art are all shaped by battlefield realities.

Technology, however, evolves differently. Through long gestation cycles, sustained intellectual investment, and institutional continuity.

Operation Sindoor crystallised this divergence. Precision drone strikes, loitering munitions, indigenous air defence systems, electronic warfare dominance, and space based ISR integration operated in concert, to determine outcomes in compressed timeframes. These were not enablers. They constituted the architecture of combat power.

At the same time, the operation revealed structural challenges, especially in joint integration, cognitive decision alignment, and the translation of tactical innovation into command level outcomes.¹ These are not shortcomings of leadership quality, but indicators of institutional frameworks, yet to fully adapt.

The contemporary battlespace spanning land, air, sea, cyber, space, and the electromagnetic spectrum has created a convergence where tactical effectiveness is inseparable from technological integration. The Indian Armed Forces must therefore transition from manoeuvre centric paradigms to systems-oriented command structures, without diluting the primacy of combat leadership.

From Platforms to Systems Orchestrated Warfare

Traditional platforms integrate combat capabilities within discrete systems. Modern warfare extends beyond platforms into interconnected networks operating across domains.

Operation Sindoor demonstrated this transition through integrated use of UAVs for surveillance and strike, electronic warfare shaping air defence outcomes, space based ISR supporting real time operations, counter UAS systems operating at scale, networked decision-making reducing dependence on hierarchical control. Technology did not support operations. It actually enabled and defined them.

This aligns with the recent global conflict trends where unmanned systems dominate tactical engagements across continents, spectrum denial directly impacts on field operations, space-based assets provide operational awareness and cyber effects increasingly shape battlefield conditions. Networks are the key enablers connecting every aspect of military operations.

The designation of 2026 as the Year of Networking and Data Centricity, reflects institutional recognition that networks not platforms, are now the backbone of combat power.²

The Structural Leadership Challenge

The central issue is not leadership quality, but structural exposure to technology domains. Existing leadership pathways are optimised for command under physical uncertainty, tactical and operational decision making and progressive field experience. Emphasis on growth of leadership to higher echelons, are primarily focussed on combat edge.

However, contemporary responsibilities increasingly include capability development and acquisitions to integrate combat power with technology prowess even at tactical levels, systems integration and lifecycle management specially of complex technology intensive platforms and doctrine formulation in emerging domains. These require familiarity with networked systems and data architectures, electromagnetic spectrum operations, cyber resilience frameworks, space-based dependencies, AI capabilities and limitations. In their absence, weapon systems do not fully deliver their capabilities, capability alignment weakens, integration across domains become fragmented and procurement cycles extended. The distinction between operational and technological domains can no longer justify limited engagement with technology.

India's procurement experience, including ongoing reviews of acquisition processes, reflects these structural frictions. The issue is not individual competence. It is institutional design lagging operational reality.

Culture, Hierarchy, and Technological Absorption

Military culture, rightly prioritises combat leadership. However, modern conflict is inherently multi domain.³ When cyber, space, and spectrum are treated as supporting functions, technology adoption is delayed, integration remains fragmented and operational effectiveness is reduced

India's strategic environment, marked by a two front challenge and adversary, emphasising on technology driven warfare, intensifies this requirement. The need is

not cultural replacement, but cultural expansion, where technological awareness becomes integral to leadership.

Bridging the Operational -Technologist Divide

A persistent divide exists where operationalists understand battlefield dynamics and uncertainty while the technologists understand systems, design, and constraints. When unintegrated, requirements are oversimplified or just not comprehended, constraints are underestimated and outcomes diverge from operational needs.

India has initiated corrective steps through Tri Service structures and specialised courses. However, true integration remains a major challenge. Both within the Services, and between the Services. The challenge is to institutionalise continuous interaction across the career pipeline, rather than rely on isolated initiatives which collapse after certain period of time.

Role of Centralised Capability Building Organisations.

Technological awareness must evolve into a structured institutional capability for providing capabilities to users. This cannot be done by a user projecting a requirement, and a different organisation steering its procurement. Users need to drive technology driven capabilities through dedicated Project management Organisations, with fast-track procurement channels adopted. Technology intensive systems cannot be driven by Procurement directorates following long cycles of procurement. Responsibility has to be with user Directorates to steer projects in a time bound manner, and take deviations, if necessary, to get the system and the capability on priority. They could also include monitoring emerging and dual use technologies, understanding supply chain dependencies, tracking AI and quantum developments, assessing evolution of EW and space systems and most importantly, encouraging indigenous capabilities. Operation Sindoor, in fact, highlighted the growing role of the private sector and innovation ecosystems. Embedding procurement of niche technology systems with users enables anticipatory capability development, risk informed procurement besides alignment of technology with operational needs. The success of many of the Network and Electronic Warfare capabilities of yester years, hold testimony to this argument.

Emerging Technologies and Command Responsibility

Future operations will involve multiple challenges with distributed sensor networks, real time, multi domain data flows, contested spectrum environments and AI assisted decision making.⁴ Commanders will not need technical specialisation, but technological cognition. They need to take note of system dependencies, interpreting risks and limitations and making informed decisions under complexity both during operations and during routine peacetime. And therefore, leadership must evolve from platform command to capability to carry out systems orchestration.

Recalibrating Leadership Pathways

The reforms required are not abstract. They emerge directly from the structural gaps identified.

Aligning Decision Authority with Technological Competence

As capability development and procurement become increasingly technology intensive, decision making authority must reflect domain understanding. Appointments in critical technology domains should prioritise officers with demonstrated technological engagement and experience, ensuring that decisions are informed by both operational and technical realities.

Programme Centric Capability Management

The complexity of modern acquisition programmes requires a shift from centralised, generalist driven procurement structures to programme-oriented user driven management models. Capability development should be anchored in user led structures with integrated technical, operational, and production expertise thereby ensuring alignment between requirement, development, and deployment. As also lifecycle management of critical systems.

Embedding Technology in Professional Military Education

The analysis above highlights that exposure gaps originate early in career pathways. Professional military education institutions must therefore transition from technology awareness to technology enabled application, incorporating real world operational scenarios involving AI, networks, and multi-domain integration.

Institutionalising Operationalist - Technologist Integration

Given the persistent divide identified earlier, structured mechanisms, cross postings, joint design teams, and embedded expertise, must be institutionalised across career stages, ensuring continuous interaction rather than intermittent collaboration.

Strengthening Technology Oriented War Fighting Mechanisms

Technological surprise increasingly originates outside traditional defence systems. Dedicated technology structures must be embedded within the institutional framework to support horizon scanning, red teaming, and long-term capability planning.

Enhancing Accountability in the Capability Ecosystem

The analysis of procurement and development challenges indicates that delays and misalignments impose operational risk. Strengthening accountability mechanisms across the development and production ecosystem within Ministry of Defence is therefore essential to ensure timely and effective capability delivery. Such analysis needs to be carried out periodically, with the users, and not the decision makers as is happening today, being involved in such exercises.

The Indian Strategic Context

India's strategic environment amplifies these requirements:

- Two front operational scenarios
- Rapid technological advancements among adversaries
- Expanding maritime and sea patrolling commitments
- Imperatives of Aatmanirbharta

Operation Sindoor demonstrated that India possesses foundational technological capability. The challenge now lies in aligning institutional structures and leadership pathways to fully exploit it.

Conclusion

The Indian Armed Forces have consistently adapted across eras of warfare. The current transition, however, is distinct in scale and velocity. Technology is no longer an enabler. It is integral to combat power.

The requirement is not for technocratic militaries, but for technologically informed leadership and operationally grounded technological expertise

Future advantage will accrue to forces that can integrate systems, anticipate technological change and align leadership with capability.

CENJOWS, as a joint warfare think tank, is uniquely positioned to shape this transformation through research, dialogue, and professional engagement.

DISCLAIMER

The paper is the author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS, the Defence forces, or the Government of India. The author certifies that the article is original in content, unpublished, and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

ENDNOTES

¹ Headquarters Integrated Defence Staff. Joint Doctrine Indian Armed Forces (JDIAF-2017). New Delhi: HQ IDS, 2017.

² Indian Army Year of Technology Absorption (2024) and Year of Networking and Data Centricity (2026) official communications and speeches.

³NATO Publications on Multi-Domain Operations and Digital Transformation.

⁴ RAND Corporation Studies on Multi-Domain Operations, AI-enabled warfare, and decision superiority.