India's Joint Doctrine for Multi-Domain Operations: A Whole-of-Nation Framework

Introduction

India's Joint Doctrine for Multi-Domain Operations[1] (MDO) was released by the *Raksha Mantri* Rajnath Singh on 27 Aug 2025 at the tri-Service seminar, '*Ran Samwad* 2025', held at the Army War College in Mhow. The publication was part of a larger release of three joint doctrine documents, including special forces operations and airborne and heliborne operations.

The doctrine represents India's move towards a whole-of-nation approach to warfare, integrating various domains including cognitive domain to counter hybrid and grey-zone threats. Rooted in Chanakya's holistic stratagems, the doctrine stresses synergy, decentralised mission command, simultaneity of actions and decision superiority through Artificial Intelligence (AI), unmanned systems, and space-based assets. It defines physical, virtual, and social environments, underscores the role of specialised defence agencies, and calls for capability audits and a common lexicon for civil–military integration.

Relevance and Structure

Modern Warfare Challenges. Modern warfare is no longer limited to massed troops but is executed by precision munitions, drones, and information dominance, employing kinetic strikes to ravage destruction without crossing borders and engaging cognitive warfare through propaganda and disinformation to shape outcomes decisively. For India, the challenge is compounded by the prospect of multi-front conflicts, with collusion between China and Pakistan and instability in the east, necessitating readiness for simultaneous operations. The revolution in military affairs underscores the urgency of self-reliance in dual-use technologies, drawing on start-ups, academia, and industry to master cyber, space and cognitive domains alongside conventional arms.

Lessons from Operation Sindoor. Operation Sindoor marked a watershed in India's military evolution, accentuating the fusion of technology with warfare and the inevitability of multi-domain hybrid conflicts. Lessons from the operation underline the need to institutionalise an armed forces–academia–industry innovation ecosystem, harness dual-use technologies through start-ups, strengthen cognitive warfare capabilities and refine doctrines through joint exercises, all while leveraging India's economic scale and technological base to secure defence self-reliance.

Essence of Joint MDO Doctrine. The Joint MDO Doctrine draws directly on these lessons. It stresses that modern conflict is multi-domain, simultaneous, and technology-driven, as evident in Ukraine, Gaza, and India-Pakistan exchanges. It emphasises the domineering need of indigenous innovation in AI, robotics, hypersonics and space systems to offset rapid obsolescence and reduce import

dependence. Most critically, it calls for a Whole-of-Nation Approach (WONA) by integrating armed forces with academia, industry, and media. It stresses that wars are fought not by armies alone but by nations, demanding doctrinal evolution, joint-force integration.

Whole-of-Nation Approach. The doctrine is a timely response to India's complex and evolving security environment shaped by unpredictable neighbours, grey-zone operations, non-state actors and increasing global competition. Recognising the limitations of traditional three-domain warfare exposed by ongoing conflicts worldwide, the doctrine advances a WONA that integrates traditional domains of land, sea, and air with the newer arenas of space, cyber and cognitive warfare. It emphasises cross-domain integration, real-time convergence of effects, decentralised mission command, simultaneity of actions and information dominance, supported by advanced technologies such as AI, unmanned systems, big data analytics, satellite-based Intelligence, Surveillance, and Reconnaissance (ISR), secure communications, and cyber resilience. The doctrine also institutionalises the role of agencies like the Defence Cyber Agency, Defence Space Agency, Defence Intelligence Agency, and the upcoming Defence Communication Agency.

Doctrine Structure and Focus. Structured across five core chapters, the doctrine covers the security environment and hybrid threats, defines domains and distinctions from joint operations, outlines key characteristics and prerequisites, reviews current and future tri-service structures and prescribes the way ahead through capability audits, mindset shifts, multi-domain wargaming, a dedicated Multi-Domain Operations Room (MDOR), common lexicon development and nationally synchronised cognitive operations. It is supported by annexures on terminology and references. The doctrine also marks a shift from platform-centric to network-centric warfare, combining military and non-military power for strategic advantage. It stresses whole-of-nation synergy, technological self-reliance, and decision superiority as India prepares for future multi-domain conflicts. The major aspects covered in the doctrine are in succeeding paragraphs.

Security Environment and Rationale. India faces complex, hybrid threats from unpredictable neighbours, non-state actors, and global power competition. Traditional three-domain warfare (land, sea, air) is no longer sufficient; space, cyber and cognitive domains are now critical. Hybrid threats (disinformation, cyberattacks, economic coercion, psychological operations) blur the line between peace and war.

Definition and Scope. MDO is coordinated, integrated, synchronised use of military and non-military capabilities across six domains, viz., land, sea, air, cyber, space and cognitive. MDO differs from joint operations as it integrates non-military entities (govt, private, space, cyber agencies), not just services. Employs a WONA to create multiple dilemmas for adversaries.

Key Characteristics. These are as under:

- Cross-domain integration for a common situational picture.
- Collaboration with public/private sector for AI, cyber, ISR, logistics.
- Non-linear and distributed operations, enabling strategic depth and surprise.
- Simultaneity of actions across domains to overwhelm adversaries.
- Convergence of effects (kinetic and non-kinetic).
- Data and network centrality, AI-driven decision superiority.
- Mission command with decentralised initiative.
- Agility and adaptability to counter hybrid threats.

Prerequisites. It highlights certain prerequisites as follows:

- **Technological**. AI-enabled planning, satellite communications, cryptography, common all domain operational picture, secure wireless networks, decision-support tools, information operations systems.
- **Policy and Infrastructure**. MDOR, cyber and space resilience, trained human resources with MDO mindset, common MDO lexicon, national-level cognitive operations strategy.
- **Structures**. The present and future Structures discussed are as follows:
  - **Present**. The army, navy, and air force, along with tri-service organisations such as the Defence Cyber Agency, Defence Space Agency, Defence Intelligence Agency, and the forthcoming Defence Communication Agency.
  - **Future**. Stronger integration, real-time decision loops across Services and civil agencies, MDOR and CADOP as nodal centres, emphasis on cognitive domain dominance.

Way Ahead. The doctrine emphasises the way ahead to include:

- Capability audits to identify gaps.
- Promote an MDO mindset beyond single-service thinking.
- Invest in training, wargaming and all-agency exercises.
- Build resilient indigenous tech ecosystems for AI, cyber, space, ISR.
- Develop a national cognitive operations framework to secure narrative dominance.

Analysis and Comments

MDO Doctrine: Vision vs. Implementation. The MDO doctrine is innovative and progressive, offering India a robust framework for future warfare through cross-domain integration and whole-of-nation synergy. However, its efficacy will depend on bridging the gap between vision and implementation and ensuring resources, training and

structural reforms keep pace. While doing so, it is also essential to avoid over-reliance on technology and address gaps in escalation management.

Strengths. These are as under:

- **Comprehensive Vision**. The doctrine captures the complexity of modern warfare and stresses the importance of cross-domain synergy.
- **Technology Integration**. Forward-looking in adopting AI, robotics, and unmanned systems.
- **Jointness and Adaptability**. Correctly highlights the need for flexible structures and interoperability.
- **Information-centric Warfare**. Recognises that future conflicts would hinge on data, perception, and narrative dominance.

Limitations. They are as follows:

- **Implementation Gap**. While conceptually sound, translating MDO into practice will require massive investments in technology, training, and inter-service coordination.
- **Overemphasis on Technology**. Risks underplaying human factors like leadership, morale, and decision-making under uncertainty.
- **Alliance Dependence**. Undue reliance on international cooperation may clash with strategic autonomy in certain scenarios.
- **Ambiguity in Grey-zone Response**. The doctrine outlines threats but does not provide concrete mechanisms for calibrated escalation control.

Implications for Defence Modernisation and Theorisation.

- **Operational Integration**. MDO doctrine sets the conceptual foundation for theatre commands, ensuring cross-domain synergy and jointness across land, sea, air, space, cyber and cognitive arenas. It provides doctrinal backing to tri-service integration, breaking single-service silos.
- **Technology Roadmap**. Anchors India's AI, unmanned systems, big data, and space based ISR investments. It guides military innovation missions under Defence Research and Development Organisation, Indian Space Research Organisation, Innovations for Defence Excellence, and private-sector defence start-ups.
- **Strategic Autonomy and Partnerships**. Reinforces India's need for indigenous capabilities in cyber and space, while also enabling interoperability with partners in Quadrilateral Security Dialogue, India, Israel, United States, United Arab Emirates (a strategic partnership initiative focused on economic cooperation, technology, food security, energy, and infrastructure), and other coalitions.

- **Cognitive and Grey-Zone Preparedness**. Explicit focus on information dominance and psychological operations addresses challenges seen in Ukraine, Gaza, and Indo-Pacific tensions. Elevates narrative warfare to the same level as kinetic operations.

- **Whole-of-Nation Security Architecture**. Brings in civilian stakeholders (tech sector, media, academia) under a common lexicon and MDOR. Marks a shift from purely military jointness to civil-military fusion in security.

Comparison with United States and China

Global Comparisons in MDO. When compared with global powers, some distinctive features emerge:

- The United States has its Joint All-Domain Operations and Joint All-Domain Command and Control, which underscore sensor-to-shooter integration and global power projection. The US model is technologically advanced, designed to maintain military supremacy worldwide.

- China's People's Liberation Army (PLA) emphasises Intelligentised Warfare, with particular focus on the cognitive and information domains. The PLA's Strategic Support Force integrates cyber, space, electronic and psychological warfare, seeking to paralyse adversary decision-making without necessarily firing a shot.

- India's approach is distinct in its emphasis on a Whole-of-Nation model and a truth-based narrative rooted in *Satyameva Jayate* (Truth alone triumphs). Unlike the US's global orientation or China's offensive psychological dominance, India focuses on regional security challenges—the two-front threat from China and Pakistan, hybrid warfare, and internal security vulnerabilities.

Implementation Challenges Ahead. The challenge for India lies in implementation with direct implications on aligning bureaucratic structures, investing in indigenous technology, and fostering inter-agency synergy. If executed well, MDO can give India an edge not only against hybrid threats but also in deterring high-intensity conflicts with technologically advanced adversaries.

Conclusion

The doctrine is progressive and lays down the essential framework for 21st Century warfare. Its success will, however, depend on overcoming institutional inertia, resource constraints, and the challenge of real-time integration across diverse domains. The doctrine considers lessons from current conflicts and seeks to integrate land, sea, air, space, cyber and cognitive domains into a single, synergised framework to ensure decision superiority and resilience in modern wars. It is a milestone step in India's military thought, aligning with global trends and preparing the nation for 21st Century conflict. Its success will depend on institutional reforms, capacity-building, inter-agency collaboration, and political will to translate vision into practice.

[1] Headquarters Integrated Defence Staff, "Joint Doctrine for Multi Domain Operations", *Integrated Defence Staff, Ministry of Defence, Government of India*, Aug 2025, accessed 10 Sep 2025, https://ids.nic.in/WriteReadData/Document/2/13/MDO%20Doctrine.pdf](https://ids.nic.in/WriteReadData/Document/2/13/MDO%20Doctrine.pdf

Brigadier PP Singh, AVSM, VSM (Retd.) is an Indian Army veteran with three and a half decades of distinguished service. He has held key command roles in counterinsurgency and border operations and has been a faculty member in various Category A Institutions of Indian Army. Post-retirement, he is a Senior Research Fellow at the United Service Institution of India and actively contributes to defence analysis and strategic affairs discourse.

Article uploaded on 12-09-2025