

From Land to Cyberspace: The Rise of Multi-Domain Warfare in the 21st Century

By Vanshika Sirohi

Modern warfare tactics like Multi-Domain Warfare (MDW) are increasingly becoming the norm in today's conflicts. In this form of war, all domains (air, land, maritime, space, and cyberspace) become part of a unified whole that operates in concert. The goal is not to undertake separate actions but rather to launch a coordinated assault. This trend can largely be attributed to the technological revolution. Gone are the days when wars were fought solely through conventional platforms like tanks, battleships, and fighters. Now, warfare can occur on different fronts, including cyberwarfare and electronic warfare. It is through the incorporation of these methods that MDW achieves an overwhelming advantage over the opponent.

Integration of Land, Air, Sea, Cyber and Space

Warfare in the 21st Century has witnessed a complete shift from the traditional notion of platform-based and domain-based warfare to what we know today as a fully integrated battlespace that includes land, air, sea, cyber, and space. Prior to the modern age of warfare, armies, navies, and air forces functioned independent of one another in their particular domains without much coordination. This was due to the fact that armed forces did not have the tools that allowed for synchronisation between different platforms. However, the advent of digital technology and communications enabled the emergence of MDW.¹

In essence, multi-domain integration can be described as the coordination of capabilities in all domains to accomplish strategic or operational objectives faster and with greater precision. Such coordination is facilitated through real-time information exchange, shared command centres, and networked systems, enabling military units to operate as a cohesive force rather than as separate service branches.²

Each domain has its own specific and interrelated functions within this structure. Land forces are used for holding and securing territory, but it depends increasingly on intelligence and surveillance information coming from the air and space. Air power offers quick mobility and precision strikes, along with intelligence, surveillance and reconnaissance capabilities that can utilise satellite and cyber-enabled data. Naval force helps ensure the control of maritime lines of communications and global reach through the extensive use of satellites and communication equipment. Cyber operations function as both offensive and defensive elements and can disrupt enemy communication channels, vital infrastructure, and command and control. Lastly, the space domain is the a critical enabler of contemporary military operations, enabling navigation through the global positioning system, satellite communication and ISR, without which the other domains cannot function effectively.³

Beyond navigation and communications, space capabilities enable missile warning, precision targeting and persistent ISR. However, increasing reliance on satellites has made space a contested domain vulnerable to anti-satellite weapons, cyber-attacks and electronic warfare.

Nevertheless, attaining this kind of synergy is no easy feat. Modern military organisations face several challenges in developing integrated multi-domain capabilities, including service competition, lack of interoperability, cybersecurity concerns, and the prohibitively high cost of implementing technological advancements.⁴ Notwithstanding this, the drive towards multi-domain integration will not cease; rather, appears increasingly irreversible.

Role of Artificial Intelligence and Data Fusion

The development of MDW is inherently based on the fast-paced growth of Artificial Intelligence (AI) and data fusion technology, which makes it possible to integrate information across different domains. In the increasingly data-intensive battlefield environment, which generates vast volumes of data from space-based assets, unmanned systems, sensors, and cyberspace sources, it is crucial to process, analyse, and act upon this information in real time. This is the key to gaining military supremacy in today's multidomain battlespace environment.⁵

AI is crucial to improving decision-making by accelerating data processing and pattern recognition, which would otherwise be difficult for human operators. AI-based technology helps process information received from various intelligence sources—ranging from satellite imagery to signals intelligence—and produces useful information for the command structure. As such, it reduces the time required for decision-making through the observe–orient–decide–act loop, thereby providing decision-makers with an advantage over their adversaries.⁶

Data fusion is another important component of multi-domain operations, wherein data from various sources is consolidated to create an operational scenario. It enables military units to merge information obtained from sensors on the ground, aerial reconnaissance systems, vessels at sea, cyber espionage, and even satellites orbiting in space to develop a comprehensive operational picture. Through data fusion, military operations can be better synchronised.⁷ For example, when a satellite detects an enemy position, cyber capabilities verify whether the site is active, while AI analyses the information and recommends the most effective course of action, enabling a precision strike by air or ground forces.

India's Doctrinal Evolution

India's traditional approach to warfare was characterised by service-specific doctrines and theatre-planning concepts. The Army, Navy, and Air Force have each operated independently under their respective doctrines. However, due to the evolving nature of warfare, which involves cyber warfare and space warfare alongside the increasing importance of real-time intelligence and precision capabilities, a paradigm shift has occurred towards a more integrated approach to warfare. Recent years have seen India move towards an updated military doctrine, incorporating aspects of MDW to prepare for future conflicts.⁸

One of the key factors driving the transformation of Indian military doctrine has been jointness between the three services. The creation of the post of Chief of Defence Staff (CDS) in 2019 was one of the important steps towards this objective. This helped establish the institutional foundation for multi-domain operations.⁹ Another related

development is the process of establishing integrated theatre commands, whereby the control of forces from all services will be centralised within a theatre command. Although the process of theatreisation is still incomplete, it underscores India's realisation that coherent action against security threats is essential.¹⁰

India has also taken significant steps to enhance its capabilities in emerging domains. The establishment of the Defence Cyber Agency, Defence Space Agency, and Armed Forces Special Operations Division shows that India is beginning to institutionalise its capabilities in cyber, space, and special operations, which are part of multi-domain warfare. This will help enhance India's offensive and defensive capabilities beyond the traditional domains, while improving coordination with conventional forces.¹¹

In terms of doctrine, Indian strategic thought appears to be increasingly adopting notions such as information warfare, network-centric warfare, and decision dominance. As has been pointed out by the Observer Research Foundation, the shift towards multidomain warfare in India can be attributed to the requirement to counter emerging challenges posed by technologically sophisticated adversaries.¹² Similarly, studies by the Institute for Defence Studies and Analyses suggest that wars of the future in which India may find itself involved will inevitably entail the employment of both conventional and non-conventional methods.¹³

India's transition towards MDW has been driven by China's military modernisation and the lessons of the 2020 Eastern Ladakh crisis, underscoring the need to integrate cyber, space, intelligence and conventional capabilities.

Challenges of Coordination and Interoperability

Although MDW offers unprecedented efficiencies and advantages, its effective application will depend on overcoming challenges related to coordination and interoperability. For one, the incorporation of different domains such as land, air, sea, cyber, and space requires technological compatibility and interoperability in doctrine, communications and operational procedures.¹⁴

One of the principal challenges is coordination among the various services. Historically, military institutions have always functioned in their own silos, which meant that they had distinct chains of command, doctrines and communication systems. For a multi-domain approach to be successfully implemented, a high degree of jointness is required, with decisions being made collectively and tasks accomplished through synchronisation. At the same time, institutional culture and rivalry among different branches could impede these processes, causing inefficiencies and delays.

Interoperability is another concept related to coordination; this term denotes the capacity of various systems, platforms, and forces to work effectively in combination. In the context of MDW, interoperability includes not only conventional forces but also cyber networks, space technologies, and artificial intelligence systems.

Additional challenges include protecting the electromagnetic spectrum, securing resilient communications, integrating logistics across multiple domains, defending against cyber-attacks and preparing for emerging technologies such as quantum computing and autonomous systems. Failure in any one domain has the potential to degrade the effectiveness of the entire operational network.

A further challenge lies in the volume and complexity of the data used in

multidomain operations. Although technological solutions like AI and data fusion are built to deal with such complex data, they they also create challenges such as data overload, system-integration problems and network-security vulnerabilities. Problems in cyberspace and space operations could affect other domains due to their interconnections.¹⁵

From an Indian point of view, organisational restructuring has further complicated these challenges. Although the process of theatreisation and joint command structures is essential, it needs to be done cautiously, and the coordination system must be flexible.¹⁶

Ultimately, technology alone cannot guarantee success in Multi-Domain Warfare. Effective leadership, realistic joint training, professional military education and an organisational culture that encourages innovation and inter-service cooperation remain indispensable for translating technological capabilities into operational success.

Conclusion

Multi-domain warfare has transformed warfare from a predominantly platform-centric approach into a dynamic, integrated and networked form of operations. The successful prosecution of war today depends on the integration of various capabilities across multiple warfighting domains using technologies like AI and data fusion.

Future conflicts are unlikely to be fought within the confines of a single domain. Instead, military success will increasingly depend upon the ability to generate and exploit cross-domain effects at a tempo faster than the adversary can comprehend or respond. Consequently, decision superiority and seamless integration across all domains are becoming the defining characteristics of modern warfare.

For India, multi-domain warfare presents both opportunities and challenges. Reforms such as the appointment of the CDS, enhanced jointness, and the creation of space and cyber capabilities represent important steps towards adapting to the changing character of warfare. Nevertheless, coordination, interoperability and technological readiness continue to pose significant challenges.

Ultimately, multi-domain warfare demands far more than technological superiority. Success depends on integrating advanced technologies with coherent doctrine, joint organisational structures and agile decision-making. For India, achieving effective multi-domain warfare will require sustained transformation across the technological, institutional and doctrinal domains.

Endnotes

¹“The U.S. Army in Multi-Domain Operations 2028” (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), accessed 04 Jul 2026, <https://www.ncoworldwide.army.mil/Portals/76/courses/mlc/ref/Multi-Domain-Operations.pdf>

² James Black, Kristian Gustafson, Alice Lynch, Davud Blagden, Pauline Paille, and Fiona Quimbre, “Multi-Domain Operations Project”, RAND Corporation, 24 Feb 2023, accessed 04 Jul 2026, https://www.rand.org/pubs/research_reports/RR528-1.html

³Andrea Gilli, Mauro Gilli, and Gorana Grgić, “NATO, Multi-Domain Operations and the Future of the Atlantic Alliance,” *Comparative Strategy* 44, no. 1 (2025): 73–91, accessed 04 Jul 2026, <https://doi.org/10.1080/01495933.2024.2445491>

-
- ⁴Centre for Joint Warfare Studies (CENJOWS), “Tri-Service Synergy for Future Conflicts”, *Synergy*, Vol. 4, Issue 2 (Aug 2025), accessed 04 Jul 2026, <https://cenjows.in/wp-content/uploads/2026/01/August-2025-Synergy.pdf>
- ⁵ RAND Corporation, “Artificial Intelligence and National Security”, accessed 04 Jul 2026, <https://www.rand.org/pubs/perspectives/PEA4079-1.html>
- ⁶ U.S. Department of Defense, “Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity”, 12 Feb 2019, accessed 04 Jul 2026, <https://media.defense.gov/2019/feb/12/2002088963/-1/-1/1/summary-of-dod-ai-strategy.pdf>
- ⁷ Andrea Gilli, Mauro Gilli, and Gorana Grgić, “NATO, Multi-Domain Operations and the Future of the Atlantic Alliance”, *Survival* 67, no. 1 (2025): 73–91, accessed 04 Jul 2026, <https://www.tandfonline.com/doi/full/10.1080/01495933.2024.2445491>
- ⁸ Centre for Joint Warfare Studies (CENJOWS), “Tri-Service Synergy for Future Conflicts: Policy Insights and Strategic Adaptations”, *Synergy*, Vol. 4, Issue 2 (Aug 2025), accessed 04 Jul 2026, <https://cenjows.in/wp-content/uploads/2026/01/August-2025-Synergy.pdf>
- ⁹ The Indian Express, “PM Narendra Modi Announces Creation of Chief of Defence Staff (CDS)”, 15 Aug 2019, accessed 04 Jul 2026, <https://indianexpress.com/article/india/narendra-modi-independence-day-chief-of-defence-staff-cds-5906922/>
- ¹⁰ ResearchGate, “Theatre Commands: The Indian Perspective”, accessed 05 Jul 2026, https://www.researchgate.net/publication/364360459_Theatre_Commands_The_Indian_Perspective
- ¹¹ Observer Research Foundation, “Bring the Defence Ministry into the Space Commission”, 31 Dec 2024, accessed 05 Jul 2026, <https://www.orfonline.org/expert-speak/bring-the-defence-ministry-into-the-space-commission>
- ¹² Centre for Land Warfare Studies (CLAWS), “Multi-Domain Warfare: How India Fits into the World’s New Power Equation”, 02 Dec 2025, accessed 05 Jul 2026, <https://claws.co.in/multi-domain-warfare-how-india-fits-into-the-worlds-new-power-equation/>
- ¹³ Akshat Upadhyay, “Fighting Future Wars: Preparing India for Conflicts in the 21st Century”, *ORF Issue Brief* No. 525 (Mar 2022), Observer Research Foundation, accessed 06 Jul 2026, <https://www.orfonline.org/research/fighting-future-wars-preparing-india-for-conflicts-in-the-21st-century>
- ¹⁴ Andrea Gilli, Mauro Gilli, and Gorana Grgić, “NATO, Multi-Domain Operations and the Future of the Atlantic Alliance”, *ibid.*
- ¹⁵ World Economic Forum, “Global Cybersecurity Outlook 2026”, 12 Jan 2026, accessed 04 Jul 2026, <https://www.weforum.org/publications/global-cybersecurity-outlook-2026/>
- ¹⁶ Waqas Khan, “Indian Military Transition Towards Theaterisation,” *AWCI Journal* 31 (2023), published 02 Oct 2024, accessed 04 Jul 2026, https://www.researchgate.net/publication/384545238_Indian_Military_Transition_Towards_Theaterisation_by_Waqas_Khan

About the Author

Vanshika Sirohi is Programme Coordinator at the Jindal India Institute, O.P. Jindal Global University. She holds a Master’s degree in Diplomacy, Law and Business from the Jindal School of International Affairs, with a specialisation in Defence and National Security. She also holds a Bachelor’s degree in Political Science (Honours) from Kirori

Mal College, University of Delhi. Her academic and professional interests include defence, national security and strategic affairs.

Article uploaded on 11-08-2026

Disclaimer: The views expressed are those of the author and do not necessarily represent the views of the organisation that he/she belongs to or of the USI of India.