# Multi-Domain Warfare: Are we Geared for it?

**Lieutenant General Dushyant Singh, PVSM, AVSM (Retd)[@]**

### Abstract

*In the face of evolving geopolitical threats, particularly from neighbouring nuclear states like China and Pakistan, India finds itself entangled in multifaceted warfare encompassing various domains beyond the traditional land, sea, and air. The emergence of digital technology has further expanded the battlefield to include space, cyber, and information domains, demanding a paradigm shift in military strategy. This article explores the concept of multi-domain operations as a comprehensive approach to address these complex security challenges.*

## Introduction

Compared to the past, revolutionary changes have transformed the landscape of warfare, driven primarily by a technological tsunami. Game-changing inventions and developments in military technology, from dynamite, telecommunication, tanks, and aircraft to nuclear weapons and space-based systems, have now culminated in a digital technology revolution. While the pace of technological changes was moderate in the past, the advent of digital technology has unleashed a storm in warfighting. Warfare is no longer confined to single dimensions such as land, sea, and air; it has expanded to include dimensions like space, cyber, robotics, and the human mind space, characterised by influence operations aimed at breaking the morale of the adversary's warfighting human capital many a times without engaging in direct

[@]**Lieutenant General Dushyant Singh, PVSM, AVSM (Retd),** is a distinguished military leader with extensive experience in various operational theatres. He held key positions, including commanding an infantry unit, brigade, and division, and served twice in the elite National Security Guards. The General is also a respected author and strategic analyst, contributing to defence journals and publishing notable works like 'Grey Zone Warfare: Way Ahead for India'. Recognised with prestigious awards such as the 'Ati Vishisht Seva Medal' and 'Param Vishisht Seva Medal,' he continues to make significant contributions to national security discourse as a prominent figure publishing in Journals think tanks and academic institutions. Presently he is the Director General of the Centre for Land Warfare Studies, a think tank under the aegis of the Indian Army.

*Journal of the United Service Institution of India*, Vol. CLIV, No. 635, January-March 2024.

conflict. India is constantly subjected to all these forms of warfare by its adversaries.

The major national security threats against India primarily emanate from its two neighbours, China and Pakistan. In addition to this, the country is targeted through Information Warfare (IW), covert operations, economic warfare, and diplomatic manoeuvrings by countries or non-state actors and agencies that do not wish to see it emerge as a major power. Furthermore, there are elements within the country that receive support from external agencies and the deep states of other countries. They use tactics such as IW, terrorism, protests, and unrest to create internal security threats, aiming to weaken the social fabric, morale of the people and security personnel, and influence regime changes. Several international powers, both state and non-state actors, aspire to keep India weak and dependent on them for survival. These realities necessitate a response employing a 'Whole of Nation Approach'. However, this also underscores the need for an effective Multi-Domain Operations (MDO) strategy to defend India against this form of warfare employing its defence forces and employing hard and soft power using the Whole of Nation Approach. Multi domain operations are no more the preserve of only the defence forces.

## Understanding MDO

The traditional domains of warfare have been land, sea, and air. Over a period, cyber and space have emerged as two other domains of warfare. To counter Multi Domain Warfare (MDW) there is a need to undertake MDO. It refers to a military concept that aims to integrate operations across multiple domains, including land, air, sea, space, and cyberspace.[1] The aim of MDO is to achieve results in the most cost-effective manner by leveraging the advantages of each domain to gain a decisive victory over the adversary. MDO aims to combine the capabilities across all domains and employ them ideally in an integrated manner to achieve the desired effects as far as the military domain is concerned. As far as adversarial action in the economic, information and diplomatic spheres is concerned, a Whole of Nation Approach is desirable. Figure 1 highlights this aspect quite vividly. "It is in this realm that the three services will have to evolve the multi-domain concept i.e., by first understanding how space and cyber domains will contribute to war fighting and then identifying the doctrine and capability required for their integration. Thereafter, redefine concepts of operations, command and control approaches, organisational structures, force structures and support structures. Once identified, an institutional process would be required to put it all together and define the required reforms or changes/ adjustments".[2]

An important precondition that is needed for an MDO to become effective is the establishment of a sound network that extends across all five domains including the three services to achieve a high degree of integration to ensure building up of a common operational picture to effectively engage the adversary through a combination of systems and elements that may be from different domains including the cyber and space beside the land, sea, and air. Therefore, the aim of any MDO would be to shorten the Observe, Orientate, Decide, Act loop.[3] A major challenge that is associated with integrating the cyber and space domain is that, it will face a similar challenge in that the three services are likely to create their own dedicated space and cyber resources whereas a more prudent thing would be to create separate cyber and space services which then provides the necessary cyber and space support to the three services. This is a similar problem to that of Air Power resources being shared by the other two services.[4] These complexities notwithstanding will have to be laid down in workable policies, structures, and communication networks to fight as a joint team.

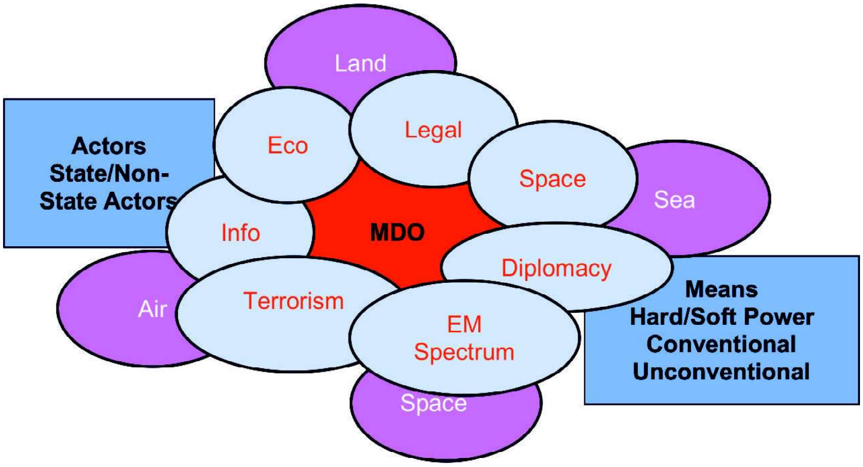

**Figure 1: The Overview of Multi Domain Warfare in Current Context. Source IMR in Article of Maj Gen GD Bakshi, SM, VSM (Retd)**

## Geopolitical Landscape

India shares borders with multiple countries, each presenting unique challenges. Two of India's neighbours are recognised nuclear states with significant military capabilities. According to the 2024 Global Fire Power Index, China ranks as the third most powerful military globally, and Pakistan holds the ninth position.[5] In a collusive threat eventuality, India will have to pull out all its punches to meet the challenge. In such an asymmetrical situation, MDO may be able to offset the disadvantages. Beyond conventional military threats, these adversaries also attack national infrastructure including military assets, infrastructure and warfighting resources through cyber-attacks. Our adversaries are also using IW, proxy warfare by employing terrorists in peace time which is likely to extend into war time as well given our past experiences and ongoing conflicts in Ukraine and Gaza. Their activities extend to the covert domain, aiming to undermine our national unity, sovereignty, and social cohesion which need to be addressed at the national level, leaving the defence forces to tackle security challenges emanating from the five domains.

In addition to these two adversaries, neighbouring countries China consistently influences other neighbours of India like Nepal, Bhutan, Myanmar, Maldives, and Sri Lanka through various means such as diplomacy, interference in the elections, covert operations, and economic enticements. China consistently aims to undermine Indian influence in South Asia and to impose its own influence. Recent instances include China's efforts to influence the elections in Maldives, leading to the establishment of a pro-China government under Muizzu.[6] In Bangladesh, China displayed relative restraint, not overtly interfering in elections. Instead, it was the West, led by the United States, actively pressuring the Bangladesh government in the name of conducting free and fair elections to engineer a regime change. Despite these efforts, Sheikh Hasina returned to power, thwarting the objectives of China and Pakistan. Similar instances of achieving strategic goals through diplomacy and non-military means exist in Nepal, Bhutan, Sri Lanka, and Myanmar.

Notably, in Sri Lanka, China made significant inroads by first installing a pro-China government led by Rajapakse and subsequently acquiring Hambantota through the Belt and Road Initiative debt trap.[7] Addressing these multifaceted threats requires

India to adopt a multidomain approach, considering various dimensions and domains. MDW enables a comprehensive strategy to counter threats from different directions.

### Tri-service Integration

The Indian Armed Forces have traditionally operated in a tri-service manner with the Army, Navy, and Air Force. As discussed above, while coordinated efforts across these services are vital for effective multidomain operations, cyber and space domains are assuming a decisive edge in the outcome of battles. Therefore, we need to decide whether there is a need to raise independent commands for marshalling space and cyber resources which can then be allocated in an optimised manner to the three services as also to undertake operations on their own at a strategic level as part of Whole of Nation Approach. The People's Liberation Army Strategic Support Force (PLASSF) is an example of this model. The PLASSF is comprised of two divisions: The Space Systems Department, which is responsible for undertaking all space-related missions, and the Network Systems Department, which has the People's Liberation Army's IW activities, including cyber.[8] While India cannot ape the model, it can take the concept and create changes in the apex structure of the defence forces which could function under the Chief of Defence Staff (CDS).

### Integration of MDO Effort: Need for a PLASSF type Organisation.

Achieving integration among the five domains through a sound net centric effective communication architecture is necessary for an effective MDO. In addition, integration also involves enhancing interoperability and cooperation among the three services. This includes joint planning, joint training, and joint exercises to ensure seamless integration during multidomain operations. To achieve these integrated theatre command structures backed by human resources that have experience of operating in a joint environment is a pre-requisite. Accordingly, the three services must resort to cross postings amongst the three services by identifying suitable billets besides those held in existing tri-service organisations such as the Andaman and Nicobar Command and the Strategic Forces Command. In addition, there is a need to gradually shift to integrated theatre command architecture to conduct an MDO.

Investments in advanced technologies, such as space-based capabilities, cyber warfare, and unmanned systems, are crucial for gaining a competitive edge in multidomain operations. India has been working on developing indigenous technologies in these domains. While efforts at the national level are well appreciated, at the tri-service level too, there is an urgent need to create an overarching organisation that can take care of the lines of military operations in the various domains and dimensions related to cyber, space, intelligence, and information operations. This can be achieved by expanding the mandate of the existing Defence Intelligence Agency (DIA) under the CDS.[9] The organisation could be rechristened as National Military Strategic Support Operation Agency (NMSSO). Organisations such as the Defence Cyber Agency (DCA), Space Vertical and the IW Vertical including the organisation of the three services dealing with public relations could be assimilated under it to suit the Indian defence requirement in this field. Similarly, the Defence Space Agency (DSA) could also be placed under this proposed organisation. Some of the critical issues are discussed below. These are discussed very briefly below:

- **Cybersecurity.** As cyberspace becomes increasingly important in modern warfare, India needs to focus on robust cybersecurity measures. Protecting critical infrastructure and ensuring the security of communication networks are integral components of multidomain warfare. The proposed organisation should assimilate the existing DCA working under the Headquarters Integrated Defence Staff. The proposed organisation needs to coordinate its efforts with various national level agencies responsible for cyber security through the National Cyber Security Advisor and Deputy National Security Advisor who are responsible for coordinating such efforts, so that the proposed Strategic Support Force efforts are not at variance with those undertaken by the military.

- **Space Domain.** Given the significance of space-based assets for communication, navigation, and surveillance, India has been working on enhancing its space capabilities. Developing counterspace capabilities and securing space-based assets are vital components of multidomain warfare. As discussed above the existing DSA can be merged under the NMSSO.[10] Besides this must beside look at the internal requirements of the defence forces who could undertake operations through the concerned Deputy National Security Advisor/Military Advisor in the National Security Council and the Director General of the Indian Space Agency.

- **Diplomacy and IW.** IW plays a critical role in shaping perceptions and influencing decision-making. Integrating diplomatic efforts with IW is essential for managing international perceptions during conflicts. The proposed organisation above NMSSO with the existing DIA component already has the Military Diplomacy component. In addition, it could also include the IW vertical under it with the Additional Director General Stratcom (erstwhile Additional Directorate General of Public Information) equivalent of all the three services under it to minimise turbulence in the transformation.

### Human Capital Development

The success of MDW relies on well-trained and adaptable personnel. Continuous training and professional development are essential for military personnel to operate effectively in diverse and dynamic environments. Accordingly, as discussed earlier, joint billets in all three services will fill up all the vacancies in the existing tri-service organisations. Along with this gradual shift towards theaterisation, it will further enhance the effectiveness of the skill levels of the human resource besides making it easier to operate effectively in a multi domain operational environment.

### Other Operations Requiring MDO Response

**Counterinsurgency and Counterterrorism.** Internal security threats, such as insurgency and terrorism, require multi-domain approaches that include intelligence, cyber capabilities, and precision strikes. India has been a victim of terrorism since independence such as in Jammu and Kashmir (J&K), Northeastern States and Naxal infested states in the red corridor of India spanning Bihar, Jharkhand, Chhattisgarh, Odisha, Maharashtra, Telangana, and Andhra Pradesh. The military needs to work in coordination with other security agencies to address these challenges effectively. MDO will greatly enhance the effectiveness of Indian operations. An example is the use of land, air, cyber, and space resources by the defence forces. Another example that stands out of MDO to counter terrorism is the Balakot strike by air in J&K sector. Similarly, aerial resources, land resources and cyber resources can be utilised to augment the other security forces more seamlessly in a multidomain environment backed by sound net-centric environment that has an interface, if required, with the non-military security forces and agencies.

## Amphibious/Hybrid Capabilities along the Coast/Island Territories

In the maritime domain, with a long coastline, number of island territories and maritime interests, the Indian military needs to maintain strong amphibious capabilities. This involves the integration of land and naval forces for operations in littoral zones. In addition, the cyber and space resources would also get involved while dealing with conventional and hybrid threats. Coupled with the need for amphibious operations the hybrid threat may need a combined land, air, space and cyber response.

## Conclusion

India is subjected to multiple threats ranging from conventional to unconventional, military to non-military and contact to non–contact. The nature of conflict is gradually shifting from a black and white texture to grey with wars and conflicts extending into the space of war to even the peace time. With grey zone war now being conducted by our adversary during peace and war through multiple means the response must adapt and respond by kinetic and non-kinetic measures. Therefore, MDW is crucial for India to address the security challenges confronted by India. The integration of capabilities across land, sea, air, space, and cyberspace, along with a focus on technological advancements and integration, will enhance India's ability to respond to a wide range of security challenges. There is a need now to create a national military strategic support organisation or agency under the CDS to meet these challenges. The proposed organisation should have cyber, space, information, military diplomacy, and intelligence components under its command.

## Endnotes

[1] Maj Gen (Dr) GD Bakshi, S. V. (2022, Nov 15). -November 15, 20220844. Retrieved Jan 2024, from Indian Military Review: https://imrmedia.in/editorial-multi-domain-operations/

[2] https://www.defstrat.com/magazine_articles/multi-domain-warfare-in-the-indian-context/#:~:text=It%20is%20in%20this%20realm,capability%20required%20for%20their%20integration.

[3] Ibid.

[4] Ibid.

[5] GFPIndex. (2024, January). Global Firepower Ranking. Retrieved from GFP Strength in Numbers: https://www.globalfirepower.com/countries-listing.php\

[6] Mishra, G. M. (2024, January 10). Explained I China's influence on Maldives. Retrieved January 2024, from Deccan Herald: https://www.deccanherald.com/world/explained-chinas-influence-on-maldives-2842834

[7] Abeyagoonasekera, A. (2023, May 03). The Communist Party of China and Its Political Influence in Sri Lanka under the Gotabaya Rajapaksa Regime. Retrieved January 2024, from CSEP: https://csep.org/reports/the-communist-party-of-china-and-its-political-influence-in-sri-lanka-under-the-gotabaya-rajapaksa-regime/

[8] Epstein, A. J. (2022, Dec 23). The PLA's Strategic Support Force and AI Innovation. Retrieved Jan 2024, from Brookings.edu: https://www.brookings.edu/articles/the-plas-strategic-support-force-and-ai-innovation-china-military-tech/

[9] Singh, D. (2023). Grey Zone Warfare : Way Ahead for India. New Delhi, India: Viz Books New Delhi.

[10] ibid