SYNERGY

JOURNAL OF THE CENTRE FOR JOINT WARFARE STUDIES

Volume 4 Issue 2 ISSN: 2583-5378 August 2025

CENJOWS
(Established : 2007)
Room No 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi - 110003 (INDIA)
Telephone Nos : 011-24364881, 24366485
Fax : 011-24366484
Website : www.cenjows.in
E-mail : cenjows@cenjows.in, cenjows@yahoo.com

ABOUT US

CENJOWS was raised in 2007 as an independent think tank, registered under the Societies Registration Act, 1860. This aims to promote Jointness as a synergistic enabler for the growth of Comprehensive National Power and provide alternatives in all dimensions of its applications through focused research and debate.

Year of Publication : 2025
Frequency : Bi-Annual
Language : English
Publisher : Maj Gen (Dr) Ashok Kumar, VSM (Retd)
Director General, CENJOWS
301, B-2 Wing, 3rd Floor
Pt. Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi-110003

RNI Number : DELENG/2022/82424

All correspondence may be addressed to:
Editor
Centre for Joint Warfare Studies (CENJOWS)
301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi-110003
Telephone: (91-11) 24366485/Telefax: (91-11) 24366484
e-mail: cenjows@cenjows.in / cenjows@yahoo.com
Website: http://cenjows.in

Price : Rs 750/- INR or US 25$
RNI No : DELENG/2022/82424

Print ISSN: 2583-5378
Online ISSN: 2583-536X

EMERGING CONTOURS OF FUTURE WARFARE

IN THE TRI-SERVICES DOMAIN

CONTENTS

NOTES:

- Views expressed in articles are individual opinions of the writers, and not of CENJOWS.
- Contributors to Synergy Journal are requested to visit the website for the theme of the next issue and guidelines.

General Anil Chauhan, PVSM, UYSM, AVSM, SM, VSM
Chief of Defence Staff

MESSAGE

Clausewitz, the Prussian veteran of the Napoleonic wars, in his most famous work 'Our War' had said "War is a continuation of policy by other means". This means that after exhausting available diplomatic, economics and ideological options, 'war' remains a rational alternative for preservation or furtherance of the state's interest.

India, today faces multifarious threats emanating from an array of state and non-state actors. The future strategic security environment requires recalibrating our capabilities and putting concerted efforts for drawing integrated strategic frameworks for planning, seamless coordination and unwavering collaboration among the three services, as well as, between government agencies and the armed forces.

In the era of Grey Zone and Hybrid warfare, critical and emerging technologies like artificial intelligence and machine learning, quantum computing, blockchain, advanced sensors and autonomous & unmanned systems need to be adopted and leveraged to stay ahead of the technological curve. Besides, Suitable structures, the armed forces have to be 'future ready' with more focus on acquiring capabilities and adopting procedures that enable multi-domain integrated operations.

This edition of 'Synergy' themed **"Emerging Contours of Future Warfare in the Tri-Services Domain"** is being published in the backdrop of Op Sindoor. It is contemporary, relevant and forward-looking publication for policy enunciation, conceptualization, planning, orchestration and implementation of future framework. I am certain that this edition will encourage further ideation towards bolstering efforts to deal with future security challenges.

I extend my felicitation to ‘Team CENJOWS’ for this outstanding effort and wish them the very best in their endeavours.

Jai Hind!

(Anil Chauhan)
General
Chief of Defence Staff

Air Marshal Ashutosh Dixit, AVSM, VM, VSM
Chief of Integrated Defence Staff to the
Chairman, Chief of Staff Committee &
Chairman CENJOWS

FOREWORD

Throughout history, the character of warfare has evolved alongside the advancement of technology and shifts in geopolitical dynamics. The 21st century witnesses a profound shift in the character of conflict which is shaped by rapid technological innovation, hybrid threats and the expanding complexity of the global security environment. Future wars are no longer confined to conventional battlefields; instead, they extend across multiple domains, demanding seamless integration and joint operations across the land, air, maritime, cyber and space realms.

In this emerging landscape, the Indian Armed Forces must anticipate and adapt to challenges that are multifaceted, ambiguous and unpredictable. The need for a unified, agile and technologically empowered Tri-Services structure has never been more critical. While traditional threats persist, the growing potency of grey-zone warfare, marked by cyberattacks, disinformation campaigns, space militarisation and economic coercion, requires a revaluation of existing doctrines and operational strategies.

Success in future conflicts will depend not just on superior firepower, but on the ability to harness cutting-edge technologies such as Artificial Intelligence, autonomous systems, quantum computing and advanced sensor networks to enable decision superiority and operational synergy.

India's strategic environment presents a unique and demanding set of challenges. With active and contested borders, a complex maritime theatre, and the proliferation of both conventional and hybrid threats, a future-ready force must be grounded in interoperability, adaptability and innovation. Building integrated capabilities that cut across Services, investing in indigenous technological solutions and fostering a whole-of-nation approach to national defence are essential for safeguarding sovereignty and advancing India's strategic interests.

This edition of Synergy Journal, themed **"Emerging Contours of Future Warfare in the Tri-Services Domain"** explores these critical issues with depth and foresight. The diverse and insightful contributions offer perspectives on how India can navigate the complexities of future conflict, leverage disruptive technologies and enhance joint warfighting capabilities. It is our expectation that the inputs presented will serve as catalysts for meaningful debates, informed policy formulation and inspire new pathways towards strengthening India's national security framework.

As we look ahead, embracing the evolving nature of warfare with clarity, creativity and collaboration will be vital to shaping a resilient and future-ready Indian Armed Forces. I compliment Team CENJOWS for underscoring a relevant issue of the Synergy Journal.

Jai Hind!

(Ashutosh Dixit)
Air Mshl
CISC

Maj Gen (Dr) Ashok Kumar, VSM (Retd)
Director General CENJOWS

FROM THE DIRECTOR GENERAL'S DESK

The security landscape of the 21st century is being reshaped by the convergence of traditional threats and disruptive technologies, necessitating a profound transformation in how nations prepare for and respond to conflict. As a strategic community, we must engage deeply with this transformation to chart an effective course forward for India's defence preparedness. The August edition of Synergy addresses precisely this imperative by bringing into focus the evolving nature of warfare within a tri-services construct.

With the emergence of new warfighting domains and tools, ranging from autonomous systems, artificial intelligence to near-space platforms and cyber capabilities where the boundaries of the battlefield are being redrawn. Future conflicts will not be linear or limited to singular services or regions. They will be characterised by fluidity, unpredictability and simultaneity across domains. In such an environment, integration across services is not merely a doctrinal preference, it is a strategic necessity.

This edition underscores the criticality of jointness and inter-service synergy in enhancing our operational readiness. From aerial innovations and joint drone doctrines to low-earth orbit satellite networks and space deterrence, each article contributes to a broader conversation on how India's military and strategic community must recalibrate for multi-domain operations. Importantly, the issue also explores the human and cognitive dimensions of warfare, reminding us that alongside systems and structures, the quality of leadership and adaptability of our human capital will be decisive.

The Centre for Joint Warfare Studies (CENJOWS), a scholastic tri-services think tank, remains committed to facilitating forward-looking scholarship and informed discourse. Through this edition, we aim to illuminate emerging trends and foster debate among practitioners, scholars and policymakers. The diversity of perspectives represented in this issue reflects a shared commitment

to anticipate, understand and respond to the contours of future warfare, in a cohesive national endeavour.

As we stand at the cusp of a technological revolution in warfare, India must strengthen its indigenous capabilities, accelerate doctrinal evolution and institutionalise mechanisms for integrated training, planning and execution. The journey toward a truly joint force structure is complex, but it is one that must be pursued with urgency, clarity and strategic foresight.

I commend the contributors for their insightful analyses and thank Team CENJOWS for curating yet another relevant and timely edition of Synergy. It is my hope that the ideas presented here will serve as catalysts for innovation, cooperation and capability development in the national interest.

Jai Hind!

(Ashok Kumar)
Maj Gen (Retd)
Director General

TRI-SERVICE SYNERGY FOR FUTURE CONFLICTS: POLICY INSIGHTS AND STRATEGIC ADAPTATIONS

Dr Sumanta Bhattacharya

Abstract

Modern warfare scenarios have changed so much that there is a need to deviate from traditional models of tri-service synergy, leading to Multi-Domain Operations (MDO) and technology-oriented military strategies. For the future, warfare will be defined by cyber attacks, Artificial Intelligence (AI) combat operations, outer space, and AI weapons, and an integrated approach across land, air, sea, cyber and space will be essential. This paper discusses the extent to which the endearing method of joint force interoperability can be further strengthened and emerging technologies and strategic mobility can provide policy insights for preparing a future-ready defense architecture. Core strategic priorities encompass leveraging AI for decision support, enhancing cyber resilience, and developing autonomous warfare systems. The paper further underlines the importance of information warfare, rapid force deployment, and sustainable defense solutions in determining next-generation military strategies. The armed forces create long-term security through defense partnerships, indigenous research and development investments, and operational adaptability. These factors serve as the lens through which this study highlights the strategic relevance of tri-service integration in supporting Near-Peer Operations, the associated barriers to integration, the subsequent challenges, and recommendations to support operational success in a changing global security environment.

INTRODUCTION

In 21st century warfare, the paradigm is changing due to advancements in technology, changes in the geo-political landscape and new security threats in (non-traditional) warfare. Traditional conflict with large-scale ground battles and hidden innovations is becoming obsolete, with Multi-Domain Operations (MDO), integrated warfare against land, air, sea, cyber and space targets, taking centre stage. The emergence of AI, quantum computing, hypersonic weapons, and autonomous systems have compounded the ambiguity between conventional and unconventional conflict. Additionally, cyber warfare has become a major front in the conflict, with state and non-state actors using advanced cyber attacks to target critical infrastructure, influence narratives, and secure geopolitical gains. Cyber and electronic warfare have become

primary components of their operational success in defending their territory and national interests, given the growing use of digital technologies in their defensive operations. Additionally, new methods of decision-making, predictive analytics, and autonomous combat systems have revolutionised the way the wars are planned, executed, and sustained, requiring an entirely new approach to defense readiness.[1] Coordination across the Army, Navy, and Air Force will be critical as future conflicts will be more complex and unpredictable. The synergised tri-services' integration of assets optimise operational capabilities, increase the level of strategic deterrence, and enable a fast, efficient and effective coordinated response to emerging threats. At a time when threats often don't recognize traditional borders and on-field capabilities, a piecemeal approach to warfare often results in inefficiencies, delay, and vulnerabilities. Maritime security, air dominance, and cyber resilience are becoming more vital than ever and hence a joint military recipe with deliberate focus on sharing intelligence, joint operations, and interoperability is imperative. This complement of land, aerial, and naval might will encourage a holistic posture on defense, enabling forces to work together against hybrid threats including cyber espionage, drone warfare, and information manipulation.[2]

Interruptions due technology is not only the challenge, but the geopolitical environment has also become more unstable, with alliances being reshaped, regional conflicts reappearing and competition among great powers defining global security processes. Military doctrines must be flexible, responsive, and future-oriented to meet challenges like border conflict, sea disputation, and asymmetric warfare. With a view to retaining a strategic edge, militaries across the world are now realizing the need for joint military doctrines, integrated command structures and network-centric warfare. This evolution in warfare requires not just cutting-edge technology, but also a strong policy foundation for collaboration across all domains of defense. Policies should emphasize integrated training initiatives, cross-service warfighting doctrines and investments in digital infrastructure to ensure the tri-services operate in unison as one coherent force.[3]

The need for interservice synergy extends beyond preparedness, playing a pivotal role in national security and economic resilience. Such an integrated defense strategy not only reinforces deterrence but also minimizes duplication of effort in the defense procurement process and provides a better allocation of resources. It enables projecting power and responding to humanitarian crises, disaster relief operations, and non-traditional security emerging threats like climate-induced conflicts and pandemics. In light of these factors, any attempt to modernize defense forces cannot afford to operate in a policy free zone, and must be embedded within a wide policy framework that institutionalizes tri-services cooperation, cultivates technological innovation, and aligns military

capabilities with evolving global security postures. It is only through a whole-of-nation, future-proof approach that countries will achieve strategic mastery in the age of fast-paced warfare.[4]

EMERGING CONTOURS OF FUTURE WARFARE

The 21st century is introducing a new paradigm of warfare, characterized by the intersection of emerging technologies, evolving geopolitical landscapes, and the multifaceted nature of threats. Just as traditional battlefields once reigned in ancient and modern conflicts, ground battles and bombardments are now gradually giving way, and, in some instances, being supplanted, by far more sophisticated multi-domain strategies that include land, sea, air, cyber and space operations. The rise of hybrid warfare, blending conventional, irregular, and cyber operations, has complicated the strategic situation even more. Both state and non-state actors are resorting to asymmetric tactics, disinformation campaigns, and economic coercion to further their agendas without a direct military showdown. Such a change in the form of warfare requires an adaptive process, where the plans of military doctrine, command structures, and defense policies align themselves to generate strategic advantages in the unpredictable face of conflict.[5]

Modern warfare is undergoing drastic transformative changes due to the increasing role of cyber and electronic warfare as primary instruments of conflict. Countries are pouring resources into offensive cyber and defensive capabilities, realizing cyber attacks have the ability to take down infrastructure, shut off communication networks or manipulate financial systems without ever having to put boots on the ground. The realm of cyber warfare is not limited to the digital domain, it is closely linked with traditional warfare execution, with effects on command-and-control structures, logistics, and intelligence gathering. At the same time electronic warfare has emerged as an essential element of battlefield supremacy, with the power to interfere with enemy communications, disrupt satellite networks and jam radar systems. These trends highlight the necessity of a cohesive cyber-defensive strategy that combines cyber resilience with traditional military readiness.[6]

AI and autonomous systems are redefining the nature of warfare. AI-powered analytics provide commanders with real-time actionable intel, empowering decisions in the midst of chaos as they anticipate enemy behavior and position resources where they are needed most. Sensing images of military installations, AI-powered reconnaissance applications, capable of analyzing large data sets in real time, are transforming intelligence and battlefield awareness. But the use of AI in war also raises ethical and legal questions, including issues of accountability in autonomous decision-making and the risk of AI-enabled conflicts spiraling out of human control.[7]

They extend into the space domain, which is becoming an increasingly contested battlefront with countries racing to dominate the lucrative satellite-based intelligence, navigation and communications sector. Precision-guided weapons, real-time surveillance and secure communication links depend now on satellite networks for military operations. But some challenges are extreme, including the threat of weaponization in space through anti-satellite weapons (ASAT), directed-energy systems, or cyber attacks aimed directly at space infrastructure that could upend entire defence networks. Space doctrines should emphasise resilience, through redundancy, decentralised command structures, and international synergy on space security. The growing militarization in space underlines the urgency to develop new defence policies that would regulate the uses of space assets and secure national security interests.[8]

The discovery of hypersonic weapons is also a game-changer in modern warfare. These weapons significantly reduce enemy reaction and pose serious challenges to missile defense systems due to their speed exceeding Mach 5. Hypersonic weapons move at very high speed, but unlike traditional ballistic missiles, they can manoeuvre unpredictably, making interception difficult. Countries are actively building hypersonic glide vehicles and cruise missiles to improve their strike capabilities, challenging military planners to rethink air defense operations. Speed is not the only advantage here, so new types of counter-hypersonic defense systems must adapt to incorporate features including directed-energy weapons that are powered by electricity, artificial AI guided interception weapons, and open space-based surveillance networks.[9]

Though hybrid warfare, a combined approach that features conventional military operations alongside cyber attacks, disinformation campaigns and economic coercion, is increasingly becoming the strategy of choice for many of the world's nations. In contrast to conventional wars that are waged on established battlefields, hybrid conflicts leverage political, social, and economic weaknesses to pursue strategic goals. Deepfake technology, AI generated propaganda, social media manipulation and information warfare etc are quickly becoming the central pillars of modern conflict. At the same time, nations must step up their defences against cognitive warfare, engaging in investments in digital literacy, media resilience, and counter-disinformation initiatives. Thus, addressing hybrid threats necessitates active collaboration among military forces, intelligence communities, and cyber defense specialists to identify and neutralize emerging threats before they evolve into broader conflicts.[10]

Also on the rise are climate change and resource scarcity as harbingers of future strife. Global warming and the resulting impacts on sea levels, desertification and extreme weather events, threatens global stability by further intensifying food and water shortages as well as forcing mass displacement and conflict over scarce resources. Military forces will have to adapt to these

new security challenges through disaster response, humanitarian assistance, and environmental security strategies. Climate-induced conflicts will require increased cooperation among defence agencies, international organizations, and scientific communities to mitigate risks and restore stability in vulnerable areas.[11]

The future of conflict will rely heavily on joint and integrated employment of forces across multiple domains, including land, air, sea, cyber, and space, also known as multi-domain operations (MDO). This innovation must move the center of gravity from service specific to joint and agile warfare in a new era of how we fight, compete and deter. Interoperability, joint training, and future military technologies. The more joint military exercises, the greater chance of preparation for threat; defense policies should focus on these aspects. India has never been more in need of a tri-service option operating as a single body of force between the Army, Navy, and Airforce. But only through the application of advanced technologies, optimized cyber defense, and reinforcement of cross-domain operational synergies will nations maintain strategic advantage of a battlefield mindset of ever-evolving warfare.[12]

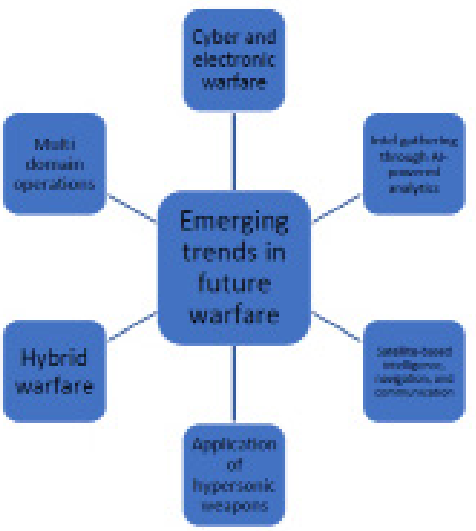


Figure 1: Emerging trends in future warfare: Strategic Imperatives for a Future-Ready Tri-Service Force, Source: Author

FOR A NEXT GENERATION TRI-SERVICE FORCE: IMPLICATIONS FOR STRATEGIC PRIORITIES

At a time when the nature of warfare is continuously transmuting, the need to ensure a tri-service future force stands tall as a critical pillar. Central to facilitating the emergence of threat-leading multispectrality is the integration of the Army,

Navy and Air Force into a single cohesive, synergistic, and interoperable force. Not only does this mean preparing for conventional conflict, but a modern military must also adapt to cyber warfare and AI-based autonomous operations resulting in shaping the future military campaigns which play out. These will rest on across technology integration, improved joint operational capacity as well as rapid command setup that can adjust quickly to fast-changing fronts. They need to have a strong strategic framework that allows the three services to coordinate with one another and act as a coherent warfighting organization.[13]

A key architectural element of a future-ready force is an integrated command structure. The old way of running the three services separately does not work anymore with modern MDO. Prioritise joint theatre commands which if created would allow real-time intel sharing, synchronized planning and unified execution of military strategies. A joint command architecture that is appropriately strengthened will not only enhance operational synergy but also enable better resource allocation, thus minimizing duplication of expenditure on defence. Command integration should be accompanied by a common operational doctrine providing unity of effort in terms of strategic and tactical objectives, along with service roles for each mission.[14]

The things such as interoperability and network-centric warfare will definitely increase the efficacy of a tri-service force. Contemporary conflicts demand quick exchange of information, real-time situational awareness, and synchronized conduct of military operations. Without operational superiority, no defense network can survive in future and therefore, robust defence network built upon surveillance systems, cyber capabilities, AI analytics and satellite-based communication will be the key to success. Joint operations have to be coordinated in a way that they not only maintains precision but also makes the necessary communication channels between the Army, Navy, and Air Force resilient and secure. Furthermore, implementing blockchain and quantum encryption technologies can strengthen cyber defense capabilities and protect sensitive military information from hostile entities.[15]

More importantly, emerging technologies like AI, Machine Learning (ML), and big data analytics should be prioritized for integration into the decision-making process for improvement. The impact of AI predictive analytics on threat assessment is extremely positive, as military leaders can start predicting future conflicts and developing proactive strategies. Equipped with robotics and AI, autonomous drones, robotic combat systems and security tools could provide increased reconnaissance capabilities and precision strikes while limiting risks to humans. By investing in innovative research and development, the armed forces will be able to remain at the forefront of cutting-edge technology enabling strategic advantage over the enemy.[16]

Institutionalizing joint training programs and war-gaming exercises to synergize the three services will enhance coordination. Frequent tri-service joint exercises, strategic war-fighting simulations and real-life combat scenarios training would allow troops to get acquainted with coordinated operational capabilities. Such training efforts will further identify potential operational planning gaps and enable updating of joint warfare plans.

Cyber and electronic warfare capabilities need to be built up for an evolving tri-service future-ready force. As cyber threats evolve, cyber resilience will play a larger role in ensuring the security of critical infrastructure and defense networks for military operations. Yes, the need of the hour will be specialized cyber warfare units equipped with AI-driven threat detection and response systems to counter cyber-attacks. To this end, the development of electronic warfare systems that can jam enemy communications, inhibit adversarial radar networks, and even neutralize space-based threats must be included in defense strategies. Future-ready tri-service force and strategic imperatives include institutional reforms, technological modernisation and cross service synergy. Adopting a policy framework focused on interoperability, integrated command structures, and next-generation warfare capabilities will help to ensure that the military is prepared to face the challenges of future conflict. Through this innovative and visionary strategy, the armed services can achieve strategic sovereignty and protect national security in an age of warfare transformation.[17]

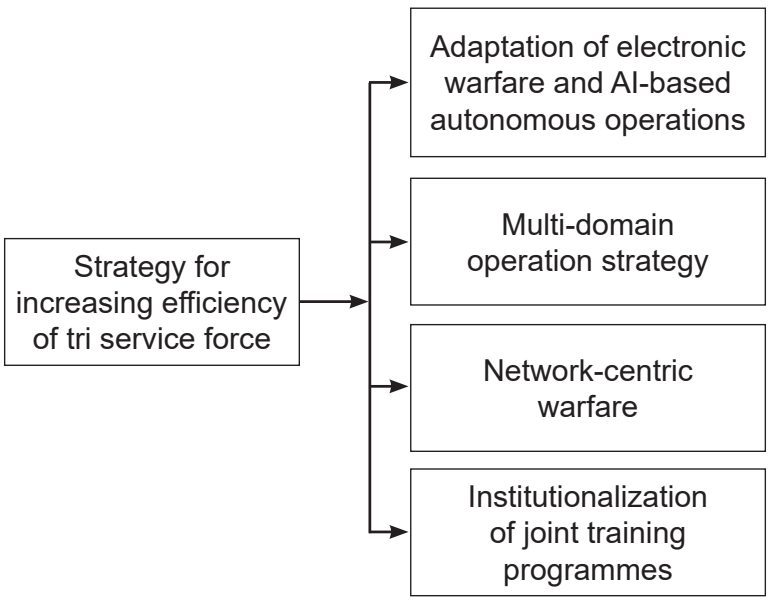


Figure 2: Strategy for increasing efficiency in tri service forces, Source: Author

POLICY INSIGHTS FOR STRENGTHENING TRI-SERVICE SYNERGY

At a time when military operations are becoming increasingly complex and multi-dimensional, the enhancement of tri-service synergy is not only a choice but also a demand of the time. We must unite the Army, Navy, and Air Force into a cohesive war-fighting entity to achieve joint operational synergy, speed of response, and strategic dominance. Recent wars are not restricted to a single domain; they cover fields such as land, sea, air, cyber and space, and thus require seamless integration amongst three services. A focus on policy frameworks at the highest echelons can help institutionalise tri-service integration, build interoperability, and streamline joint operations to forge a formidable future-ready force. Formation of the Joint Theatre Command (JTC) typifies one of the cardinal guiding policies of ensuring tri-service synergy. A unified command system allows all three services to work together under a single chain of command, enabling faster decision-making and improving coordination during crises. Indeed, many of the world's leading military powers have implemented joint commands to ensure member forces are deployed and resources allocated in the most effective way. And it would all put JTCs in place in those theatres, eliminating redundancies, speeding responses and increasing strategic effectiveness. Policies need to address institutionalizing joint doctrine development and set a fundamental baseline that all three services should adhere to a unified strategic vision and share standard operating modes of integrated warfare.[18]

Network-Centric Warfare (NCW) principles account for another vital aspect of the tri-service synergy. The 21st-century battlefield calls for the sharing of real-time intelligence, rapid data processing and advanced surveillance capabilities. We must prioritize a strong, secure, and interoperable communications network between the three services. Policymakers must promote investment in digital defense infrastructure, such as AI-based command-and-control problems, big data analytics, and blockchain-based cybersecurity technology. A shared military cloud system with underlying connectivity will also allow seamless data transfer between the Army, Navy, and Air Force to boost situational awareness and provide rapid and integrated responses to new threats. Joint operations must also integrate cyber warfare capabilities, as cyber attacks have become a key element of modern hostilities. Now, policies must enforce the creation of dedicated cyber warfare units with AI-powered threat detection and mitigation tools.[19]

Joint training programmes and integrated war-gaming exercises must be made compulsory to enhance tri-service collaboration. Joint operations are effective when personnel from different services can work together. A policy framework must also institutionalise cross-service training academies, facilitated through

joint training of officers and soldiers across the three services. Full scale tri-service exercises both in house as well as with allied nations should also be conducted to validate the operational joint doctrines, while fine tuning the synergistic approach for planning, execution and command modes. Policies must also incentivize knowledge-sharing through exchange opportunities, whereby officers from each service are exposed to the other branches' operational capabilities and challenges.[20]

The aspect of tri-services synergy must also be aligned in defense procurement and capability development. Policies should institutionalize a unified defense acquisition approach that evaluates procurement decisions across the needs of all three services in lieu of isolated service-based decisions. Control of acquisitions should operate under a centralized defense procurement body to maintain interoperability between military platforms and unnecessary redundancy of assets. Indigenous defense technologies must be invested, where the private sectors should also be establishing a partnership between the sectors, academic institutions, defence startups. A focus on developing multi-role platforms, for example, an aircraft to serve the Air Force and Navy, or unmanned systems that operate across domains, will only bolster integration.[21]

Psychological operations and strategic information war are inherently joint capabilities that must be exercised and coordinated across the tri-services in the hybrid warfare era. Today, adversaries employ everything from disinformation campaigns to AI-generated propaganda to social media manipulation to destabilize countries. It is imperative we adopt a synchronized approach to countering information warfare, which also requires a tri-service information warfare command to track and neutralize such threats. These strategies are driven by the emergence of new adversaries that share the cyber space along with their default strategies of augmenting narratives through specialized AI technologies.[22]

Logistics and resource optimization is another crucial area of policy. This will require developing a unified logistics framework where resources are allocated efficiently and effectively across all three services. Integrating maintenance programs, sharing logistical hubs, and establishing common supply chains can greatly improve operational readiness. A single national defense logistics agency must be responsible to ensure the smooth flow of personnel, equipment, and supplies, mitigates operational bottlenecks in improving interactions with the logistics and supply chain. Along with the above, policies need to encourage sustainable military logistics, such as renewable energy solutions in deployed defence and eco-friendly defence infrastructure and energy-efficient transport solutions.[23]

Lastly, legislative and bureaucratic changes need to be introduced that institutionalize triumvirate synergy. A National Defense Management Authority (NDMA) is needed to manage the three services in terms of joint operational planning, budget allocation, and policy implementation. The roles and responsibilities of each legal branch in joint operations must be clearly understood to prevent duplication of jurisdiction with joint operations, and even more importantly to avoid a collapse in the chain of command. Equally important, all of these policies should reinforce deeper civil-military cooperation through the integration of defense planning with national security and economic development planning.[24]

Figure 3: Policy for strengthening Tri-Service Synergy. Source: Author

STRATEGIC ADAPTATIONS FOR FUTURE READINESS

Ensuring future readiness within the realm of national defence, however, is not static, and will require a re-evaluation of strategy to meet the demands of an evolving battlefield. Land, sea, and air domains through traditional combat models have limited applicability in countering asymmetrical threats of cyber warfare, AI-assisted warfare, unmanned weapon systems, and also the threats in space domain. The future of military forces requires agile and technology-fuelled Multi-Domain Operations (MDO), streamlined joint forces, and the advancement of emerging technologies. Understanding the challenges of tomorrow and preparing today will define military effectiveness.[25]

The transition to multi-domain integration is one of the most important strategic adaptations. Our next war would not be fought in a single domain, rather a simultaneous fight across land, air, sea, cyber, and space domains. A coherent

plan has to guarantee seamless interoperability among all of the fighting services to speed up intelligence exchange and synchronize operations. This necessitates having a joint Command-and-Control (C2) center where all domains are fused with real-time data. These decision-support systems can provide AI-driven recommendations that improve situational awareness, allowing commanders to make informed, data-driven decisions in combat operations. Furthermore, modernization of investments in space-based reconnaissance, cyber warfare forces, and autonomous unmanned systems will prove integral to sustaining a dominant edge in contested environments.[26]

The second major adaptation is the use of emerging technologies to improve military capabilities. AI and machine learning, quantum computing, robotics is reshaping the ways in which wars are fought. The military must therefore establish R&D units specialized in next-generation weapons systems, cyber and electronic warfare systems to maintain technological superiority. Innovation would be catalyzed by collaborations with defense technology startups, academic institutions, and the private sector as well. In addition, the use of AI-powered predictive analytics in military planning can enhance threat analysis and resource distribution, reducing risks and maximizing combat preparedness.[27]

This should also include cyber resilience and electronic warfare preparedness, as elements of strategic adaptions. With warfare increasingly moving into digital and information-based domains, cyber threats are the biggest danger to national security. State-sponsored cyber attacks, hacking attempts on defense infrastructure, and misinformation campaigns can destabilize military operations. This would entail enhancing encryption measures, utilizing anomaly detection systems powered by AI, and developing specialized cyber warfare units capable of responding to and neutralizing attacks in the digital domain. Furthermore, future operational constructs must also include electronic warfare capabilities such as jamming enemy communications, disrupting satellite networks, and employing counter-cyber measures.[28]

Another key tenet of future readiness is the modernization of training and force development. Advancements in building simulations and training programs based on Augmented Reality (AR) and Virtual Reality (VR) also need to be integrated into traditional training models. Soldiers of the future will need proficiency in digital skills, cyber defense, and cross-domain operations. Institutionalising joint force training exercises to improve coordination among land, air, naval, and cyber units is a must. Such new warfare dynamics will necessitate not just military training for personnel using simulated cyberattacks, space-based conflicts, and AI-assisted combat scenarios during war-gaming exercises but will need to be trained together.[29]

Finally, improvements in logistical and strategic mobility need to be integrated to enable rapid employment and sustainment of forces in contested environments. Supply chains for future military operations will have to not only use autonomous resupply systems, but also utilise AI-driven logistics and strategic airlift capabilities. Policies need to incentivise the evolution of modular and multi-role military platforms that can be rapidly re-purposed for a variety of combat situations. An advanced logistics network will play a crucial role in an expansive defense structure.[30]

Military forces need to stay future-ready through force-level strategic adaptations that embrace technological trends, strengthen joint force cooperation, and facilitate preparations for multi-domain conflicts. Thus, a proactive strategy focused on cyber resilience, AI-driven warfare and rapid operational adaptability will guarantee enduring military effectiveness in an ever-more uncertain global security environment.

Figure 4: Strategic adaptations for effective tro0service synergy. Source: Author

FUTURE DIRECTIONS

Military forces should approach wars of the future with a sense of being ready with future possibilities, ever mindful that strategic dominance requires sustained attention to overcoming uncertainties. With rapid advancement of technologies, shifts of geopolitical power, and emerging threats across all domains: future wars are going to be significantly different from past wars and hence will require holistic military modernization and policy adaptations. As

such, rethinking for future-ready defense elements will be crucial to maintaining national security and global stability.

The full integration of the MDO is among the most critical future directions in the military strategy. Conventional warfare dealt with land, air, and sea, but modern warfare also deals with space, cyber, and information warfare. Future military strategies, therefore, need to establish seamless coordination across all of these domains, enabling the Army, Navy and Air Force to operate as a single unified force. It will necessitate the establishment of joint command architectures, real-time data-sharing capabilities, and AI-assisted decision-support tools to improve operational effectiveness. Budgetary allocations for the development of advanced surveillance technologies, space-based reconnaissance systems in addition to quantum computing to encourage secure communications will also be critical to enhance multi-domain warfare capabilities in the future.The other key area of focus is the uptake of emerging and disruptive technologies. In the future, AI, machine learning, and quantum computing are going to transform our defense strategies. AI-driven autonomous system, from Unmanned Aerial Vehicles (UAVs) to robotic ground forces, will increase battlefield agility and decrease the risk to human soldiers. Military forces will also rely on quantum encryption, which will provide them with communications networks that cannot be intercepted, which in turn will ensure cybersecurity superiority. R&D in these domains must become the cornerstone of future defense strategies, enabling partnerships with tech innovators, defense start-ups, and academic institutions to counter adversarial tech developments.

New types of military operations will also include cybersecurity and information warfare as a cornerstone of future military operations. The growth of digital infrastructure makes defense networks vulnerable to cyber attacks, espionage, and misinformation campaigns. This could include the integration of sophisticated cyber-defense technologies, the implementation of automated threat assessment algorithms, and countermeasures against adversaries who may exploit vulnerabilities in cyberspace in the context of warfare. Moreover, in the battle for hearts and minds, shaping the narrative around the information will be important to plug narrative errors. The use of psychological warfare and digital influence operations will become a more strategic element in the conflict, and there will be a need for dedicated units that will monitor and neutralize the threat posed by disinformation as well.

Strategic mobility and rapid force deployment will also be priorities for future military operations. The dispatch of troops, equipment, and logistics support to contested regions at rapid speed will be a key determinant of military victory. Thrusts in hypersonic transport systems, autonomous resupply drones, and mobile command centers will allow for enhanced operational flexibility. Modularity in military platforms that can adjust to changing circumstances

and multiple combat scenarios is more likely to lead to operational agility and responsiveness in unknowable future theatre of war environments. Tied down by having a constantly problematic relationship with its own temper will need the far too much effort and time to adjust. The development of global defense partnerships and enhanced military alliances will be a critical component of rapidly projecting force and cooperating in matters of collective security. Sustainability and resilience in defense operations will ultimately come to define how military strategies are executed in the future. Defence solutions will need to be eco-friendly to face climate change and the new world apportioning of resources. Embracing renewable energy, electric-driven military vehicles, and green logistics significantly reduce defense industries' environmental impact and boost energy security only adaptive, technology-enabled, service-integrated and multi-domain capable forces can compete in such a rapid and changing conflicts. The integration of these elements will enable military forces to adapt to the evolving security landscape, promoting readiness for future conflicts and upholding national security and global stability.

CONCLUSION

The future of warfare is changing quickly as military operations, policies, and application of technology need to make a strategic shift. National security amidst the global uncertainty of 2025 would revolve around the concepts of MDO, adversary AI driven decision making, cyber resilience, space based capability development etc. Technological advancement, interoperability and rapid force deployment holds the key for a future-ready tri-geographic enemy facing force. Cybersecurity, information warfare, and sustainable defense solutions will also be vital. Pursuing stronger defense partnerships, investing in indigenous innovations, and securing strategic mobility will be crucial to maintaining operational advantage. Military forces must be agile, adaptive, and foresighted as conflicts become more abstract and technology-driven. By adopting strong policy initiatives and transformational innovations, the tri-service forces can set up a future-ready and resilient defence platform to meet the future challenges of warfare.

❖❖❖

Dr Sumanta Bhattacharya is a globally recognised scientist listed in the World's Top 2 percent Scientists (AD Index). He serves as an Expert Commission Member of the International Union for Conservation of Nature (IUCN) and is a registered Individual Consultant with the Asian Development Bank. Additionally, he is an IPL Expert at UIPL (UNESCO) and a VIDWAN Expert under the NME-ICT initiative of the Ministry of Human Resource Development (MHRD), Government of India. He is currently pursuing his Ph.D. at Asian International University.

NOTES

1. Upadhyay, A. (2023, February 17) Amid Changing Nature and Character of War, the Need for Tech-Oriented Military Commanders for India; *Observer Research Foundation;* https://www.orfonline.org/research/amid-changing-nature-and-character-of-war-the-need-for-tech-oriented-military-commanders-for-india
2. Ankit, K.; Bommakanti, K. (2025, February 19) A case for India's Joint Training Command New, unified approach to training can help prepare armed forces for complex modern warfare; *Deccan Herald;* https://www.deccanherald.com/opinion/a-case-for-indias-joint-training-command-3411484
3. Sutisna, Y.; Muttaqin, M. I. (2025) Global Security Transformation Amid Regional Conflicts in the Middle East: Challenges and Opportunities; *Proceedings of the International Conference on Strategic and Global Studies (ICSGS 2024), Atlantis Press*; https://doi.org/10.2991/978-94-6463-646-8_20
4. Liu, W., Feng, Z., Luo, X. (2024). Measurement of Synergy Management Performance in Prefabricated Building Project Supply Chain. *Sustainability*, *16*(24), 11025. https://doi.org/10.3390/su162411025
5. Rajagopalan, R. P.; Patil, S. (2024, February 12) Future Warfare and Critical Technologies: Evolving Tactics and Strategies; *Observer Research Foundation;* https://www.orfonline.org/research/future-warfare-and-critical-technologies-evolving-tactics-and-strategies
6. Korda, D. R.; Dapaah, E. O. (2023) The Role of Cyberattacks on Modern Warfare: A Review; *International Journal of Research and Innovation in Applied Science* VIII (VII); : https://doi.org/10.51584/IJRIAS.2023.8733
7. Bajwa, J., Munir, U., Nori, A., Williams, B. (2021). Artificial intelligence in healthcare: transforming the practice of medicine. *Future healthcare journal*, *8*(2), e188–e194. https://doi.org/10.7861/fhj.2021-0095
8. Aiman (2024, December 24) The Final Frontier: Satellite Warfare and the Future of Space-Based Military Surveillance; *Modern Diplomacy;* https://moderndiplomacy.eu/2024/12/24/the-final-frontier-satellite-warfare-and-the-future-of-space-based-military-surveillance/
9. Tripathi, P. (2024, March 2) How hypersonic weapons are redefining warfare; *Observer Research Foundation;* https://www.orfonline.org/expert-speak/how-hypersonic-weapons-are-redefining-warfare
10. Gadeock, S. K. (2023, April 17) Preparing for the Future: The Need for India to Develop Hybrid Warfare Capabilities; *Observer Research Foundation;* https://www.orfonline.org/research/preparing-for-the-future-the-need-for-india-to-develop-hybrid-warfare-capabilities
11. Mimura, N. (2013). Sea-level rise caused by climate change and its implications for society. *Proceedings of the Japan Academy. Series B, Physical and biological sciences*, *89*(7), 281–301. https://doi.org/10.2183/pjab.89.281
12. Anumbe, N., Saidy, C., Harik, R. (2022). A Primer on the Factories of the Future. *Sensors*, *22*(15), 5834. https://doi.org/10.3390/s22155834
13. Munir, A., Aved, A., Blasch, E. (2022). Situational Awareness: Techniques, Challenges, and Prospects. *AI*, *3*(1), 55-77. https://doi.org/10.3390/ai3010005
14. Rashid, A. B.; Kaushik, M. A. K. (2024) AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications; *Hybrid Advances,* Vol. 7, 100277; https://doi.org/10.1016/j.hybadv.2024.100277
15. ibid
16. ibid

17. Bistron, M., Piotrowski, Z. (2021). Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens. *Electronics*, *10*(7), 871. https://doi.org/10.3390/electronics10070871
18. George, S. (2025, February 19) Adani Defence plans to wage a digital war using AI, cybersecurity tools; *The Economic Times;* https://economictimes.indiatimes.com/news/defence/war-in-the-digital-age-ai-cybersecurity-take-command-at-aero-india-2025/articleshow/118151477.cms?from=mdr
19. Teixeira, J., Pais, L., dos Santos, N. R., de Sousa, B. (2024). Empowering Leadership in the Military: Pros and Cons. *Merits*, *4*(4), 346-369. https://doi.org/10.3390/merits4040026
20. ibid
21. ibid
22. Clemente-Suárez, V. J. (2022). New Training Program for the New Requirements of Combat of Tactical Athletes. *Sustainability*, *14*(3), 1216. https://doi.org/10.3390/su14031216
23. Daghfous, A., Belkhodja, O. (2019). Managing Talent Loss in the Procurement Function: Insights from the Hospitality Industry. *Sustainability*, *11*(23), 6800. https://doi.org/10.3390/su11236800
24. Kwak, C.-J., Kim, J.-S. (2021). Improving Disaster Risk Management According to Development Projects. *Risks*, *9*(11), 193. https://doi.org/10.3390/risks9110193
25. Kostopoulos, N., Stamatiou, Y. C., Halkiopoulos, C., & Antonopoulou, H. (2025). Blockchain Applications in the Military Domain: A Systematic Review. *Technologies*, *13*(1), 23. https://doi.org/10.3390/technologies13010023
26. Bu, X.-D., Liu, S.-D., Hou, M., Liu, C., & Zhang, X. (2024). A Novel Self-Adaptation Approach for Multi-Domain Communication Considering Heterogenerous Power Service in Data Centers. *Electronics*, *13*(12), 2334. https://doi.org/10.3390/electronics13122334
27. Licardo, J. T., Domjan, M., Orehovački, T. (2024). Intelligent Robotics—A Systematic Review of Emerging Technologies and Trends. *Electronics*, *13*(3), 542. https://doi.org/10.3390/electronics13030542
28. Tzavara, V., Vassiliadis, S. (2024) Tracing the evolution of cyber resilience: a historical and conceptual review. *Int. J. Inf. Secur.* 23, 1695–1719 https://doi.org/10.1007/s10207-023-00811-x
29. Upadhyay, A. (2024, October 18) Virtual Reality, Augmented Reality, and Warfare; *Observer Research Foundation;* https://www.orfonline.org/research/virtual-reality-augmented-reality-and-warfare
30. Riad, M., Naimi, M., Okar, C. (2024). Enhancing Supply Chain Resilience Through Artificial Intelligence: Developing a Comprehensive Conceptual Framework for AI Implementation and Supply Chain Optimization. *Logistics*, *8*(4), 111. https://doi.org/10.3390/logistics8040111

❐❐❐

UNDERSTANDING TRENDS FROM CONTEMPORARY CONFLICTS APPLICABLE IN INDIAN CONTEXT

Lt Gen (Dr) KJ Singh, PVSM, AVSM (Retd)**

"Those who cannot remember the past are condemned to repeat it."
--George Santayana

Abstract

Traditional wisdom about lessons and template for wars and conflicts have been under severe challenge, in the ongoing conflicts, like the unending Ukraine-Russia war. There are new paradigms and emerging trends, yet it may be bit premature to promulgate and codify them as gospels, without due validation. They may also be specific to contending parties, their allies and catalyzed by peculiarities of terrain and war fighting doctrines applied. Gaza type of operation is unlikely to be replicated by us. Notwithstanding, these realities, it is important to study these and examine them for application in our operational context. Indian Armed Forces have special interest as we also employ similar inventory of Soviet origin platforms. Real life testing of armaments and platforms is the best validation to validate their efficacy. Analysis of performance, efficacy and vulnerabilities would help us to devise mitigation measures in the hardware, as also in employment techniques and doctrines. Many disruptive technologies like drones and commercial ones like Starlinks have made significant difference in outcomes triggering quest for counter-measures, both offensive and defensive. Besides technology, conflict is likely to proliferate in newer domains like cyber, space and cognitive warfare. It is going to be application of Comprehensive National Power (CNP) with 'whole of nation' approach. Trends from Operation Sindoor are flagged and merit further analysis as non-contact, limited duration operation with defined objectives and for dominance of escalation ladder by India.

INTRODUCTION

The world has witnessed two major ongoing conflicts, Ukraine-Russia war (since February 2022) and Israel-Hamas (since October 2023). The war in Ukraine can be traced back to annexation of Crimea by Russia in February 2014 and Gaza conflict to series of unresolved wars in Palestine and Middle East. Under President Donald Trump of USA, attempts to broker cease-fire in both conflicts have intensified, yet they continue to fester. War between Armenia and Azerbaijan seems to have got resolved for the time being with cease-fire. Concurrently, the world continues to be bedevilled by low order of

brewing conflicts/insurgencies, unleashed by Houthis, Kurds, Islamic State in Syria/Levant (ISIS), Hezbollah, Hamas and other militants and even private militias like Wagner Army. This arc of instability currently extends from Mali-Sudan-Syria-Lebanon to Yemen.[1] In addition, more importantly, grey zone warfare in form of coercive posturing by China on Sino-Indian border since 2020 and aggressive deployment and aerial/maritime manoeuvres of Chinese in South China Sea targeting Taiwan need to be very carefully monitored. It will be pertinent to mention that most of these conflicts have been festering for decades and timelines indicated are only for the current round of hostilities. The current round of paused conflict between India and Pakistan, Operation Sindoor-1 could even get re-initiated though chances appear remote.

These conflicts particularly Ukrainian war have been described as the test bed for new technologies and armaments. Even the recent Operation Sindoor tested efficacy of Chinese, Israeli, French, Russian technologies, coupled with indigenous ones. It is axiomatic that these campaigns are analysed with a view to derive trends and lessons relevant in our context. These would act as catalysts for research and development laying down template for modernization and transformation. President Trump's push for peace is unlikely to stop or slow down the military industrial complex. Even PM Narendra Modi had remarked that "it is not era of wars". Despite these assertions, European nations, Japan and South Korea have significantly enhanced defence spending. Well-armed, prepared and ready Armed Forces are the best guarantee for deterrence and peace. It will be apt to quote Mark Twain, "History does not repeat itself, but it does rhyme." The nature of war remains the same but character is increasingly transforming to cyber, non-contact and cognitive domains.

The paper intends to focus on current major ongoing or recently concluded conflicts like Ukraine-Russia war, Gaza conflict, yet draw trends that merit further analysis in our context. The aim is to flag these and simulate further discussions. The subject is analysed in the context of relevance of mapped attributes/trends as applicable in our environment. Relevance and applicability are over-riding criteria for this analysis. However, trends from paused Operation Sindoor are only flagged as these need detailed analysis.

TEMPLATE FOR ANALYSIS

It seems prima-facie risky and somewhat pre-mature to draw lessons from unresolved wars and conflicts, yet some important trends and significant pointers need to be deciphered. In these unending, long-drawn-out conflicts, new paradigms of war fighting specially harnessing of technology are evolving along with possible countermeasures. Many of these pointers and trends may solidify into principles and defining postulates in future. Drone warfare has emerged as proven disruptive technology on battlefield. Drones and Loitering

Munitions have made a significant contribution in the ongoing Operation Sindoor. Long Range and deadly munitions with lethality and precision are providing options in non-contact kinetic domain. Air-Defence surveillance and weapons are emerging as new force-multipliers.

Consequently, salience of tanks and fighter aircrafts has been considerably degraded. Yet notwithstanding, the hasty obituaries, Russian tanks duly fortified are back in Ukraine and modified, even Ukraine has been scouting for Leopards. Fortified Israeli Merkavas have been fielded in Gaza. Retrofitting is particularly relevant in Indian subcontinent, with all nations having large inventory of tanks. On balance, combination of manned-unmanned platforms would be more effective and reliance on single weapon system needs to be reduced.

Emerging inferences in uncertain, dynamic flux of on-going conflicts need to be not only validated but also customized to the local environment and terrain. In our context, in Ladakh, drones and much touted Chinese technology like microwave weapons are likely to have limited efficacy due to high altitude and environmental factors. Israeli forces were recently leading attacks into Gaza with fortified Merkava-4. In contrast, India prefers to secure populated areas with combined arms teams and limits employment of tanks in urban warfare. Hence, appropriate lessons as per our war fighting doctrines and for application in rural/semi-urban areas have to be postulated. An optimum mix of technology and well-trained human resource is the way forward.

India is not really in the conflict crucible of Middle East North Africa (MENA) and the latest hot-spot of Eurasia, yet we have serious existing challenges posed by aggressive China and Pakistan on our borders with proxy-wars fostered by external abettors. More importantly, our adversaries are increasingly in collusive mode. The conflicts seem to be ever present, though latent and lurking in the shadows.[2] They get triggered by surprise and isolated events like Hamas raid in Gaza on 7 October 2023, even when the region was headed for an impending re-rapprochement between Israel and Saudi Arabia. In a recent interaction, two of our former Chiefs on digital media have flagged internal challenges as our main threats, hence, the need is to keep our guard up and be vigilant against both external threats and internal fault lines. The recent dastardly attack in Pahalgam has validated gravity of internal challenges, often vectored as proxy war.

MAPPING-EMERGING MACRO TRENDS

The evolving nature of contemporary conflicts reveals several interconnected factors that shape the strategic environment. Some of the important ones have been discussed in the following paragraphs:

- **Application of Force:** The first defining trend is that application of kinetic force has limited effect and utility. It is certainly not adequate for a decisive end-state. Putin's so called special operations, designed to capture Kyiv and effect regime change (in the garb of de-Nazification) to ensure neutrality or keeping away western powers was planned to be achieved in two weeks. It started in February 2022, the conflict has entered fourth year. This notwithstanding, the fact that annexation of Crimea and areas in Donbas region by Russia, started in 2014. Even the planned counter-offensives by both sides are stalemated with negligible progress. Similarly, Israeli Defence Force (IDF) operations in Gaza launched in October 2023 are unlikely to ensure lasting peace. Resource control, huge technical asymmetry and relentless operations are yet to get IDF, the desired objectives and end state despite passage of 21 months. In our context, resolute stand adopted by India in Ladakh has certainly derailed Peoples Liberation Army (PLA) game-plan of forcing India into capitulation and scoring uncontested grey zone victory. The slew of measures leading to de-escalation in Depsang and Demchok validate this inference with softening of Chinese stance. Corollary to this emerging paradigm is preference for non-contact kinetic exchange in limited conflict as applied by India in Operation Sindoor.
- **End State and Exit Options:** As a complementary inference, it will be pragmatic for nations to avoid belligerence and application of kinetic force. Even if forced into it, it will be prudent to stipulate realistic goals with clearly defined end-state. It is also axiomatic to build interim exit options, which may be required for conflict termination and face saving. Both Putin and Zelinsky seem to be caught in a never-ending logjam and ego-trap, on this account. Even in Gaza, Hamas's objective of getting the focus back on Palestine and Gaza seems to have turned into wanton destruction and suicidal. Despite complete ascendancy, securing the release of hostages has been tortuous exercise accompanied with and significant concessions. Calibration of response strategy after Pahalgam attack starting with politico-diplomatic measures and suspension of Indus Water Treaty (IWT) is indicative of mature approach and exploitation of non-kinetic measures, to set the stage for retribution kinetic actions. Operation Sindoor with non-escalatory and proportionate targeting merits further analysis for achieving cessation of hostilities after mere 88 hours of non-contact, kinetic matrix.
- **Duration of Conflict and Aftermath:** The next major corollary is debunking of long held belief that wars are likely to be short, swift and decisive. In the India-Pakistan context, the 14 days operational cycle was being used as a template with Air Force recommending discrete

operational cycles. Consequently, stocking and war reserves were being revised and planned for 21 days of combat. Long drawn-out conflicts with indeterminate objectives are more likely to be the norm and the new normal in future. Mere 88 hour paused Operation Sindoor needs to be further analysed. In addition, conflicts are likely to degenerate into extended hybrid wars/insurgencies, especially in Palestine, where Hamas may get temporarily marginalized, albeit only till more dangerous variant of Hamas sprouts in its place. Joseph Nye noted analyst has opined that "promise of short war is seductive".[3] Wanton destruction of population centres is becoming the new normal- Aleppo, Grozny, Mariupol and Gaza have been razed to ground. Conflicts are invariably being accompanied by humanitarian crisis with large scale civilian casualties and displacement of refugees.

- **Defence Lines:** Another major trend is, validation of the seminal maxim that no defence line is impregnable, especially in the face of determined Fedayeen's like Hamas. The famed Gaza Barrier has got added to compromised ones like the French Maginot and German Siegfried Lines (World War-II), Berlin Wall (Cold War) and Barlev Line (1973 Arab Israeli war), just to list the important ones. While breaching of defence lines is inevitable, it is the immediate response that is the key imperative. IDF slipped up badly on this account during audacious Hamas raid. It has been repeatedly seen that information though available and in plenty, is not collated and analysed to convert it into operational and actionable intelligence. Hence, timely analysis of information and surveillance are most important. We certainly need to revamp our analytics of surveillance and intelligence structures/mechanisms, as we have been repeatedly surprised in Kargil (1999) and again in Ladakh (2020). Continued infiltration in Kathua- Samba belt underscore requirement of surveillance, backed by defence in depth with multi-layered deployment along with agile Quick Action Teams.
- **Resilience and Sustenance:** For long conflicts, nations need to build resilience in logistics chain and spurt capabilities, to ramp-up inventories rapidly. It is witnessed that Russia, famed for its depots and military-industrial complex, now scouting for spares and munitions. Attrition and casualties have resulted in crisis in numbers and boots on ground. Russia has been tapping countries like North Korea, India, Sri Lanka, Nepal and African nations. It has also led to proliferation of mercenaries, private militias and contractors to maintain combat strength with human element on front lines.
- **Whole of Nation Approach and Civil Military Fusion:** At one time, India was planning, stocking for just 21-days, intense conflict. With long

and festering wars, it is time to adopt a 'whole-of-nation' approach, with civil-military fusion, enabling dual-use technologies and applications. An apt example is fielding of Elon Musk's Commercial of the Shelf (COTS) satellite communications, Starlinks terminals by Ukrainians to circumvent Russian electronics warfare.[4] Another interesting aspect is use of crowd funding in Ukraine to field low-end drones like the employment of ham operators in world wars. Fielding of such dual use devices is the obvious and economical way forward. These conflicts have literally become trial and testing ground for armaments. Large manufacturers are exhausting munitions, nearing the end of their shelf-life. In a no victor, no vanquished scenario, the only winner seems to be the military-industrial complex with bulging order books. We also need to boost our defence industry eco-system and infuse dual-use stakes through civil-military fusion.

- **Drones- Disruptive Game Changer:** It is seen that disruptive effects like top-attack by armed drones and loitering munitions, like Turkish, Bayraktar-TB2 drones, Switchblade 'Kamikaze', Israeli- Harpys and Harop loitering munitions, have given out of proportion results. The biggest advantage is their affordability, coupled with ease of production/ assembly.[5] In Ukraine, they have become cottage industry and hobby activity with proliferation of assembly kits.[6] Ukraine launched 'Million Drone Army'.[7] They have also been versatile and lethal in application against tanks, ships and other bigger targets. They are finding application for surveillance, communication and combat logistics.
- **Long Range Vectors and Missile Shields:** Transition to non-contact domain has been catalysed by precise and lethal long-range vectors. This is being countered by missile shields - Iron Dome and air-defence systems- IACCS and Akash Teer as evidenced in Indian context during Operation Sindoor.
- **All Arms and Integrated Battle Groups:** The quest for the elusive silver-bullet or game-changer weapon is never ending but is unlikely to yield a conclusive result.[8] No single weapon like tanks, fighter aircrafts or even current favourite, drones can win battle on their own. The most obvious, case in point is the pre-mature sounding of death-knell for tanks, consequent to disruptive top-attack effects, unleashed against Armenian tanks. In rear guard action, tanks are already getting retrofitted with cage-like structures as part of Tank Top-Attack Survival Kits. In addition, high end Active Protection Systems like Trophy and Shtora are being fitted and tanks fielded within Air Defence envelope and umbrella. Drones and anti-drone measures are being incorporated on Zorawar light tank, under development. In aerial domain, manned-

unmanned combinations integrating aircrafts/helicopters with drones are being fielded. The crux is synergistic application of combined all arms teams duly backed up by smart logistics. In sum, it is optimum mix of existing and emerging weapons, more importantly, correctly applied by efficient and resilient crews.[9]

- **Relevance of Training:** Nations strive for technological asymmetry, yet a determined adversary doesn't allow adversary to acquire debilitating advantage by closing the gap. It is established that technology has limits, and human element has continued relevance.[10] To harness technology well, training remains critical, best technology can be wasted by untrained crews and lack of motivation. Inability of USA to achieve desired objectives in Vietnam, Iraq and Afghanistan validate this point. Human elements and operators (men/women) behind machine (guns) remain very much relevant. This is especially relevant in high altitude, where environmental factors degrade equipment performance. The correct training and application of tactical concepts like dispersion, convoy discipline and intelligent use of ground would have drastically reduced Russian casualties in Ukraine. In this context, it is relevant to recall Indian crews exploiting their improvisation (jugaad) in antiquated Centurion tanks to defeat much superior and modern Patton (M-48) tanks in 1965 war. Another example is audacious employment of helicopters along with floatation of tanks in 1971 war to bounce the formidable Meghna River and effect a siege on Dhaka from the most unexpected direction. In essence, well trained and motivated human capital can offset technical asymmetry to a reasonable extent. Ukraine war has thrown up ample improvisations and utilisation.
- **Vulnerability of Nuclear Installations in Combat Zone:** The most worrying aspect has been that nuclear installations like power plants are getting caught up in combat zone. In the Ukrainian conflict, ancillary facilities of Zaporizhzhia, nuclear power-plant were damaged, while in Gaza conflict, Israeli Sdot Micha base, housing Jericho missiles, was targeted by Hamas rockets, likely accidentally. In both cases, luckily, nuclear hubs were not impacted and there was no radiation fall-out. More recently, Indian missiles targeted bases in proximity of Pakistan nuclear facilities at Kirana Hills. It underscores the need to ring-fence such facilities as danger of radiation fall-out and proliferation are very real.
- **Proliferation of Nuclear Threat:** Any attempt to reduce or surrender nuclear stockpile is unlikely to find traction, in the light of Ukrainian experience. It had surrendered its arsenal in 1994 in return for a Russian nuclear umbrella and guarantees. In case it had retained its weapons,

the same would have deterred Russians. It was predicted by John Mearsheimer that without nuclear weapons, Ukraine will be subjected to war.[11] Consequently, the quest for nuclear weapons and retaining them is likely to increase. Iran seems to be the next serious contender and on the verge of threshold limits, in this quest.

- **Limited Utility of Alliances and Transition:** Security alliances like North Atlantic Treaty Organization (NATO) or less formalized ones like QUAD as a hedging strategy are unable to ensure requisite deterrence.[12] Ukraine has got caught in such a pincer as its partners are most reluctant to put boots on ground; in fact, fatigue is creeping in on the issue of material support. In effect, such linkages have severe limitations and at best support can come in the form of resources, but operating crews need re-orientation. President Trump has overturned the very cohesion of NATO sending European nations scampering to put together collective European effort without the US.
- **Transition and Self-reliance:** Fielding of such externally supplied armaments by allies, like American F-16 and German Leopard tanks have drawbacks, in terms of training and complexities of integration in the existing combat architecture, surveillance, communication and command grids of the beneficiary. For Ukraine, it's a transition from Russian to Western inventory is a serious challenge. We are going to face similar challenges as we are reducing dependence on Russian equipment. In our context and in a larger context, we must build smart partnerships, integral capabilities and concurrently strive for self-reliance (Atam-Nirbhata).[13]
- **Chinese Reticence:** In the power play, China has opted to remain in the background in physical involvement in conflicts. This trend is witnessed even in United Nations force deployment with minimal deployment of troops. It bears reiteration that performance of the People's Liberation Army (PLA) in Sudan and Chinese drones in Syria has been sub-optimal. Chinese reluctance remains a moot question.
- **Dynamic Geo-strategic Flux:** The basic paradigm of national interests being enduring and long term is undergoing a radical shift in polarized, binary flip-flops at the apex level of security management, especially in the USA. This is starkly evident in the transition from President Obama's 'Pivot to Pacific' to President Trump's 'Fortress America' and Make America Great Again (MAGA). Now, we are witnessing President Biden's QUAD and Build Back Better World (B3W). Concurrently, focus on NATO, dealing with Russia and China has drastically changed between Democratic and Republican dispensations. Even in China,

transition from Deng's 'Hide your Shine-Bide your Time' to Xi's Wolf-Warrior aggressive China surprised many, like India. The lesson for us is to endeavour to forge bipartisan consensus on key security challenges and promulgate a clearly defined long-term national security strategy.

- **Cognitive Warfare and NonTraditional Domains:** Conflicts are increasingly characterized by relentless narrative wars on social media, electronic and print mediums, which were highlighted in Ukrainian conflict.[14] In Gaza conflict, it is concurrent clash of two narratives-Terrorist Hamas vis-a-vis genocide in Gaza. Cognitive warfare is only going to escalate and proliferate. It's important to be suitably prepared for it with policy, organizations (like PLA's Strategic Support Force) and training. Competition and contests including conflicts are proliferating in emerging domains like Cyber, Space, Artificial Intelligence (AI), Robotics and Autonomous Weapons backed by quantum computing. It will be pragmatic if certain basic global norms and protocols are devised for these domains like Chemical, Biological, Radiological and Nuclear (CBRN) protocols. In our context, concerted research and development (R&D) in AI, autonomous platforms and quantum computing as also upgrading organizations in cyber and space domain is recommended.
- **Increased Relevance of Geo-Economics:** Geo-strategy is yielding ground to geo-economics, hence there are conflicts in economic domain like rare earth, energy supply through application of sanctions. In addition, the sabotage of Nord-Stream pipeline disrupted energy supply to Europe from Russia. However, economic coercion through sanctions have limited utility as has been the effect on sanctions on Russian energy supplies. It is also apparent that economic interdependence is not enough to prevent conflicts. Ideally, it must be judicious application of smart power combining soft and hard power.[15]
- **Clash of Connectivity Corridors:** Connectivity is another new frontier for power projection, which was flagged by Mike Pompeo, former US Secretary of State, when he dubbed Chinese connectivity corridors like Belt and Road Initiative (BRI) as more geo-strategic than economics driven. The American counter strategy is routed through India Middle East Economic Corridor (IMEC); however, it is currently under a shadow due to the conflict in Gaza. The US establishment has claimed that Hamas raid was an attempt to disrupt IMEC initiative. Chinese Maritime Silk route including Kra Canal project are attempts to overcome the Malacca dilemma and build energy security. India must remain vigilant about these challenges and stay invested in relevant connectivity corridors like International North-South Transportation Corridor (INSTC), Chabahar, Kaladan besides IMEC to build redundancies.

CONCLUSION

The seminal wisdom, change is the only constant is most relevant in the security domain. Maverick leaders like President Trump and Elon Musk are literally rewriting the rule book and winding up security structures/establishments. Our Armed Forces are undertaking major transformation and modernisation, hence it is important to keep track of emerging trends and analyse them in our context and operating template. In a theatre-based force, it will require fine balance and interfacing between services and theatres. Individual Services and joint training establishments will have to validate these. Theatres would have to absorb and apply them through interfacing mechanisms after due validation in war games and test bedding them in the formation battle schools. In sum, for us, it is keeping ahead in the learning curve, validation and customisation to suit our environment. He was conferred with Maharaja Ranjit Singh Chair in Punjab University. He is regular columnist and has recently authored his highly acclaimed book, General's Jottings.

❖❖❖

Lt Gen (Dr) KJ Singh, PVSM, AVSM (Retd)** is former Western Army Commander and Sikkim Corps Commander. After re-attirement, he was Advisor to CM Haryana and State Information Commissioner. He was conferred with Maharaja Ranjit Singh Chair in Punjab University. He is a regular columnist and has recently authored his highly acclaimed book, General's Jottings.

NOTES

1. Global Conflict Tracker, https://www.cfr.org
2. Singh KJ Lt Gen, General's Jottings, (Chandigarh, The Browser, 2024),p-3.
3. Nye Jr Joseph S, Old and New Lessons from Ukranian War, (Australian Strategic Policy Institute, The Strategist), https://www.aspistrategist.org
4. Nye Jr Joseph S, Old and New Lessons from Ukranian War.
5. Chinoy Sujan R, Tech Wars or Old Battlefields: Lessons from the Recent Conflicts, Raisina Edit 2024 https://www.orfonline.org/expert-speak/tech-wars-or-old-battlefields-lessons-from-the-recent-conflicts
6. Liang Schori Christina Dr, Ten Lessons from Russia-Ukraine War, Geneva Centre for Security Policy, https://www.gcsp.ch/publications/ten-lessons-russia-ukraine-war
7. Liang Schori Christina Dr, Ten Lessons from Russia-Ukraine War.
8. Sukman Daniel Col, US Army, Something Old and Something New- Lessons from Ukraine-Russia, https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/Lessons-Ukraine-Russia-War/
9. Nye Jr Joseph S, Old and New Lessons from Ukranian War.

10. Sukman Daniel Col, US Army, Something Old and Something New- Lessons from Ukraine-Russia.
11. Mearsheimer, John J, The Case for Ukranian Nuclear Deterrent, (Foreign Affairs, Summer 1993), https:// www.foreignaffairs.com
12. Sharma Rakesh, The Ukraine-Russia War-Military Lessons for India, https://www.natstrat.org/articledetail/publications/ukraine-russia-war-military-lessons-and-legacies-for-india-133.html
13. Tiwari Subham, 10 Lessons from Russia-Ukraine War as it Enters Third Year, India Today, Feb 24, 2024 https://www.indiatoday.in/world/story/russia-ukraine-war-10-lessons-from-war-as-it-enters-third-year-2506521-2024-02-24
14. Chinoy Sujan R, Tech Wars or Old Battlefields: Lessons from the Recent Conflicts
15. Nye Jr Joseph S, Old and New Lessons from Ukranian War.

❐❐❐

TRANSMOGRIFICATION OF THE MDO CONCEPT, ASSESSING MDO CAPABILITIES OF CHINA AND IMPLICATIONS FOR INDIA

Col Nayyer Siddiqi

Abstract

Since the US National Defence Strategy of 2018 introduced the term Multi Domain Operations it has become the US defence hierarchy's new Shibboleth. The ibid concept extends the traditional domains of land, air and sea by incorporating the newly introduced space and cyber domains. US prior to 2018 had focused its military effort towards the Global War on Terror (GWOT). However, the growing Anti Access Area Denial (A2AD) capabilities of Russia and China are the likely triggers for the development of the Multi Domain Operations Concept. The concept though being espoused since 2018, may need additional time for full adoption (even by the US) due to lack of a formalised hierarchy for the Space and Cyber domains which are normally dominated by civil organisations. The article aims to do an analysis of the evolving MDO concept together with future Chinese MDO capability assessments which may produce important indications for modernising Indian military operations, policy formulation for MDO adoption and warfighting approaches.

INTRODUCTION

Multi Domain Operations (MDO) emerged because of technological progress in space and cyber domains to counter Russian and Chinese revisionist powers. The US introduced the term in its 2018 National Defence Strategy before other militaries across the world modified the 'MDO Concept' to match their geo strategic needs and operational capabilities. The term 'MDO' may therefore not refer to a rigid well-defined concept or 'set of rules'. Not lagging far behind the United States, the People's Liberation Army (PLA) have created their own version of MDO called Multi-Domain Precision Warfare (MDPW) (likely to parallel the original idea). The development of Multi Domain Operations (MDO) concept began in US in the year 2010 wherein the US Department of Defence (DoD) identified that domain specific approaches focusing separately on land, air, sea, space and cyberspace were not adequate to combat the cross domain strategies.[1] The US Army and Air Force identified that there was a perceptible shift now in the character of warfare wherein China and Russia could leverage advanced technologies like hypersonic weapons, cyber tools and antisatellite capabilities to counter force projection in multiple domains simultaneously.[2] After conducting Counter Insurgency (CI) Operations in Iraq and Afghanistan, the

US military veered towards 'revisionist powers of Russia and China' as clearly given in US 2018 National Defence Strategy.[3] The conflicts earlier waged by US involved air campaigns preceding land offensives, however, the Anti Access Area Denial strategies developed by China and Russia highlighted the need for a framework to counter integrated multi domain threats.[4] The official designation of Cyberspace as a separate domain in itself of warfighting in the year 2011 by the US DoD accelerated the development of this concept.[5] The U.S. Army formally introduced the MDO concept in 2016-2017 through the Multi Domain framework, later refined as Multi Domain Operations in 2018.[6] This article looks at the genesis of MDO, its transmogrification, evaluates China's capabilities to execute MDO versus those of India, analyses the gaps and challenges in India's capabilities to execute MDO and finally lists out measures to overcome these gaps and challenges for India's military modernisation.

GENESIS OF MDO

The MDO concept has been crystallising since 2014, with Russia's invasion of Crimea being a powerful catalyst for American military and civilian experts in the US Department of Defense.[7] Combining successful elements of earlier concepts, American thinkers base the concept on the doctrinal principles of air-land battle, applied to an expanded and integrated battlespace that involves incorporating new domains such as Space, Cyber, Electromagnetic Spectrum (EMS) and the Information environment in addition to the traditional land, sea and air. As illustrated in the figure below the EMS enhances space, providing essential capabilities for air, land and sea domains, hence enabling influence or control over the human domain.[8] The interdependence of domains involves generating a situation in which failure in one area triggers cascade repercussions in one or more domains.

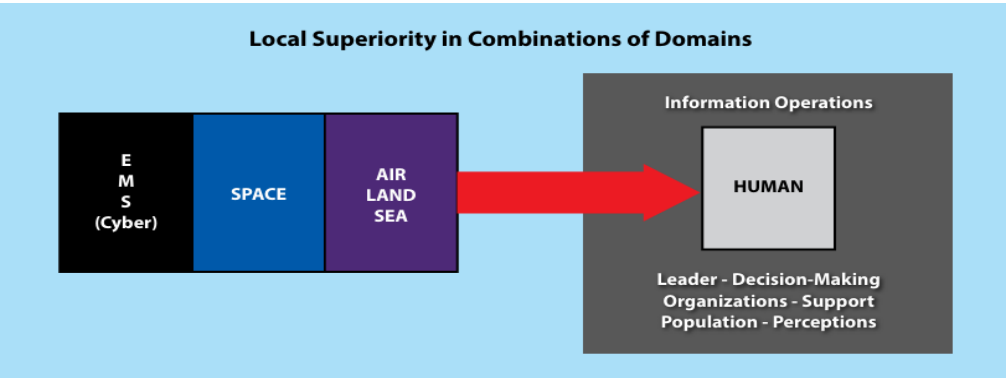


Figure 1: Continuum of Domains and their Interdependence. Source: Dr. Jeffrey M. Reilly. Multidomain Operations: A Subtle but Significant Transition in Military Thought.

Also, establishment of the Cognitive Hierarchy is a key enabler for Multi Domain Operations. The Cognitive Hierarchy diagram shown below serves as a practical blueprint for implementing the principles of MDO in live, complex and contested environments. It shows how raw data collected from the battlefield is transformed step-by-step into actionable decisions through layers of processing. Each layer's transition into another layer reflects a shift in complexity, abstraction and strategic value. As threats become more distributed and complex, the relevance of such models will continue to grow across all domains of conflict, land, sea, air, space and cyber.[9]

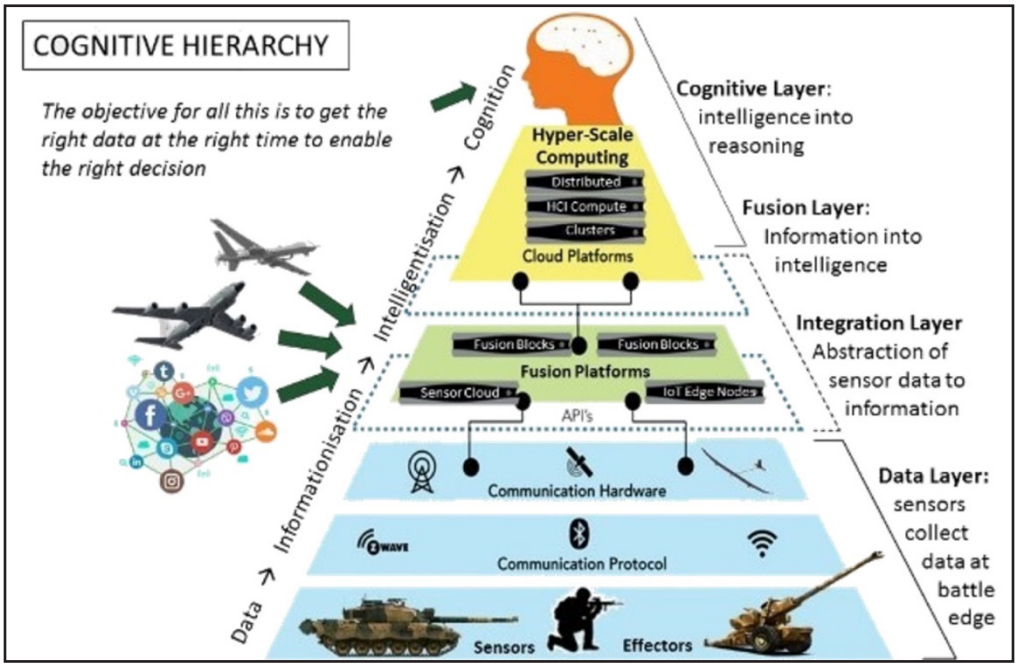


Figure 2: Cognitive Hierarchy of Multi Domain Operations. Source: Crilly Martin. Multi-Dimensional and Domain Operations (MDDO).

The MDO Concept describes how the Joint Force and its partners converge capabilities to create windows of superiority that enable cross-domain manoeuvre to include manoeuvre physically, virtually, cognitively, or any combination, executed simultaneously across the expanded battlespace. It seeks to directly attack critical vulnerabilities in the adversary's systems and foil his plans in different ways to create multiple dilemmas for the enemy. Creating multiple physical, virtual and cognitive dilemmas for the enemy overwhelms the adversary's systematic approach to fracturing friendly forces' cohesion and allows the Joint Force and partners to achieve friendly objectives.[10] A resilient technical architecture provides connectivity to pass critical information

between headquarters, units, aircraft or ships at critical moments in operations. Flexible command relationships allow the rapid reallocation of multi-domain capabilities and formations across functional components and echelons to achieve convergence.

TRANSMOGRIFICATION OF THE LEXICON AND ITS DEMYSTIFICATION

Having seen the genesis of the MDO concept, it is pertinent to note how it is being evolved further by another militaries. As explained by Brig Richard Simpkin in his brilliant work 'Race to the Swift', an evolution in the method of warfighting is usually preceded by a technological development. For instance, the development of the AFV also led to several contending military theories being hypothesised in the immediate aftermath of World War I, Russian thinkers like Mikhail Tukhachevskii (Deep Operation Theory), British thinkers like Basil Henry Lidellhart (Indirect approach) and Bewegungskrieg (Manoeuvre Warfare) by the Germans essentially were 'developed to use the existing modern technology (i.e. AFVs) in the most advantageous way'. One can draw a parallel with the beginning of previous century when we are on the cusp of a significant evolution in the method of warfighting. The figure below visually maps the correlation between technological innovations and corresponding peaks in military theories. It emphasises on how changes in warfare technology have historically triggered waves of military theory and doctrinal development. Each technological leap causes a corresponding increase in military theorising.[11]

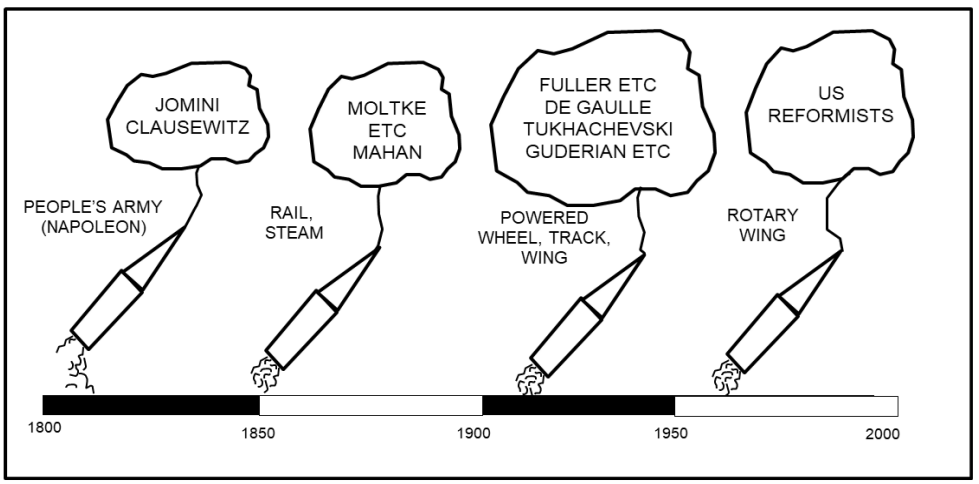


Figure 3: Innovations in technology and peaks in military theorizing. Source: Richard Simpkin. Race to the Swift.

Like the AFV, there have been strides made in the domains of space, cyber as also new age weapons like hypersonic weapons, precision ammunitions, stealth technology and unmanned platforms. As was the case in the immediate

aftermath of World War I (and contemporary development of AFV), these technological advancements have led each advanced military to develop its own version of Multi Domain Operations Concept. The concept while initially espoused by US in 2018, is now getting tweaked by each advanced military to suit its own geo-political realities and capabilities leading to transmogrification of the concept. While the common theme is a strategic framework to synchronise capabilities across land, sea, air, space, cyber and electromagnetic domains. The figure below illustrates the historical trajectory of military innovation and associated doctrinal development over the decades culminating in the contemporary concept of Multi-Domain Operations (MDO). This visual timeline traces how technological advancements in each era have served as catalysts for military theoretical evolution. Each innovation ushering in a corresponding wave of new operational doctrines. Each major technological disruption led to a revolution in military theory, eventually converging in the 21st century's demand for seamless, synchronized operations across all warfighting domains the core of MDO.

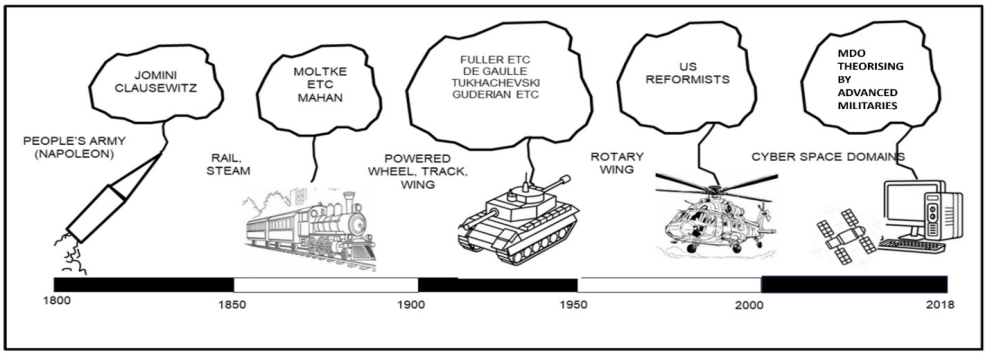


Figure 4: Technological developments propelling MDO theorising by advanced militaries. Source: Author

The succeeding paragraphs discuss these specific attributes of each nation's version of Multi-Domain Operations.

The United States: The US military executes MDO through Joint All-Domain Command and Control (JADC2), which provides real-time connectivity between sensors, platforms, and decision-makers across all domains.[12] Through Artificial Intelligence (AI), cloud computing, and 5G networks, the United States unifies data from different systems, including satellites, drones, ships, and others, into a single operational picture. The Advanced Battle Management System (ABMS) of the Air Force and Project Convergence of the Army serve as examples to test integration capabilities.[13] The annual exercise Project Convergence 2023 linked assets across Army, Navy, Air Force and Space Force to execute quick AI driven targeting against simulated threats using MDO capabilities.[14] The 2018

'Multi-Domain Operations 2028' doctrine provides direction for implementation by focusing on 'convergence' (the ability to mass effects across domains faster than adversaries can respond).[15] The integration of services and legacy systems and cybersecurity vulnerabilities present probable challenges to successful implementation. The figure below illustrates U.S. Army's Multi-Domain Operations (MDO) concept. It outlines how integrated military efforts across multiple domains (land, air, sea, cyber and space) can counter adversary stand-off strategies. It illustrates the breadth of activities, spaces, distances and interrelationships for which MDO must account. It presents a holistic and synchronised approach to warfare, showcasing how U.S. can penetrate and disrupt adversary A2/AD systems across multiple domains.

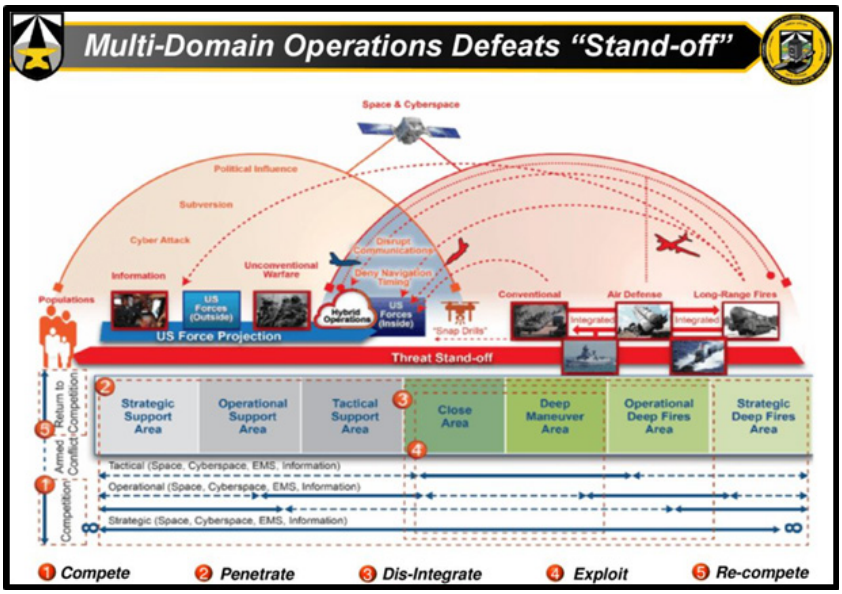


Figure 5: MDO vs Standoff (A2AD Strategy). Source: Two day learning curriculum on MDO by US Army Future Command

China: China's People's Liberation Army (PLA) implements its version of MDO as Multi-Domain Precision Warfare (MDPW), adopted in 2021, focusing on precision strikes and information dominance.[16] The PLA integrates its Strategic Support Force (SSF) to coordinate space, cyber and electronic warfare, supporting kinetic operations with systems like the DF-26 missile and BeiDou satellite network.[17] China employs AI-driven command platforms and autonomous weapons (e.g. loitering munitions) to enhance decision-making and target adversary weaknesses, as seen in South China Sea exercises. Civilian technologies from companies like Huawei (5G) and commercial satellites bolster military capabilities, enabling seamless domain integration.

MDPW prioritises Anti-Access/Area-Denial (A2/AD) to deter US forces in the Indo-Pacific, tested through live fire drills near Taiwan.[18]

Russia: Russia implements MDO through a hybrid approach, blending conventional, cyber and electromagnetic capabilities to achieve strategic effects, often under its 'New Generation Warfare' concept.[19] Operations in Syria and Ukraine showcase Russia's ability to combine air strikes, electronic jamming (e.g. Krasukha-4 systems) and cyberattacks to disrupt enemy command and control. Russia deploys advanced Electronic Warfare (EW) systems like the Murmansk-BN to jam NATO communications, paired with hypersonic Kinzhal missiles for kinetic effects.[20] The Russian military uses disinformation campaigns in cyberspace to shape narratives, as seen in the 2014 Crimea annexation, complementing physical operations. Russia's approach emphasizes flexibility over rigid doctrine, adapting MDO principles to its resource constraints and asymmetric goals.

NATO: NATO and its allies, including the UK, France and Australia, implement MDO through collective exercises, interoperable systems and shared doctrines to counter threats from Russia and China. NATO's Steadfast Defender 2024 and Australia's Talisman Sabre 2023 integrate air, sea, land and cyber forces from multiple nations, testing MDO against simulated peer adversaries.[21] The UK's Future Combat Air System (FCAS) and France's Rafale upgrades incorporate space and cyber capabilities, while NATO's Allied Command Transformation develops MDO frameworks. NATO's Multi-Domain Operational Concept emphasises standardised data sharing platforms (e.g. Link 16 enhancements) to enable military operations.[22] In the Baltic region, NATO integrates cyber defences with air patrols and naval deployments to counter Russian hybrid threats. Based on the above, shown below is a 'visual comparison to the approach to MDO by various nations' and NATO Allies (Figure 6: Comparative Approach to Multi Domain Operations). The diagram presents the author's visualisation on level of emphasis (Y axis, scale 1-5) on key components of MDO (shown on X- Axis). The emphasis levels (1–5) are author accessed scores based on open-source policy analysis, military exercises and capability demonstrations rather than direct quantitative data. US shows a well balanced, high level emphasis across all domains, with strong capability in AI, precision and interoperability. China mirrors US but places slightly less emphasis on interoperability. Russia focuses more on electronic warfare and disinformation, with less emphasis on interoperability. NATO excels in interoperability and AI, with a conservative posture in precision and space.

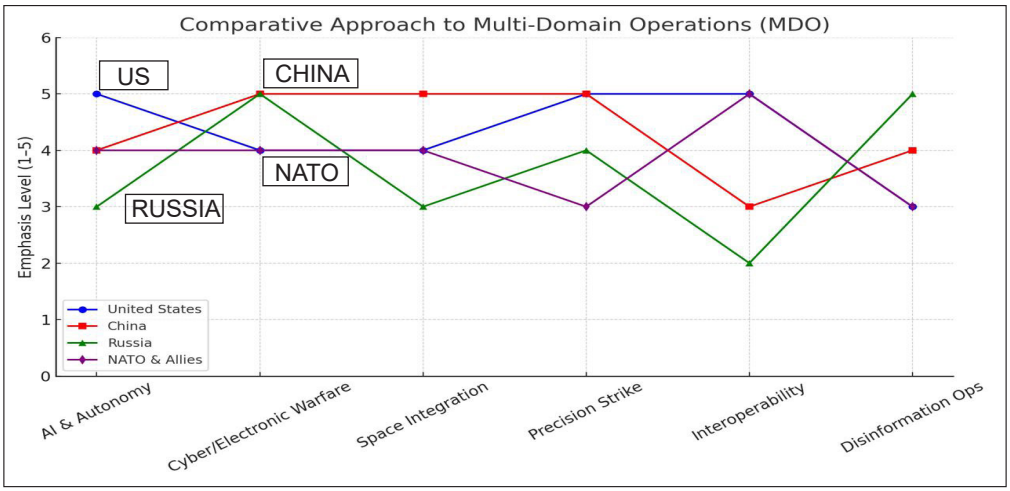


Figure 6: Comparative Approach to Multi Domain Operations. Source: Author

COMPARISON OF CHINA'S MDO CAPABILITIES WITH INDIA

China and India have pursued multi domain integration to project power and respond to multifaceted threats. Their capabilities differ significantly due to variations in resources, technology and strategic priorities. The following paragraphs compares their respective capabilities and integration levels to execute MDO.

Land Domain: The People's Liberation Army (PLA) achieved advanced land domain integration through its 2015 reforms which created five Integrated Theatre Commands (ITCs) to execute joint operations. The commands utilise advanced C4ISR systems to connect land forces with other military domains through command-and-control systems. The PLA strengthens its capabilities through Artificial Intelligence (AI) implementation in ground combat vehicles and Electronic Warfare (EW) systems which are backed by a strong defence industrial sector.[23] The Indian Army operates with intra service command structures which results in 17 single-service commands that prevent effective joint operations. The proposed Integrated Theatre Commands seek to achieve land domain integration, yet their implementation moves at a slow pace. The Indian Army needs to make strides in Make-in-India initiatives to reduce dependence on foreign made equipment and spares.

Air Domain: The PLA Air Force (PLAAF) demonstrates superior air domain integration capabilities through its operation of 200 stealth aircraft including J-20, J-35 and J-36 alongside advanced air defence systems HQ-9. The PLA Strategic Support Force (SSF) boosts air operations through space-based ISR and cyber capabilities which receive AI-powered command and control (C2)

systems for informatised warfare. The Indian Air Force (IAF) lags because it does not possess stealth aircraft, while it continues operating ageing aircraft owing to slow modernisation. The IACCS (India's Integrated Command and Control System) system enhances coordination between forces. The S-400 air defence systems provide strong protection, yet China has deployed them at a higher density than India. The Tejas fighter and other modernisation efforts face production delays and budget constraints that slow down their development, though they are picking up pace row.

Sea Domain: The PLAN benefits from integration achieved through advanced data link systems and centralised command structures under the Northern, Eastern and Southern Theatre Commands, enabling coordinated operations across its large fleet. The PLA Navy (PLAN) has transformed into a blue-water force [Operating two modern aircraft carriers (Shandong and Fujian) and one refitted Liaoning (purchased from Ukraine in 1998)]. One aircraft carrier Type 004 is under construction since 2024. It operates three fleets with Type 055 destroyers and Type 076 amphibious assault ships. The compact and efficient SSF-based sensors, provide ISR (Intelligence, Reconnaissance and Surveillance) for maritime operations, enhancing navigation and targeting capabilities.[24] India's Indian Navy (IN) maintains a geographic advantage in the IOR but lags in terms of scale and technology. Operating two aircraft carriers, including the indigenous Vikrant, the IN's fleet is smaller, with limited replenishment capabilities. Space-based surveillance via CARTOSAT and RISAT satellites supports naval operations, but integration with space assets (e.g. GSAT-7 for Naval Operations) is less advanced than China's. Recent initiatives like the National Maritime Domain Awareness project aims to improve integration. India's IRNSS and GAGAN are being progressed to support military operations.

Cyber Domain: China's cyber capabilities, managed by the SSF's Network Systems Department, are second-tier globally, integrating military units, state-backed hackers and firms like Huawei for offensive and defensive operations. The 2016 National Cybersecurity Strategy highlights cyberspace sovereignty, instituting laws mandating domestic data storage. The PLA's cyber doctrine focuses on the concept of 'pre-emption' to disrupt adversary C4ISR systems. India's Defence Cyber Agency (DCA), established in 2018 needs to be further enmeshed with the military to a similar degree as that of SSF.[25] Limited coordination among agencies like the Defence Intelligence Agency and National Technical Reconnaissance Organisation needs to be further strengthened for India's cybersecurity framework. Reported Chinese cyberattacks on ISRO and power grids underscore vulnerabilities, despite growing public-private partnerships, and enhanced focus is required.

Space Domain: China's space capabilities, overseen by the SSF's Space Systems Department, include over 300 satellites, kinetic and non-kinetic anti-satellite (ASAT) systems, and the BeiDou Navigation Satellite System for autonomous global positioning.[26] The 2007 ASAT test and AI-driven satellite management enhance China's space integration. India's space program, led by the Indian Space Research Organisation (ISRO), is advancing but trails China's. The Defence Space Agency (DSA), established in 2018, is developing integration, with the 2019 ASAT test showcasing capabilities. However, India's 50-satellite constellation is smaller and reliance on foreign GNSS systems like GPS limits autonomy. The DSA's integration into a 'penta-theatre' doctrine is ongoing but incomplete. The table shown below summarises the aforementioned aspects.

INFERENCES FOR INDIAN MILITARY'S MODERNISATION AND WARFIGHTING

The succeeding paragraphs cover a comparison of India's MDO capabilities with those of China's gaps, challenges and strategies for India to implement MDO effectively against China.

GAPS IN INDIA'S EFFORTS TO ADOPT MDO

While India is on the fast track towards modernisation and adoption of MDO, the following gaps exist towards adoption of MDO: -

- **Absence of an Official Doctrine:** India is yet to promulgate a comprehensive and authoritative MDO doctrine akin to those released by the United States or China. The present discourse is primarily derived from concept notes, public statements and internal deliberations.[27] Indian armed forces currently operate without a unified tri-services command structure. Proposed theatre commands are still in the conceptual phase and are subject to institutional debate.[28]
- **Technological Deficiencies:** There is limited development in the domestic development of key technologies essential for MDO like artificial intelligence, real time ISR capabilities and autonomous systems. Furthermore, India's capabilities in space based and cyber warfare tools remain comparatively underdeveloped. The strengths of ISRO and the IT warfare yet to become a 'force multiplier' military.[29]
- **Challenges in Data Fusion and Interoperability:** The lack of joint communication networks among tri services battlefield management systems hampers effective interoperability among the services. Existing communication and data-sharing platforms are not synchronised to a degree which would enable jointness.[30]

- **Need for Doctrinal Revision with Contemporary Threats:** Several components of India's defence posture continue to rely on legacy doctrines, which inadequately address modern hybrid, Grey Zone and non-kinetic threats.[31] The necessity for agile, flexible and real time operational response frameworks is becoming increasingly urgent.

CHALLENGES IN THE ADOPTION OF MDO BY INDIA

Besides the gaps, there also exist certain challenges in the adoption of MDO by the Indian armed forces:

- **Institutional and Bureaucratic Impediments:** A Limited amount of jointness within the services and rigid institutional practices may obstruct integration efforts needed for MDO. The separation between civil and military hierarchies in strategic decision-making processes could also contribute to delayed implementation.[32]
- **Fiscal and Resource Constraints:** Budgetary limitations in Capital Procurement Plans may impede the acquisition and deployment of necessary advanced systems. Competing priorities between maintaining traditional, manpower intensive forces and investing in technology-driven modernisation exacerbate the challenge.[33]
- **Human Capital and Training Limitations:** India currently lacks a unified tri-service training doctrine aligned with MDO requirements. There is untapped potential in specialised domains of cyber, AI and Electronic Warfare.[34]
- **Inadequate Civil-Military Collaboration in Strategic Technologies:** There exists limited synergy between the armed forces and civilian research institutions in fields critical to MDO, including AI, space and cyber domains. The defence research and procurement ecosystem need fast tracking.[35] India's cyber infrastructure remains vulnerable to intrusion. India's offensive cyber capabilities need further enhancement. There is an urgent need to step up against strategic competitors like China in the development of information and cognitive warfare capacities.
- **Unclear Space Domain Strategy:** There is an urgent need to establish an operational military space command or articulate a dedicated doctrine for space-based deterrence or conflict, despite possessing significant space assets.[36]
- **Lack of tools to Achieve Interdomain Effects:** The coordination of the aspects necessary to carry out MDO operations currently seems rather difficult to achieve at the operational level, which aims at innovatively combining the specific tactics of the services to achieve operational and

strategic level objectives. India is currently is need of tools for planning and conducting military actions to achieve interdomain effects.

MEASURES TO OVERCOME GAPS AND CHALLENGES

The succeeding paragraphs provide the measures which India needs to implement to fast track adoption of MDO by the Indian Military.

- **Indian MDO Doctrine:** Indian armed forces should endeavour to establish a Joint MDO Command, unifying the Army, Navy, Air Force and tri-service agencies (e.g. Defence Space Agency, DCA) under a C4ISR network modelled on US JADC2 but tailored to India's needs.[37] Prioritise cost-effective, high-impact systems (e.g., drones, cyber tools) to offset China's numerical and technological edge. Also, there is a need to leverage India's IT sector for AI-driven analytics and autonomous systems, accelerating decision-making against China's 'Intelligentsia' warfare.
- **Establish Unified Theatre Commands:** Expedite the restructuring of the Army's 17 Corps into IBGs (Integrated Battle Groups), with 3 to 4 IBGs per corps, as planned.[38] Prioritise converting pivot corps (defensive formations) into dual-role IBGs capable of both holding ground and limited offensive actions, and strike corps into offensive IBGs optimised for rapid, deep strikes. Aim for 10 to 12 IBGs by 2028.[39] Fast-track IAF integration into the planned ITCs (Northern, Western, Maritime) by 2027, ensuring air assets are dynamically allocated to support Integrated Battle Groups (IBGs) and naval operations. Establish a dedicated Air Operations Cell within each ITC to coordinate MDO.[40] This will need legislative support and inter-service coordination to overcome bureaucratic resistance.
- **Boost Indigenous Defence Production:** DRDO's funding for the year 2025-26 has been 3.2 billion dollars (an increase of 12.41% over the previous year),[41] however, it is only 1.2% of the total defence budget for R&D (much below the global average of 3.4%).[42] Hence, to have indigenous cutting-edge tech, India's investment in R&D needs to increase by at least 15%. Also, India's defence production reached USD 15.34 billion in 2023-24 (an increase of 16.7% from the previous year with the Private Sector contributing 20.8% and PSUs contributing 79.2%).[43] However, to further incentivise the defence production, this percentage must change radically in favour of the private sector. The private sector with well-established players like Larsen and Toubro, Bharat Forge, Tata Advanced Systems and Mahindra Defence Systems should be prioritised over PSUs like HAL, BEL and Mazgaon Dock Shipbuilders Limited (PSUs still dominate production with 85% of the output).[44]

- **Strengthen Cyber Defence:** India's cyber defence suffers from fragmented coordination among agencies like the Defence Cyber Agency (DCA), National Technical Reconnaissance Organisation, and Defence Intelligence Agency. To address this, India must create a National Cybersecurity Command (NCC) modelled on China's Strategic Support Force (SSF) wherein The NCC should centralise cyber operations across military and civilian domains, reporting directly to the National Security Advisor. This would streamline command and control, ensuring rapid response to cyber threats.

  India must also endeavour to legislate a Cybersecurity Framework by enacting a comprehensive law mandating data protection standards, incident reporting and inter-agency collaboration, similar to China's 2016 National Cybersecurity Strategy.

  Advance Space Capabilities: The Defence Space Agency, established in the year 2019 must be evolved into a full-fledged four-star Indian Defence Space Command (INDSPAC) to coordinate tri-service operations. The space operations must be integrated with the IAF's Integrated Air Command and Control System for seamless air and space coordination. Under the INDSPAC, the enhanced scope of the Integrated Air Command and Control System (IACCS) must endeavour to incorporate real-time data from space (satellites), cyber (network monitoring) and ground (IBG sensors). India should exploit AI-driven decision support systems in the IACCS to prioritise targets across domains.[45] Refine India's ASAT capabilities by building on the success of Mission Shakti (2019), which demonstrated India's ability to neutralise a satellite in LEO to counter-space capabilities to deter Chinese space threats. Lastly, India should endeavour to achieve complete independence from GPS and GLONASS by integrating NAVIC and GAGAN with all military equipment. To strengthen ISRO's cyber defence integration, as discussed earlier, increased funding is critical. Earmarking of 5 to 10% of ISRO's budget (Rs.650–Rs.1,300 crore) for space cybersecurity, focusing on AI-driven satellite protection and integration with the ibid INDSPAC, will accelerate military exploitation of India's space potency.
- **Leverage International Partnerships:** Deepen QUAD cooperation for technology transfers in AI, cyber, and space domains. India signed COMCASA with the U.S., enabling encrypted communications; however, similar agreements can be signed with Japan and Australia. Joint exercises with the United States and Japan can enhance interoperability and C4ISR integration. Joint R&D projects within

QUAD for example development of hypersonic defence systems (given China's hypersonic advances), AI-based C4ISR systems will go a long way in developing strategic deterrence against China. Use defence cooperation agreements (e.g US Foreign Military Sales) to procure critical MDO systems like MQ-9B drones and precision munitions at subsidised rates.[46] If such technology for MDO operations is given to India, QUAD can be India's key enabler for becoming a true multi-domain power by 2030.

- **Air Domain:** Besides the aforementioned suggestions on capability development of IACCS, Indian Air Force (IAF) should accelerate induction of Rafale jets and indigenous Tejas Mk-1A fighters to counter China's J-20 stealth aircraft, supported by airborne Early Warning systems like the Netra AEW&C.[47] IAF should further integrate Brahmos air-launched missiles and develop hypersonic weapons to match China's H-6 bomber capabilities. IAF must expand the Integrated Air Defence System with indigenous Akash missiles and Israeli Barak-8 systems to counter Chinese drones and missiles.

CONCLUSION

India's defence budget (USD 81 billion in 2024) lags behind China's (USD 230 billion) but focus on aforementioned cost-effective solutions and private sector involvement can bridge the gap. Our echelons above brigade (Division, Command and Corps) are the linchpin for all of the actions and must be resourced as such. These are more than headquarters. They will be multi-domain capable formations that converge capabilities in all domains and environments during armed conflict. Our current force, although lethal and experienced, requires broad-based modernisation (both force equipping and in integrating capabilities) If it is to accomplish the tasks required to win in future conflict. This concept is integral in developing and testing the capabilities, doctrine, organisations, soldiers, and leaders needed to conduct MDO. Its publication represents the first step toward the development of the future Army force.

❖❖❖

Col Nayyer Siddiqi is an alumnus of Military School Dholpur and National Defence Academy. He is a graduate of Defence Services Staff College, Wellington. He has served as a platoon commander in the Indian Military Academy and Instructor in Gunnery in the School of Artillery, Devlali. He has served as a Military Observer and a Staff Officer in the Military Observer's Regional Headquarters in the United Nations Mission in the Democratic Republic of Congo (MONUSCO).

NOTES

1. U.S. Department of Defence, *Military and Security Developments Involving the People's Republic of China 2023* (Washington, DC: Office of the Secretary of Defence, 2023), 12.
2. Thomas G. Mahnken, *Technology and the American Way of War Since 1945* (New York: Columbia University Press, 2008), 189.
3. U.S. Department of Defence, *Summary of the 2018 National Defence Strategy* (Washington, DC: Office of the Secretary of Defence, 2018), 4.
4. Andrew S. Erickson, *China's Maritime Gray Zone Operations* (Annapolis, MD: Naval Institute Press, 2022), 45.
5. Joint Chiefs of Staff, *Joint Vision 2020* (Washington, DC: U.S. Government Printing Office, 2000), 8.
6. U.S. Army, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: Training and Doctrine Command, 2018), 1.
7. Monoranu, Andrei. "Approaches to the Concept of 'Multi-Domain Operations' in the Doctrinal Vision of NATO and Its Main Strategic Competitors." *Romanian Military Thinking* 1 (2025): 123–135. https://en-gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20reviste/RMT/2025/1/MONORANU.pdf. Accessed on 25 April 2025.
8. Reilly, Jeffrey M. "Multi-Domain Operations: A Subtle but Significant Transition in Military Thought." Air & Space Power Journal 30, no. 1 (Spring 2016): 61–73. https://www.airuniversity.af.edu/portals/10/aspj/journals/volume-30_issue-1/v- reilly.pdf. Accessed on 25 April 2025.
9. Crilly, Martin, and Alan Mear. "Multi-Dimensional and Domain Operations (MDDO)." Wavell Room, January 19, 2022. https://wavellroom.com/2022/01/19/multi-dimensional-and-domain-operations-mddo/. Accessed on 25 April.
10. TRADOC, 'TRADOC Pamphlet 525-3-8 – U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045', December 2018
11. Builder, Carl H. *The Masks of War: American Military Styles in Strategy and Analysis*. Baltimore: Johns Hopkins University Press, 1989.
12. U.S. Department of Defence, *Joint All-Domain Command and Control (JADC2) Strategy* (Washington, DC: Office of the Secretary of Defence, 2021), 5.
13. Sydney J. Freedberg Jr., "Project Convergence: Linking Army Missile Defence, Offense, & Space," *Breaking Defence*, October 12, 2023, 2.
14. U.S. Army, *Project Convergence 2023 After Action Report* (Fort Eustis, VA: Training and Doctrine Command, 2023), 15.
15. U.S. Army, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: Training and Doctrine Command, 2018), 10.
16. U.S. Department of Defence, *Military and Security Developments Involving the People's Republic of China 2023* (Washington, DC: Office of the Secretary of Defence, 2023), 45.
17. Elsa B. Kania and John K. McCaslin, *The PLA's Strategic Support Force and AI Innovation* (Washington, DC: Center for a New American Security, 2021), 25.
18. Michael McDevitt, *China as a Twenty-First-Century Naval Power* (Annapolis, MD: Naval Institute Press, 2021), 145.
19. Charles K. Bartles, "Russia's New Generation Warfare," *Military Review* 96, no. 3 (May-June 2016): 12.

20. Roger McDermott, “Russia’s Electronic Warfare Capabilities to 2025,” *International Centre for Defence and Security*, September 2017, 18.
21. 1Australian Department of Defence, *2023 Talisman Sabre Exercise Report* (Canberra: Commonwealth of Australia, 2023), 22.
22. NATO Allied Command Transformation, *NATO Multi-Domain Operations Concept*, 15.
23. Harsh V. Pant and Kartik Bommakanti, “Towards the Integration of Emerging Technologies in India’s Armed Forces,” ORF Occasional Paper No. 392, February 2023, Observer Research Foundation.
24. “India and China’s space and naval capabilities: A comparative analysis,” Observer Research Foundation, August 11, 2023, https://www.orfonline.org. Accessed on 25 April 2025.
25. “India a third-tier country in cyber warfare capabilities, report says US more powerful than China,” India Today, June 28, 2021, https://www.indiatoday.in. Accessed on 25 April.
26. “India-China Outer Space Competition: Implications for Strategic Stability,” RSIS, March 26, 2025, https://rsis.edu.sg. Accessed on 25 April 2025.
27. Bhatia, Vinod. “Multi Domain Warfare – Future Challenges in the Indian Context.” Centre for Joint Warfare Studies, February 2022. https://cenjows.in/wp-content/uploads/2022/02/2-Lt-Gen-Vinod-Bhatia.pdf; accessed on 10 April 2025.
28. Singh, Arushi. “Multi Domain Operations and India (Part 1).” Wavell Room, November 10, 2021. https://wavellroom.com/2021/11/10/multi-domain-operations-india-1/; accessed on 10 April 2025.
29. Kumar Singh, Gaurav. “Technology Driven Multi Domain Operations (MDO) for Joint Warfighting.” Centre for Joint Warfare Studies, November 25, 2024. https://cenjows.in/technology-driven-multi-domain-operations-mdo-for-joint-warfighting; accessed on 10 April 2025.
30. “Multi-Domain Warfare in the Indian Context.” Defstrat. https://www.defstrat.com/magazine_articles/multi-domain-warfare-in-the-indian-context; accessed on 10 April 2025.
31. Joshi, Shashank. “The Army in Indian Military Strategy: Rethink Doctrine or Risk Irrelevance.” Carnegie Endowment for International Peace, August 2020. https://carnegieendowment.org/research/2020/08/the-army-in-indian-military-strategy-rethink-doctrine-or-risk-irrelevance; accessed on 11 April 2025.
32. Singh, Arushi. “Multi Domain Operations and India (Part 1).” Wavell Room, November 10, 2021. https://wavellroom.com/2021/11/10/multi-domain-operations-india-1/; accessed on 11 April 2025.
33. “Multi-domain operations are the future.” The Tribune. https://www.tribuneindia.com/news/defence/multi-domain-operations-are-the-future/; accessed on 12 April 2025.
34. Kumar Singh, Gaurav. “Technology Driven Multi Domain Operations (MDO) for Joint Warfighting.” Centre for Joint Warfare Studies, November 25, 2024. https://cenjows.in/technology-driven-multi-domain-operations-mdo-for-joint-warfighting/; accessed on 12 April 2025.
35. “Multi-Domain Warfare in the Indian Context.” Defstrat. https://www.defstrat.com/magazine_articles/multi-domain-warfare-in-the-indian-context/; accessed on 13 April 2025.
36. “Multi-domain operations are the future.” The Tribune. https://www.tribuneindia.com/news/defence/multi-domain-operations-are-the-future/; accessed on 13 April 2025.
37. Gurmeet Kanwal, *India’s Joint Military Doctrine: Towards Multi-Domain Operations* (New Delhi: Pentagon Press, 2022), 52.

38. Bommakanti, Kartik. “Integrated Battle Groups: Reforming the Indian Army for Future Warfare.” Observer Research Foundation, August 10, 2020. https://www.orfonline.org/research/integrated-battle-groups-reforming-the-indian-army-for-future-warfare/. Accessed on 20 April 2025.
39. Joshi, Yogesh. “The Indian Army’s Integrated Battle Groups: A New Era of Warfare.” The Diplomat, November 5, 2019. https://thediplomat.com/2019/11/the-indian-armys-integrated-battle-groups-a-new-era-of-warfare/. Accessed on 21 April 2025.
40. Pandit, Rajat. “Theatre Commands: India’s Path to Integrated Warfare.” Times of India, August 2, 2023. https://timesofindia.indiatimes.com/india/theatre-commands-indias-path-to-integrated-warfare/articleshow/102345678.cms. Accessed on 25 April 2025.
41. Indian Defence Research Wing. 2025. “Budget Allocation for DRDO Increased to 26,816.82 Cr for FY 2025-26.” Indian Defence Research Wing, February 2. https://idrw.org/budget-allocation-for-drdo-increased-to-26816-82-cr-for-fy-2025-26/
42. Indian Aerospace and Defence Bulletin. 2024. “India’s Military R&D Investments: A Global Perspective with India’s Strategic Imperatives.” Indian Aerospace and Defence Bulletin, March 29. https://www.iadb.in/indias-military-rd-investments-a-global-perspective-with-indias-strategic-imperatives/ Accessed on 28 April 2025.
43. India Brand Equity Foundation. 2025. “Defence Budget Will Go Up by 9.5% to Rs. 6,81,000 Crore (US$ 78.32 Billion) in 2025-26: Defence Secretary Mr. Rajesh Kumar Singh.” IBEF, February 19. https://www.ibef.org/news/defence-budget-will-go-up-by-9-5-to-rs-6-81-000-crore-us-78-32-billion-in-2025-26-defence-secretary-mr-rajesh-kumar-singh.
44. Economic Times. 2025. “DRDO Boosts Indigenous Defence Manufacturing with Over 2,000 Tech Transfers in 2024: Official.” Economic Times, July 9. https://economictimes.indiatimes.com/news/defence/drdo-boosts-indigenous-defence-manufacturing-with-over-2000-tech-transfers-in-2024-official/articleshow/111614667/cms
45. Katoch, Prakash. “Integrated Air Command and Control System: IAF’s Backbone for Network-Centric Warfare.” SP’s Aviation, June 2023. http://www.sps-aviation.com/story/?id=2987. Accessed on 24 April 2025.
46. Smith, Jeff M. “US-India Defence Trade: Opportunities and Challenges.” Heritage Foundation, June 10, 2023. https://www.heritage.org/asia/report/us-india-defence-trade-opportunities-and-challenges. Accessed on 20 April 2025.
47. Ankit Panda, “Rafale and Tejas: India’s Air Force Modernisation,” *The Diplomat*, January 25, 2024, 10.

❐❐❐

45-59

MULTIDOMAIN OPEARTIONS IN THE EMERGING THREAT ENVIRONMENT: AN INDIAN PERSPECTIVE

Brig Devendra Pandey

Abstract

The concept of Multi Domain Operations was first advocated by the US Army and is slowly being adopted by almost all Arms of the US Armed Forces. Domains of warfare have evolved with evolution of technology. Five universally accepted domains of warfare in current strategic thought are – Maritime, Land, Air, Space and Cyberspace. Russia and China, two identified strategic competitors of the USA, extensively studied the American way of war-fighting demonstrated in two Gulf Wars. China evolved the Anti-Access/Area Denial (A2AD) concept and Russia formulated its new generation warfare capability. Conceptual framework of MDO was postulated by the US Army to counter the new concepts of war by China (and also Russia). It entails penetration of the multi layered defence of adversary, gaining freedom of manoeuvre and disintegrating its A2AD systems. Calibrated Force Posture, Multi Domain Formations and their Convergence in space and time are the three tenets of MDO. The US Army has formed Multi Domain Task Force to conduct MDO.

India with its peculiar geostrategic compulsions has a unique operating environment to deal with. The US model of MDO may not meet the Indian operational challenges. India will have to adopt MDO concept with suitable modifications as per its operational realities and requirements. Two key components for conduct of MDO are - state of the art, all-inclusive Multi Domain Sensors and Kinetic as well as Non-Kinetic Shooters. An automated and networked architecture must be synthesised by seamlessly integrating the two components and their sub components utilising niche technologies like AI, Quantum Computing and Machine Learning. Challenges of organisational peculiarities, civil military relations, Tri Services Synergy and vast requirements of resources will have to be overcome. The ongoing military transformation and rolling out of the Integrated Theatre Commands is an excellent opportunity to parallelly create organisations for adopting MDO by the Indian Armed Forces.

INTRODUCTION

Multi Domain Operations (MDO), as a formally articulated warfighting concept is just about a decade old and is still evolving. The concept of MDO was first advocated by the US Army. It was initially criticised by military thinkers as a ‘desperate attempt by the US Army to find relevance for itself’ in the

emerging operating environment, where the US strategic monopoly was being challenged.[1] Since then, this concept of MDO has been analysed and widely debated amongst the strategic community. It is slowly being adopted by almost all Arms of the US Armed Forces.

Multi Domain Warfare finds a mention in the Indian Army Land Warfare Doctrine of 2018 and other such documents. MDO has been an essential element of the Indian strategic discourse since past few years. Indian strategic community and various Think Tanks have been intensely debating 'MDO in the Indian context'. The ongoing Military modernisation and likely rolling out of the Integrated Theatre Commands in very near future, have made this debate more serious. Indian Armed Forces are at a cusp of transformation. It is relevant at this juncture to analyse various factors and outline how Indian Armed Forces can adopt MDO.

This paper aims to trace the evolution of MDO and outline its enunciated execution by the US Army, since they propounded this concept. It also recommends a way ahead for the Indian Armed Forces to adopt MDO in the emerging threat environment.

DOMAINS OF WARFARE AND OPERATING ENVIRONMENT

From warfare and military operations point of view, the term 'domain' does not have a universally accepted definition amongst the strategic community. NATO explains 'domain' as a "Critical macro manoeuvre space whose access or control is vital to the freedom of action and superiority required by the mission".[2] Other definitions are, "A domain is a space in which forces can manoeuvre to create effects"[3] and "The sphere of influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects."[4] A related term 'Operating Domain' is defined as, "A distinctive sphere of capabilities and activities principally capable of, or optimised for, action in particular environments."[5]

The term 'Operating Environment' is defined as "the surroundings for activities which exist prior to, during and after their occurrence".[6] Joint Doctrine Publication (JDP) 0-01 of the NATO Forces defines the 'Joint Operational Environment' as, "The overall space, conditions and surroundings within which military forces operate."[7] By this definition, an 'Operating Environment' may encompass one, some or all 'Domains'.[8]

Domains of warfare have evolved with the evolution of technology. Till very recently, Land, Air and Maritime used to be considered as three traditional domains of warfare. Space and cyber domains found broad consensus subsequently. Electromagnetic spectrum and information domains were also propagated. New domains of warfare are often propagated by strategic analysts.

In one such classification, "Eight domains- Land, Air, Sea, Subsea, Seabed, EM, Space, Cyber and three matrices- range, speed and precision aided by new talent pipelines, innovation and civil - military fusion are considered essential to deliver 'combat overmatch' in modern warfighting.[9] 'Cognitive Domain' is also considered as a separate domain of warfare by some analysts.[10] However, in the current strategic discourse these are yet to find a wider acceptability.

Five universally accepted domains of warfare in current strategic thought are, Maritime, Land, Air, Space and Cyberspace. Further deliberations in this paper have been restricted to these five domains. 'Cyber Domain' denotes a wider connotation and includes electromagnetic spectrum, electronics and all elements associated with IT equipment.

GENESIS OF MDO

In the contemporary debate around multi domain, the genesis of the term is attributed to an article by Frank Hoffman and Michael C. Davies in 2013.[11] However, some strategic commentators assert that the MDO thinking originated in 2011, when the then Training and Doctrine Command (TRADOC) Commander, who rose to be Chairman of the Joint Chiefs of Staff, General Martin E. Dempsey asked the question: "What's after joint?".[12] General David G. Perkins, the next TRADOC Commander, continued with further development of the MDO concept. It was formally expressed in the US Doctrine in 2017. Initially it was termed as 'Multi Domain Battle (MDB)', probably due to the preceding warfare terms viz- the Air-Land (and Air-Sea) Battle. Multi Domain Battle was primarily a US Army operating concept. It postulated a US response to Russia's New Generation Warfare and China's actions in the South China Sea.[13] The word 'Battle' was subsequently replaced with 'Operations' and the term 'Multi Domain Operations' was adopted. It apparently gives a more comprehensive approach to cater for complexities of the modern conflict.

US ARMY'S CONCEPTUAL FRAMEWORK FOR MDO

The US National Security Strategy of 2017 formally identified China and Russia, as the strategic competitors, "China and Russia challenge American power, influence, and interests, attempting to erode American security and prosperity".[14] North Korea, Iran, and non-state actors like transnational terrorist and criminal organisations were also identified as threat to the US security.[15] However, the focus clearly was on emerging threats posed by strategic competition with China and Russia. The US National Defence Strategy of 2018 reiterated, re-emergence of long-term strategic competition with 'revisionist powers', particularly China and Russia as the central challenge to US security.[16] It identifies statecraft and economic power as well as subversion, coercion, disinformation, and deception as various ways and means through which the

adversaries of the USA can achieve their strategic objectives.[17] The US Army analysed the future emerging operating environment with this backdrop**.** It is perceived to be dominated by a sense of cooperation, collaboration and competition which may graduate to confrontation/ conflict and ultimately lead to a clash or war.[18]

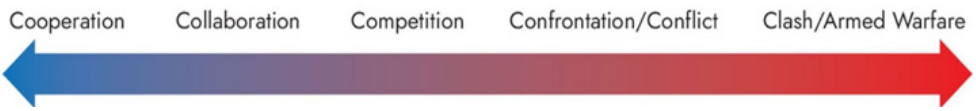


Fig 1, Continuum of Major State Interaction Postures, Source: National Defence University, URL: https://wmdcenter.ndu.edu/Portals/97/Strategic-Assessment-2020.pdf

The competition continuum in the future operating environment is a spectrum from 'cooperation' to 'armed conflict' through 'competition below armed conflict'.[19] Russia and China, two identified strategic competitors of the USA, extensively studied the American way of war-fighting, since Op Desert Storm.[20] To counter the US advantage of joint and combined operations, they have made significant doctrinal, technological and structural advancements. They formulated their own response mechanism. China evolved the A2AD concept and Russia formulated its new generation warfare capability. To counter their designs, the US Army postulated the conceptual framework of the MDO. It visualises a prominent role for the Army during all stages of the conflict continuum.

Fig 2, MDO Across Conflict Continuum, Source: Mad Scientist Library, URL: https://madsciblog.tradoc.army.mil/349-weighing-effort-in-the-future-strategic-environment-2028-2035/

ENUNCIATED EXECUTION OF MDO BY THE US ARMY

The US Army asserts that, "Strategic competitors like China and Russia are synthesising emerging technologies with their analysis of military doctrine and operations. They are deploying capabilities to fight the US through multiple layers of stand-off in all domains of the warfare viz–sea, land, air, cyber and space. Therefore, the American way of war must evolve and adapt."[21] The TRADOC Publication, 'The US Army in Multi-Domain Operations, 2028', outlines the doctrinal approach to deal with their adversaries in the future.[22]

The key concept of the MDO is that, "Army Forces, as an element of the Joint Forces, conduct MDO to prevail in competition. When necessary, Army Forces penetrate and disintegrate enemy Anti Access and Area Denial systems and exploit the resultant freedom of manoeuvre to achieve strategic objective win and force a return to competition on favourable terms."[23] A schematic representation of the MDO Solutions is depicted below:

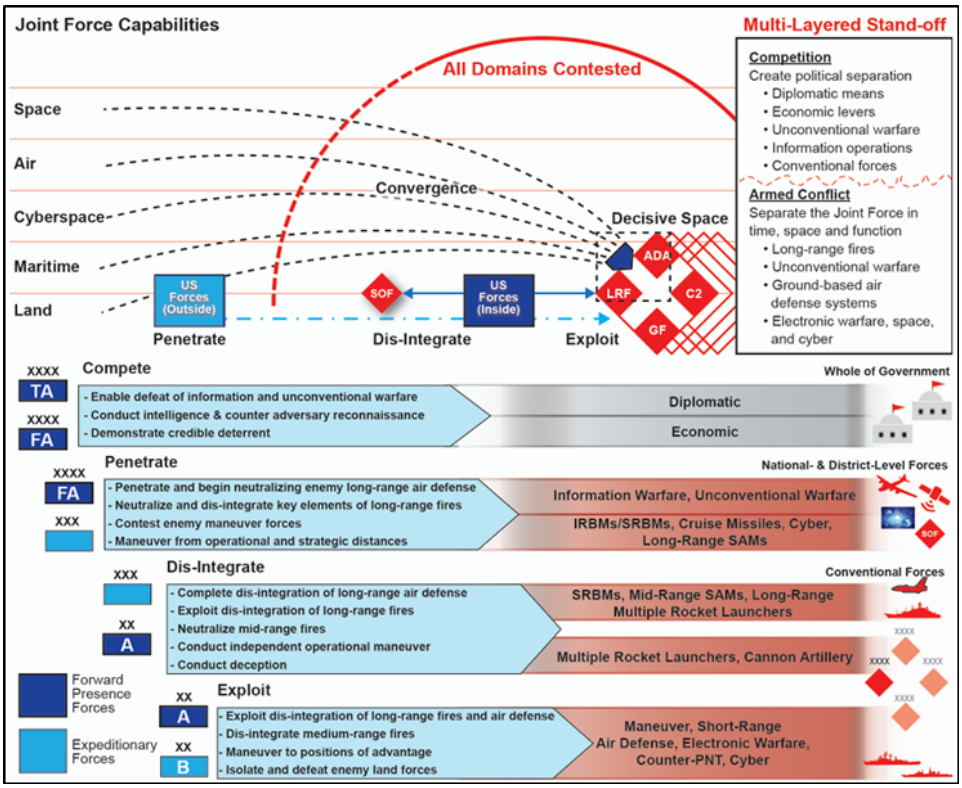


Fig 3, MDO Solutions, Source: TRADOC Pamphlet, URL: https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf

MULTI-DOMAIN TASK FORCE (MDTF) - ORGANISATIONAL CENTREPIECE FOR US CONSTRUCT OF MDO

MDO seamlessly integrate the domains of warfare. In the operating environment of 'strategic competition' graduating to 'armed conflict', the ultimate aim is to create desired kinetic or non-kinetic effects in various operating domains. The US Army has organised a theatre level, Multi-Domain Task Forces (MDTFs) for creating this effect.[24] The two main elements in the MDTF are for:

- Long-range precision effects such as electronic warfare, cyber, space and information operations.

- Long-range precision fires.

MDTFs integrate these capabilities under one commander. Various components conduct distributed operations to enhance survivability. Effects of all elements across domains are synchronised by the MDTFs.[25]

The US Army plans to build five MDTFs: two aligned to the Indo-Pacific region, one aligned to Europe; one stationed in the Arctic region and oriented on multiple threats, and a fifth MDTF aligned for global response.[26] The organisation of MDTFs are supposed to be as per the requirements of the theatre. The US Army's first MDTF was established in 2017. It was an experimental unit stationed at Joint Base Lewis McChord. It is focused on the Indo Pacific. The second MDTF was operationalised on 16 September 2021 at US Army Garrison Weisbaden in Germany and is aligned to Europe.[27] Broad organisation of a generic MDTF is given below:

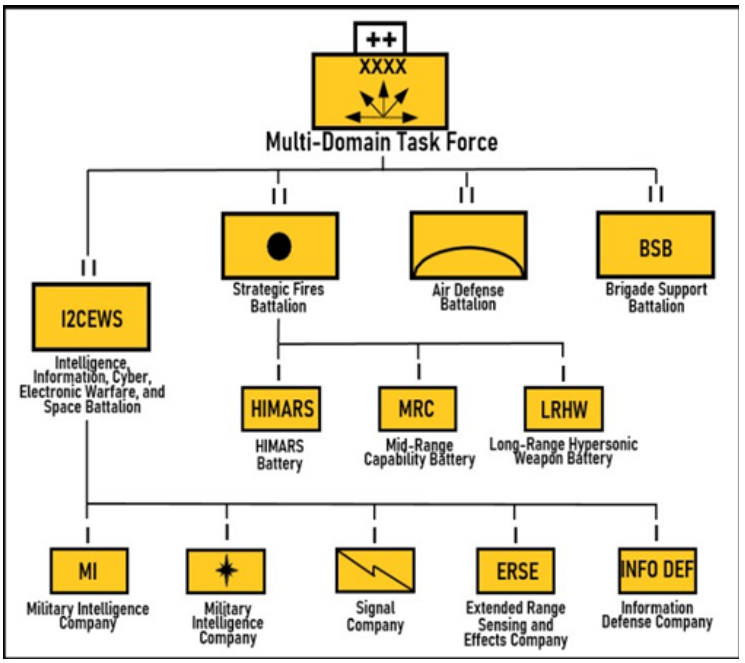


Fig 4, MDTF, Source: Chief of Staff Paper, URL: https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf

Two most important components of the MDTF organisation are the Intelligence, Information, Cyber, Electronic Warfare and Space (I^2CEWS) Unit, also termed as Multi-Domain Effects Battalion and the Strategic Fires Battalion. An Air Defence Battalion with missile defence capabilities, a Direct Energy Battery and a security force is also orbatted force protection. In addition, it has a Brigade Support Battalion which plans, directs and supervises supply distribution and

logistics, including field maintenance and medical capabilities. An All-Domain Operations Centre (ADOC) is established to integrate the diverse components of the MDTFs.[28]

ADOPTION AND EXECUTION OF MDO BY THE INDIAN ARMED FORCES

Assessed Threat Perceptions and Envisaged Future Operating Environment for the Indian Armed Forces

The Joint Doctrine of the Indian Armed Forces- 2017 assesses character of future wars as, "ambiguous, uncertain, short, swift, lethal, intense, precise, non-linear, unrestricted, unpredictable and hybrid".[29] Though the oft repeated prediction of a 'short and swift wars' has been challenged by strategic thinkers and the idea of "long wars with heavy political consequences"[30] have also been opined. The ongoing conflicts are justifying this viewpoint. India, with its vast borders, two definitely hostile and few not very friendly neighbours as well as myriad internal security problems has a very peculiar operating environment to deal with.[31] Two main external threats for India are assessed to be 'Pak sponsored terrorism which could spiral into a larger conflict between two nations' and the 'unsettled border with China giving it an opportunity to forcibly assert its claims'.[32] In the Indian context, Grey Zone Operations have gained importance where the Nation is neither at peace nor at war. In relation to India's two hostile neighbours, this can be equated to the 'competition below armed conflict' stage in the conflict continuum of the MDO. "Threat of India being targeted through information warfare, covert operations, economic warfare, and diplomatic manoeuvrings by countries or non-state actors and agencies that do not wish to see India emerge as a major power" adds another dimension to it.[33]

Given the current Geopolitical and Geostrategic realities, India, in all probability, will have to be continuously in operations in Grey Zone, limited conflict or (ultimately) in an all-out war. The Nation has to be geared up to deal with all possible external and internal threats. With these peculiarities, the future military operations involving the Indian Armed Forces will definitely be in multi domain.

Apart from the formidable Rocket Force, PLA has also developed significant space, cyber, information and Electronic Warfare (EW) capabilities. In case of any misadventure by China, these capabilities of PLA will definitely manifest against India in all possible domains. Practice of 'Unrestricted Warfare' – which advocates to transcend all boundaries and limits,[34] is also attributed to China. MDO as enunciated by the US Army, primarily aims to defeat China's A2/AD concept. It is imperative for India to understand and adopt the MDO concept suitably modified as per own peculiarities and requirements.

Adopting MDO is inevitable for the Indian armed forces. However, the US way

of executing MDO (or for that matter PLAs concept of A2AD) cannot be blindly templated by the Indian Armed Forces since the envisaged threats, operating environment and the resources of the two nations are grossly different. The CDS, General Anil Chauhan in an interview mentioned that, "… when we are looking at future warfare, we are not looking at how advanced militaries are going to fight in future and then trying to copy them. No. We are trying to say as to how 'we' are going to fight in future…"[35] This indicates the approach that the Indian Armed Forces should adopt.

At times, it is felt that the Indian Armed Forces may have lagged behind in adopting Revolution in Military Affairs (RMA), timely[36] and are late in modernising and transforming. However, adopting to MDO need not be a sequential process and the Indian Armed Forces can suitably acquire requisite capabilities to conduct MDO.

The Indian Armed Forces are undergoing a well-planned modernisation and transformation. The National Security Apparatus and the Higher Defence Organisation appear to be in firm control of the situation. Integration of the Indian Armed Forces has gathered momentum. Proposed structures (for the Integrated Theatre Commands) have been evolved and the plans are ready to be presented to the Government.[37] This is indeed an important milestone and the Integrated Theatre Commands may roll out very soon.

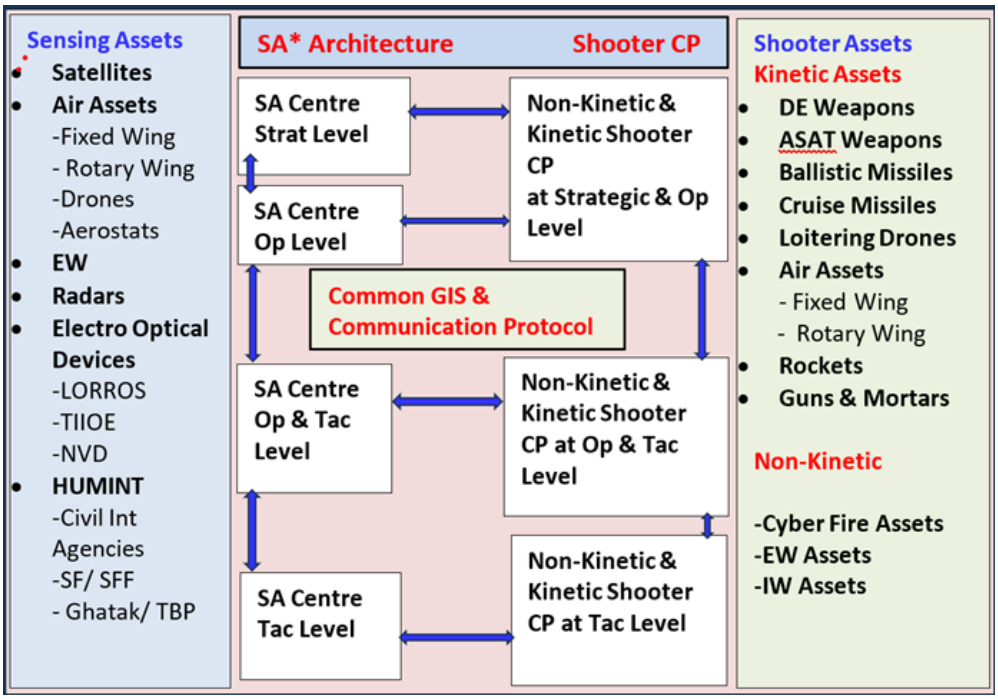
MDO- THE KEY COMPONENTS

US Army's construct of MDO and its proposed execution has been deliberated above with a view to understand the fundamentals and derive a template for adoption and application in the Indian context. Semantics and jargons apart, two fundamental components of MDO**,** which can be deduced from discussions so far, are: Multi Domain Situational Awareness Systems: for Deep Sensing[38] and Intelligence, Surveillance, and Reconnaissance (ISR). It is imperative that Commanders at all level viz Strategic, Operational or Tactical, must be provided adequate and timely inputs for complete situational awareness to facilitate combat decision making. This will require continuous and seamless 'Operating Environment Transparency'. Optimum coordination, cooperation and synergy amongst various Government agencies is needed to transform into a future ready force capable of conducting Multi Domain Operations. Multi Domain Non-Kinetic and Kinetic Capabilities: For Non-contact and contact warfare in the anticipated operating environment. In essence, kinetic capabilities denote kinetic weapons like missiles, rockets and guns. Non-kinetic capabilities refer to cyber, info and electronic warfare capabilities.

ARCHITECTURE FOR THE CONDUCT OF MDO

The two components for the conduct of MDO mentioned above and their sub

components must be seamlessly integrated in time and space with an aim to operate in the intended domain. A uniformly operable, robust and redundant communication protocol and GIS with seamless connectivity amongst all stakeholders for national security should be ensured.[39] A postulated pictorial representation of such an architecture for effective conduct of MDO is depicted below:



SA*- Situational Awareness

Fig 5, Networked and Automated Situational Awareness, Non-Kinetic and Kinetic Shooter CP for Executing Multi Domain Operations. Source: Author

To operationalise such automated, integrated, networked and secure architectures, seamless multi domain data connectivity is the foremost requirement. This will require extensive collection, collation and interpretation of data. Dedicated data servers and data clouds will be needed. This can only be achieved by extensive use of niche technologies like AI, Quantum Technology and Machine Learning.

MDO IN THE INDIAN CONTEXT: CHALLENGES AND GAPS

- **Organisational Peculiarities:** India is a vibrant and robust democracy which has very well-established institutions. The democratic system has its own peculiar governance model following rules, procedures and protocols. Any significant change generally takes more time than an

autocracy or a military ruled country.

- **Civil Military Relations and the Armed Forces Synergy:** Civil Military Relation in India has its own legacy and peculiarities. Also, the three services have their own independent organisational realities, ethos and work culture. Achieving synergy amongst the three services, bureaucracy and polity needs a lot of coordination. Rolling out of Integrated Theatre Commands is a case in point.
- **Requirement of Resources:** MDO components, architectures and structures postulated above require niche technologies and state of the art technical know-how. Capacity and capability building for adopting MDO will require significant resources and time.

SUGGESTED ROADMAP FOR ADOPTION AND IMPLEMENTATION OF MDO BY THE INDIAN ARMED FORCES

Necessity to deliberate upon the concept of MDO and adopt it suitably by the Indian Armed Forces, is very well established. The training commands of the Army, Air Force and Navy under the concerned branch of the IDS, should take lead and drive necessary joint doctrinal changes to adopt the MDO concept for India's operating environment. There can be two possible approaches to evolve requisite common structures for executing MDO in the Indian context.

- De Novo Structures for conducting MDO, or
- Empowering and enabling Joint Structures coming up for Integrated Theatre Commands to conduct MDO.

Given the organisational peculiarities and complexities involved in formulating anything new across three services; the second option of empowering and enabling structures coming up for integrated theatre commands to conduct MDO will be a more practical option.

The ensuing organisational and structural transformations likely to take place while establishing Integrated Theatre Commands have afforded a golden opportunity to parallelly adopt MDO by the Indian Armed Forces. Integrated capacity and capability building plans must be reoriented to acquire necessary systems and sub systems for key components of MDO.

Certain conceptual and capability building requirements to adopt MDO by the Indian Armed Forces are:

- An integrated, networked and automated battle management system must be put in place on priority.
- Immense expertise of the ISRO and vast IT skills of the nation must be co-opted for meeting situational awareness requirements for executing

MDO.[40]

- India must have its exclusive constellation of small, Earth Observation satellites in good numbers with high revisit rate. This will improve the C^4I^2SR capability, help improve the sensor-shooter integration and make the connectivity and data transmission between various surveillance equipment in space, air or ground more robust.[41] Private space tech companies like Planet Lab and Maxar, operating earth observation satellites, have demonstrated the utility of employing LEO satellites for ISR. Started just about a decade ago by former NASA engineers, they cover almost the entire globe and supply high definition images even for military operations.[42] With its experience and expertise, India must boost its space capabilities. Operationalisation of the Small Satellite Launch Vehicle (SSLV) will facilitate launch of Low Earth Orbit Satellites.
- India must enhance its strategic deterrence. Adequate long, mid and short-range precision fire capabilities must be developed. Adequate capability of the nuclear and conventional missiles, long range vectors, guns, rockets, aviation assets, fighter jets, bombers, attack helicopters UAVs and UCAVs must be built up.[43]
- Artillery and the Air Force are no more the sole custodians of the firepower or surveillance assets. The kinetic attack vectors like ASAT weapons, Directed Energy weapons, Ballistic and Cruise Missiles, Attack Heptrs, Loitering Drones, UAVs and UCAVs are now held with different Arms and Services. Combined arms synergy of the highest order must be achieved.
- While it is desirable to have the state of art systems, weapons, ammunition and equipment in abundance, the optimum utilisation of the existing inventory is equally important. A balance must be ensured in procuring new weapons and systems and accessories/ supporting systems for optimal utilisation of the existing inventory.
- Fiscal prudence, Atmanirbharta and Indigenisation are a must to meet the requirement of resources for such systems, weapons and equipment.[44] The idea of 'Swadeshikaran se Sashaktikaran'[45], needs to be adopted in letter and spirit.
- Safe, secure and robust logistic capabilities and supply chains must be ensured.
- The procurement policies and procedures must be reviewed. Universal, generic and strict General Staff Qualitative Requirements (GSQRs) for procurements mandating uniform equipment and systems for the entire Armed Forces across all terrains, need a rethink. Many a times, during

field trials, an equipment fails to comply with some minute random criteria in one specific sector. It may have performed optimally in other sectors and the users may be satisfied with the performance, but the procedures make it very complicated to modify the GSQR at such a late stage. This causes inordinate delays. India has vast borders in varying terrains. Separate equipment, with slightly differing capabilities, for operating in three terrains viz high-altitude areas and mountains, obstacle ridden terrains and the deserts should be considered. Improved IT skills and automation facilitate inventory management. Multiple e-commerce companies are managing huge inventories encompassing anything and everything. Cyclic procurement should be adopted.

- Training of all ranks must be given a De-Novo look. The Future Warfare Course[46] mentioned by the CDS during the India Defence Conclave is a pioneering initiative in this direction. Its second edition has recently been conducted by the CENJOWS under the aegis of HQ IDS.[47] However, it should be emphasised in correct perspective that "…mere structural corrections won't be enough but other cognitive corrections are also important…".[48] Technical education infrastructure in the country has developed significantly in past few years. Large number of students are getting trained with better technical education. HR Management policies should be reviewed to ensure that better qualified candidates are recruited to handle sophisticated equipment.[49]

CONCLUSION

War and warfare will continue to evolve. The Air Land Battle concept and technical prowess of the USA and the West were on display in the two Gulf Wars. This propelled China to formulate its A2AD concept. China embarked on extensive modernisation of its Armed Forces. It developed a formidable Rocket Force as well as space, cyber and information warfare capabilities. Russia also seems to have regrouped and trying to gain its erstwhile dominant place in the world order.

Russia and China have been identified as two strategic competitors by the USA. To counter China's A2AD concept, the US Army postulated the concept of MDO. In the past decade, this concept of MDO has gained traction in the strategic community and the Armed Forces, world over.

India, with its peculiar operating environment, need to adopt this concept keeping in mind the operational realities and requirements. Ongoing transformation of the Indian Armed Forces and rolling out of the Integrated Theatre Commands provide an excellent opportunity to put in place the architecture for conduct of MDO in the Indian Operational context.

❖❖❖

Brig Devendra Pandey is a serving Indian Army Officer. He is pursuing his PhD in Defence and Strategic Studies. His study interests are Strategic Deterrence, Non-Contact Kinetic Warfare, Multi Domain Operations, Training and Leadership issues.

NOTES

1. Dr Manbrata Guha, 'Multi Domain Warfare: Waging Unrestricted Warfare', SYNERGY-Journal of the CENJOWS, February 2019.
2. Rand Corporation Report "Multi-Domain Integration in Defence- Conceptual Approaches and Lessons from Russia, China, Iran and North Korea" https://www.rand.org/pubs/research_reports/RRA528-1.html
3. Lt Gen P R Shankar (Retd), "Era of Disruption in Military Affairs: Need for Multi Domain Operations**",** October 22, 2019; https://bharatshakti.in/era-of-disruption-in-military-affairs-need-for-multi-domain-operations
4. Ibid
5. Rand Corporation Report, op cit. The definition given by Development, Concepts and Doctrine Centre (DCDC) of the Ministry of Defence, the United Kingdom
6. Ibid.
7. Ibid
8. Ibid.
9. Tweet by Lt Gen Raj Shukla (Retd), Raj Shukla@Gen_RajShukla. (28 July 2023).
10. Mahajan Neeraj, 'Cognitive Domain the Sixth Domain of the Warfare', February 06, 2023. DEFSTRAT. Vol 16 Issue 6. Jan – Feb 2023. https://www.defstrat.com/magazine_articles/cognitive-domain-the-sixth-domain-of-
11. Rand Corporation Report. Op cit. The referred article by Frank Hoffman and Michael C. Davies, "Joint Force 2020 and The Human Domain: Time for A New Conceptual Framework" was published in "The Small Wars Journal" in 2013.
12. János Csengeri, "Multi-Domain Operations – A New Approach in Warfare", International Scientific Journal 'Security & Future', Year v, Issue 3, p.p. 78-80 (2021).
13. Gen. David G Perkins, 'Multi-Domain Battle Driving Change to Win in the Future', https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2017/Perkins/
14. National Security Strategy of the United State of America December 2017, pp 2, accessed at https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
15. Ibid.
16. Thomas F. Lynch III, Strategic Assessment 2020, https://ndupress.ndu.edu/Media/News/News-Article-View/
17. Cordesman Anthony H, Commentary on, 'The U.S. Joint Chiefs New Strategy Paper on Joint Concept for Competing', March 17, 2023 https://www.csis.org/analysis/us-joint-chiefs-

new-strategy-paper-joint-concept

18. Thomas F. Lynch III, Strategic Assessment 2020. Op cit.
19. Kelly McCoy, “In the Beginning, There Was Competition: The Old Idea Behind the New American Way of War”, 04 November 2018, Modern War Institute, accessed at https://mwi.westpoint.edu/beginning-competition-old-idea-behind-new-american-way-war/
20. Chief of Staff Paper #1, Army Multi-Domain Transformation-Ready to Win in Competition and Conflict, 16 March 2021, pp 3, accessed at, https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf
21. TRADOC Pamphlet 525-3-1, “U.S. Army in Multi-Domain Operations, 2028”, Foreword.
22. Ibid.
23. Ibid, pp vii
24. Congressional Research Service Paper, ‘The Army’s Multi-Domain Task Force (MDTF)’. March 29, 2021
25. McEnany Charles, ‘Multi-Domain Task Forces: A Glimpse at the Army of 2035’. March 02, 2022 https://www.ausa.org/publications/multi-domain-task-forces-glimpse-army-2035
26. Congressional Research Service Paper. Op Cit.
27. McEnany Charles. Op cit.
28. Ibid.
29. Joint Doctrine of the Indian Armed Forces 2017. https://bharatshakti.in/wpcontent/uploads/2015/09/
30. Lt Gen DS Hooda (retd), PVSM, UYSM, AVSM, VSM** (Retired), “Swift wars are a myth, India needs to prepare for other modern forms of warfare as well”, The Print, 25 October, 2017, https://theprint.in/opinion/short-war-india-information-warfare/13328/
31. Brig Devendra Pandey, “Niche Technologies For ISR Structures – Enhancing Effectiveness Of Artillery In Non-Contact Warfare”, The Artillery Journal 2024
32. Lt Gen DS Hooda, PVSM, UYSM, AVSM, VSM** (Retd), “Indian Military Strategy in Future Conflicts”, February 4, 2021, https://www.claws.in/event/11-02-divya-drishti -2021-annual-army-seminar-cum-webinar-on-multi-domain-operations-future-of-conflict/
33. Lt Gen Dushyant Singh, PVSM, AVSM (Retired), Multi Domain Warfare, Are We Geared Up for It? https://www.usiofindia.org/publication-journal/Multi-Domain-Warfare:-Are-we-Geared-for-it.html
34. Dr Manbrata Guha, Op cit.
35. Gen Anil Chauhan, CDS & DMA, “CDS Elaborates on New Technologies and Structural Changes in The Armed Forces.” Interview by Mr Nitin Gokhle, India Defence Conclave, September 20, 2024, audio 08.20’, https://bharatshakti.in/cds-elaborates-on-new-technologies-and-structural-canges-in-the-armed-forces
36. Lt Gen Raj Shukla, PVSM, YSM, SM, ADC (Retired), “Theaterisation: Way Ahead in Achieving Convergence”, https://www.claws.in/event/11-02-divya-drishti -2021-annual-army-seminar-cum-webinar-on-multi-domain-operations-future-of-conflict/
37. Gen Anil Chauhan, CDS & DMA, Interview by Mr Nitin Gokhle, Op Cit, audio 20.10’.
38. Andrew Glenn, “Deep Sensing: The Next Frontier in Military Decision Making”, March 11, 2024, https://www.linkedin.com/pulse/deep-sensing-next-frontier-military-decision-making-andrew-glenn-l60be
39. Brig Devendra Pandey, ‘Integrating Drones for Long Range Precision Fires and Time

Sensitive Targeting – An Indian Perspective', SYNERGY- Journal of the CENJOWS, Vol 2 Issue 2, September 2023.

40. Brig Devendra Pandey, 'Modernisation of the PLA Rocket Force and its Implications for India', The Artillery Journal 2021.
41. Kartik Bommakanti. "Strengthening the C4ISR Capabilities Of India's Armed Forces: The Role Of Small Satellites." ORF Occasional Paper. (15 Jun 2020).
42. https://www.nasaspaceflight.com/2018/01/planet-labs-targets-search-engine-world/
43. Suyash Desai, '4 Lessons for India from China's October 20019 Military Parade'. The Diplomat. December 03, 2019 www. thediplomat.com
44. Brig Devendra Pandey, "Joint Precision Fires- Key Instrument of Success in Multi Domain Operation", The War College Journal 2023
45. Interview: Chief of the Army Staff, Def Strat, Vol 18 Issue 6 Jan – Feb 2025, accessed at https://www.defstrat.com/magazine_articles/interview-chief-of-the-army-staf/
46. Gen Anil Chauhan, CDS & DMA, Interview by Mr Nitin Gokhle, Op Cit
47. https://pib.gov.in/PressReleseDetailm.aspx?PRID=2122831&reg=3&lang=1
48. Lt Gen Raj Shukla, op cit.
49. Brig Devendra Pandey, "Artillery in Emerging Multi Domain Operations Environment- An Indian Perspective", The Artillery Journal 2023

❐❐❐

AI AS A SERVICE AND FUTURE WAR - A TRYST WITH TECHNOLOGY

Lt Gen (Dr) Anil Kapoor, AVSM, VSM (Retd)

> "Whatever can be precisely defined can be perfectly designed and developed. If data is the new oil, technology is the new oil refinery. Let us create and perfect the emerging tech eco system. Technology is the indispensable special purpose vehicle that will pave the way for Viksit Bharat 2047"
>
> The Mantras of Era of Disruption

Abstract

In the rapidly evolving landscape of global conflict, warfare is no longer defined solely by physical might, but by digital supremacy and technological agility. This article explores the transformational role of Artificial Intelligence as a Service (AIaaS) in shaping the future of warfare, particularly in the context of India's strategic aspirations as a technologically sovereign power. Anchored in the convergence of five foundational pillars, like automation, autonomy, precision, positioning, and AI, the future battlespace is one where data fusion, cognitive decision-making, and algorithmic warfare take center stage.

The Indian Armed Forces, navigating the threshold of Viksit Bharat@100, must integrate AI into all dimensions of operations, from intelligence to combat, logistics to cyber defense, through an adaptive AIaaS framework. This platform enables real-time situational awareness, multi-domain decision support, and seamless synthesis of inputs from the Internet of Battlefield Things (IoBT), sensor arrays, and intelligence networks. Using real-world scenarios and mission simulations, the article demonstrates how AI can drive operational superiority, accelerating the OODA loop, enabling autonomous unmanned systems, and ensuring resilience even in GPS-denied or cyber-contested environments.

However, this AI revolution comes with challenges like doctrinal ambiguity, interoperability gaps, and the ethical dilemma of machine autonomy in lethal decisions. The article argues for a national security doctrine aligned with a robust AI strategy, supported by strong political will, institutional innovation, and a 'whole-of-nation' approach. As AI evolves into the electricity of the Fourth Industrial Revolution, India must harness its full potential, transforming warfare without a single shot fired, yet commanding unmatched strategic influence.

INTRODUCTION

In an era marked by unprecedented technological disruptions, the nature of warfare is undergoing a rapid and transformative shift. The future battlefield will no longer be won by numerical strength or conventional might alone, but by agility and dominance in the digital domain. The future war zone is defined by mastery over five tech pillars, automation, autonomy, precision, positioning and AI as the building blocks. The fusion of soldier and tech systems, Internet of Battlefield Things, (IoBT), algorithmic precision and merging technology with strategy and tactics will define India's tech-driven transformation to ensure that our Armed Forces are always future-ready, mission-adaptive, and unquestionably dominant. That said, Armed Forces of Viksit Bharat, India@100, must be technologically sovereign, secure, self-reliant and strategically supreme, as behoves a global power centre.

The Indian Armed Forces stand at the cusp of a defining transformation. The battles of tomorrow will not be fought solely with muscle power, but with machines, minds, and mastery over emerging technologies. To secure India's sovereignty, shape its regional influence, and uphold global stability, we must pivot, decisively and urgently, towards a tech-empowered force. This journey demands whole of nation approach, strong political will, visionary leadership, institutional courage, and relentless innovation. 'Roadmap 2047' is not a blueprint of aspirations instead, it is a doctrine of inevitability. We need to develop a National Security Strategy and a matching National Technology Strategy.[1]

TRYST WITH TECHNOLOGY – IOBT SCENARIO BUILDING

Savour the technology driven warfare in daily life – not a shot fired yet the turbulence, chaos and VUCA impact of war is rife. The technology driven scenarios can herald a war autonomously. On a D Day, the transportation systems comprising metros, airlines and railways face a major cyber-attack resulting in non-operational airports in metros and a few major rail accidents. D-plus One, the banks, digital public infrastructure and National Power Grid undergo a major disruption. D-plus Two, major hospitals are under cyber attack, and C2 affecting availability of internet across the country. We have the nation coming on knees. All this happening in the backdrop of social media abuzz with disinformation of tribal rivalries, religion-driven riots, attack on religious places and then planted intelligence reports of major threats of drone swarms on the borders, underwater unmanned autonomous systems in coastal areas etc. The Nation gets into heightened security threat, a fear psychosis and the Government paralysed with the breakdown in essential services with no fall back options. Not a shot fired but coercive diplomacy is on display.[2] This is the

playbook of manoeuvre warfare in contrast to the kinetic attacks and heavy explosions reminiscent of attrition warfare.

FUTURE TECH - TRYST WITH AI IN THE REAL WORLD-AIAAS

The technology is on the gallop. Sensors and software, data and technology are two sides of the same coin and need to be harnessed for creating a formidable int, operational and combat management system, and in this regard, AI is an inherent enabler. That said, AI as an offshoot of the Fourth Industrial Revolution (IR) is synonymous with electricity of the Second IR. Electricity replaced the steam in 2IR while the world experienced the power of digital footprint replacing analogue systems in the 4IR. The data overload and information obesity with high-speed compute has made AI an inevitable choice, if not a compulsion for growth. That said, while electricity can be looked at with a problem solving technology perspective, the best value of electric systems is harnessed by establishing an electric grid. In a similar vein, the true value of AI can be harnessed by creating an adaptive framework through an AI platform of AI as a Service (AIaaS) that look at this tech through a problem-solution compendium. Two examples will make this concept crystal clear. AI as a Service and AI-driven OODA loop.

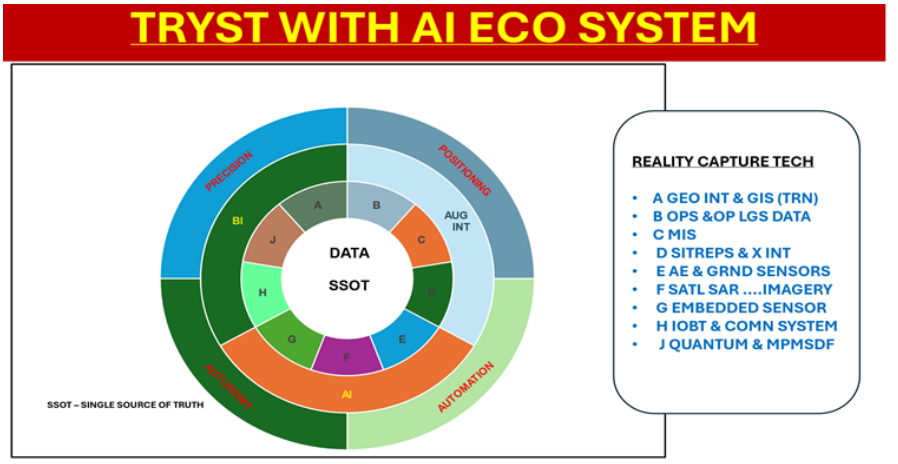


Figure 1, Anatomy of AI in Defence. Source: Author

Before we dwell in AIaaS, an application oriented AI analysis would be in order. AI algorithms as mathematical models for predictive analytics have been highly reliable in solving probabilistic problems. A good example is the guidance control relationship in a guided missile which predicts the future position of a manoeuvring target till it finally locks on. The data set for training this is derived from simulations of varied target and guided missile manoeuvres. Typically, these models do curve fitting with data sets. This was in vogue till the digital

transformation created a revolution in the tech world. With the advent of high data storage and high-speed compute GPUs, Machine Learning (ML) and Deep Learning (DL) models through neural networks has brought in a paradigm shift in AI. Today we have Small Language Models (SLM) and Large Language Models (LLMs) with Convoluted Neural Networks (CNN) and Generative Pre-Trained Transformers (GPTs) creating the Gen AI and Agentic AI. A typical AI-based Defence Application Eco System (Figure above refers) would, therefore, have the following AI tech stack.[3]

- **Sensor Based Data Collection:** Data is gathered based on a number of Optoelectronic Sensors (OE) sensors, capturing devices like radar, lidar, sonar, satellites, UAS and processed for business intelligence for fact sheet, and augmented intelligence for decision support. AI is used for multi platform-multi sensor data fusion, data veracity, trend analysis and predictive analytics. ML, DL and SLMs are typical AI applications based on CNN. SLMs can handle millions of parameters and are normally deployed on the edge of sensors for AI based agile analytics.
- **Processing and Understanding Data:** Processing data and creating the cognitive human brain intelligence and actionable info is done through graph neural networks and AI is employed for identification of cyber and network threats using SLMs. AI drives automation to autonomous systems for precise positioning so important in targeting.
- **C2 and Decision Support Systems:** AI driven ISR, C2, mission planning, op logistics planning, battlefield management systems and decision support systems employ LLMs with billions of parameters. The DSS under complex dynamics with a huge amount of data inputs, historical, past and present, can best be harnessed by AI platforms for giving courses of action, contingency plans and KPIs for effective decision support. In an ultimate analysis, autonomous decision-making seeker shooter systems can be designed and developed to include Unmanned Autonomous Systems(USA) terrestrial, aerial, sea surface and under water. Deep reinforcement learning, SLMs, LLMs can be configured for swarm based military operations with (MuMTs) or without man in the loop.
- **Invisible Warfare:** AI driven defensive and offensive cyber and EW systems have the potential of sustaining invisible warfare by creating generative adversarial networks to disrupt commercial and military C4 systems. AI based lethal autonomous weapons are the next wave which can autonomously sense, seek and destroy targets. Immense research is in progress to model the heart brain, and gut brain neural networks to build emotion/ empathy and instinct-based AI DSS, respectively.

AI AS A SERVICE - AN ADAPTIVE FRAMEWORK.[4]

An AI platform was developed for satellite imagery interpretation and to create Multi-Platform Multi-Sensor Data Fusion (MPMSDF) to identify military objects of interest and importance. With humungous number of inputs of unstructured and structured data there is often an info overload in a tactical / operational / higher HQ. The info complexity increases exponentially in the hierarchy. Given the elaborate security apparatus with inputs coming from satellite SAR, opto electronics and other forms of imagery, COMINT, SIGINT inputs, HUMINT, social media and diverse inputs from IB, RAW etc, at all levels, it has become a human limitation to sift and decipher all inputs to create a cogent comprehensive picture in HQ. The situation becomes hugely complex in war, especially when info nuggets of historical importance which are institutional memories in transition leaving much to be desired in terms of actionable preparedness for int, combat and decision support. It is in such scenarios that AI becomes an inevitable service for Real Time Situational Awareness (RTSA) and Common Operating Picture (COP). The AI software based decision support system can become a powerful tool for tactical, operational and strategic commanders to create real time situational awareness and common operating picture, involving a host of satellite, SAR, OE imagery and all the aforesaid int inputs, to create an actionable info decision support update by putting together relevant historical inputs backed up with real time info. An experiment was conducted with satellite and SAR imagery for creating a COP using AI algorithm. The exercise which was taking over 24 hours was rendered most efficient and effective in 15 minutes with a truth value assigned for each target. The challenge, however, was getting adequate imagery data points for training the AI model. A tank was eight pixels, a gun six pixels approximately and finding tanks and guns in an image of one million pixels was like finding a needle in a hay stack. The AI model was developed for IFF, decode mission package of combat teams, combat groups, combat commands and had contours of C7I2SR DSS (Command, Control, Communication, Computer, Cybertronics, Cognition and Combat).[5] This same MPMSDF AI platform was then deployed for early stage cancer detection since cancer cells are also in a similar pixel range of six to eight pixels, and based on multiple tests for change detection. In a later instance this AI platform was deployed for management of COVID hospitals to identify bed availability and monitor patient care in wards based on CCTV cameras. The versatility of AI platform as a service is profound, both in military and commercial applications.

THE OODA LOOP

AI is a past master in executing the, Observe, Orient, Decide, Act (OODA) loop the fastest. In aerial combat scenario building and net assessment exercises AI driven Unmanned Aerial Autonomous Systems Aircraft (drones) out performed

manned aircraft in aerial combat scenarios due to their inherent capabilities of huge data-based decision-making capacities with LLM, and executing upwards of 8G manoeuvres, thereby responding to change much quicker. AI platforms can be designed and developed for multi domain combat operations for Tri services and integrated theatre command real time situational awareness, common operating picture and C7I2S2R decision support.

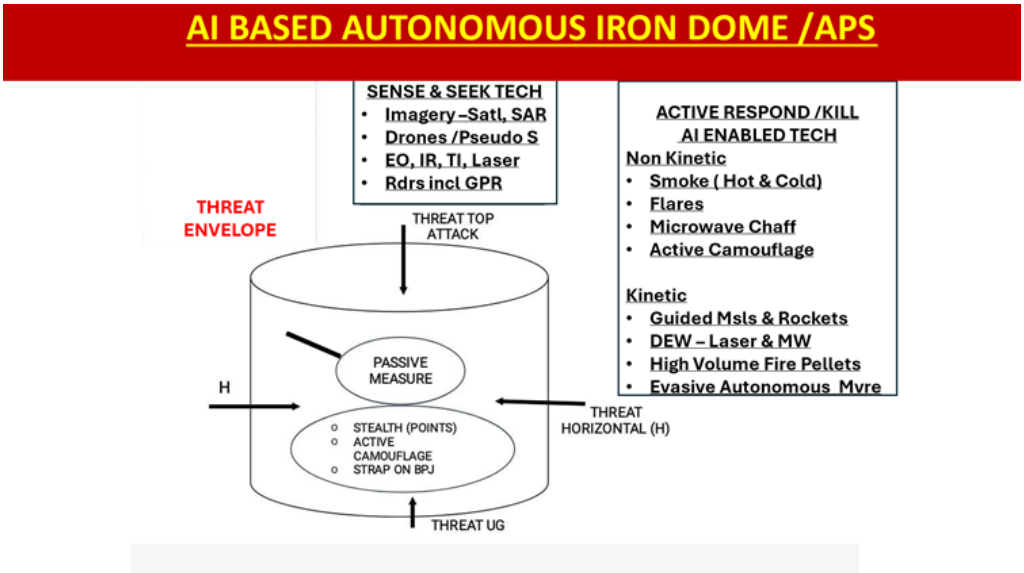


Figure 2: The Iron Dome and Active Protection System (APS). Source: Author

The sketch above explains the AI-based autonomous Iron Dome and APS. 360 degree threat envelope from underground, underwater, terrestrial vectors and aerial vectors needs a system of sense and seek sensor technologies. The data inputs duly evaluated by AI on the sensor edge or on the AI platform can assess and create a threat envelope based on Identification, Friend or Foe (IFF) in a few milliseconds. It can then take appropriate decision to earmark shooters to destroy the threat. The actions may be pre programmed as non-kintetic and kinetic, and based on the parameters, including reaction time, active protection to Vulnerable Points (VPs) and Vulnerable Areas (VAs) can be configured.

AI IN TRI-SERVICES ENVIRONMENT AND INTEGRATED THEATRE COMMAND.[6]

In an era of disinformation and deepfake AI-driven campaigns, AI is the panacea and stands out as a transformational force multiplier. That said AI based info, decision support systems are capable of redefining command structures, battlefield awareness, and real-time decision-making in extremely ambiguous scenarios. Future conflicts are likely to be fought in contested,

info and disinformation-rich environments demanding rapid synthesis of vast data across multiple domains, land, sea, air, space, EW and cyber. The combat readiness and agility will be defined by multi-platform, multi sensor data fusion to sense and seek actionable intelligence and info, discern friend from foe, IFF, and annihilate the threat with appropriate shooters. This calls for integration of AI into the theatre command C7 architecture, Command, Control, Communication, Cyber, Computer, Cognition and Combat Decision Support Systems (DSS), so imperious for maintaining strategic superiority.[7] AI-powered DSS can integrate inputs from all domains, generating synchronised, mission-tailored recommendations to support coordinated responses across integrated battle group (IBG) force components. In high-stakes environments, time is a critical resource. Autonomous DSS can offer real-time analysis of adversary posture, recommend proportionate deterrence options, and even simulate escalation ladders, helping commanders at all levels manage crisis scenarios without overcommitting or miscalculating. Autonomous Decision Support Systems (ADSS) infused with AI can process and analyse volumes of battlefield data far beyond human capacity. This cognitive augmentation allows commanders to manage more complex operations effectively, acting as a force multiplier across echelons.[8]

OPERATIONAL RESILIENCE IN CONTESTED ENVIRONMENTS

AI-enabled DSS systems guarantee precision in Joint and Multi-Domain Ops, force multiplication through cognitive automation and a faster OODA loop for effective escalation control. The systems can be designed to operate semi-independently in GPS-denied, communication-contested, or cyber-compromised environments. This ensures command continuity and mission execution when traditional systems are disrupted by adversary electronic warfare or cyberattacks.[9] Using AI-generated war gaming scenarios and data-driven level decision trees, autonomous DSS can also be used for strategic, operational and tactical exercises and virtual mission rehearsals. This fosters continual learning for commanders and enhances readiness without needing full-scale deployments, as an Offensive Weapon of Mass Destruction can launch virtual surgical strikes. AI-driven silent arsenal of lasers, jammers, and cyberattacks could paralyse the enemy command and control structures, tilting the battlefield before a single shot is fired. As satellite networks falter, precise cyber intrusions escalate. Ground stations face disruptions, command systems buckle under data surges, and inter-service coordination slows to a crawl. These strikes are surgical, not designed to obliterate, but to disorient, sowing confusion in the fog of war.[10]

C7I²S²R DSS FRAMEWORK FOR INTEGRATED THEATRE COMMAND BASED ON SENSOR SHOOTER DRIVEN BY AI

Component	Functional Necessity	Functionality in AI-Driven Warfare
C^2 (Command & Control)	Battlefield command execution and coordinacion	AI-optimized mission planning and force deployment
C^2 (Communication & Computers)	Secure data transfer and real-time digital operations	AI-driven spectrum management AI-optimized computing systems, quantum integration and encryption
C (Cybertronics)	Defensive and offensive cyber operations	AI-powered cyber threat detection, EW, deception, responses and countermeasures
C^2 (Cognition & Combat All	AI-driven tactical decision making and adaptability	Predictive analytica, wargaming, real time decision support, adaptive response strategies
I^2 (Information & Intelligence)	Mutti-source intelligence and real-time data processing based on SSOT (Tvalue)	AI-powered intelligence fusion from ISR, HUMINT, SIGINT, COMINT, IMINT, GEOINT
S^2 (Secure Surveillance-Situational Awareness & COP)	Multi Layered GeoAI Grid, Continuous battlefield monitoring and tracking	AI-driven ISR, MPMSDF, IFF and mapped trend-real time battlefield insights-FLOT
R (Reconnaissance & Targeting)	Autonomous and real-time enemy tracking	AI-guided UAS surveillance, autonomous threat engagement mci Recce in Force
DSS (Decision Support System)	AI-enhanced C2, operational decision -making and contingency planning	Real-time AI analytics besed on MPMSDF and mission packaging for strategic and tactical execution, autonomous DSS

Table 1, C7I2S2R DSS Framework for Integrated Theatre Command based on Sensor Shooter Driven by AI. Source: Author

AI SYSTEM OPERATIONALISATION CHALLENGES

Notwithstanding the above, Armed Forces worldwide are still grappling with integrating autonomous systems into traditional chain-of-command structures. It is crucial to understand, who would hold the final authority when an AI DSS recommends a lethal action and how are liability and responsibility apportioned if outcomes go wrong. Joint and coalition operations demand seamless interoperability. However, differences in data standards, AI architectures, and security protocols across Services and the Integrated Theatre Command ecosystem can hamper real-time data sharing and synchronised decision-making. It is in this context that a well thought through roadmap for deployment of AI systems comprising doctrinal reforms, tech development milestones, testbeds and simulations, human-machine and machine-machine interface designs and R&D in humanising AI through the triad of head, heart and gut becomes relevant.

STRATEGIC PATHWAYS FORWARD FOR THE ARMED FORCES

There is a dire need for the Indian Armed Forces to prepare and be prepared for technology-based threat scenarios. Possible policy initiatives and courses of action to create a formidable AIaaS platform are as follows:

- **Data As a Service DaaS:** Fix a common Tri Service Data Infrastructure. Unlike a data lake we create a data garden comprising deweeded Single Source of Truth (SSOT) driven structured data and unstructured data duly encrypted both in rest residing in Tri Service Cloud and transferred through cyber-secure channels in motion.
- **Infrastructure As A Service (IaaS):** Prepare a blueprint for high tech infrastructure scenarios through sensors and IoBT. Inherent in this technology stack info, communication and cyber (ICoCy) defence of own critical infrastructure and a credible capability to steer, caliberate and sustain offensive ICoCy technologies. Technology-based ICoCy surgical strikes may be launched to convey subtle messages to inimical neighbours in the West and North.
- **Platform As A Service (PaaS):** AI as an application is best deployed as a platform comprising a number of APIs for variety of applications duly networked for effective decision support. JARVIS was a AI platform created by a startup for imagery interpretation and was deployed for a large number of other applications through computer vision based on LLM. Tri Service AI based PaaS needs to be developed for effective DSS.
- It is essential to design and develop role-based Unmanned autonomous systems (aerial, ground, sea and underwater).[11] Some of the critical areas are:
    - **Logistics and Supply Chain:** For advanced winter stocking, advance monsoon stocking, air maintenance of winter isolated posts, casualty evacuation, para jumping, sky diving, infiltration operations and facilitating operational logistics in military operations,10kg to 150 kg, logistics and supply chain play a crucial role.
    - **Surveillance:** All terrains, tactical int gathering operations and targets of interest in depth, LIDAR, RADAR, SAR, EO and COMMUNICATION PAYLOADS for military operations, both Counter Insurgency-Counter Terrorism (CICT) and conventional ops.
    - Build waves of autonomous combat systems and Manned Unmanned Teams (MUM-Ts) based operational scenarios as eyes and ears on the land, in air or sea for search-seek-destroy missions, lethal weapon platforms, mining ops by carrying mines for scattering in the face of the enemy, reconnaissance (recce) and recce in force missions, kamikaze operations and other Tri Services integrated combat missions.
- Based on the technology it is essential to strategy, organise Territorial Army Technology Development Units comprising subject matter experts

from Armed Forces, Academia, Government and Industry to create AI-based Tri-Service C7I2S2R DSS as a program akin to Integrated Guided Missile Development Programme **(**IGMDP). To responsibly and effectively configure AI-based autonomous DSS.[12] In the Armed Forces, a multi-dimensional roadmap is essential:

- **Doctrine Development:** Evolve doctrines that define AI's role in combat decisions, engagement rules, and escalation protocols.
- Develop a robust AI-driven C7I2SR DSS for both autonomous and human-in-the-loop ops.
- **Human-in-the-Loop AI Systems:** Institutionalise human-machine collaboration, MumTs with tiered levels of autonomy based on mission risk.
- **AI Literacy and Wargaming:** Train leaders in AI literacy, integrate DSS into military education, and routinely test them in realistic simulations.
- **Red-Teaming and Adversarial Testing:** Expose AI systems to stress tests and cyber threats to improve robustness.
- **Ethics and Governance Frameworks.** Develop AI systems with the head, heart, gut triad, develop robust AI-driven DSS and establish robust oversight bodies to ensure compliance with international humanitarian law and ethical norms.

CONCLUSION

Technology Sovereignty is a Journey and Not a Destination, let the Marathon begin. Developed and developing nations today, in contemporary times, have three common strategic pillars towards a formidable National Development Program–National vision with strong political will, whole of nation approach and an insatiable thirst for disruptive emerging technology development. This mantra has seen Turkey, Singapore, South Korea, and South Africa join the well-known bandwagon of the US, Russia, China, Israel, France, and South Africa to name a few.

A resurgent India on the move has embarked on a multi front National development strategy. The First Front is the Make in India, as a precursor to Made in India, the Second Front is Aatmanirbhar Bharat as a call for self-reliance, third Front is Start Up India to champion the agile ignited young minds into entrepreneur ventures and then there is Skill India, Invest India, Digital India, Gati Shakti, Mission Quantum, Mission Semiconductor and the listing goes on. All these coming up concurrently has created an enormous technology and innovation bandwidth and excitement in India, which has worldwide tech reverberations. A nation known for technical prowess comprising strategic

thinkers and technology wizards globally, the white collared tech enabled professionals and skilled innovative tech workforce at the grassroots, all this with vibrant Captains of Industry and a strong political will to do, has ushered an era in technology development by giving the world two major game changing concepts Jugaad which means a resourceful approach to problem solving and atmanirbharta which means self-reliance. These initiatives, and more, are visible in the past few Global Tech Expos, Aero India, and Defence Expos, epitomising that India has made the mark in the technology world.

The future battlespace demands speed, precision, and adaptability, qualities that only AI-driven autonomous DSS can deliver. For the Armed Forces, these systems represent both a transformative opportunity and a strategic vulnerability. Design and development of AI based decision support system is a compulsion and no longer a choice. Multi-domain multi platform integration and situational awareness, cognitive load reduction for commanders, autonomous response and countermeasure capability, increased decision speed and accuracy, configuring AI driven cybertronics defence and interoperability across weapon platforms are battlefield gamechangers in future warfare. The effective deployment of AI in C7I2S2RDSS systems can redefine battlefield dynamics, enabling militaries to outpace, outmanoeuvre and outthink adversaries. Opportunities beckon!

❖❖❖

Lt Gen (Dr) Anil Kapoor, AVSM, VSM (Retd), superannuated as Director General Electronics and Mechanical Engineers on 31 December 2020. He was also the Director General Info Systems.

NOTES

1. Lt Gen Anil Kapoor (Retd), Six Strategic Lessons from Russia Ukraine War, CLAWS, Jan 23
2. Prakhar Gupta, The Next War with China Will Not Begin With A Bang, But With A Blackout — And India Is Not Prepared For It Swaraj, 22 Apr 25
3. Lt Gen Anil Kapoor Retd, AI in Defence Challenges and Opportunities, Nine Inf Div Seminar, Februr 2025
4. Lt Gen Anil Kapoor Retired, 'AI As A Service – A Perspective', Podcast BharatShakti.Com
5. 5 Lt Gen Anil Kapoor (Retd), Proliferation of Unmanned Aerial Systems, RRU Journal Oct 2024
6. Ibid
7. Lt Gen Anil Kapoor Retired, ' Proliferation Of Unmanned Autonomous Systems : A Prognosis', RRU Journal 2024
8. Ibid
9. Ibid

10. Prakhar Gupta, “The Next War with China Will Not Begin With A Bang, But With A Blackout — And India Is Not Prepared For It Swaraj”, 22 Apr 25
11. Ibid Nine Inf Div Seminar
12. Lt Gen Anil Kapoor Retired, ‘ Six Strategic Lessons From Russia Ukraine war’, CLAWS Journal 2023

BIBLIOGRAPHY

1. Agarwal A, Gans J, Goldfarb A ‘Prediction Machines : Simple Economics of AI’, 2018
2. Arkin RC,’ Governing Lethal Behaviour in Autonomous Robots’, 2009
3. Floridi L, ‘The Philosophy of Information – A Framework for Thinking About AI Holistically’, 2011Top of Form
4. Gorman Brian, “Change Leadership: Why Your Head, Heart And Gut Are Critical To Listen to “, 04 Mar 2019
5. Horowitz MC, ‘The Ethics & Morality of Robotic Warfare’, 2016
6. Lt Gen Anil Kapoor Retired, ‘AI As A Service – A Perspective’, Podcas BharatShakti.Com
7. Lt Gen Anil Kapoor Retired, ‘ Proliferation Of Unmanned Autonomous Systems : A Prognosis’, RRU Journal 2024
8. Lt Gen Anil Kapoor Retired, ‘ Six Strategic Lessons From Russia Ukraine War’, CLAWS Journal 2023
9. Park J, ‘Opportunities for Neuromorphic Vision Systems: From Sensors to Applications’, 2021
10. Pickard RW, ‘ The Concept of Emotionally Aware AI Systems - Affective Computing’, MIT Press 1997
11. Prakhar Gupta, The Next War with China Will Not Begin With A Bang, But With A Blackout — And India Is Not Prepared For It Swaraj, 22 Apr 25
12. Tucker P, ‘The Future of Manned Unmanned Teaming is Now. Defense One’, 2021

❐❐❐

INNOVATIONS IN AERIAL COMBAT AND INTEGRATION OF AIR POWER WITH GROUND AND NAVAL OPERATIONS

Air Marshal Daljit Singh, PVSM, AVSM, VSM (Retd)

Abstract

Recent past has witnessed rapid technological advances, especially in computer applications, information technology, sensors and propulsion systems. Air power attributes of reach, responsiveness, flexibility and firepower necessitate continuous absorption of technological advances to remain relevant. As the Air Forces absorb these technologies, innovative operational applications of air power are developing at a fast pace. Unmanned Aerial Vehicles (UAV) are now integrated elements of all operations and they are being deployed in many innovative roles, that includes attacks on combat vehicles, troops and other combat elements. Artificial Intelligence (AI) has enabled UAVs to gain more autonomy in navigation and targeting. Only ethical considerations and lack of trust in AI, are restraining UAVs in complete autonomy of operations. Sixth generation fighters are being developed as more lethal, survivable, multiple sensors fitted, and networked platforms, that would collaborate with Unmanned Combat Aerial Vehicles (UCAV) to execute operations much more effectively. This article provides details of evolution of air combat, innovative applications in air combat, present status in India and challenges involved in adapting to the innovations. The article concludes with the recommended best approach for the Indian armed forces to adapt the new technology judiciously.

INTRODUCTION

Major armed conflicts all over the world, substantiate the importance and dominance of the air power in influencing their outcome. With ability to operate in the third dimension of airspace, the air power provides the capability to bypass ground engagements and strike at the critical hubs and centers of gravity of the hostile forces to achieve the desired strategic and operational effects, much faster. The crucial aerial strike of the Residence of the Governor of the then East Pakistan by the Indian Air Force fighters, on 14 December 1971, that shocked the entire governing body so much that it precipitated an immediate decision by Gen Yahya Khan to an unconditional Surrender of the East Pakistan Forces, which led to Independence of Bangladesh. Such is the impact of air power over the psyche and fighting spirit of the adversaries. Responsiveness, reach, mobility and flexibility being the ingredients of air power, it provides the nations with an effective tool to observe, act and strike the hostile targets fast,

and with major damaging effects. Air power provides these advantages for joint operations in other domains of land and sea and generates quick response with adaptability and lethality to create the lasting impact on overall conduct of operations.

The application of air power commenced with air observation, to assess and anticipate hostile actions and conduct aerial attacks with small bombs. Aerial combat followed soon to gain control of the air and protect own ground forces from aerial attacks. Rapid and disruptive technological advances of today, in sensors, communications, computing power, propulsion systems and aerodynamics have brought in tremendous operational capabilities of the Air Forces to provide real-time intelligence, precision strike capability, and simultaneous multiple target attacks. Control of the air still remains a prerequisite for ensuring freedom of operation in the air, on ground and in the sea. However, innovations in employment of low cost armed and autonomous UAVs have changed this situation, as seen in the recent Russia – Ukraine Conflict, where Ukraine Forces could strike deep inside, even up to Moscow, the capital of Russia with UAVs despite having no degree of Control of the air. Even the non-state actors are employing air assets in an innovative manner that inflict heavy costs to the defenders in countering inexpensive, low-cost projectiles and missiles. It is, therefore, important to understand the technological advances that influence the employment of air power and innovations perceived in its application. This would help in shaping the perspective plans of the IAF.

- **Present Characteristics of Air Power:** The core characteristics of air power are reach, flexibility, mobility, responsiveness, offensive lethality and trans-domain operational capability.[1] More efficient aero engines and provision of air-to-air refuelling have generally led to much longer reach of the manned fighters, cruise and ballistic missiles that have trans-continental reach. In Exercise Gagan Shakti 2018, IAF aircraft flew from Eastern bases, hit targets in Southern India, and continued to the Andaman Islands on 8-10 hour missions. The operator has flexibility to employ the aerial assets as per the operational situation. The fighters could be deployed for both the offensive and Air Defence roles. Aerial assets can quickly activate and respond to operational situations, making them ideal to counter air intrusion or natural disaster responses. One of the most prominent developments in the aerospace power has been induction of long-range air to ground precision weapons capable of striking targets deep inside enemy territory when launched from within own territory. The latest technological advances in computer technology, communications, data management, Artificial Intelligence (AI), Robotics and Machine Learning (RML) have revolutionised the operational applications of the air power.

- **Scope:** During operations, the IAF first fights to achieve the required degree of control of the air. Thereafter, IAF conducts strategic air operations independent of other services, towards achieving strategic and national objectives. Simultaneously, 'coordinated air operations' are carried out for and in coordination with own Land and Maritime forces either in furtherance of their objectives or an integrated military objective. These operations emerge from the military strategy and involve all air operations that are carried out in cooperation or in direct coordination with friendly surface forces to deter, contain, neutralise, or defeat the enemy's surface forces over land and sea.[2] The sequencing is not rigid and may undergo a change based on national aim.

  To ensure high degree of success of the air operations, improve situational awareness and minimise attrition, other enabling operations, that include Intelligence Surveillance and Reconnaissance (ISR), Electronic Warfare (EW), Air to Air Refuelling (AAR), Airborne Warning and Control Systems (AWACS) and air mobility operations are conducted to support main air operations. Fighter aircraft, UAVs and helicopters are the main airborne platforms that are employed for strategic and coordinated operations. The scope of this article is to discuss innovations in employment of these airborne platforms that are being considered as the 'air combat' elements. Other enabling air elements would be discussed during the 'Integration of Air Power with Ground and Naval Operations.'

DEVELOPMENT OF AERIAL COMBAT

- **Evolution:** Having understood the potential of 'higher ground', the aeroplanes were first employed to observe and gain intelligence on the deployment of the hostile forces during World War I. Aerial attack on ground troops soon followed by dropping small bombs and grenades. The aerial combat between the opposing forces thereafter commenced to achieve 'control of air' and prevent hostile air elements from interfering with friendly ground operations. The ace pilots who devised their attack tactics, involved spotting the hostile aircraft first, judge its relative position, attack and escape. For the next fifty years, the pilot eyes were the only sensors to spot the hostile aircraft, and machine guns were the main weapons to shoot down the opponent. The effective range of aerial gunnery improved from 50 m during WW-I to about 500 M by the sixties.[3] Pilots needed to position the aircraft behind the target to shoot it down, requiring speed, acceleration, and manoeuvrability in fighter designs. By mid-sixties, the fighters were fitted with basic air to air radars as sensors and Air to Air Missiles (AAM) with Infrared (IR) guided seekers were fired during the conflicts in the Southeast Asia

(Vietnam), Middle East (Arab-Israel) and during Indo-Pak war of 1965. These missiles were required to be fired from rear quarters of the target aircraft and the firing ranges extended to around two nautical miles, which was withing the visual range of pilots. Active radar seeker guided Beyond Visual Range (BVR) missiles were inducted in due course which could be fired from any aspect and increased the kill ranges to nearly 15 nm. Initial reliability of the airborne radars was poor especially when looking down and the kill probability of the BVR was low due to its manoeuvring limitations. From 1965 through 1968, during Operation Rolling Thunder, AIM-7 Sparrow missiles succeeded in downing their targets only 8 percent of the time and AIM-9 Sidewinders only 15 percent of the time.[4] Pre-conflict testing indicated expected success rates of 71 and 65 percent respectively.[5] Over the last fifty years there has been tremendous advancement in airborne intercept radars, other sensors and AAMs, which has expanded the kill envelop of the AAMs to beyond 100 km and advanced missile propulsion technology has expanded the 'no escape zone' of the missiles within which the target aircraft would not be able to out- manoeuvre the AAM. As the BVR missiles have been the most successful weapons in air-to-air engagements, the attributes of the latest fighter designs have accorded lower priority to speed, manoeuvrability and acceleration. Multiple sensor data fusion, securely networked capabilities and protection against electronic attacks are being given higher priority in fighter designs.

- **UAVs:** There was rapid development in fighter designs after World War II and long-range bombers were developed as deterrence forces during the 'Cold War' period. Some old aircraft were modified as radio-controlled unmanned target for training the anti-aircraft gun operators. It was after the U.S. High altitude spy plane U-2 was shot down over the erstwhile USSR, that the U.S. started developing unmanned systems for reconnaissance and intelligence missions. These systems mainly flew pre-planned routes over the hostile territory and could be remotely controlled. However, the UAVs were further developed to undertake the roles of reconnaissance, Signals Intelligence (Sigint) and Battle Damage Assessment (BDA) and were abundantly employed by the US during Vietnam. The Israel Defence Force (IDF) employed the UAVs very effectively during the 1973 Arab-Israeli War as decoys to trigger the hostile Surface to Air Missiles (SAM) and geolocate them for hard kills. The Bekaa Valley operation of 1982, conducted by the IDF in Lebanon saw heavy employment of the UAVs to stimulate the hostile Air Defence Network, map the electronic transmissions and effectively undertake both hard kill and soft kill operations. The entire

world took note of the operational potential of the UAVs and ever since then the UAVs have been integrated into all major aerial operations. As employment of UCAV, the 'Hellfire' air to ground missile was fired for the first time from the Predator UAV on 7 October 2001, to neutralise the terrorists in Afghanistan.[6] The armed UAVs have distinct advantage of obtaining intelligence on target geolocation and striking it and minimising the decision cycle. However, the Medium and High Altitudes Long Endurance (MALE/HALE) UAVs operated very well in a benign operational environment, however, they suffered many losses in a contested environment. Iran has shot down many of the US MALE/HALE class of UAVs including the Global Hawk RQ-65. Anti-national elements like Houthis have adapted to exploiting the munition laden UAVs and ballistic missiles to attack civil and strategic targets of target countries and imposing high costs for the affected countries in fielding their countermeasures. Hamas and Hezbollah terrorist groups had employed UAVs for surveillance and for destroying the Israeli Border Posts during 7 October 2023, attack on Gaza Envelop of Southern Israel. Present conflicts have witnessed very fast advances in UAVs and their innovative employment concepts. The 2020, conflict between Armenia and Azerbaijan witnessed significant increase in employment of low-cost UCAVs with strike capability. More than one hundred T-72 Tanks of Armenia were destroyed by Turkey supplied TB-2 UAVs, which also demoralised the Armenian troops. The UCAVs made armoured vehicles and towed artillery guns quite vulnerable to UAV attacks. Russia-Ukraine war has witnessed many innovative employments of UAVs. There are large number of AI embedded autonomous and remote-controlled UAVs of various sizes which have been employed during the last three years. The U.S. Army Chief of Staff General Randy George observed that the Ukraine war, "has demonstrated the value of small, attritable drones on the battlefield."[7] In December 2024, the Ukraine Forces employed 'First-Person View' (FPV) drones to successfully attack the Russian positions. Kamikaze FPV drones have inflicted heavy casualties to both the forces. More and more AI enabled drone swarms are being employed by the Ukraine Forces, that reach targets autonomously and remain deployed till a target is allocated.

KEY TECHNOLOGICAL ADVANCEMENTS LEADING TO INNOVATIONS

- **Sensors and Data Fusion:** Both active and passive sensors have witnessed tremendous capability enhancements in the last decade. Incorporation of Active Electronic Steering Antenna (AESA) technology achieved through development of Transmitter Receiver Modules (TRM)

and digital doppler processing, has led to much advanced airborne radars that have instantaneous beam steering capability, interleaving operating modes of air detection, ground mapping and synthetic aperture radar modes. The detection ranges have increased to hundreds of km. Electronic jamming of limited frequency range has been incorporated in modern radars. Passive Radar Warning Receivers (RWR) have achieved capability to geolocate hostile transmitters accurate enough to launch hard kill. Digital techniques and high processing capability and improved antenna designs have facilitated this improvement. In infrared frequency regime, Infrared Search and Tracking (IRST) system is now capable of detecting, identifying and synchronising operations with onboard radars and missiles, is a standard fit on all modern fighters. Electro-optical systems have matured with technology to operate in conjunction with IRST for day and night operations. Advances in IR and Ultraviolet radiation detectors have matured missile approach warner systems for timely detection of incoming missiles to counter them with lasers, and other countermeasures. Sensors operating in multiple frequency bands ensure much enhanced performance as it reduces the individual limitations in detection, field of view, and angular resolutions in all types of atmospheric attenuation. UAVs have inherent advantages as it carries multiple sensors thanks to miniaturisation and skin embedded antenna designs. To ensure filtered, accurate and actionable inputs to the pilot, data inputs from all sensors is fused onboard aircraft using advanced computer algorithms. This improves situational awareness of the pilot beyond the operational bubble, declutters the displays and facilitates faster decision making.

- **Artificial Intelligence:** Artificial Intelligence (AI) is being incorporated into all segments of air operations viz, data analysis, communication management, decision making, target analysis, platforms and weapon systems. It will transform the future of operations by improving operational efficiency and decision-making process. The simulated combat between the AI embedded fighter and experienced pilot operated same type of aircraft has repeatedly shown the superiority of the AI flown aircraft. Teaming of unmanned UAVs and manned aircraft requires more advanced AI capability to ensure collaborative operation especially in an electromagnetic spectrum restricted environment. Other ethical issues and lack of complete trust on total autonomy of operation of unmanned systems would take time. Human in the loop will continue to stay in the foreseeable future.

- **Stealth Technology:** This technology in aircraft design involves incorporation of technical features in the aircraft body for reduction of Radar Cross Section (RCS) and infra-red detection. This is the first considered design feature of combat aircraft and UAVs. An intelligent fusion of aircraft manoeuvrability and stealth is a complex design consideration which requires deliberate commitment as this design cannot be changed during the aircraft life span. The stealth effectiveness is restricted to a limited frequency band and all aspect stealth effectiveness is hard to attain due to engine exhaust and control surfaces. Advances in aircraft detection systems and radars have diluted the stealth effectiveness and ECM payloads are now considered complimentary to enhance effectiveness.
- **Communications and Net Centricity:** Innovations in information technology, software, hardware, and digitisation have enhanced the reliability, resilience, and data flow of communication networks. Satellite communication has added another important layer of connectivity in remote and inaccessible areas. Networking of sensors, decisionmakers and shooters have improved situational awareness and compressed decision cycle. All forces around the world have adapted net-centric operations which has force multiplying impact on operations.
- **Hypersonic Technology:** Hypersonic platforms can fly at five times the speed of sound, that corresponds to speed of more than 1.6 km per second. Mainly two types of hypersonic weapons are being developed, that include, Hypersonic Glide Vehicles (HGV) that are launched like ballistic missiles, before gliding to hit the target, whereas the Hypersonic Cruise Missiles (HCM) are powered throughout the flight. Development of scramjet technology has led to stable propulsion system throughout the hypersonic regime and metallurgy has matured to produce material that can withstand high frictional heating stress throughout the flight.

PERCEPTION AND PROGRESS ON INNOVATIONS IN AIR COMBAT SYSTEMS

- **Next Generation Fighters:** Fight for control of the air would continue to be prerequisite in future, along with control of the electromagnetic spectrum and cyberspace. Next generation fighters will have to fight in a highly contested and well-defended airspace, as long-range integrated Air and Missile Defence Systems are being fielded. To that end, many next generation fighter programs are being progressed that will see dominance of manned fighters for the next three decades, as these fighters will be adaptable, upgradable and networkable with other combat elements. All the next generation fighters will have much more

advanced stealth features incorporating Broadband All Aspect (B2A2) stealth, multi-spectral sensors for all around situational awareness, AI supported for scalable autonomy, more lethality with long range precision strike weapons, efficient propulsion system, onboard date processing capability and ability to control and collaborate with intelligent unmanned systems through secure pluggable, robust and resilient communication network. More powerful propulsion system will provide adequate power to have lasers as Directed Energy Weapons (DEW) and EW protection systems to improve survivability. All NGFA are being designed and configured to operate as team leaders of 'Manned-Unmanned teams'(MUMT). Many NGFA programs have progressed significantly, and the development process is being compressed by employing digital engineering techniques. The UK has launched 'Tempest' sixth generation fighter aircraft, under Future Combat Aircraft System. BAE Systems was awarded the contract in 2021, to design and develop the aircraft. Italy and Japan have joined the UK in The Global Combat Air Programme (GCAP), established in 2022, is an international partnership between the UK, Japan and Italy which will design, manufacture, and deliver a next-generation crewed combat aircraft. The collaborative development phase of the programme is scheduled to commence in 2025 and aims to create a highly advanced, interoperable, adaptable and connected fighter jet. The Tempest is scheduled to be in service with the British Royal Air Force (RAF) by 2035. The fighter aircraft will serve as a connected node within a system of systems across all domains in the battlespace.

It will operate in co-ordination with other systems in the FCAS, such as uncrewed combat aircraft, civil platforms, satellites and cybersecurity centres, in future conflicts. The aircraft will employ AI, machine learning and autonomous systems to provide manned/unmanned flying capabilities. It is also expected to use swarming technology to control drones.[8] In Europe, France, Germany and Spain have teamed up to develop SCAF/FCAS New Generation Weapon System (NGWS) in which crewed fighter aircraft will be teamed with unmanned aerial systems, and well connected with other remote systems in the air, on the ground, at sea and in cyberspace via a data cloud called the 'Combat Cloud.' Building Block approach is being followed to achieve scalable enhanced situational awareness, followed by manned unmanned teaming by 2040. The US has planned development of Next Generation Air Dominance (NGAD), system. The NGAD family or system of systems includes the NGAD fighter program, as well as the Collaborative Combat Aircraft (CCA) program to develop variants of uncrewed, semiautonomous aircraft that could fly as 'loyal wingmen' with the NGAD fighter or other fighter aircraft.[9] Boeing has won

the contract to develop this sixth generation fighter dubbed as F-47, which is likely to enter service by 2030 and replace the F-22 fighter. The jet will have exceptional stealth capability, communications and weapon systems. Many other countries have planned development of similar advanced fighters. The prominent amongst these are, SU-57 of Russia, F-X of Japan and KAAN of Turkey. China recently demonstrated two sixth generation fighters designated J-36 and J-50, which took the world by surprise. Some of these fighters have undertaken many flights and have consolidated the designs. Some important aspects are as under:

- **Collaborative Combat Aircraft Plans:** Introduction of AI and ML into unmanned airborne platforms has led to well proven unmanned air vehicles that can fly autonomously and in collaboration with other fighters. General Atomics Aeronautical Systems (GA-ASI) and Tech Company Shield AI flew MQ-20 'Avenger' UCAV totally autonomously during test Exercise 'Orange 25-1' conducted by the U.S. Air Force Test Centre on February 19-21, 2025, at Edwards Air Force Base.[10] At the same Base an AI controlled F-16 fighter flew autonomously against a crew manned F-16 and engaged in a dogfight. These developments have been prompted by disruptive advances in AI and ML. In future most of the air combat operations will be conducted as manned-unmanned teams where UCAVs with various payloads will be coordinated by the teaming fighter. The UCAVs would be the 'loyal wingman' to the fighter that could undertake ISR, fighter escort, stand-off strike or EW missions in synchronisation with the fighter. This ensures an excellent combination of manned and unmanned assets for undertaking operations.
- **Hypersonic Weapons:** Ballistic missiles with hypersonic speeds have been in existence for nearly seven decades. What differentiates the HGV from Ballistic missiles is that they do not follow the parabolic and predictable trajectory, they gain much lower height trajectory and can conduct programmed manoeuvres during flight to prevent successful interception. HCM fly at lower altitudes due to which, the conventional radars are unable to detect them in time and they cannot be intercepted with the present systems. Russia has employed the air launched Kh-47M2 Kinzhal hypersonic missile to strike targets in Ukraine on many occasions.[11] Russia has also demonstrated a ship launched hypersonic cruise missile 'Zircon'. Many countries including India are conducting extensive research on hypersonic technology. China has claimed to have developed air launched, ground and sea based HCM. The main advantage of the missile is that it strikes the target in a very short time and with pinpoint accuracy. Its kinetic energy itself generates massive destructive power. However, the missiles are expensive and would

always be limited in numbers. They would be employed against time sensitive, high value and in-depth targets. Research is already on to develop satellite-based detection systems to counter hypersonic missiles.

- **UCAV and Other UAVs:** UCAVs are being regularly employed to hit time sensitive targets with precision. Long loiter time and capability to detect and destroy the target simultaneously, is a unique capability that will be exploited in the future. While adequate autonomy has be achieved in UCAV operations, man-in-the-loop concept to take final decision for strike is likely to prevail in future, till ethical issues and trust in the system are resolved. Small FPV UAVs and swarm UAVs have matured for employment and their deployment will be integrated with all ground operations. Loitering munitions are the standard inventories of all regular forces. Non-state actors are already employing such UAVs to strike civilian and military targets and their employment by them will continue to increase. The next-generation UAS will handle ISR, surface strike, air defence, aerial refuelling, and air delivery missions either in collaboration with the teaming fighters or independently.

INDIAN STATUS

Advance Medium Combat Aircraft (AMCA) is the fifth-generation stealth fighter project being led by Aeronautical Development Agency (ADA) in collaboration with Hindustan Aeronautics Ltd HAL). In 2009, the Government had sanctioned Rs. 90 crores for the feasibility study and additional funds have been allocated for further development. The AMCA is envisaged as a 25-ton twin-engine stealth aircraft with an internal weapons bay and diverter less supersonic intake. It is intended to have an internal carriage of 1,500 kg of payload and 5,500 kg of external payload with 6,500 kg of internal fuel. The IAF plans to induct seven squadrons (126 aircraft) with first two squadron powered by GE- F 414 American engine followed by the indigenous engine for the rest. The first prototype flight has been delayed extensively and is now planned for 2028. The production is likely to commence in 2034. HAL is progressing with Combat Air Teaming System (CATS) as part of manned unmanned teaming system. Initially LCA Mk1trainer aircraft is planned to be the Mothership for Air Teaming Exploitation (MAX). Private industry NewSpace Research and Technologies, DRDO and NAL participate in the project. Various unmanned platforms such as the CATS Warrior, CATS Hunter and CATS Air Launched Flexible Asset (ALFA) can operate under mothership or independently as per operational scenario. Relevant sensors and communication networks are being planned, and the project will take some time to fructify. DRDO had initiated development of MALE class of UAVs named ‘Rustom’ and ‘Tapas.’ Some flights were conducted to

progress the development; however, the project has not been successful. In the meantime, India has procured 31 MQ-9B Reaper HALE UAV from General Atomics Company and India has joined as 'observer' in the Euro drone MALE UAV program of the Europe, which is being developed by Airbus Defence and Space, Leonardo Spa and Dassault Aviation. DRDO has been conducting comprehensive research to develop scramjet engine, control mechanisms and other materials for developing Hypersonic weapons.

PRESENT CHALLENGES

- **Integration of Present Assets:** The present fleet of fighters and other combat support elements will continue to be operational for the next decade at least. They lack in multiple sensors; computing power and connectivity will restrict their integration with other combat support elements. The F-22 fighter aircraft of the U.S. was not integrated with other airborne fleets for more than a decade due to communication connectivity issues. Innovation in air combat would, therefore, require incremental and adaptive approach.
- **Control over EMS:** Air combat innovations are highly dependent on communication connectivity and efficient operation of active and passive sensors. MUMT and UCAV operations would be disrupted when hostile forces employ offensive EW measures to disrupt connectivity and degrade onboard sensors. EW will play more crucial role in future operations and all forces around the world have prioritised research on this aspect of EW. The forces would require resilient communication with multi-spectral redundancy.
- **Trust in AI and Ethics:** The AI has matured enough to start employing autonomous weapons and systems. However, the leaders have yet to gain trust in the AI enabled autonomous systems. The autonomous systems being employed to kill human beings is yet to accepted ethically and it will require lots of deliberation at international level to decide on this sensitive issue. Use of Lethal Autonomous Weapon Systems (LAWS) is being debated in international fora, with no consensus reached so far.
- **Cost Factors:** Most of the countries have scaled down the operational requirements of the future combat aircraft to scale down the procurement and operations cost. The NGAD fighter is likely to cost half the price of the F-22 fighter. Survivability and reliability of the Collaborative UCAVs would increase their costs resistance to offensive EMSO will further escalate the prices. All countries will face this budgetary challenges to adapt to the technological advances.

- **Standardisation and Interoperability:** Open architecture and standard software for connectivity and exchange of information amongst the operational elements would be essential. The present IAF aircraft inventory procured from different countries does not have this standardisation and compatibility. This will need to be addressed for future inductions. The armed forces have yet to achieve complete interoperability amongst UAVs, airborne platforms and ground-based sensors, even though considerable effort is being made in this regard.
- **Status of Indian Defence Industry:** R&D in the Indian Defence Industry has not kept pace with the technological developments. Even DRDO requires much more push in this area. This will impact the pace of technology absorption by the armed forces.

INTEGRATION WITH GROUND AND NAVAL FORCES

- **Air Power:** Air power influences the outcome of all operations due to requirement of control of air for other services to prosecute war. Joint operations require constructive collaboration in operations where unique attributes of each service in their domains are exploited effectively. The Air power attributes of responsiveness, reach, flexibility, precision strike and elevated horizon provide excellent support to operations of the other services, while the IAF parallelly conducts its own independent operations as well. Airspace management, control of the air and an inegrated umbrella of area air defence ensure well-coordinated operations with high degree of non-interference from hostile air forces. At present, the integration between the two services with organisation of IAF Advance Headquarters and Maritime Air Operations Centre is quite well established. The present support of the IAF to the Army and Navy providing vertical air lift, protection against hostile air elements, battlefield air strike, intelligence and air situation picture are well understood, it is important to understand how future innovation in air combat would be integrated with ground and naval forces and what would be the payoffs.
- **Ground Forces:** Networked operations would provide much better situational awareness, much more in-depth actionable and filtered intelligence to the ground forces for better and faster operational and tactical decisions. AWACS scanning deep inside hostile airspace will provide sufficient early warning to the ground forces against hostile air threat. Long range precision strike capability would ensure better air interdiction of hostile ground forces that would prevent them from effective reinforcement of men and material. Jointly networked forces would ensure much better conduct of operations. MALE/HALE would be optimally deployed, without any duplication of effort, as the air situation

inputs would be available to all the forces in real time. It is inevitable that the ground forces will employ many types of UAVs, integrated with other ground operations, management of airspace to ensure freedom of operation without fratricide would be crucial. With networked operations, the airspace management would be more streamlined. Induction of Brahmos class of missiles in the Army would require coordination of targeting with the IAF offensive force to optimise the operational resources.

- **Naval Forces:** Good maritime domain awareness is essential for effective planning and execution of maritime operations. With extensive networking of aerial assets of the IAF and the Indian Navy (IN), the naval decision makers and the combatants will have much better situational awareness in the air and in the sea. Maritime Patrol Aircraft (MPA) would seamlessly share data with the IAF AWACS and CATS elements. The IAF would effectively support the IN in attacking shore based and in the sea hostile targets, with employment of stealth platforms having long range weapon delivery capability. Due to networked operations, both the forces would be able to share assets to enhance intelligence and increase the weight of attack. Air cover and EW assets would be better integrated and shared to provide comprehensive protection to friendly forces. As the naval fighter aircraft will invariably have range restrictions when they get airborne from aircraft carriers, the IAF AAR would be crucial to support the Naval fighter operations for long range strike and for combat air patrols. Integrated operations will mature further as the technological advances are imbibed in the services.

RECOMMENDED WAY FORWARD

- As the technological advances are absorbed by the armed forces, it is important to ensure that the operational assets are provisioned to get seamlessly networked to share information and enhance situational awareness. All airborne assets and associated ground command and control centres must have interoperable communication equipment.
- The future operations will utilise much larger part of electromagnetic spectrum, as much more sensors, communication networks and aerial assets would be employed simultaneously. EM spectrum management would be crucial to avoid mutual electromagnetic interference and exploit available em spectrum efficiently. This would require coordination at Headquarters, Integrated Defence Staff (HQ IDS).
- Serious effort is required to acquire the capability to monitor the hostile EMS operation, especially communication networks, and capability to

deny/degrade the freedom to the hostile forces to operate effectively in EMS. All aspects of EW require serious development in India, to operate effectively in future operational environment.

- Indian Defence Industry must gear up to embed AI and ML in future aerial assets, sensors and weapons. More emphasis should be on research and Development, which should be supported by DRDO with adequate funding.
- Most of the new projects in the world are progressing with collaboration and cooperation with other countries to exploit the expertise of many defence companies. This will accelerate absorption of technology and help in sharing the developmental costs. India has taken initiative in this regard. However, more commitment in this regard will ensure timely induction of modern assets.

CONCLUSION

Air power has always been insatiable to absorb and exploit technology. In a comparatively short time, the airborne fighting machines have developed from biplanes with piston engines to omni role supersonic, smart airborne platforms embedded with multiple sensors, hundreds of computer chips, computer managed aircraft control systems and powerplants and much larger combat zones, firepower reach and long-range precision strike capability. In the last decade there has been disruptive technological advances in computers, information technology, sensors, communications and propulsion systems that has brought in innovations in air power applications. Induction of artificial intelligence and robotics have ushered in unmanned systems with high degree of autonomy in operations and affordable air power capabilities. Most the Air Forces around the world are progressing towards innovative air combat concepts. Sixth generation fighters, that operate as system of systems by teaming with unmanned UCAVs, are developing at a fast pace. Employment of UAVs has proliferated extensively around the world amongst the conventional as well as asymmetric forces. Hypersonic weapons have already been employed operationally, however, it will take some more time to evaluate their employability considering the costs. India is also imbibing these technologic advances gradually. AMCA and CATS are progressing steadily. However, there are challenges of EMS management, disruption to net-centric operations by hostile EW action and interoperability issues. Indian Defence Industry is required to gear up to absorb the technological advances and make the modern systems available to the armed forces in time. Collaboration with expert foreign defence companies will accelerate this technology absorption process, and gain expertise for future developments.

❖❖❖

Air Marshal Daljit Singh, PVSM, AVSM, VSM (Retd) was an Air Officer Commanding-in-Chief of an operational Command. He regularly writes article on defence strategy in various magazines and has been a keynote speaker in many International Seminars on Electronic Warfare and Air Defence.

NOTES

1. Doctrine of Indian Air Force, IAP 2000-22 (Indian Air Force Air Headquarters Vayu Bhawan Rafi Marg New Delhi 110106) p-04
2. Ibid, p-53.
3. Trends in Air-to- Air Combat, Implications for Future Air Superiority. John Stillon, Centre for Strategy and Budgetary Assessments, 2015. 1667 K Street NW Suite 900, Washington DC-20006. Summary, p-I
4. Ibid p-10
5. Doctrine of Indian Air Force, IAP 2000-22 (Indian Air Force Air Headquarters Vayu Bhawan Rafi Marg New Delhi 110106) p-04
6. Gp Capt. RK Narang, India's Quest for UAVs and Challenges, KW Publishers Pvt Ltd, New Delhi.p-30
7. Samuel Bendett and David Kirichenko, Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine. Madern War Institute at West Point, January 10, 2025.accessed on March 15, 2025
8. Tempest Future Combat Aircraft System (FCAS) UK, January 22, 2024. https://www.airforce-technology.com/projects/tempest-future-combat-air-system-fcas-aircraft-uk/?cf-view&cf-closed accessed on March 21, 2025
9. Jennifer DiMascio, Analyst in U.S. Defense Policy, U.S. Air Force Next-Generation Air Dominance (NGAD) Fighter, Congress Research Service (IN FOCUS), updated on January 17,2025.
10. Andrea Daolio, General Atomics MQ-20 Avenger unmanned combat aerial vehicle autonomously flown with Shield AI's Hivemind software at Orange Flag exercise. Published on March 06, 2025. https://theaviationist.com/2025/03/06/mq-20-avenger-flies-autonomously-hive. Accessed on March 22, 2025.
11. Lyle Goldstein and Nathan Waechter, (2024), "China Evaluates Russia's Use of Hypersonic 'Daggers' in the Ukraine War", RAND, URL: https://www.rand.org/pubs/commentary/2024/01/china–evaluatesrussias–use–of–hypersonic–daggers–html

❐❐❐

87-105

AI - ENABLED DRONES: A JOINT PERSPECTIVE

Lt Col Akshat Upadhyay

Abstract

This paper aims to understand conceptually the integration of artificial intelligence-enabled drones (AI-enabled drones) into the doctrinal framework of armed forces from a joint planning and utility perspective. To do this, the author introduces the concept of a 'techno-platform', a hybrid platform which flips the concept of how war-fighting platforms are envisaged. Instead of centering the platform as the mainstay of war fighting and then upgrading it through increments or technological packages, the techno-platform accords primacy to the overall technological hybrid, with the system or network effect dominating over individual attributes of the platform. Through this viewpoint, the hi-tech requirements of a budget-constrained force can be distilled and used for practical policy recommendations. The article also attempts to slightly shift the focus from the 'What' of the capabilities to the 'How'. Assuming a repertoire of capabilities, out of which a force can select certain critical ones relevant to a particular geo-political context, how does that force then ensure the application of that inventory of capabilities in the most optimal manner? This requires a careful selection, Research and Development (R&D) and vetting of platforms based on the three pillars of interoperability, standardisation and compatibility.

Case studies from the Nagorno-Karabakh, Russia-Ukraine and Gaza conflicts reveal accelerating innovation in the use of drones for a number of purposes across aerial, land, maritime, Electronic Warfare (EW) and cyber domains. The reason behind choosing these studies is to highlight the breakneck speed at which innovations (measures and countermeasures) are being undertaken by adversaries. Sparks of the trinity, as mentioned before, are visible in a majority of the cases. These examples make more sense for the Russian and Ukrainian forces since there is a distinct service-specific culture within these forces and therefore a deliberate attempt to use multi-domain approaches in drone applications is appreciable. On the other hand, the Israeli Defence Force (IDF) does not face such a challenge due to unity of command.

Though the recommendations are meant for the Indian Armed Forces, the approach is more conceptual and broader in nature since a number of projects and technologies are under wraps and there is little clarity on the number of structural and procedural issues, even within the forces.

INTRODUCTION

The use of Artificial Intelligence (AI) enabled drones on the battlefield is affecting outcomes in favour of the side using it more frequently and at scale.

One may attribute this to the classic prime mover advantage, however the reality is far more complex. A combination of a general usage platform (aerial drones) and powerful technology (AI), the green shoots of their usage were initially seen during the war between Azerbaijan and Armenia over the disputed territory of Nagorno-Karabakh, with later uses in Ukraine and Gaza amplifying and proliferating both quantity and concepts. As generally observed during the deployment of any nascent or previously-untested technology on the battlefield, this usage has provided ideas and concepts to the latter players. The pace of real-time innovation seen on the battlefield has been exhilarating and as a result of this speed, a number of innovations seen in this and other fields are yet to be concretised and formalised into Tactics, Training and Procedures (TTPs). The ongoing war in Ukraine has accelerated the pace of development and deployment of these drones, with innovations and ideas occurring at a rapid pace on both sides. Hopping from the aerial domain, the use of AI-enabled drones has now moved on to the land and maritime domain as well.

There are a number of countries, including India, which are concurrently developing AI-enabled platforms to use on future battlefields in all three traditional domains of warfare. However, the kinds of threats that militaries across the world face and will face in the future, will require joint and multi-domain war waging capabilities. AI-enabled drones, with their inherent advantages, will form one of the main components of this change. This paper, therefore, looks at the broader conceptual framework of AI-enabled drones, various methods of classification and possible operational concepts. Learning vicariously from actors already using this 'techno-platform', this paper will analyses case studies from the Russia-Ukraine, Armenia-Azerbaijan and the Israel-Hamas wars to look at the future implications. Finally, this paper will lay out the three main aims that need to be looked at by a joint force attempting to absorb this techno-platform into its own doctrines and concepts ie standardisation, interoperability and compatibility. The unifying ideology of the techno-platform will bind together these three concepts and provide an effective milestone for service and joint procurement requirements.

WHAT IS A 'TECHNO-PLATFORM'?

The author introduces a new term called a 'techno-platform'. This is to distinguish it from industrial-era systems such as tanks, jets and armoured personnel carriers. A techno-platform is a convergence of established physical warfighting platforms with abstracted and emerging technologies, each mutually transforming and affecting each other's capabilities. This latest phase of military technological evolution represents fully developed digital technologies looking for physical embodiment to act in and impact the physical world. In other words, technologies are looking for platforms rather than the other way round. To make

this concept more clearer, imagine a drone with a specific imaging payload. We assume that the drone is equipped with an Infrared (IR) camera and intends to carry out a silent reconnaissance of an adversary platoon position in the dark. Once spotted, it would be required to perform a number of actions, based on its mandate. It can either conduct persistent reconnaissance, send images and data back to a command centre for analysis or if equipped and authorised, conduct a kinetic strike. However, all this requires a lot of to and fro between the platform and the command centre and further, if the drone is just a reconnaissance platform, imposing avoidable delays in engaging a movable and opportunity target. However, what if the analysis, networking and kinetic capabilities are spread and diffused across a network of drones and command centres with edge computing capabilities spread across the system based on mission parameters. This is the capability that a techno-platform possesses. An onboard AI can classify and analyse the images, call on a network of drones, some for Air Defence (AD) and some for kinetic strikes, while another set performs Post Strike Damage Assessment (PSDA), all without reference to a human operator. The power of the techno-platform is not in the individual platforms but the connections and the capabilities between the platforms, powered by the class of niche and emerging technologies.

Certain key parameters of these techno-platforms need to be introduced here. These include bi-directional integration where instead of traditional platforms simply hosting technologies, mutual adaptation occurs between the technology and the platform; capability augmentation where the combined capabilities of the platform are far greater than the individual components; dynamic reconfigurability where dynamic and real-time software updates or modular swapping of hardware such as payload, propeller or sensor can be achieved in a rapid time frame, allowing for the same platform to achieve multiple aims; and cross-domain applicability where the same set of technologies can be used across multiple physical platforms with minimal modifications (climbing up the generality ladder).

It is crucial to understand, how are these how are these systems different from the industrial-era systems or, more broadly, the entire philosophy underpinning the traditional military-industrial complex. The primary value of the industrial-era systems is derived from their physical characteristics, for example the development of tanks took into account their armour protection, firepower and speed, among other considerations. Their capabilities are usually fixed at the design stage and take years (10-30) of experimentation and testing for development and manufacturing, with performance improvements occurring on an incremental basis and strictly on hardware modifications. Over the operational lifecycle of the platforms, the capabilities degrade gradually due to wear and tear.

Traditional platforms also have a predictable performance envelope with hardly any space for any 'countermeasure holiday'[1] since most of their counters have already been developed, and it is more a question of either a 'mix and match' of capabilities or just creating a more powerful 'anti-system'. For example, a powerful tank can be countered by a more powerful Anti-Tank Guided Missile (ATGM). An Explosive Reactive Armour (ERA) can be defeated by a tandem warhead. There is only so much that a traditional weapon platform can improve upon since it is based solely on the individual capacity of the particular platform. Systems like these, therefore, rely heavily on human operators. The more adept an operator is, the more effectively the platform performs. Again, the philosophy is that of an individual machine. These platforms were designed and developed when the field of electronics had not even been birthed, and the focus on human dexterity is an outcome of this thinking. This creates a training paradigm focused on developing muscle memory through repetitive practice, connecting causally the operator's individual performance with the system's output. As per this framework, the physical equipment holds primary value, while information exchange and network capabilities serve merely as auxiliary functions, if at all. These systems typically offer minimal integration with other platforms, resulting in military doctrines that remain fundamentally limited by the inherent constraints of the equipment itself.

In contrast, the techno-platform represents a shift in approach. It fundamentally challenges the existing thought process about how military force is conceptualised and applied. Instead of being constrained by the physical characteristics of the platform, one can visualise the desired effects first, then develop techno-platforms to deliver those effects across the kinetic and non-kinetic domains. The doctrines can be co-evolved along with the platforms. Consider, for example, a swarm of low-cost drones powered by intelligent swarm algorithms. Individually, these drones do not account for much in terms of either speed, firepower, mass or manoeuvrability. However, once assembled in a swarm, these drones communicate with each other in real-time, continuously distributing processing power between them based on mission requirements. A Suppression of Enemy Air Defence (SEAD) mission may require some drones to 'sacrifice' themselves, identifying the Air Defence (AD) platforms in the process. The swarm will, based on the pattern of firing of the AD systems, redistribute or redivide itself to form a precision weapon and can saturate a particular position with ease, with zero human casualties. The value of the techno-platform, therefore, is derived mainly from the information processing and decision capabilities of the algorithm combined with the platform. The technology and platform act as perfect partners, complementing each other. Interestingly, the performance differentiation is usually invisible to physical inspection since the upgrades are in the processing power and computing.

As a result, the core capabilities can be increased exponentially with minimal hardware upgrades. The techno-platforms, in terms of development, form a hybrid cycle, with the hardware taking years (still much less than industrial-era systems) and software months. Throughout their lifecycle, the capabilities can be continuously upgraded. Even if the platform gets degraded due to wear and tear, it can be swapped out with the same or a better model since the techno-platform is optimised for adaptability and technology integration. The individual platform is never the centre of attention. It is seen as a node in a wider network, with different nodes ingesting, processing and distributing information based on mission requirements. Information sharing is the most important function, both in terms of communication and decision making, and effectiveness of the system is enhanced by system interactions. The performance envelope becomes dynamic and more importantly, unpredictable for the adversary due to the emergent characteristics of the technology. This can lead to a persistent 'countermeasure holiday'[2] where the prime mover gets a temporal lead over his adversary due to the lack of any countermeasures. The most important attribute, however, of this platform is its interfacing with human users. Instead of skills, the focus shifts to cognition and decision-making since semi-autonomous or autonomous systems are performing the actions and manoeuvres on ground. Certain challenges with the bodily functions of human beings such as emotions, fatigue etc can be mitigated through the use of AI algorithms. Training shifts from muscle memory formation to human-machine teaming.

A TECHNO-PLATFORM PARADIGM SHIFT IN MODERN DEFENCE MANUFACTURING

The broad idea behind the creation of techno-platforms is now being extended into the design and development (D&D) of legacy platforms, with entire companies embracing this process. A short dive into two case studies will help to illustrate this idea.

GLOBAL COMBAT AIR PROGRAMME (GCAP)

The Global Combat Air Programme (GCAP) is a multinational initiative led by the UK, Japan and Italy and aims to jointly develop a sixth generation stealth fighter, with an aim to replacing the Eurofighter Typhoon in service with the Royal Air Force (RAF) and Italian Air Force, as well as the Mitsubishi F-2 with the Japanese Air Self-Defence Force (JASDF).[3] Unlike traditional fighter development programs, the GCAP is visualised with a digital architecture, where a core software-defined computing environment separates hardware from software functions. While, in traditional aircraft, systems like radar, flight control, weapons management etc are physically integrated through dedicated hardware connections, the GCAP's entire functionality is composed of three

layers viz core infrastructure layer (high-performance computing network distributed throughout the aircraft),[4] middleware integration layer (handles resource allocation, manages communication between the systems and established standardised applications programming interfaces or APIs for all aircraft functions)[5] and, finally the application layer (combat functions of the aircraft such as radar, sensors, EW, flight control and weapons management implemented as software applications).[6] This is the best example of the creation of a techno-platform with four advantages of software-based upgrades, parallel development of different sub-systems, real-time and rapid integration of new technologies, and spiral development.

ANDURIL'S HYPERSCALE DEFENCE MANUFACTURING

Anduril is a US based manufacturer of autonomous defence platforms. Its approach to manufacturing these systems is radical and quite different to conventional manufacturing. As stated by Gen David Petraeus (Retd) during the recently convened Raisina Dialogue 2025, Anduril, instead of waiting for procurement orders or tendering processes, has already built up a new manufacturing facility for producing autonomous systems.[7] That facility is called 'Arsenal'[8] which forms the core of the company's software-defined manufacturing and is powered by the Arsenal Manufacturing Operating System (OS). The startup secured a $1.5 billion in funding to construct 'Arsenal', which sprawls an area of almost five million square foot.[9] As per the company's website, the Arsenal OS is a "proprietary manufacturing execution software system that manages threat-based operational analysis, modeling, simulation, drawing, testing, bill of materials management, work orders, production, and data management across the product lifecycle".[10] The company focuses on low-cost materials and Commercially available Off-The-Shelf (COTS) products such as electronics and sensors to rapidly iterate prototypes in a spiral development model.[11] This allows them to incorporate emerging technologies continuously rather than freezing designs early in development. Instead of piecemeal construction, the company intends to rapidly produce tens of thousands of autonomous systems.

As seen from the two examples above, the twin paradigms of software-defined capabilities and techno-platforms are steadily being integrated into the D&D of legacy platforms, envisioning the platforms and their manufacturing processes anew. Emerging technologies and processes are not only being embedded within the platforms but also being used to drive innovation in their very construction and production. Now let's pivot to the AI-enabled drone and see how this techno-platform paradigm can be used to think about new concepts for the deployment of these platforms from a joint perspective.

DEFINING AN AI-ENABLED DRONE

AI-enabled drones refer to Unmanned Aerial Vehicles (UAVs) equipped with AI algorithms and sensor systems that enable autonomous operation, real-time environmental analysis and adaptive decision-making without continuous human intervention.[12] These drones integrate Machine Learning (ML), Computer Vision (CV) and sensor fusion technologies[13] to process data from cameras, Light Detection and Ranging (LiDAR), Global Positioning System (GPS) and other sensors, allowing them to navigate complex environments, avoid obstacles and optimise mission execution.[14] When referring to drones, all three domains are being considered i.e. aerial (Unmanned Aerial Systems or UAS), land-based (Unmanned Ground Vehicles or UGVs) and maritime (Unmanned Underwater Vehicles or UUVs and Unmanned Surface Vessels or USVs). These systems serve as platforms where AI and other payloads such as sensors, communication links, routers and weapon systems may be mounted based on the mission objectives, in a modular fashion. In terms of attributes, an AI-enabled drone possesses onboard computational capability. This can manifest in multiple ways. For example, a drone can have edge computing when operating in a denied environment or when carrying out a mission where communication latency with a centralised server is low.[15] Onboard computation can also involve fog computing which implies creating a distributed layer of computing resources between the edge device ie the drone and the server. These are relevant from the perspective of swarm operations and resiliency.[16] Startups are now experimenting with Visual-Language-Action models mounted on drones which combine the pattern recognition of Large Language Models (LLMs) with proprietary models developed for routing and autonomous operations.[17] The drone also has some amount of decision making capability within defined parameters and maintains varying degrees of autonomy based on different mission phases and functions. In terms of functionalities, an AI-enabled drone comprises six functions: perceive and interpret; navigate and manoeuvre; identify and classify objects or situations; make tactical decisions; learn from operational experience or context; and communicate and coordinate.

CASE STUDIES

Before moving on to the conceptual framework for the possible use of AI-enabled drones in the Indian Armed Forces, it is important to look at how these techno-platforms are being utilised in contemporary conflicts. Analysis of these uses will help highlight important points with respect to the deployment of these drones in the Indian context. The analysis will focus on how AI-enabled drone capabilities have evolved over conflicts and what are the major areas that have seen major developments in these conflicts.

Distinct patterns have emerged over a period of last five years in the usage of AI-enabled drones in conflicts. In fact, one can discern three major phases: early autonomy during the Armenia-Azerbaijan conflict where Harop Loitering Munitions (LM) with pre-programmed search patterns and autonomous radar targeting were used in consonance with Bayraktar TB-2 drones using Machine Learning (ML) algorithms for identifying armoured vehicles.[18] Adaptive AI, edge computing and swarm drones are being demonstrated in the ongoing Russia-Ukraine war while the Hamas-Israel war has seen mass deployment of ML algorithms for generating mass targets especially by Leveraging Large Language Models (LLMs) and commercial AI,[19] as well as enhanced uses of Human Machine Teaming (HMT), where AI handles data processing and humans approve strikes. One can see a kind of sine curve in the pattern of AI-enabled drones, where the initial use witnessed a heavy use of AI platforms, however, these were very limited in their capabilities. The use of AI-enabled drones has been put on steroids in the ongoing Russia-Ukraine war. This war represents the high watermark of the usage of these platforms in terms of pushing their applications of autonomy vis-a-vis human control. The Wild West sorts of innovation currently being witnessed on the battlefield also implies a lot of trial and error on the go, lack of any formalisation of TTPs and dilution of many safeguards facilitating human machine interaction and teaming. There is also a lot of contextual innovation relevant to the prevailing conditions on the battlefield, which may make it difficult to replicate the same results or organisations anywhere else. Finally, the Israel-Hamas conflict has witnessed the other side of the curve, where human operators and algorithms have collaborated to create a massive identification and targeting machine that has, at times, made no difference between terrorists and civilians.

Looking at the use of AI-enabled drones across these conflicts, most are concerned with Electronic Warfare (EW), autonomous targeting and steering and counter-EW measures. The Ukrainian battlefield is currently witnessing innovations at an unprecedented speed and tempo, with measures and countermeasures being devised almost instantly. There is, however, a subtle difference visible in the way the Russians use their drones versus their Ukrainian counterparts. The former are absorbing them in their already established hierarchy, while the latter are experimenting with new structures, mostly due to two reasons: a proactive attempt to do away with the Soviet doctrines and war-waging philosophy that both sides have been trained on; and melding and integrating diverse systems from other countries together. These attempts are ongoing along with the ad-hoc measures mentioned above. As per the commander of Ukraine's drone forces, they are pursuing a 'robots first' military strategy. In terms of functionalities, AI-enabled systems are being used primarily in the fields of target acquisition, terrain mapping, counter UAS and creation of

swarms. A functional classification of these uses may assist in understanding these use-cases further:

- **Target Acquisition:** Orbiter-3 drones were used in the Armenia-Azerbaijan conflict where AI-driven surveillance was used for artillery fires coordination. The Russians are currently using the “Vetr” series of FPV drones with AI-enabled autonomous target acquisition and attack to launch attacks on Ukrainian positions. The Vetr 10 and Veer 13 have payload capacities of 3.5 kg and 8 kg, respectively. Both can reach targets upto 20 km away and gain speeds upto 150 kmph. The onboard capability allows them to engage the target with minimal human input, once they are launched manually in the general area.[20] Similar AI features have also been observed in the “Mikrob” series of kamikaze drones, with the additional features that up to 40 drones can be controlled by a single team.[21] Apart from attacking Ukrainian ground positions, the Russians have also developed the “Sokol" interceptor drone, capable of countering Ukrainian reconnaissance drones and the Baba Yaga-type attack UAVs. Upon receiving target information from a detection system, the drone can automatically deploy to engage the threat and return to its base.[22] Russian drone components recovered by Ukrainian forces point to the use of target acquisition and auto-following software modules on these drones.[23] In major battles such as Chasiv Yar and in the Zaporizhzhia Oblast, the majority of Ukrainian casualties were due to FPV drones or explosives dropped by them.[24]

  In Ukraine's case, due to major technological and infrastructure support from countries and Big Tech in the West, the variety and quantity of drones supplied has been immense. For example, the Russians recovered an Edge Tensor Processing Unit (TPU), optimised for large scale parallel processing from a downed Ukrainian quadcopter.[25] As per a report, the Ukrainians have taken publicly available AI models and fine-tuned them on their own extensive real-world data from combat positions and deployed them on their own drones, allegedly increasing their kill effectiveness three to fourfold.[26] This tuning is very specific and selective, often homing on to a “specific sector of the front and specific types of drone”.[27] A company called ZIR System is developing a modular AI-based Automatic Target Recognition (ATR) kit that can be onboarded on any drone. The system is a combination of hardware (compact module with a computer and a digital camera) and software (pretrained AI model capable of identifying targets and autonomous navigation). The company also uses an open-source autopilot software called ArduPilot that supports “autonomous navigation, waypoint planning, and real-time telemetry”.[28] Due to the use of optical systems

rather than GPS for navigation, drones equipped with this software can also function effectively in GPS-denied environments.

In the Israel-Hamas war, AI-enabled drones have been used in a distributed computing format where control centres with algorithms like Lavender and Gospel have been used for creating kill-lists of Hamas terrorists, with Fire Factory AI processing targets at ultra-high speed.[29] Elbit has integrated AI into its bombing guidance systems, including the Hermes 900 drone for analysing terrain, movement patterns and heat signatures to identify human targets but the AI is biased in terms of assuming that all Palestinians are terrorists.[30]

- **Terrain Mapping:** AI modules mounted on drones offer powerful capabilities for terrain mapping in challenging environments. Before moving on to specific examples, a quick look at the various types of technologies and platforms being used in this scenario are important. Terrain mapping relies on technologies such as Lidar, Photogrammetry, Simultaneous Localisation and Mapping (SLAM), Real-Time Kinematics (RTK) GPS and ML algorithms. In combat, these are used for battlefield intelligence, route planning, infrastructure assessment, environment monitoring, artillery spotting and assessing the amount of heat (intensity of firefight etc). There have been no examples of use of AI in terrain mapping during the Aremnia-Azerbaijan war.

  In the Russia-Ukraine war, Ukrainian special forces have used Eagle Eyes AI software to compare live drone camera feeds with pre-stored 3D terrain maps and then use this function to navigate autonomously when GPS signals are jammed.[31] Similarly, a Ukraine-based company called Atlas Aerospace has created a Virtual Lidar which measures 'optical flow' (tracking how terrain features move across a drone's camera to create real-time elevation maps) to eliminate the need for deploying Lidars, which are both expensive and emit detectable lasers.[32] The Styx AI system, developed by Swarmer, a US-based company, enables drones to autonomously map and navigate battlefields in coordinated groups. Each drone shares terrain data across the swarm, predicting movements of others to avoid collisions and optimise routes.[33] There are some discussions on certain social media platforms regarding the use of AI to detect ground disturbances from buried mines.[34] Drones equipped with multispectral cameras and vibration sensors analyse soil texture changes to find out if any minefield has been buried.[35] However, open source proven news regarding the same remains unverified.

  The IDF is using Exodigo, an underground AI mapping app "with multi-sensing tech developed through the simulation of multiple sensors,

3D visualization and data merging",[36] for pinpointing Hamas tunnels in Gaza. Another innovation is the Vision 60 semi-autonomous robotic dog units, which are used for pinpointing Hamas-laid traps and locations.[37] Not exactly terrain mapping, but these fall into the same category of utilising terrain-based data to create accurate maps of environments to assist soldiers in combat operations.

- **Counter UAS:** Starting with the Russia-Ukraine war, one of the most widespread uses of AI has been in C-UAS systems, especially combined with the use of EW. One of the major products out of the US's Replicator initiatives is Anduril Industries' Ghost-X platform which functions, on behalf of the Ukrainians, in the form of a flying mesh-network. Drone swarms swap and relay data between each other when flying against heavy EM interference by the Russians. The networks, based on the location of the Russian jammers, reconfigure their geometry to keep flying and in the process, may even sacrifice a few drones, to continue with the mission.[38] This is another example of the value of the techno-platform being greater than its individual components. Another Ukrainian innovation, to escape Russian jamming, is to use a lock on to target' function where the user 'selects the target, the drone flies the rest of the way, so no control signal is required though the jamming zone'.[39] Commercial drones such as DJI's Neo now come with an Active Track function, which allows the operator to draw a box around an object and have the drone follow it, offsetting the jamming-prone control signal link between the operator and the drone.[40] In order to produce more drones equipped with AI cheaply, Ukrainians are using the Raspberry Pi Zero basic computing unit[41] or the Google Coral AI dev board.[42] With the YOLO vision family software.[43] Russian units, on the other hand, have installed AI-based 'video interceptors in their vehicles that intercept the unencrypted FPV video signals from enemy drones'. Russian drones such as Orlan and Zala now come equipped with video signal jammers which automatically detect the frequency of the Ukrainian FPV's video channel and then overwhelm that frequency with the same frequency at a much higher power, blinding the drone.[44] Another innovation from the Russian side, to offset optical sensors on Ukrainian AI drones, is the fitting of strobe jammers that target the drone's video camera sensors, reducing the effectiveness of their ML algorithms to correctly identify targets to near zero.[45]

  Israel has used a host of AI-based counter-drone systems in its war against Hamas against Gaza. These include the Drone Dome, EnforceAir2 Maritime, Sentrycs Horizon, ELT Group Karma, Smart Shooter, Xtend and Axon.[46] These all use variants of either AI-enabled

ground-based AD weapon systems or AI-enabled drones and are powered by novel contributions by academia and industry.

- **AI-enabled Swarm:** Ukraine has been experimenting with swarms of drones to conduct long range strikes on oil refineries and military infrastructure deep inside Russia. Trembita drones have been used in a unique mix of decoys and drones. In one of the attacks on Russian facilities, a 100-drone swarm, with only 10% equipped with explosives, was launched in Kursk. While the Russians were able to destroy 85 targets, the remaining 15 were still able to power through and strike their designated targets.[47] This technique leverages the low-cost nature of the drone, which is used to expend costly AD missiles and ammunition. In March 2025, Ukraine coordinated more than 80 'Liutyi' kamikaze drones (carrying 550 lb warheads) with Rubaka decoys to strike Novorossiysk's oil terminals. AI prioritised high-value targets while decoys absorbed the costly S-400 missile fire.[48] The Russians, on the other hand, have used saturation raids of drone swarms to overwhelm Ukrainian AD systems. Russia launched 188 Shahed drones in a single night in November 2024, mixing thermobaric variants with unarmed decoys. The swarm targeted Zaporizhzhia and Odesa, exploiting gaps in Ukraine's AD coverage. The decoys in the strike carried live-feed cameras to geolocate Ukrainian defences for follow-up missile strikes.[49] In one of the most talked about strikes comprising majorly of unmanned systems, Ukrainian forces attacked Russian positions near the village of Lyptsi in the Kharkiv region using a combination of unmanned ground vehicles (UGVs) and FPV drones.[50] Another major innovation used by both sides is the concept of motherships carrying FPV drones.[51] Ukraine's VTOL type motherships with FPV drones combine human oversight with AI-driven navigation. Operators approve targets, while AI handles terrain mapping (using optical flow or preloaded 3D maps) and obstacle avoidance during GPS-denied conditions.[52] The FPV drones also use NOGPS targeting to visually tag objectives during initial human-guided phases.[53] If jamming serves the link, AI completes the strike using terrain maps. Russia's 'Pchelka' carrier uses AI to recharge FPV batteries mid-flight via an internal combustion engine, ensuring the mothership returns to base with enough power to hover and land.[54]

JOINT FORCE INTEGRATION

The Development and Deployment (D&D) paradigm for drones in a joint force can be seen from multiple perspectives such as size, functionality, weight criteria and payload characteristics. However, one of the most critical parameters for jointness and integration within the Armed Forces is the interaction between

seemingly similar capabilities and how they complement and supplement each other. The use of drones in a multi-domain concept is one such example. For example, in the ongoing Russia-Ukraine conflict, there are reports of Unmanned Surface Vessels (USVs) launching FPV aerial drones to take out enemy positions.[55] This trend will expand dramatically as cognitive, space, EM and cyber domains increasingly interact with these advanced platforms. Such cross-domain integration demands three essential pillars: interoperability, standardisation, and compatibility.

- **Interoperability:** The best way to understand interoperability is that it establishes the governance and regulatory framework for enabling different services to share authority and information across domain and service boundaries. In the context of AI-equipped drone systems, there is a need for a military nervous system allowing information to flow seamlessly while coordinating actions across the different domains. Interoperability has four key attributes**:** command delegation protocols (or who controls what and when), decision authority framework (or how authority shifts during operations), information classification and sharing (or what data can be shared with whom) and mission control architecture (or how objectives are interpreted and translated into actions). A hypothesised system architecture must facilitate real-time intelligence sharing across service boundaries while allowing for unified control of assets regardless of the service ownership. This will create a tension between centralised command and decentralised execution in multi-domain operations. One potential solution involves 'federated autonomy',[56] where a central command establishes strategic objectives and mission parameters, but tactical decisions and real-time adjustments happen at the edge or within the drones themselves. The techno-platform framework is best suited to achieve this.

  This can work through a shared data foundation where services exchange information based on mission needs. However, common data standards are crucial. Military commanders should focus on defining mission outcomes while facilitating the flow of resources and removing barriers to data sharing and bandwidth allocation. The actual tactical and operational choices should be delegated to commanders on the cutting edge or the techno-platform themselves. Additionally, there is a need for flexible delegation to ensure the transfer of control to whichever service requires or is able to execute a particular mission best. Challenges arise when these systems face varying data classification levels, mismatched communication protocols and service-specific command structures that muddy the operational picture. These limitations often force commanders

back to basic capabilities, undermining the advantages these advanced platforms provide.

To overcome these challenges, armed forces must strictly implement a cross-domain authentication framework which allows information to flow securely between classification levels, develop dynamic command delegation protocols that shift control based on mission phase rather than service boundaries and create data standards that enable mosaic-warfare analogous concepts, where capabilities can be rapidly recombined regardless of platform origin. This approach transforms network-centric operations into truly data-centric operations, where the value lies not just in the network but also in the strength of the connection of the network, mediated by interoperability, to deliver decision-quality information to any node that needs it, regardless of domain or service.

- **Standardisation:** Standardisation creates a common technical language between platforms and technologies that ensures systems can communicate with each other based on a set of mutually-agreed upon protocols. It has four key components: data formats and exchange protocols (how information and therefore intelligence is created), interfacing and modularity protocols (how systems connect to each other physically and digitally), training data sets and AI parameters (how systems learn and evolve) and performance standards and testing procedures (how capabilities are measures). Standardisation enables systems to use the same operational language and respond to commands consistently, reducing friendly fire incidents, enabling modularity or swapping of parts and payloads as well as enabling shared learning across the joint force. When platforms share common AI training datasets, control interfaces and communication protocols, they develop a collective 'hive-mind' that transcends individual domain limitations. The main challenges for this are divergence of service-specific requirements based on unique operational environments, resistance to adaptation by legacy systems to new standards and the threat of obsolescence of standards before D&D due to the exponential technological curve. To address these challenges, armed forces should establish mechanisms that balance domain-specific requirements with joint interoperability needs, implement containerised AI architectures that allow algorithms to be securely deployed across platforms regardless of hardware differences and create evolutionary standardisation frameworks where core interfaces remain stable while implementation details can evolve. These measures treat AI capabilities as interchangeable 'tiles' that can be rapidly recombined across domains, creating unpredictable operational patterns that adversaries will struggle to counter.

- **Compatibility:** Compatibility ensures that diverse systems across domains and services practically coexist in a shared physical and EM environment. Conceptually, compatibility ensures that aerial platforms can operate in proximity with UGVs, UUVs, USVs or other drone-based capabilities without EM interference, allowing for technical innovations from one domain to rapidly transfer to others through aligned software architectures and standardised interfaces. This congruence extends beyond technical specifications into logistical compatibility, where maintenance processes, spare parts and support equipment can be shared across service boundaries, reducing deployment footprints and enabling sustained operations. The major issues seem to emerge from the proliferation of proprietary systems with vendor-specific interfaces (both hardware and software), complexity of EM spectrum management in contested environments and cybersecurity vulnerabilities due to standardised systems. These bottlenecks often create isolated 'islands of excellence' that cannot scale across the entire force, limiting the potential of techno-platforms. To overcome these constraints, armed forces must implement Modular Open-Systems Approaches (MOSA)[57] that decouple hardware, middleware and applications; develop dynamic spectrum allocation systems that allow platforms to adaptively share EM resources; proliferate EM, data and communication protocols on a joint basis; and create robust cybersecurity frameworks to protect the interfaces while maintaining operational efficacy. These measures enable data-centric operations where information flows seamlessly between domains, supporting network-centric warfare by ensuring that every platform, whether underwater, surface, aerial or space-based, can contribute to and benefit from the collective intelligence of the joint force regardless of service origin or technical architecture.

CONCLUSION

The concept of a 'techno-platform' serves as the essential binding framework that integrates interoperability, standardisation, and compatibility into a cohesive approach for AI-enabled drones. These techno-platforms can be considered as nodes in a wider network and hence interoperability is a must. Standardised protocols are required for enabling 'plug and play' modularity across separate service-specific platforms. Finally, successful operations across domains requires that systems can coexist in shared EM and physical spaces. Given the fact that a number of emergent characteristics can develop through the interaction of technologies and platforms within the techno-platform paradigm, compatibility becomes must. The analysis of recently concluded and ongoing conflicts has brought home the fact that techno-platforms, AI-enabled drones in

this context, have the potential to change the future of warfare but that requires the parallel and synchronised development of attributes that comprise the three parameters of a techno-platform.

❖❖❖

Lt Col Akshat Upadhyay is currently serving with HQ IDS. He has authored numerous peer-reviewed papers as well as op-eds and articles in prestigious national and international publications on the issues of home-grown radicalisation, lone wolf terrorism, social media mobilisation, IW and emerging and niche technologies. He has authored the books titled, "India's Coercive Diplomacy against Pakistan", "Absorption of Disruptive Technologies in the Indian Armed Forces" and "Emerging Frontiers: Technology Absorption in the India Army". He was also a Research Fellow At MP-IDSA where he wrote extensively on disruptive technologies, non-contact warfare and semiconductors.

NOTES

1. Edward Luttwak and Eitan Shamir, The Art of Military Innovation: Lessons from the Israeli Defence Forces (London: Harvard University Press, 2023), 13.
2. Ibid.
3. Charlotte E., Global Combat Air Programme, BAE Systems, [online:web] Accessed 29 March 2025, URL: https://www.baesystems.com/en/product/global-combat-air-programme.
4. Trevor Taylor and Isabella Antinozzi, "Unlocking Sixth-Gen Air Power: Inside the Military Capability for GCAP," *Royal United Services Institution (RUSI)*, 15 May 2024.
5. Confluent, Middleware: Intro to Messaging and Integration, Confluent, [online:web] Accessed 30 March 2025, URL: https://www.confluent.io/learn/middleware.
6. Trevor Taylor and Isabella Antinozzi, "Unlocking Sixth-Gen Air Power: Inside the Military Capability for GCAP," *Royal United Services Institution (RUSI)*, 15 May 2024.
7. "Raisina Dialogue 2025 II Live - Day 3 II Verses and Wars: Navigating Hybrid Theatres," YouTube video, 56:30, "Observer Research Foundation," 19 March 2025, https://www.youtube.com/watch?v=QnO7X6RjtO4&t=2312s.
8. Anduril, Anduril Raises $1.5 Billion to Rebuild the Arsenal of Democracy, Anduril, [online:web] Accessed 28 March 2025, URL: https://www.anduril.com/article/anduril-raises-usd1-5-billion-to-rebuild-the-arsenal-of-democracy.
9. Anduril, Anduril Building Arsenal-1 Hyperscale Manufacturing Facility in Ohio, Anduril, [online:web] Accessed 28 March 2025, URL: https://www.anduril.com/article/anduril-building-arsenal-1-hyperscale-manufacturing-facility-in-ohio.
10. Anduril, Anduril Raises $1.5 Billion to Rebuild the Arsenal of Democracy, Anduril, [online:web] Accessed 28 March 2025, URL: https://www.anduril.com/article/anduril-raises-usd1-5-billion-to-rebuild-the-arsenal-of-democracy.
11. David George and Brian Schimpf, "How AI is Changing Warfare with Brian Schimpf, CEO of Anduril," 28 January 2025, in *The a16z Podcast*, produced by a16z, podcast, streaming, 35:22.

12. Saiwa: From Vision to Innovation, AI-Based Drone Operation | AI in Drones use cases, Saiwa.ai, [online:web] Accessed 30 Mar 2025, URL: https://saiwa.ai/blog/ai-in-drones.
13. Grepow, All You Want to Know about AI Drones, Grepow, [online:web] Accessed 01 April 2025, URL: https://www.grepow.com/blog/all-you-want-to-know-about-ai-drones.html.
14. IG Drones, Discover how AI-Enabled Drones are transforming Industries in India, [online:web] Accessed 01 April 2025, URL: https://www.linkedin.com/pulse/discover-how-ai-enabled-drones-transforming-industries-india-x6tsc.
15. Patrick McEnroe, Shen Wang and Madhusanka Liyanage, "A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges,"*IEEE Internet of Things Journal* 9, No 7 (2022): 15435 - 15459.
16. Xiangwang Hou, Zhiyuan Ren, Wenchi Cheng, Chen Chen and Hailin Zhang, "Fog Based Computation Offloading for Swarm of Drones," *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, (2019), https://ieeexplore.ieee.org/abstract/document/8761932.
17. Rebecca Pool, "Drones with Edge AI: The Future of Warfare?," EE Times Europe, 05 March 2025, https://www.eetimes.eu/drones-with-edge-ai-the-future-of-warfare.
18. Eric Rudenshiold, "Drones Over the Caspian: How UAVs are Shaping Regional Power in the Caucasus and Central Asia," Caspian Policy Centre, 22 January 2025, https://www.caspianpolicy.org/research/category/drones-over-the-caspian-how-uavs-are-shaping-regional-power-in-the-caucasus-and-central-asia.
19. Michael Bisecker, Sam Mednick and Garance Burke, "As Israel uses US-made AI models in war, concerns arise about tech's role in who lives and who dies," Associated Press, 18 February 2025.https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108
20. Defense News Army 2024, "Russia Deploys AI-Equipped Vetr Unmanned Aerial Vehicle in Ukraine," armyrecognition.com, 06 August 2024, https://armyrecognition.com/news/army-news/army-news-2024/russia-deploys-ai-equipped-vetr-unmanned-aerial-vehicle-in-ukraine.
21. Boykov Nikolov, "3,000 AI drones reportedly sent to Russian army in Ukraine," Bulgarianmilitary.com, 22 January 2025, https://bulgarianmilitary.com/2025/01/22/3000-ai-drones-reportedly-sent-to-russian-army-in-ukraine.
22. Ashish Dangwal, "Battle Of Algorithms: Russia Develops New AI-Powered "Interceptor Drone" That Can Counter Ukrainian UAVs," The Eurasian Times, 25 January 2025, https://www.eurasiantimes.com/ukraines-advanced-v-bat-drone-faces-new-threat-from-russia.
23. Simplicius, "Tech Surge of the SMO: AI, Drones, EW, Countermeasures, and More of the Latest Advancements," Simplicius's Garden of Knowledge (Substack), 04 January 2025, https://simplicius76.substack.com/p/tech-surge-of-the-smo-ai-drones-ew.
24. David Kirichenko, "The Rush for AI-Enabled Drones on Ukrainian Battlefields," Lawfare, 05 December 2024, https://www.lawfaremedia.org/article/the-rush-for-ai-enabled-drones-on-ukrainian-battlefields.
25. Simplicius, "Tech Surge of the SMO: AI, Drones, EW, Countermeasures, and More of the Latest Advancements," Simplicius's Garden of Knowledge (Substack), 04 January 2025, https://simplicius76.substack.com/p/tech-surge-of-the-smo-ai-drones-ew.
26. Sydney J Freedberg Jr, "Trained on classified battlefield data, AI multiplies effectiveness of Ukraine's drones: Report," Breaking Defense, 06 March 2025, https://breakingdefense.com/2025/03/trained-on-classified-battlefield-data-ai-multiplies-effectiveness-of-ukraines-drones-report.

27. Ibid.
28. Kateryna Bondar, “Ukraine’s Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare,” Centre for Strategic and International Studies (CSIS), 06 March 2025, https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare#h2-ai-in-autonomous-navigation.
29. u/Altru_Iris, “Inside Israel’s AI Kill Lists & Automated Bombing Systems,” Reddit, 18 March 2025, https://www.reddit.com/r/Palestine/comments/1jecwzs/inside_israels_ai_kill_lists_automated_bombing.
30. Ibid.
31. u/lost_library_book, “Many Ukrainian drones have been disabled by Russian jamming: Their latest models navigate by sight alone,” Reddit, 05 June 2024, https://www.reddit.com/r/ukraine/comments/1d4dyqi/many_ukrainian_drones_have_been_disabled_by.
32. Ibid.
33. David Kirichenko, “The Rush for AI-Enabled Drones on Ukrainian Battlefields,” Lawfare, 05 December 2024, https://www.lawfaremedia.org/article/the-rush-for-ai-enabled-drones-on-ukrainian-battlefields.
34. r/UkraineWarVideoReport, "QUESTION: Could Ukraine use LIDAR equipped drones and reveal minefields and possible corridors within these minefields to overcome this hurdle and be more successful in the offensive?,” Reddit, 05 April 2023, https://www.reddit.com/r/UkraineWarVideoReport/comments/15nzwdc/question_could_ukraine_use_lidar_equipped_drones.
35. Ibid.
36. Ozer Khalid, “Gaza – Ground Zero for AI Warfare,” Criterion Quarterly 19, no 4, 14 January 2025. https://criterion-quarterly.com/gaza-ground-zero-for-ai-warfare.
37. Meir Rinde, “Philly manufacturer of military robot dogs is a target of Gaza war protests,” Billy Penn at Whyy, 22 April 2024. https://billypenn.com/2024/04/22/israel-palestine-gaza-robot-dogs-ghost-robotics.
38. Patrick Tucker, “Newest Replicator drones proven on battlefields of Ukraine,” DefenseOne, 13 November 2024, https://www.defenseone.com/technology/2024/11/newest-replicator-drones-proven-battlefields-ukraine/400997.
39. David Hambling, “Ukrainian FPV Operator Reviews AI-Enabled ‘Lock On Target’ Drones,” Forbes, 05 March 2025, https://www.forbes.com/sites/davidhambling/2025/03/05/ukrainian-fpv-operator-reviews-ai-enabled-lock-on-target-drones.
40. Ibid.
41. Ibid.
42. Simplicius, “Tech Surge of the SMO: AI, Drones, EW, Countermeasures, and More of the Latest Advancements,” Simplicius’s Garden of Knowledge (Substack), 04 January 2025, https://simplicius76.substack.com/p/tech-surge-of-the-smo-ai-drones-ew.
43. David Hambling, “Ukrainian FPV Operator Reviews AI-Enabled ‘Lock On Target’ Drones,” Forbes, 05 March 2025, https://www.forbes.com/sites/davidhambling/2025/03/05/ukrainian-fpv-operator-reviews-ai-enabled-lock-on-target-drones.
44. Simplicius, “Tech Surge of the SMO: AI, Drones, EW, Countermeasures, and More of the Latest Advancements,” Simplicius’s Garden of Knowledge (Substack), 04 January 2025, https://simplicius76.substack.com/p/tech-surge-of-the-smo-ai-drones-ew.

45. Ibid.
46. Startup Nation Central, “C-UAS: Israel’s Innovative Response to UAVs, ” Startup Nation Central, 04 March 2025. https://startupnationcentral.org/hub/blog/c-uas-israels-response-to-uavs/#:~:text=They developed the renowned Drone,in complex and challenging environments.
47. u/TheSleepingPoet, “Ukraine Is Daring Russia To Open Fire On Swarms Of New Trembita Drones. Many Of The Drones Will Be Decoys.,” Reddit, 05 March 2025, https://www.reddit.com/r/worldnews/comments/1ivwvpd/ukraine_is_daring_russia_to_open_fire_on_swarms.
48. Don Rassler and Yannick Veilleux-LePage, “On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism,” *CTCSentinel* 18, No 3 (2025), https://ctc.westpoint.edu/on-the-horizon-the-ukraine-war-and-the-evolving-threat-of-drone-terrorism.
49. Emma Burrows, Hanna Arhirova and Lori Hinnant, “Russian plan mixes deadly thermobaric drones among swarms of decoys launched at Ukraine,” *The Times of Israel*, 16 November 2024. https://www.timesofisrael.com/russia-mixing-deadly-thermobaric-drones-among-swarms-of-decoys-launched-at-ukraine.
50. Mick Ryan, “The Battle of Lyptsi: Robotic Land Combat,” Futura Doctrine (Substack), 22 December 2024, https://mickryan.substack.com/p/the-battle-of-lyptsi-robotic-land.
51. Simplicius, “Tech Surge of the SMO: AI, Drones, EW, Countermeasures, and More of the Latest Advancements,” Simplicius’s Garden of Knowledge (Substack), 04 January 2025, https://simplicius76.substack.com/p/tech-surge-of-the-smo-ai-drones-ew.
52. Rebecca Pool, “Drones with Edge AI: The Future of Warfare?,” EE Times Europe, 05 March 2025, https://www.eetimes.eu/drones-with-edge-ai-the-future-of-warfare.
53. u/lost_library_book, “Many Ukrainian drones have been disabled by Russian jamming: Their latest models navigate by sight alone,” Reddit, 05 June 2024, https://www.reddit.com/r/ukraine/comments/1d4dyqi/many_ukrainian_drones_have_been_disabled_by.
54. Vijainder K Thakur, “Ukraine’s Next Big Headache — Russian Drone Motherships Carrying FPV Kamikaze Drones That Can Strike Deep & Hard,” The Eurasian Times, 31 January 2025, https://www.eurasiantimes.com/ukraines-next-big-headache-russian-drone-motherships.
55. Simplicius, “Tech Surge of the SMO: AI, Drones, EW, Countermeasures, and More of the Latest Advancements,” Simplicius’s Garden of Knowledge (Substack), 04 January 2025, https://simplicius76.substack.com/p/tech-surge-of-the-smo-ai-drones-ew.
56. Nagendra Bandaru, "Federated Autonomy Fuels Organizational Growth And Innovation,” Forbes, 10 January 2022, https://www.forbes.com/councils/forbestechcouncil/2022/01/10/federated-autonomy-fuels-organizational-growth-and-innovation.
57. Defense Standardization Program, “Modular Open Systems Approach (MOSA), Defense Standardization Program, n.d. https://www.dsp.dla.mil/Programs/MOSA.

❐❐❐

106-117

MILITARY DOCTRINE FOR DRONE INTEGRATED WARFARE

Lt Gen A B Shivane, PVSM, AVSM, VSM (Retd)

Abstract

Drones provide a quick, cheap, economy-of-force capability with a high time-to-kill ratio and saturating attacks through precise mass application. This has led to an era of drone-enabled warfare to 'Fight Lean, Fight Cheap and Fight Smart'. The Indian Military must acquire, adopt, adapt and integrate this force multiplier into its deterrence and warfighting doctrine to be future-ready.

Three factors merit a rethink of doctrine-one, the operational environment has changed measurably driven by technology and new threats; two, technology has disrupted the spatial dimension of contemporary military operations, commonly referred to as battlefield geometry and three, the transition from battlefield to battlespace has assumed a multidomain character.

The future operational philosophy will need to focus on a 'capability-cum opportunity based' approach to optimise what exists and not what does not exist, with deterrence reorientation on 'denial and domination strategy'.

The objective of a 'Drone Integrated Warfare Doctrine' is the application of AI-enabled precision drones to provide the best time-kill ratio, with low cost and high impact by overwhelming the adversary capability. The three lines of effort must be: Build the Force Capability, Optimise Force Readiness (effectiveness and preparedness); and Integrate into the Force Design. The aim must be to achieve operational flexibility, integrating drones across all warfare levels and domains, while balancing autonomous capabilities with human oversight.

EVOLVING BATTLESPACE AND TRANSFORMATION

Indian Military is the finest in the world with a proven battle record and the most professional human resource. However, contemporary wars have witnessed a tectonic shift in the goals of war, the rules of war, the players and the instruments of war, reshaping its character and unlimiting its boundaries.[1] The military will have to innovate, adapt and integrate new capabilities to deter, detect, deny and defeat future threats. Unfortunately, the military world over is conservative by nature and guilty of preparing not only for the last war but often for the wrong one. The simple truth is that warfare evolves faster than warfighters do. The challenge remains as how to generate a military advantage in such an environment.

The battlefield is going digital, automated and exponentially more unconventional mandating being innovative and adaptive for the right war. Future battlefields will be characterised by a mix of high-end systems deployed in smaller numbers, with low-cost, attritable systems deployed in far greater numbers. The challenge remains one, to break the cobwebs of present thinking to purely focus on building a small batch of complex and expensive conventional weapons at a high price to fight yesterday's war; two, plagued procurement approach chasing yesterday's technology; and three, outdated military doctrine that fails to address contemporary threats. A bold, transformative leadership to overcome inertia and old ways of doing business is required.

The military cannot fight tomorrow's conflicts with yesterday's weapons, doctrines and structures. Based on this context the Indian Army Vision@2047 envisions to "Transform into a modern, agile, adaptive, technology-enabled and self-reliant future ready force, capable to deter and win wars in a multi-domain environment, across the full spectrum of operations to protect our national interests in synergy with other services".[2] In the spirit of pursuing this vision, the Indian Army is observing 2023-2032 as a Decade of Transformation and 2024-25 as Years of Technology Absorption.

MILITARY'S FOCUS AND NEED FOR DRONE-ENABLED WARFARE CAPABILITY

Drones and AI are one such sunrise sector that has the potential to act as key enablers in this transformation. They provide a quick, cheap, economy-of-force capability. This has led to an era of mass empowered by precision to 'Fight Lean, Fight Cheap and Fight Smart'. The Indian Military must acquire, adopt, adapt and integrate this force multiplier into its deterrence and warfighting doctrine to be future-ready. An EY-FICCI report indicates that the defence drone industry market potential will see a growth from 38,300 Cr in 2025 to 1,01,100 Cr in 2030 with a level of indigenisation rising from the present 40% to 60%.[3] This opportunity must not be lost. In fact, effort should be made for 100% indigenisation.

Indian military's focus on Unmanned Aerial Vehicles (UAVs) and autonomous systems is set to intensify in 2025, with the launch of advanced drone platforms for reconnaissance, surveillance, and strike missions. The Defence Minister's recent statement on 02 Jan 2025 highlighted the push for indigenous kamikaze drones, swarm drones, and combat UAVs as part of defence modernisation in preparing for future wars. Collaboration with private industry and startups will be the key to accelerating innovation in this domain.

India's move towards developing drone swarms, advanced Medium Altitude Long Endurance (MALE) and High Altitude Long Endurance (HALE) platforms, and weaponised UAVs reflects a long-term vision of evolving its military

capabilities. The present gap is being bridged by the import of predator drones MQ-9B from the US. This transformation is indicative of the intent for drones with AI-enabled autonomy, modular payloads and counter-drone capabilities. The integration of drones into the Indian Military doctrine along with a drone ecosystem with advanced indigenous technologies will be the key to capability building of a future-ready force.

LESSONS FROM CONTEMPORARY CONFLICTS

The Ukraine conflict has provided a fresh impetus toward the employment of drones, offering valuable lessons for militaries.[4] Ukraine's innovative employment and Russia's mass application of drones have highlighted their operational utility in operations. For India, the conflict provides a clear roadmap: invest in indigenous drone development, enhance counter-drone systems, and generate capabilities for the evolving dynamics of modern warfare. Ukraine's ability to modify commercial drones and Russia's success with systems like the Lancet highlight the importance of domestic innovation. Ukraine's use of civilian apps and platforms like Starlink showcases the importance of civil-military fusion. The conflict has also brought forth the importance of AI-enabled drone/swarm technologies, foolproof communications and advanced Counter-Drone (C-DRONE) Systems. A new era of battlespace transformation through 'Drone-Based Warfare' is revolutionising conflict.

However, the war has also highlighted limitations as stated in the recent RUSI report[5] as Tactical drones have significant limitations. Between 60 and 80% of Ukrainian FPVs fail to reach their target, depending on the part of the front and the skill of the operators. Of those that do strike their targets, a majority fail to destroy the target system when striking armoured vehicles. The success rate in wounding infantry is high. Furthermore, either EW or the weather significantly degrades drone operations. Despite these limitations, tactical UAVs/drones currently account for 60–70% of damaged and destroyed Russian Systems.

China has reportedly enhanced its capabilities in high-altitude warfare with the deployment of integrated AI-powered combat drones along the Line of Actual Control (LAC). To counter threats from adversaries like China and Pakistan, India must develop a robust indigenous drone industrial ecosystem (both mass production and AI-enabled technology), enhance acquisition, and induction, and foster military adaptation through doctrinal review, adaptive training, and collaboration with start-ups. Further, the present threat cum capability building model must give way for a more proactive and perspective capability cum opportunity-based model to be ready and relevant for the future. This will empower a pre-emptive and proactive operational military strategy and also help in adding teeth to a redefined deterrence based on denial and domination.

Technology is also remaking warfare with the return of mass meeting precision.[6]

Advances in Artificial Intelligence (AI), C5ISR and autonomous systems are eroding the binary between mass and precision. This is the era of future warfare of precise mass. Reduced manufacturing costs are also enabling militaries and non-state actors to bring 'mass' back to the battlefield. This facet is increasingly evident in Ukraine and the Middle East conflicts, necessitating militaries to review force application to endure prolonged conflicts at least cost and optimum payoffs. China focuses on such technology capability building.

Another interesting lesson from the Ukraine War has been the 'Transformation Under Contact' or 'Innovation Under Fire'.[7] It is a bottom-up, 'transformation in contact' approach with empowered forward workshops and electronic labs under a PPP model with experts Innovating, testing and providing state-of-the-art technology capability in compressed time frames functioning as Centres of Innovation and Repair.

DRONE TECHNOLOGY PERSPECTIVE

The imperative is to develop robust, technologically advanced drones capable of operating in diverse operational conditions, providing pervasive real-time intelligence, and executing precision strikes.

Four major technological developments contributed to changing the world's perception of drones by the early 2000s: enhanced endurance of modern drones, replacing the use of radio signals with satellite networks, AI enablement resulting in swarm autonomy, and arming drones to step up their abilities from ISR to striking targets. The turnaround distance and endurance will be a factor of size, technology, attendant cost, and mission level requirement.

The Indian Military must invest in swarm drones equipped with AI for decentralised control and complex attack strategies. Swarms have manifested in the Indian skies on various demonstrative occasions but combat swarms for saturation attacks and counter-drone missions require decentralised autonomy technologies and intelligent framework which can overwhelm the enemy without being vulnerable to hacking or countermeasures. AI-enabled autonomous drones for threat identification, target tracking, and autonomous decision-making for targeting are thus vital.

Drones should have superior onboard processing abilities to relay real-time data back to ground stations or frontline units for decision superiority. This requires high-processing modules for sensor fusion, combining data from optical/Charge Coupled Device (CCD) HD cameras, Mid Wave Infrared (MWIR), and radar sensors into a cohesive operational picture at altitudes of 4-5 km.

To ensure standardisation and logistics, the need is for a family of drone platforms with a plug-and-play capability of modular payload selection ranging from ISR payloads, loitering ammunition, mine dispensation, electronic warfare

suites, artificial aperture radar, signal intelligence payloads and precision-guided munitions like laser-guided bombs and air-to-ground missiles are essential. The explosive payload for a strike mission can be shaped charge (CE), Thermobaric, or High Explosive (HE) airburst according to target specification to eject mini Kamikaze UGVs/drones from the mother drone.

Stealth is another critical feature for drones operating in contested environments, against advanced enemy air defence systems and C-UAS systems. Signature management includes visual, acoustic, thermal, IR and seismic signatures. Drones must project a minimal radar cross-section (0.1sq m) to avoid detection and engagement.[8] Radar-absorbing materials, reduced heat signatures, and low infrared observability are technologies which must find application.[9]

Counter-UAS is an important factor of drone warfare with niche technologies providing critical hard and soft kill options against drones. These advanced systems detect, identify/classify, locate, track and neutralise UAS threats. The neutralisation techniques use technologies such as RF Based Drone detector, Video-based Drone Identification and Tracking, X band 3D Counter-UAS RADAR, Data fusion and Command Centres, Drone RF Jammer to disable links between the Ground Control Centre (GCC) and drone, acoustic or optical sensors and multiple hard kill options such as laser, drone catcher nets, high burst cannons/guns and even swarm on swarm technology.

The key imperative of technology induction is vulnerability mitigation through the indigenous character of critical hardware and software components. The challenge is twofold, first, to develop high-performance drone technologies that meet defence requirements without relying on foreign components, and second, to support Indian drone manufacturers for mass production and securing their indigenous firmware, avionics, flight controllers and encrypted communication systems and AI-driven anomaly detection against cyber threats. The recent incidents of hacking and spoofing of Indian drones with Chinese components must sound alarm bells. The need is for technology mapping, ascertaining the depth of indigenous content and homegrown supply chain management. This requires an integrated drone ecosystem with startups like Arkin Labs with state-of-the-art indigenous flight controllers, gaining greater traction and encouragement.

THE NEED TO RETHINK DOCTRINE

The Indian military defence doctrine is essentially dominated by defensive orientation and at best orthodox offensive character exhibited in its Pro-Active Operations doctrine which remains essentially an intent. Doctrinal innovations like the Cold Start Doctrine sought to optimise rather than rethink a new doctrinal construct.[10]

Three factors warrant a doctrinal rethink and are dicussed below:

- One, the operational environment post Kargil 1999 and Galwan 2020 has changed measurably and is driven by technology. Both China and Pakistan are indulging in military coercion below the threshold of all-out war. Proxy war by Pakistan and incremental territorial transgression by China both on the LAC and Indian Ocean have assumed a new dimension. This is related to hybrid and grey zone warfare as the more predominant flavour. The notion of victory in future wars has accordingly assumed a new cloak of ambiguity with perception management invoking new narratives to suit the players.
- Two, technology has disrupted the spatial dimension of contemporary military operations, commonly referred to as battlefield geometry.[11] Disruptive technologies like Artificial Intelligence (AI) and Unmanned Autonomous Systems (UAS) emerging as data-driven decision-making tools are extending the reach and precision of military operations and transforming battlefield geometry. This necessitates a doctrinal rethink on how technology-enabled force application can optimise force capabilities for future wars. Digit, digitisation, digitalisation and disruption are today synonymous with contemporary warfare.
- Three, the transition from battlefield to battlespace has assumed a multidomain character. MDO will seamlessly integrate physical domains of land, sea, air, space, and cyber with informational and cognitive realms. It aims to achieve a surface-to-space and physical-to-cognitive continuum with intent-based synergy across all domains.[12] Cognitive warfare has assumed a new dimension as a potent weapon in hybrid warfare and grey zone warfare in an era where kinetic, non-kinetic, contact, non-contact, manned and unmanned and information warfare are merging in the battlespace.

REVITALISING DETERRENCE AND OPERATIONAL PHILOSOPHY

Deterrence in the Indian strategic security construct which is aimed at punitive deterrence (assured retribution) on the Western front and dissuasive to credible deterrence (defensive) on the Northern front**.** Our deterrence has been repeatedly put to test in the recent past, and ironically led to the exposure of strategic and operational doctrinal voids and vulnerabilities. These are being addressed expeditiously but need greater time-critical resources and a doctrinal reconstruct.

At the strategic and operational level, we need a doctrinal reconstruct to keep pace with the realism of evolving geopolitics, the character of war and emerging threats to national security. India's military strategy entails managing threats

on its disputed border by a 'defensive holding' psyche with attritionist 'force-on-force' application rather than an 'offensive domination and manoeuvre warfare' orientation.[13] While the erstwhile orthodox defensive strategy has been doctrinally replaced by a Proactive Operations Strategy post Operation Parakram, its defensive character and reactive mindsets remain deeply embedded in the legacy of the past. The focus must be on 'dominating spaces' instead of universally 'holding ground' by manpower. The concept of 'Pre-emption, Dislocation and Disruption' as the three empirical means of defeat as stated in the Indian Army Doctrine requires greater technological teeth, offensive reorientation and integrated force restructuring.

At the strategic politico-military level, India needs to review its approach to state versus state and state versus non-state threats. As a nation with disputed borders and inimical neighbours, the military must orient essentially for the state versus state conflict and adapt to the state versus non-state threats. The severity and consequences of the former are more severe and face greater capability-building challenges. India for the foreseeable future will thus need to balance its force structure to counter existent threats to its continental, aerospace and maritime domains while simultaneously building military capabilities in equally critical future domains like AI, IW, Space, Cyber etc.

The operational focus must be based on a proactive operational construct to pre-empt, dislocate, disrupt and neutralise enemy threats. This would require a tri-service force application of both kinetic and non-kinetic means in a synergised operational spectrum. The need is for an agile technology-enabled integrated force structure led by adaptive and thought leadership to optimise joint force application.[14] Drones must empower deterrence at operational and tactical levels with precision mass employment and proactive force orchestration and application to deter and defeat threats.

The Indian defence forces traditionally are beset with no loss of territory syndrome rather than territorial integrity and a defensive cum reactive culture as has been evident in the recent conflicts**.** This has led to tactical vulnerabilities being exploited and operational imbalance due to surprise. The need is for the operational philosophy to transit from 'threat cum capability' to 'capability through opportunity' and deterrence based on 'denial and domination' to orientation through a state of art technology capability acquisition, adoption, adaption and integration. This requires a review of present doctrine, structural reorientation, reviewed Progressional Military Education (PME), technology induction and HR issues for holistic capabilities.

CONTOURS OF A DRONE INTEGRATED WARFARE DOCTRINE

The objective of a 'Drone Integrated Warfare Doctrine' is the application of AI-enabled precision drones to achieve the best time-kill ratio, with low cost

and high impact by overwhelming the adversary capability. This is also called precise mass doctrine.

The three lines of effort must be: 'Build the Force Capability', 'Optimise Force Readiness (effectiveness and preparedness)' and 'Integrate into the Force Design'. The focus must be on empowering IBGs along both fronts with innovative tactics, technology exploitation, lean structural review and training for future wars and threats to the Indian operational environment. The key must be on Drone Integrated Warfare Doctrine integrating all other force multipliers and technologies.

It must be appreciated that despite the commercial hype, drones have severe limitations to EW, cyber and weather as observed both in Ukraine and the Middle East. Thus, they are force multipliers with transformative technology to be integrated in warfighting in shaping the conventional battle space rather than sustained standalone weapons of war. It is here their role and application for counter-terrorist operations, surgical strikes and conventional war needs to be defined with clarity. They do not replace tanks, artillery or aircraft but supplement them for greater effect or outcome. Drone technology has empowered warfighters but boots and tracks in the Indian context remain primary, especially with disputed borders under perpetual turbulence.

The focus must be to achieve operational agility, integrating drones across the entire spectrum of warfare, while balancing autonomous capabilities with man-in-the-loop by MUM integration. The doctrine must cater for multi-domain operations based on a family of integrated platforms with a modular plug-and-play capability. Tri-service standardisation cum interoperability as far as possible particularly in aspects such as communication and counter cyber threats must be ensured.

The doctrine must focus on smart warfighting for future wars with greater agility and adaptability without over-matrixing or creating turbulence or vulnerabilities in the transition management. The equipping focus on 'capability through opportunity' must be embedded in the national construct of Atmanirbharta.

PRINCIPLES DRIVING THE DRONE INTEGRATED WARFIGHTING DOCTRINE

- **Operational Agility:** The drone application must manifest across the entire operational environment while empowering the cutting-edge tactical battlespace as a priority. Drones must energise the Intelligence Preparation of the Battlefield (IPB) matrix to 'detect, disrupt, degrade, dislocate and deny' enemy forces. Thus, the empowerment must be bottom-up for smart warfighting while the top-down approach integrates and builds capabilities at the strategic and operational levels.

- **Multi-Domain Integration:** The doctrine should ensure drone interoperability across air, land, sea, and cyberspace, enabling a seamless connection between all services and domains. Accordingly, they must also proliferate as a multi-domain asset at all levels of conflict.
- **Technology and Human Synergy:** While drones should maximize autonomous capabilities, the doctrine must ensure a close integration between human operators, AI, and autonomous systems to balance decision-making. The final trigger must rest with the man behind the machine.
- **Scalability and Adaptability:** A dynamic approach that allows drones to perform across different operational environments, from counterinsurgency to conventional warfare, deserts to high altitudes, under hostile counter-drone and EW environments with easy adaptability to changing technological landscapes.
- **Family of Platform Approach:** The solutions must rest on the commonality of a platform and a family of drones for plug-and-play as per the required operational mission. The size and configuration (jammers, seekers and shooters) of the swarms and the type of payload must be variable as the mission requirements. This would ease logistic and training requirements besides cost.
- **Economy of Effort:** In an era where time and decision dictate outcomes under a hostile EW environment and shortened OODA cycle, the need is for an integrated approach of sensor-shooter autonomous drones that are survivable and intelligent for mission execution.
- **Air Space Management and Frequency Management:** The proliferation of unmanned aerial systems along with multiple aerial platforms will need careful airspace management, discreet scaling cum utilisation authority and frequency spectrum management.
- **Drone Integrated Joint AD Architecture:** This aspect needs a review and redefinition as a permanent Joint Air Defence Centre (JADC) along the borders and over Vulnerable Areas (VAs)/Vulnerable Points (VPs) with a reviewed tri-service policy architecture.
- **Training and Tactics:** Encourage innovations in tactics, and adaptive structures, and train to integrate as a warfighting function. It is one thing to fly a drone. It is another to prosecute drone-enabled warfare in a contested operational environment. A similar analogy is driving tanks and prosecuting tank warfare. A working group of mechanised warfare practitioners, technology experts, and drone entrepreneurs be constituted to assess and validate the impact of swarms on mechanised forces structures and tactics. A similar model be followed for Infantry

and artillery in mountains, plains and CI grid. Establish Centres of Excellence for specialised training of First Person View (FPV)/Inf drones at Inf School, Swarms at Armoured Corps Centre and School (ACC&S) and UAVs at Arty School. The employment of drones as integrated training is part of all training institutions under ARTRAC.

- **Force Structuring:** Technologies enable warfare structures to evolve and reorient for smart and lean warfighting. Presently a fair redundancy exists in the present structures to be tweeted without accretions to be adaptable and responsive for optimised drone-centric warfare capability. Single drones and FPV drones be integrated into the present equipment/ organisation profile and swarms at the Brigade or IBF level as an aerial arm or manoeuvre or for application as precise mass for integrated saturating attacks.
- **Ethical and Legal Guidelines:** The doctrine must lay down key ethical and legal guidelines ensuring that technological advancements in warfare remain aligned with ethical standards and global security norms.
- **Concept of Mass Application:** In a drone conflict, the outcome of that drone conflict will not only entail superior kill ratios but also mass availability and application as saturating attacks. Being attriteable, superior mass can obviate superior kill ratios.
- **Swarms as Aerial Arm of Manoeuvre:** While swarms can be utilised as stand-alone surgical strike or search and strike missions, their optimal employment is as an aerial arm of manoeuvre with IBG/mechanised forces. This capability construct must be refined and validated by the mechanised forces without manpower accretion or over-matrixing.
- **IBG Orientation.** The concept and validation of offensive and defensive IBGs having crystallised, the need is to integrate and validate the employment of drones and swarms into the IBG matrix and test bed to validate its efficacy. It must have an all arms combined warfare orientation.
- **Scaling and WWR.** These issues for disposable Kamikaze drones and loitering ammunition will need to be decided.

CONCLUSION

The future battlespace is going through tectonic changes in the character of warfare emphasising the need for innovation, adaption and integration into the warfighting doctrine to be future-ready. The multidomain battlespace and its spatial battle geometry are being revolutionised by the strategic application of technologies like AI, drones and cyber which offer critical time-kill ratio advantage with economy of force and precision mass effect.

The Indian Military must integrate drones into its operational doctrine, robust indigenous production, and strategic procurement of technologies to build a capable, versatile, and future-ready force. This requires bold, transformative leadership to overcome inertia and old ways of doing business.

❖❖❖

Lt Gen AB Shivane, PVSM, AVSM, VSM (Retd) is the former DG Mechanised Forces and a Strike Corps Commander. The Officer is a defence analyst and prolific writer on matters military. Presently, he is Distinguished Fellow and COAS Chair of Excellence at CLAWS.

NOTES

1. Lt Gen A B Shivane, Embracing Change in the Future of Warfighting, Faultline, SATP, https://satp.org/Docs/Faultline/30_Future-Battlespace--Embracing-Change-in-the-Fabric--of-Warfighting.pdf
2. Lt Gen AB Shivane, Indian Army Needs Drone-Centric Warfare Capability, Raksha Anirveda, Jan 14, 2025, https://raksha-anirveda.com/indian-army-needs-drone-centric-warfare-capability/
3. EY - FICCI report, Aug 2022, “Making India the drone hub of the world”, https://www.ey.com/content/dam/ey-unified-site/ey-com/en-in/insights/government-public-sector/documents/ey-ficci-drones-report-final.pdf
4. Jack Watling and Nick Reynolds, “Tactical Developments During the Third Year of the Russo–Ukrainian War”, RUSI Feb 2025, https://static.rusi.org/tactical-developments-third-year-russo-ukrainian-war-february-2205.pdf
5. David Hambling, New RUSI Report: Drones Now Inflicting Two Thirds Of Russian Losses, Feb 18, 2025, https://www.forbes.com/sites/davidhambling/2025/02/18/new-report-drones-now-destroying-two-thirds-of-russian-targets/
6. Michael C. Horowitz, “Battles of Precise Mass:, Foreign Affairs Oct22, 2024, https://www.foreignaffairs.com/world/battles-precise-mass-technology-war-horowitz#
7. Jorge Rivero, “Innovating Under Fire: Lessons from Ukraine’s Frontline Drone Workshops”, Modern War Institute, March 25, https://mwi.westpoint.edu/innovating-under-fire-lessons-from-ukraines-frontline-drone-workshops/
8. Global Security Organisation, “Radar Cross Section”, URL: https://www.globalsecurity.org/military/world/stealth-aircraft-rcs.htm?utm_
9. Science Direct, (2012), “Radar Absorbing Material”, URL: https://www.sciencedirect.com/topics/engineering/radar-absorbing-material?utm_source=chatgpt.com
10. Arzan Tarapore, Paper: “The Army in Indian Military Strategy: Rethink Doctrine or Risk Irrelevance”, August 10, 2020, Carnegie India - Carnegie Endowment for International Peace, https://carnegieendowment.org/research/2020/08/the-army-in-indian-military-strategy-rethink-doctrine-or-risk-irrelevance?lang=en

11. Robert Allardice and George Topic, “Battlefield Geometry in our Digital Age”, NDU, https://cjsl.ndu.edu/Portals/94/Documents/8-Battlefield_Geometry_in_our_Digital_Age.pdf?ver=2020-05-12-160047-540
12. The US Army’s multi-domain-operations Doctrine December 2022, https://www.iiss.org/publications/strategic-comments/2022/the-us-armys-multi-domain-operations-doctrine/
13. Lt Gen A B Shivane, “Restructuring for India’s Disputed Borders: An Appraisal”, CLAWS Journal, Winter 2021, http://ojs.indrastra.com/index.php/clawsjournal/article/view/131/137
14. Lt Gen A B Shivane, Book, “Professional Military Education: Making of the 21st Century Warrior”, KW Publishers, 2023, http://kwpub.in/Home/product/9789394915381/professional-military-education-making-of-the-21st-century-warrior

❐❐❐

118-132

NEAR SPACE-BASED TECHNOLOGIES: AN ALTERNATE TO OUTER SPACE FOR FUTURE WARFARE

Gp Capt (Dr) Swaim Prakash Singh

"Future warfare is all about air, space and sub-surface domains. The conventional land and sea domains will restrict to holding territories."

--Author

Abstract

The persistently unending debate of changing the character of warfare has at least built the narrative that there is a decisive shift from the conventional domain of warfighting. Although all land, sea, and air domains are significant but contemporary. and futuristic warfare will not be limited to them. The traditional warfare landscape is being redefined by the decisive shift towards the air, space, and sub-surface domains, as evidenced by the evolving nature of global conflicts. The function of land and sea operations will be reduced to that of holding and securing territories, as future warfare will increasingly depend on the dominance of these invisible realms. This transformation is readily apparent in modern conflicts, where strategic advantage and operational outcomes are being influenced by air and space capabilities. Without air, space, and sub-surface dominance, conventional forces may become ineffective and susceptible to technologically advanced adversaries. The future of warfare lies in the air and space domains, and space-driven technology will not only be necessary for victory but also for ensuring domination and maintaining a strategic edge over enemies. This is something that traditional land and sea domain thinkers and practitioners need to acknowledge. Future warfare is impossible to imagine without utilising these domains.

Thus, military doctrine and strategy must undergo a paradigm change in line with the preponderance of the air, space, and sub-surface domains. Nations must invest in cutting-edge technologies, including near-space flight vehicles with onboard sensors and shooters, hypersonic weapons, electronic warfare capacity, and robust space architecture. Space technology is the linchpin that connects and enhances capabilities across all domains of warfare from higher heights and greater distances. Space assets facilitate the operational efficiency and connectivity necessary for contemporary military strategies, from satellite-based Intelligence, Surveillance, and Reconnaissance (ISR) to precision navigation, communication, and targeting. In order to capitalise on future conflicts, it will be imperative to implement robust space policies. This paper aims to explore the potential of the near-space regime to serve as a viable alternative to satellites in outer space and to serve as the primary

category of technologies for space applications in the joint military domain in response to the regional threat posed by the space domain.

SPACE APPLICATION IN TRI-SERVICE CONVENTIONAL DOMAIN

Despite the increasing importance of air, space, sub-surface domains, and space influencers for commercial purposes, land, air, and sea warfare, there is a need to evolve beyond analogue and digital Command and Control (C2) structures to a much more connected battle space. The convergence of space-based capabilities with traditional military operations will define the effectiveness of the Army, Navy, and Air Force in future conflicts. Space technology is considered indispensable for national security because of its unparalleled advantages in strategic deterrence, navigation, communication, and surveillance. The primary requirements of the services through the medium of space and near-space are explained in the following table.

Land Warfare	Sea Warfare	Aerial Warfare
Persistent Surveillance and Battlefield Awareness	Persistent Maritime Domain Awareness (MDA)	Persistent Intelligence, Surveillance and Reconnaissance (ISR)
Secure Land Communication and Coordination	Underwater Communication and Submarine Detection	Secure Operational data Link and Command and Control
Secure Tactical Battle Area networked operations	Secure Fleet Communication and Navigation	Network-Centric Warfare
Precision Targeting and Strike Coordination	Anti-Submarine Warfare (ASW)	Precision Strike Capabilities
Electronic Warfare and Cyber Operations	Electronic Warfare and Cyber Operations	Airborne Electronic Warfare and Cyber Operations
Humanitarian Assistance and Disaster Response (HADR)	Humanitarian Assistance and Disaster Response (HADR)	Humanitarian Assistance and Disaster Response (HADR)
Out of Area Contingency	Out of Area Contingency	Out of Area Contingency
--	--	Space-Based Missile Defence and Strategic Deterrence
--	--	Meteorological and Environmental Monitoring

Table 1: Space Application in Tri-Service Conventional Domain. Source: Author

SPACE INFLUENCERS

The protracted confrontation between Russia and Ukraine has given the world plenty of military and political lessons. However, interestingly, one of the critical observations is the rising impact and involvement of one individual, Elon Musk. Today, Musk has become a synonym for space commercialization and impacting the outcome of conflicts through space warfare. His bold and aggressive stance on internal and global geopolitics shows an overgrowing convergence of national security with private business interests.

The world has seen his active indulgence in the US presidential election to the extent of completely overshadowing the political contenders. This often gave the impression that the election was more about Musk's strategic foresight instead of simply being a rivalry among candidates. This was further evident with he being given the responsibility of the newly created Department of Government Efficiency (DOGE). Elon Musk's influence was evident from President Trump's inaugural speech, which laid out a vision for the future of space through Mission Mars and said that it is time to leave this planet.[1]

The concern remains whether a millionaire today determining the course of countries, the planet, and finally, outer space. This is a largely unavoidable reality. Musk's technological investments in space have helped him become a major player in world strategy. The dominance of space technology in defining future warfare strategies is becoming increasingly evident, ranging from military applications to economic expansion, business ventures, and space tourism.

The significance of space-based assets in contemporary warfare, including real-time intelligence and surveillance and satellite communications, was again emphasised during the Russia-Ukraine conflict. Musk's Starlink satellite system, though a non-governmental project gave Ukraine robust communication capabilities, demonstrating how directly private space assets may affect military results.[2] This intentional use of space assets emphasises even more the idea that space technology will be at the forefront of future conflicts. While Elon Musk might have separated from President Trump but his pronounced impact regarding space use is going to stay.

The overarching lesson for military strategists worldwide is clear. Space is not the new or final frontier, but it is definitely no longer a distant frontier; instead, it is an active theatre of geopolitical competition. The integration of space capabilities into national defence strategies is imperative. Space superiority will not only dictate military dominance but also economic leverage, technological leadership, and geopolitical influence.

TRAVERSING INTO OUTER SPACE THROUGH INNER SPACE

Space influencers, through technology and funding, have made outer Space a new global market sector. US-led Artemis Accords and the collaborative efforts of China and Russia for the International Lunar Research Station (ILRS) are the disruptors in both space exploration and warfare. However, not much has been heard about dominating the higher altitudes of Earth's atmosphere (Inner Space), commonly classified as 'Near space'. The Inner Space is globally accepted from the ground level to 100 km of height. The 100 km mark is commonly known as the Karman line, which divides Inner and Outer Space.[3] The span of 100 km from the Earth's surface is a sovereign space utilized by the aircraft. However, interestingly, aircraft usually fly to an altitude of 20 km, beyond which the law of aerodynamics suffers drastically due to the rarified air. Thus, it practically amounts to the non-usage of altitudes between 20 km to 100 km.

Since space-faring nations and the technological industries concentrate mainly on space technology at Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geostationary Orbit (GEO) and beyond in outer space, inner space is widely available for civil and military purposes. As aspiring space-faring nations, countries remain focused on venturing into outer space compared to inner space, mainly to showcase their prowess in outer space technology. However, outer space has many limitations and restrictions for the military application of space assets due to international law and regulations.

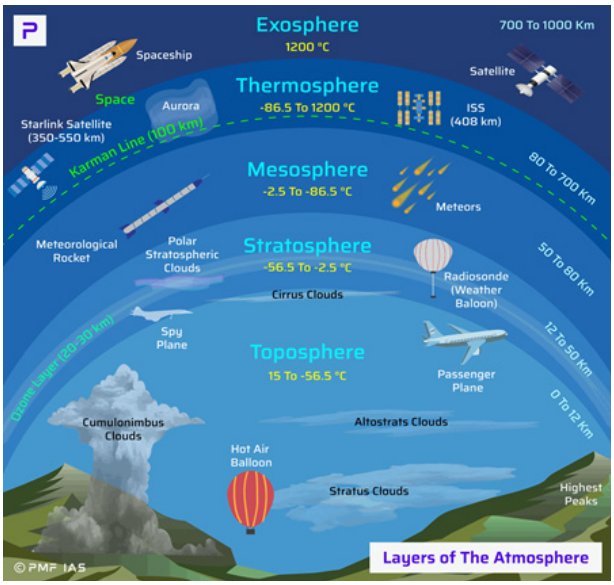


Figure 1: Layers of Atmosphere. Source: PMF, IAS, URL; https://www.pmfias.com/karman-line/

As previously mentioned, the region known as near space constitutes a segment of Earth's atmosphere and is regulated by air law. According to the Chicago Convention of 1944, the atmosphere above a nation's territory is regarded as the sovereign domain of that particular country.[4] Consequently, there exists no legal obligations regarding military applications in near space.

NEAR SPACE AS AN ALTERNATE TO OUTER SPACE

The near-space region presents a strategic opportunity for military applications as an alternative to LEO, MEO and GEO in outer space. As space-based military assets face increasing threats from anti-satellite (ASAT) weapons, jamming, and space debris, near space offers unique advantages in terms of persistence, manoeuvrability, reduced vulnerability, and cost-effectiveness for ISR, communications, and hypersonic strike operations. Given the challenges of operating in outer space, the militarisation of near space can provide a robust and resilient defence architecture in this region.

CHALLENGES IN NEAR SPACE

The near-space region presents some challenges for space activities because of the basic rules of physics and aerodynamics. Often referred to as the stratosphere, mesosphere, and lower thermosphere, this area suffers a mix of aerodynamic forces, extreme temperatures, low air pressure, and strong turbulence. In this area, the atmospheric density reduces sharply with height, which influences the lift and drag forces experienced by hypersonic vehicles, drones, and high-altitude balloons. The low pressure highly affects the aerodynamic stability, which requires specialised propulsion systems. Despite these challenges, near-space technologies such as hypersonic flight, High-Altitude Pseudo-Satellites (HAPS), and suborbital space travel are gaining increasing popularity.

ADVANTAGES OF NEAR-SPACE WARFARE

Considering the possible dangers associated with LEO, MEO, and GEO satellites, as well as the increasing buildup of military capabilities in outer space, it is necessary to develop a comprehensive approach to near-space combat operations. Highly mobile low altitude persistent surveillance systems, paired with hypersonic or energy-based weapons and sophisticated, robust communication systems can transform remote warfare as we know it today. In a nutshell, near space has the potential to outperform the traditional air domain as it can offer responsive, flexible and much cheaper battlespace within the legal boundaries and jurisdictions, unlike outer space. Merging artificial intelligence and autonomous system innovations with next-generation propulsion, sensor, and shooter systems will make near space a decisive area

for military operations and offer guarantees for winning strategic superiority in subsequent conflicts.

As obvious, the rarefied environment in near space is unfit for traditional aircraft. Thus, Near-Space Flight Vehicles (NSFV) are made or developed to withstand a spectrum of demanding environmental conditions, including UV radiation low atmospheric pressure, and strong storms. In contrast to higher orbits, near space will also offer a cheap and bearable proposition for deploying satellites. Reaching near space below the Kármán line does not require (~7.8 km/s)[5] orbital velocity. Instead, it can be deployed and maneuvered using low thrusters such as ionic ones. Also, there is a significantly reduced cost with lesser logistical complexity. Maintaining NSFVs for a prolonged period may have maintenance issues. However, those can be overcome by replacing and recovering them after the completion of mission objectives. Such an economy of cost will lead to expanding the NSFVs network exclusively for military needs in the near space region.

Near space also provides relative benefits compared to LEO satellites and aircraft, including fuel usage, freedom from orbital mechanics, and survivability. NSFVs can hover, loiter, or manoeuvre on demand over a fixed area without the need for complex orbital adjustments like LEO. Thus, fuel can be used entirely for mission-specific purposes. Ground threats may be less relevant to near-space assets, as these operate above the reach of most conventional surface to air missiles and radar detection envelopes. Also, unlike satellites, which follow predictable paths and can be tracked and targeted, NSFVs can alter course, manoeuvre, and even descend or evade if necessary. Near space as a 'sweet spot' between air and space could become a highly contested area, influencing the course of future conflicts through operational efficiency, tactical flexibility, and persistent presence, all of which make it an excellent tool for both offensive and defensive military operations. The following are some roles and technologies that can be substantially accrued from near space:

- **Constant ISR and Targeting Capabilities:** As discussed, NSFVs like HAPS possess ISR capabilities that are more affordable and persistent than satellites. Unlike LEO satellites, which orbit the earth every 90 minutes,[6] at 28,000 kmph, near-space ISR vehicles can hover above the areas of interest, providing constant surveillance and reconnaissance for longer and intended periods. NSFVs such as Zephyr UAV can operate between 18 km and 30 km,[7] altitudes, providing incessant imaging, Electronic Intelligence (ELINT) and Signal Intelligence (SIGINT). According to the Navier-Stokes equations, these platforms are less subjected to atmospheric drag and require relatively fewer station-keeping manoeuvres. Due to the closer proximity to the intended target

than LEO Satellites, it provides lesser image distortion from atmospheric turbulence, resulting in higher image quality and greater resolution.

- **Secure and Resilient Military Communications:** Unlike predictable orbital paths of satellites, near-space assets present a viable alternative to the communication satellites in MEO (2000 km–35786 km) and GEO (35786 km), which remain highly vulnerable to ASAT weapons, cyber threats and interference.[8] Near-space communication nodes can drastically cut down on latency which is a major drawback of geostationary satellites due to their high altitude. This can effectively improve C2 and battlefield awareness in real-time. Also, it will help make the relay systems more effective. The adaptive beamforming and frequency-hopping antennas in the inner atmosphere can lessen the risk of jamming and interception and will tremendously help mitigating electronic warfare threats.
- **Mitigating Emerging Hypersonic Threats:** In relation to space, there is an increasing necessity for quick and nimble platforms for military applications due to the emergence of Hypersonic Glide Vehicles (HGVs) and Hypersonic Cruise Missiles (HCMs). High-speed missiles posed a complex challenge to traditional early warning satellites in LEO and MEO because satellites were built to track ballistic missiles, which follow predictable arcs and emit strong thermal signatures. In contrast, HGVs and HCMs manoeuvre unpredictably, generate less heat than ballistic missiles and often fly at lower altitudes, making them harder to detect and track. The gap in tracking hypersonic threats can be bridged with the help of near-space infrared tracking and radar systems that allow persistent line-of-sight coverage and lower atmospheric clutter.
- **Missile Defence Systems:** In addition, near space can be utilised as a stealthier transit area by hypersonic weapons, enabling them to evade conventional missile defence systems that rely on exo-atmospheric and atmospheric engagement. Interceptors based at high altitudes and in near-space, as well as other Directed Energy-Based Weapons (DEWs), can provide a critical line of defence against missiles. While spaceborne assets and ground-based interceptors form the backbone of traditional missile defence strategy, both have their disadvantages. Examples of underproduction near space DEWs with the US and China could be used to defeat incoming threats at altitudes with low air resistance, including high-powered lasers or electromagnetic railguns which would increase range and accuracy.
- **Stealth and Tactical Mobility for Combat Operations:** Near-space platforms can offer a distinct advantage in stealth and electronic warfare

operations. Near-space assets are less vulnerable to targeting because they can dynamically change their position, speed, and altitude, unlike satellites, which follow predictable orbital paths that adversaries can monitor and counter. Conducting deep penetration ISR missions using high-altitude low-RCS UAVs or space vehicles augmented with Electronic Countermeasures (ECM) payloads can be particularly advantageous in the near-space environment. These UAVs can be effectively employed for stealthy counter-sensor capability to establish EW or decoy attack missions against an enemy's key communication, radar locations, or integrated air defences within a framework of destruction/suppression of enemy air defences.

- **Improving Space Situational Awareness (SSA) and Space Domain Awareness (SDA) with Near-Space Sensors.** Important aspects are as under:
    - SSA and SDA in outer space are complex challenges without an integrated global network of sensors capable of detecting and tracking satellites and space debris. LEO, MEO, and GEO regions are becoming congested with life-expired and junk satellites and debris fragments. Ground-based optical and radar systems have a limited view of outer space from Earth. Space-based sensors have their merits, although they remain vulnerable to ASAT and other non-kinetic means.
    - These sensor chain gaps decrease the efficiency of space traffic control and collision avoidance initiatives, which produce blind spots in SSA/SDA. However, these constraints do not apply to the near-space region because many countries currently have long-range high-altitude radars in place for airspace surveillance and Ballistic Missile Defence (BMD). Over-The-Horizon Radars (OTHRs), phased-array radars, and space-tracking radars are among the radar systems that can precisely detect and identify objects in near and outer space. For instance, the US Space Fence system tracks debris as small as 10 cm in LEO using S-band phased-array radar.[9] Likewise, China’s Yuan Wang’s space-tracking system and Russia’s Don-2N radar are essential components of their respective national SSA initiatives. Critical gaps in global SSA/SDA are filled by these ground-based radars, which, when paired with airborne and near-space sensors, provide continuous high-resolution tracking of space objects.
    - Operating above most atmospheric interference but below LEO, near-space sensors use infrared to track CubeSats, stealthy satellites,

or small debris to detect faint optical signatures. Better cataloguing and characterisation of Resident Space Objects (RSO) will also guarantee improved safety and threat identification. Furthermore, it allows continuous observation of valuable orbital assets, particularly in congested or disputed space over sovereign territory.

- India has also made significant progress in this regard by using its BMD sensor network for SSA and SDA purposes. The indigenous Swordfish Long-Range Tracking Radar (LRTR) technology, capable of tracking objects up to 1500 km[10] away, gives India a reliable means of detecting satellites and space debris in LEO and MEO. Another such development is the creation of an indigenous space surveillance network through the Netra SSA project, led by Indian Space Research Organisation (ISRO) in association with the Defence Research and Development Organization. It aims at the integration of tracking stations, radars, and telescopes on the ground. The next Multi-Object Tracking Radar (MOTR) coming up at Sriharikota will be able to eye real-time activities in space. With such developments, near-space assets can prove to be more reliable and affordable, and an ideal substitute for SSA/SDA techniques in the outer space.

CHINA'S NEAR-SPACE CAPABILITY: CURRENT STANDING AND STRATEGIC SIGNIFICANCE

China has achieved tremendous success in developing its near-space capabilities. It established the Near-Space Command, its fifth military branch under the Central Military Commission (CMC) in December 2023.[11] The country's defence against threats in the near space falls under the purview of this command. The Chinese military has developed hypersonic glide vehicles, near-space drones, and high-altitude balloons with great aggressiveness to achieve strategic advantage in this field. High-altitude balloons are a key part of China's near-space capability. The PLA has made huge investments in stratospheric surveillance platforms to operate above conventional air defence systems. Chinese near-space platforms have been used for intelligence gathering, electronic warfare, and atmospheric research. Beijing's capability of long-duration surveillance missions, as exemplified by the Chinese balloon discovered over the United States in 2023, is the testimony of its scientific prowess in this regime.[12]

Lately, China has also made strides in near-space hypersonic technology. Successful testing of the DF-17 hypersonic glide vehicle indicates that China can use fast and agile weapons that can break through missile defence systems.[13] Wuzhen-8 technology for high-altitude drones also indicates the

ability to maintain near-space operations for military and intelligence use. Other examples include China's development of solar-powered UAVs such as the CaiHong series, which can stay airborne for long durations, providing continuous communication relay and surveillance capabilities. Another notable endeavour is the Tengyun project by the China Aerospace Science and Industry Corporation (CASIC), a reusable near-space flight vehicle.[14]

China Academy of Aerospace Aerodynamics (CAAA) and CASIC have been instrumental in developing a coherent national strategy in fusing the agencies of research and development, private aerospace companies and military institutions for creation of near-space technologies. China, which is in close competition with the US and Russia, is one of the few countries with sophisticated near-space capabilities. However, the US continues to lead in hypersonic technology and strategic reconnaissance capabilities such as X-37B[15] reusable unmanned spacecraft and DARPA projects, but China has quickly caught up with like the DF-ZF HGV,[16] showcasing operational capabilities that go against conventional air and missile defence architectures. China's dominance in near space is expected to grow further with ongoing investments in high-altitude platforms and hypersonic weapons, shifting the strategic balance in contemporary warfare.

The capabilities of China's growing emphasis on near-space technologies go beyond those of conventional satellites and low-altitude UAVs, enabling more extensive real-time surveillance with possibly lower latency and wider coverage. It also offers precise strikes capability, particularly with the use of hypersonic weapons or sophisticated missile systems, which may provide a significant tactical edge. China's growingly advanced near-space capabilities raise concerns about military escalation and regional deterrence stability. The calculation in any India-China conflict could change if China were to acquire such capabilities. As a result, India must make these investments while maintaining the credibility of its own conventional and nuclear strategic deterrence.

IMPLICATIONS FOR INDIA

Given the growing military and strategic competition between the two countries and perpetual adversaries on the Western side, the concept of 'Near-Space' in China's military strategy holds significant relevance in the Indian context. It reiterates that space and near-space capabilities are relevant not only to land borders but also to the peninsular region in the Indian Ocean Region (IOR). Figure 2 highlights the regions requiring constant surveillance from Space and near Space to ensure national security from the space domain.

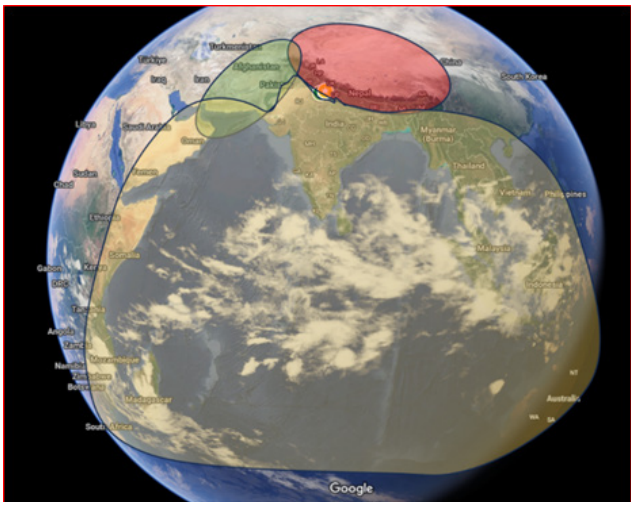


Figure 2: Area of Interest for Constant Surveillance Source: Author's articulation on the google map (Approximated Scale)

INDIA'S RESPONSE POLICY/DOCTRINE/VISION

India's deterrence strategy must take into consideration its near-space capabilities, making sure that its communication and command systems are resilient to Chinese technological breakthroughs. In order to secure its airspace, India would have to develop near-space capabilities through a multifaceted strategic approach that incorporates research defence infrastructure and technological innovation. To meet its operational requirements for strategic dividends in both peace and war, the defence forces, under the aegis of the Defence Space Agency (DSA), will need to take a different and separate approach to space and near space. The country's endeavour of Viksit Bharat@2047 would benefit greatly from the creation of a near-space policy, doctrine or vision solely for military purposes. Some crucial elements that may be considered in the proposed Policy, Doctrine or Vision are as follows:

- **Near-Space Flight Vehicles (NSFV):** As discussed earlier, near-space refers to the region between 20 km to 100 km above Earth's surface, where aircraft operations are generally prohibited due to atmospheric conditions. Futuristic drones and pseudo-satellites would operate in a unique environment with specific challenges in this region. India needs to develop specialized NSFVs, such as high-altitude drones and HAPS. Stratospheric balloons are another means that China has heavily relied upon. However, in the Indian context, this technology may be precluded from consideration due to sustainability, atmospheric conditions, and potential international litigation and criticism.

HAPS could have ISR and kinetic versions in the form of hypersonic glide vehicles for rapid swarm strikes and targeting capabilities purely for strategic effects. Such weapons may not be intended for tactical strikes or operations, as sustaining such weapons in abundance in the near space may not be feasible at all times.

- **Power Source:** Such high-altitude near-space vehicles would require advanced propulsion technologies. These could include solar-powered propulsion systems or hybrid engines that offer longer endurance and higher efficiency in the near-space environment. The ionic thrusters may be the best option for such vehicles in the regime. The possibility of nuclear-powered propulsion systems may also be explored, keeping technological capabilities and limitations in mind. It is expected that nuclear-powered vehicles will be able to stay aloft for long periods, providing real-time intelligence and continuous surveillance over sensitive areas, including border regions, critical infrastructure, and maritime zones. It will also entail severe and foolproof layered mechanisms, procedures and protocols to mitigate any nuclear source malfunctions.
- **Sensor Technology:** It is evident that NSFV would require advanced sensor systems capable of functioning in thin air, low temperatures, and high-radiation environments. These could include high-resolution imaging sensors, multi-spectral radar systems, and laser communication systems that can be deployed in NSFV for surveillance and intelligence gathering.
- **National Jurisdiction:** Special care should be taken in the doctrine, as these near-space vehicles will not be subjected to orbital or suborbital trajectories. These vehicles would act as temporary or pseudo satellites/surveillance systems in near space and operate within the sovereignty of the nation. These vehicles will still be governed by air laws and not space laws. Therefore, it will require reiteration of air laws beyond the limits of Air Traffic Control and services. The integration of air laws and their intricacies at the higher altitudes in the Integrated battle management system will have to be reformulated in the training schemes of the C2 centres of the defence forces. Primarily, it would include launch, recovery, manoeuvring, near-space traffic control and management, etc.
- **Seamless Integration:** By integrating near-space assets with satellite constellations, especially LEO satellites, India can achieve seamless ISR, and targeting capabilities. India can expand and further strengthen its existing network of military satellites for cross-domain information fusion to improve response time and battlefield situational awareness.

- **Integration of Near-Space with Air Defence:** A comprehensive approach to airspace security will require bringing NSFVs into India's existing air defence systems. NSFVs with appropriate payloads could provide critical information for Priority-I targets and/or be integrated with the Integrated Air Command and Control System (IACCS), if not for all air and air defence operations. This will be the first step towards adequately integrating space-based (near space) capabilities. Early Warning Systems need to be dovetailed into the IACCS, which is the nerve centre of the entire gamut of air operations in the Indian sovereign airspace.
- **Other Areas of Near-Space Exploration:** Within the realm of technological feasibility and based on the laws of physics, the aspects of communication and electronic warfare, or jamming and spoofing, such as Slingshot Aerospace's GPS jamming detection, spoofing detection, and geolocation,[17] could be part of the new concepts on Near-Space employment doctrine. Overlapping these with cyber operations could add more teeth to this futuristic thought.

CONCLUSION

The ongoing Russia-Ukraine conflict unexpectedly reveals as to how the space technology developers can shape future military engagements and global political dynamics. The transformation of space exploration into a private enterprise domain shows significant global implications while redefining what was once government-exclusive territory. It is now becoming evident that the 21st century global leadership paradigm will hinge upon the intricate development and control of space technology sectors. Nations competing to safeguard their space resources will find private-sector partnerships essential, a fact that Elon Musk consistently demonstrates.

It is also not far to internalise that future conflicts are destined to unfold within air, space and subsurface realms while land and sea operations may function as auxiliary methods to secure strategic and tactical geographical entities. Therefore, to dictate outcomes of future conflicts, the grasp and application of space technology are essential determinants for achieving supremacy across all aspects of modern warfare. The exploration of near-space zones inside Earth's atmosphere emerges as a practical choice due to the intricate legal issues that restrict military activities in outer space. India's military operations can undergo a complete transformation through NSFVs, which enhance electronic warfare capabilities alongside missile defence systems and strategic deterrence while boosting intelligence gathering.

Despite the unique operational needs of the Army, Navy, and Air Force, a Unified Near-Space Strategy (UNSS) can enhance force performance against

escalating Chinese and Pakistani threats. India and its armed forces, in particular, must boost near-space research by investing in domestic platforms and collaborating with international partners to maintain its strategic advantage in all domains of modern warfare.

❖❖❖

Gp Capt (Dr) Swaim Prakash Singh is a cat AYE, MFC, Command Examiner, qualified APM, and AWACS Mission Commander with over 1000 hours of flying. He has also been Directing Staff at DSSC, Wellington.

NOTES

1. Tim Hains. Trump: "The United States Will Once Again Consider Itself a Growing Nation" Real Clear Politics, January 20, 2025, https://www.realclearpolitics.com/video/2025/01/20/trump_the_united_states_will_once_again_consider_itself_a_growing_nation.html?utm Accessed on February 9, 2025.
2. Jason Rainbow. “As U.S. blames Russia for KA-SAT hack, Starlink sees growing threat” Space News, May 11, 2022 https://spacenews.com/as-us-blames-russia-for-ka-sat-hack-starlink-sees-growing-threat/ Accessed on April 19, 2025.
3. Jonathan C. McDowell. “The edge of space: Revisiting the Karman Line” Science direct, https://www.sciencedirect.com/science/article/pii/S0094576518308221#sec55 Accessed on February 11, 2025.
4. “Airspace Sovereignty” International Civil Aviation Organization. https://www.icao.int/Meetings/atconf6/Documents/WorkingPapers/ATConf.6.WP.080.1.en.pdf Accessed on February 11, 2025.
5. Allan McInnes. “Launching satellites” University of Waikato, Science Learning Hub. https://www.sciencelearn.org.nz/resources/272-launching-satellites Accessed on January 13, 2025
6. “AU-18 Space Primer” Air University Press, https://www.airuniversity.af.edu/Portals/10/AUPress/Books/AU-18_Space_Primer_2023.pdf Accessed on February 11, 2025.
7. Xiongfeng Zhu, Zhongxi Hou. “Solar-powered airplanes: A historical perspective and future challenges” Science direct,https://www.sciencedirect.com/topics/engineering/high-altitude-flight#:~:text=The%20high%20flight%20altitude%20feature%20of%20solar%2Dpowered,is%20not%20an%20issue%20for%20these%20airplanes Accessed on February 11, 2025.
8. Vijay Kumar Saxena, “Anti Satellite Weapons: A Likely Future Trajectory” Occasional paper May 2016, Vivekananda International foundation, https://www.vifindia.org/sites/default/files/anti-satellite-weapons-a-likely-future-trajectory.pdf Accessed on February 11, 2025.
9. Sally Cole. “Space Fence radar system to identify, track space junk” Military embedded System, https://militaryembedded.com/radar-ew/sensors/space-track-space-junk Accessed on February 11, 2025.
10. Bodhideep Roy “List of India’s Indigenous Radar Systems” Indian Defence Network. January 26, 2025, https://www.defencexp.com/list-of-indias-indigenous-radar-systems/ Accessed on February 20, 2025.
11. PC Katoch “PLA's Fifth Force – Near-Space Command” SP’s Aviation, December 11, 2023

https://www.sps-aviation.com/experts-speak/?id=791&h=PLAs-Fifth-Force-Near-Space-Command Accessed on March 20, 2025.

12. Zhao, Y. (2018). China's Intellectual Property System in the Process of Catch-up: With Patent in Focus. https://core.ac.uk/download/157586292.pdf Accessed on February 11, 2025.
13. Zuzanna Gwadera "Intelligence leak reveals China's successful test of a new hypersonic missile" The International Institute of Strategic Studies, https://www.iiss.org/online-analysis/online-analysis/2023/05/intelligence-leak-reveals-chinas-successful-test-of-a-new-hypersonic-missile/ Accessed on February 11, 2025.
14. Ibid.
15. Ravi Hari. "US Space Force's mysterious X-37B spaceplane returns to earth after 434 days in orbit– What did it discover?" mint, March 9, 2025, https://www.livemint.com/news/us-news/us-space-force-s-mysterious-x-37b-spaceplane-returns-to-earth-after-434-days-in-orbit-what-did-it-discover-11741462725909.html Accessed on March 15, 2025.
16. PC Katoch "Hypersonic and Drone Wars" SP's Naval Forces, November 27, 2024 https://www.spsnavalforces.com/experts-speak/?id=763&h=Hypersonic-and-Drone-Wars#:~:text=The%20Chinese%20DF%2DZF%20is%20an%20HGV%20integrated,China%20successfully%20tested%20a%20nuclear%2Dcapable%20hypersonic%20ICBM. Accessed on January 15, 2025.
17. "Slingshot Aerospace Selected to Provide Technology to USSF to Detect GPS Jamming and Spoofing Threats to International Security" Slingshot Aerospace, January 15, 2025 https://www.slingshot.space/news/slingshot-aerospace-selected-to-provide-technology-to-ussf-to-detect-gps-jamming-and-spoofing-threats-to-international-security Accessed on February 11, 2025.

❐❐❐

133-146

STRENGTHENING INDIA'S SPACE DETERRENCE: THE STRATEGIC IMPERATIVE FOR CO-ORBITAL COUNTERSPACE CAPABILITIES

Col (Dr) Kaushik Ray (Retd)

Abstract

With space emerging as a critical domain for national security, India's strategic posture vis-à-vis space needs to adapt to the altered threat environment. Direct-Ascent Anti-Satellite (DA-ASAT) weapons are overt means but these also create space debris, threatening all other satellites in the orbit, irrespective of friend or foe. Co-orbital systems offer more discreet, flexible, and potentially non-destructive options for neutralising adversary satellites. India must therefore prioritise developing co-orbital counterspace systems as a crucial step in enhancing its space deterrence capabilities.

The security of India's civillian and military space assets are threatened by China's expanding military space capabilities and its demonstrated willingness to deploy kinetic and non-kinetic counterspace systems. In such a security environment, India's current space deterrence is limited by its declaratory posture and lack of non-debris-producing counterspace assets.

Co-orbital counterspace capabilities can serve as a credible deterrent, offering calibrated, escalatory response options. With a lowered risk of debris or offering reversible effects, such systems also align with norms of responsible behaviour in space. Developing co-orbital counterspace capabilities would involve overcoming technical and policy hurdles, including dual-use technology concerns and integration with broader strategic doctrines.

India, therefore, needs to adopt a proactive, integrated strategy that includes doctrinal clarity, institutional coordination, and investment in indigenous space technology. Co-orbital counterspace systems are not merely space weapons but also serve as tools for strategic signalling in space, escalation control, and safeguarding national interests in the increasingly contested space domain.

SPACE SECURITY IN THE INDIAN CONTEXT

India's venture into outer space is undergoing transformational change. In its early days, its space programme was oriented towards developing an understanding of the space environment and for developmental purposes befitting a nation emerging from poverty. Over the last few decades, the space program has gradually realigned its efforts towards conducting pioneering scientific research aimed at unravelling the mysteries of outer space while exploiting space for

developmental, commercial and national security purposes. With more than 50 operational satellites in orbit today, the vulnerability of our critical space systems to kinetic and non-kinetic attacks has emerged as a prime national security concern. India's burgeoning space capabilities, new geopolitical realities and rapid militarisation of space by the major space powers make it crucial for India to consider the security of its space-related assets and freedom of access to space in its strategic thinking in a more concerted and focused manner. India shares a complex geopolitical relationship with the space weapons states and therefore needs to analyse its threat perception in space, considering these geopolitical nuances.

WEAPONISATION OF SPACE

The race for weaponisation of space was triggered for the second time after the Cold War when China conducted a successful DA-ASAT test in January 2007. The US responded a year later, demonstrating its DA-ASAT capability (Operation Burnt Frost) in February 2008. With rapid advances in space technology, global space powers (US, Russia, and China) have subsequently ramped up their space weaponisation capabilities over the next two decades.

SECURING INDIA'S SPACE ASSETS

Over the years, as a national security imperative, India's space programme acquired its military footprint through the launch of dual-use satellites for remote sensing, navigation, communication, etc., followed by dedicated military assets for surveillance and communication purposes. While the US and Russian counterspace capabilities do not pose an immediate threat to India in space, growing Chinese counterspace capabilities are a cause of serious concern. Geopolitical realities vis-à-vis China make it imperative for India to secure its space assets from possible Chinese attack and to contest Chinese military activities in space.

Consequently, developing a viable deterrence in space emerged as a strategic necessity to maintain a minimum level of space deterrence and retain a geopolitical equilibrium in South Asia and IOR vis-à-vis China. Also, it was anticipated that an international agreement akin to MTCR and NPT could come into play, segregating the ASAT haves and have-nots. In March 2009, India's Ministry of External Affairs press release unambiguously stated: "India expects to play a role in the future in the drafting of international law on prevention of an arms race in outer space . . . in its capacity as a major space-faring nation with proven space technology".[1]

In 2019, India marched into the exclusive club of DA ASAT capable nations with its successful destruction of an old ISRO satellite using a Prithvi Defence Vehicle Mark-II missile. India's prime objective for the test was to demonstrate

its capability to secure its space assets from any ASAT threat, to deter China's aggressive overtures in space, and to position itself as a significant player in the global space race.

NEGATIVE IMPACT OF DA ASAT ENGAGEMENTS ON THE SPACE ENVIRONMENT

Direct-Ascent Anti-Satellite (DA-ASAT) missiles pose significant risks to the space environment. On impact with the Kinetic Kill Vehicle of a DA-ASAT missile, the target satellite breaks down into hundreds or even thousands of fragments of varied sizes. Most of this space debris thus generated remains in orbit for years and even for decades, polluting the space environment and posing a collision risk to all satellites in a nearby orbit. Such debris, however tiny, travels at extremely high speeds (up to 28,000km per hour). If such debris collides with a functional satellite, it can severely destroy the space assets. The International Space Station, with astronauts aboard, is often threatened by such incoming debris created by DA-ASAT engagements and needs to take evasive measures. Such evasive manoeuvres by satellites and spacecraft require excessive use of thrusters, consuming additional fuel, otherwise meant for routine station keeping (maintaining desired orbit), thus reducing the operational lifespan of the satellite. Such debris from DA ASAT engagements may collide with other satellites, causing a chain reaction of collisions. This is known as Kessler Syndrome, and may, in future, render entire orbits unusable. To avoid such a potential situation, the United Nations Office for Outer Space Affairs (UNOOSA) has issued several guidelines for sustainable and responsible space activities. DA-ASAT tests contradict these guidelines by creating long-lasting hazards.

Globally, spacefaring nations are increasingly opposed to any further pollution of the congested orbital regimes. In April 2022, the US announced a unilateral moratorium on destructive (DA-ASAT) missile testing, pledging to stop such tests that create orbital debris, and encouraged other nations to follow suit.[2] The US cited the dangers of orbital debris created by such tests, which can remain in low Earth orbit (LEO) for years or decades, posing a threat to other satellites and space activities.[3] In December 2022, the United Nations General Assembly overwhelmingly adopted resolution A/RES/77/41 in support of the destructive DA-ASAT testing moratorium.[4]

NON-DEBRIS PRODUCING COUNTERSPACE SYSTEMS

Since debris generated by a DA ASAT engagement would endanger even own and friendly satellites in a nearby orbit, space weapons states have, over the years, developed a bouquet of alternative counterspace systems. These non-debris producing alternative systems are mounted on highly manoeuvrable,

Rendezvous and Proximity Operations (RPO) capable satellites that can close in with a target satellite in orbit and engage it employing Radio Frequency (RF) jammers, Kinetic kill vehicles, robotic grappling mechanisms, High-Power Lasers, High-Power Microwaves, chemical sprayers and other evolving techniques that do minimal damage to the space environment. Targeting satellites with RF jammers, lasers, microwaves etc, though possible from ground stations as well, requires very high-power levels, which again suffer considerable attenuation over such large distances through the atmosphere. The current status of the development and operationalisation of co-orbital counterspace systems by space weapons states is as under:

- **China:** China raised the Strategic Support Force in 2015 with a Space Systems Department to manage its space security requirements. Beijing is increasingly integrating space-based capabilities into its military doctrine. Even seemingly pure scientific ventures like human space flight and the space station have overtly offensive military usages. China is rapidly developing and fielding a myriad suite of offensive counter-space systems, including direct-ascent anti-satellite missiles, co-orbital counterspace systems, Space Electronic Warfare (SEW) and space cyber network warfare, and directed-energy systems. These systems pose a threat to India's space-based assets and capabilities. China has developed a vast array of dual-use space systems capable of co-orbital counterspace operations using ultra-agile satellites, space robots etc.[5] Prominent among these are:
    - **Aolong 1:** In January 2016, China launched the Aolong-1 satellite on a CZ-7 launcher from Wenchang Space Launch Centre, Hainan. The satellite was designed by the CALT, ostensibly to physically grab space debris and throw it on a re-entry trajectory into the atmosphere. The satellite has obvious anti-satellite applications. Aolong-1 likely carried a sub-satellite for use as a target for grabbing by the robotic arm. It re-entered the atmosphere in August 2016.[6]
    - **Shijian 6:** In September 2004 the Shijian series was revived as a military satellite with the launch of the Shijian-6 A and Shijian-6 B on a CZ-4B launcher from Taiyuan. While the 6A was the larger (975 kg) non-maneuverable Fengyun-type satellite, the 6B was small (375 kg) and maneuverable. After both the satellites attained their initial orbit at around 600 km altitude, the smaller 6B manoeuvred around the larger 6A. In October 2006, another Shijian-6 pair, the 'Shijian-6 Group 2' undertook similar manoeuvres. The third and fourth set of Shijian-6 launched in 2008 and 2010 also carried out several such manoeuvres.[7]

- **Shijian 7:** The Shijian-7 was launched into a Sun Synchronous Orbit (SSO) in July 2005. After several manoeuvres undertaken to adjust its orbit, the Shijian-7 participated in a close manoeuvre with the Shijian-15.
- **Shijian 12:** The Shijian-12 was launched on 12 June 2010. Five weeks later, it undertook a series of close manoeuvres with Shijian 6-3A coming within 200 m on 19 August. Similar maneuvers were carried out with the Shijian 6-4A in November 2010.[8]
- **Shijian 15:** In July 2013, China launched the Shijian-15 on a CZ-4C launcher together with a satellite named Shiyan-7 (SY-7) and the Chuangxin-3 (CX-3) in 2013. The SY-7 was fitted with a robotic arm for conducting space maintenance. The SY-7 remained silent in orbit before it released another spacecraft and drew away from it before closing in followed by robotic grappling of the separated spacecraft. Multiple such separations and grappling manoeuvres were conducted between the two satellites. This demonstrates a dual-use capability of the SY-7 fitted with a robotic arm, which can be used for deorbiting both space debris and enemy spacecraft, giving it a potential counterspace capability. The SJ-15 after launch, initially manoeuvred around the CX-3 before closing in with the Shijian-7 up to a few hundred metres.[9]
- **Shijian 17:** China's Shijian-17 launched in November 2016 on a CZ-5 Heavy Launcher conducted several close approaches with a Chinasat 5A, demonstrating capability for employment as a co-orbital ASAT system.[10]
- **Shijian 21:** In October 2021, the Shijian 21 (SJ-21) was launched as an experimental space debris mitigation satellite. It performed Rendezvous and Proximity Operations (RPO) manoeuvres around its upper stage Apogee Kick Motor (AKM) and then undertook rendezvous with a dysfunctional Compass G2 satellite. SJ-21 performed several RPOs around this satellite before docking and then moved the derelict Compass G2 into an, even higher orbit, hundreds of kilometres above the traditional GEO belt.[11]
- **Shiyan 12:** The Shiyan-12(01) and the Shiyan-12(02) were launched into GEO in early 2022. Thereafter, the satellites engaged in a close manoeuvre with a U.S. Geosynchronous Space Situational Awareness (SSA), getting away quickly whenever the U.S. satellite attempted a close approach.[12]
- **Shiyan-24C and Shijian-6 05A/B:** In 2024, China conducted a series of complex RPO close manoeuvres involving three Shiyan-

24C satellites and two experimental satellites, Shijian-6 05A and Shijian-6 05B.[13]

- **The US :** The US by far has the most advanced military capabilities in space. It has operationalised full-spectrum counterspace capabilities to include ground and air-launched DA-ASAT capability, co-orbital ASAT systems, and ASAT DEW systems, besides a potent space EW and cyber network warfare capability. The United States Space Force was founded in 2019. Technological advancements, including co-orbital counterspace systems and Directed Energy Weapons (DEWs), further enhanced US space defence capabilities.
- **The Geosynchronous Space Situational Awareness Program (GSSAP):** is a surveillance constellation located in the GEO for the conduct of SSA operations employing electro-optical systems and electronic emissions sensors. GSSAP satellites are highly agile and capable of performing Rendezvous and Proximity Operations (RPO) on objects of interest in space.[14] RPO-capable systems can rendezvous with other satellites to observe, inspect, and collect emissions from those systems, thus having the potential to act as an ASAT weapon that can impact/de-orbit an adversary's satellite. Each GSSAP satellites weigh around 650 to 700kg and probably carries adequate onboard propellant needed to adjust their orbits frequently.[15] After the creation of the US Space Force, the Space Delta 9, which is responsible for the conduct of orbital warfare, has been assigned the responsibility of managing the GSSAP constellation,[16] indicating its probable utility as a co-orbital ASAT.[17]
- **Russia:** After the dissolution of the Soviet Union, Russia re-established its ASAT program, likely in response to perceived advancements by China and the US in counterspace technologies. Besides a potent ground and air-launched DA ASAT capability, Russia has developed several Rendezvous and Proximity Operations (RPO) satellites in both Low Earth Orbit (LEO) and Geo-synchronous Earth Orbit (GEO) with potential co-orbital ASAT capability.

  Due to the high maneuverability of the latest Russian anti-satellite vehicles, it seems realistic that they could use lasers or small kinetic weapons instead of explosives and shrapnel to eliminate their targets. Furthermore, once the first satellite is hit, a miniature spacecraft might be used to attack a second one. However, since Russian satellites appear to be smaller in size, their fuel carriage capability and hence maneuverability may be limited. Some of the Russian RPO satellites and their identified manoeuvre activities are:

- **Kosmos-2491 and Kosmos-2499:** On 25 December 2013, a Rocket (commercial nomenclature Briz-KM) booster carried out a launch of four satellites from Plesetsk. In addition to three Rodnik communications satellites, it included a maneuverable satellite named Kosmos-2491**,** which undertook several orbital maneuvers over the next few months. Again, on 23 May 2014, a Rockot booster launched four satellites from Plesetsk Cosmodrome, which included the Kosmos- 2499 which commenced orbital maneuvers between 29 May and 31 May 2014. After numerous such manoeuvres brought it closer to the inert upper stage of the Briz-KM, on 9 November after a sequence of manoeuvres, the Kosmos-2499 came as close as 0.76 kilometres to the Briz-KM upper stage, at a relative speed of 4.6 meters per second. The Kosmos-2499 again undertook a close rendezvous with the Briz-KM on 25 November 2014. Kosmos-2499 made several orbital manoeuvres around the Briz-KM over the next three years till 2017. It subsequently broke up in orbit in 2021.[18]
- **Luch/Olymp:** The Luch or 'Olymp' was launched into the GEO in September 2014 on a Proton-M rocket with a Briz-M upper stage. Over the next several months, Luch conducted a series of manoeuvres that brought it close to other operational satellites around the GEO belt. The Luch conducted several close manoeuvres with other nations satellites in GEO afterwards.[19] In March 2023, the Luch Olymp 2 was launched into the GEO on a Proton-M rocket. It has also conducted several close manoeuvres with other Russian satellites in GEO.[20]
- **Kosmos-2504:** The Kosmos-2504 satellite was launched on 31 March 2015, together with three other satellites of the Rockot Briz-KM booster from Plesetsk. After separation from the Briz-KM, the spacecraft performed several manoeuvres and rendezvoused with the upper stage of its booster on 16 April 2015. By 8 October 2015, Kosmos-2504 moved towards the vicinity of the upper stage and stayed there for the rest of the month. In March and April 2017, the satellite again conducted a series of manoeuvres. Then Kosmos-2504 moved again in November 2019, coincident with the manoeuvres of the newly launched Kosmos-2542/-2543 pair.[21]
- **Kosmos 2521:** On 23 June 2017, Kosmos 2521 was launched on a Soyuz 2-1V booster from Plesetsk. At the beginning of August 2017, the Kosmos 2521 manoeuvred into a similar orbital inclination as the Kosmos 2486/ Persona reconnaissance satellite, probably for an inspection mission. Kosmos-2521 also released a sub-satellite,

the Kosmos-2523, at a high relative velocity, arousing the suspicion that it might be an ASAT test. Kosmos-2521 eventually re-entered the Earth's atmosphere in September 2019.[22]

- **Kosmos 2542 and Kosmos 2543:** On 25 November 2019, Kosmos-2542 was launched from Plesetsk mounted on a Soyuz 2-1V and on 6 December 2019, a small sub-satellite Kosmos-2543 separated from the multi-functional platform in orbit. By 9 December, Kosmos-2543 boosted its perigee by four kilometres and by mid-December 2019, the sub-satellite boosted its perigee by 55 kilometres. The Kosmos 2542 entered orbit within one degree of inclination from the USA-245 military reconnaissance satellite launched by the United States. Both Kosmos 2542 and Kosmos 2543 also continued to make similar manoeuvres through 2020. After several such manoeuvres, by 15 June 2020, Kosmos-2543 was around 60 kilometres from another Russian satellite, Kosmos-2535 and by 17 June 2020, the two satellites were less than 100 meters apart, which was officially corroborated a month later by the Russian Ministry of Defence. During the summer of 2021, Kosmos-2542 manoeuvred to re-synchronize its orbit with that of the USA-245 military satellite, and on 2 August, Kosmos-2542 passed as close as 34 km from USA-245, and on 13 August, it was within 53 km of its purported target.[23]

NEED FOR ENHANCED SPACE DOMAIN AWARENESS

India’s Space Situational Awareness (SSA) is achieved through a network of ground-based telescopes and radar as part of the Network for Space Object Tracking and Analysis (NETRA) system together with similar inputs received from space agencies of friendly space-faring nations, particularly the US and the European Space Agency. India’s indigenous SSA capability at present is limited and only caters for predicted orbits of known spacecraft and identified space debris. It cannot predict the hostile intent or capability of unknown spacecraft or co-orbital counterspace systems, a capability gained through enhanced Space Domain Awareness (SDA). Co-orbital counterspace capabilities with an adversary can therefore overtly or covertly target our spacecraft without warning. A pre-requisite for effectively defending our space assets from such overt or covert attacks is to develop a viable SDA capability.

COUNTERSPACE CAPABILITY BEYOND DA-ASATS

The Chinese military can engage India’s critical space assets by employing its co-orbital counterspace systems. Besides targeting India’s civillian space capabilities for navigation, communication, remote-sensing, weather prediction

and disaster management etc, it can target India's space-based military C4ISR, PNT and missile-detection capabilities, crippling India's military in a future conflict without producing unacceptable space debris.

Also, with India's limited indigenous SDA capability, the forewarning for such a kinetic/non-kinetic attack in space or even ascertaining attributability after a space attack would be difficult. Even in a pre-conflict situation, in consonance with its Three Warfare strategy, China may launch psychological warfare through unattributable attacks on civilian or military space infrastructure.

While India has demonstrated DA ASAT capabilities, it presently does not have any non-debris-producing, clean counterspace system to deter or respond to such an attack in space. The only option available to India would be to use a DA ASAT system, producing unwanted debris. With a much larger fleet of military satellites, China's military space capabilities can be seriously dented only by engaging several Chinese satellites, compounding the generation of debris to an unacceptable level, endangering all spacecraft, friendly or hostile, present in the particular orbital regime. DA ASAT capability in isolation therefore does not offer the deterrence that India seeks vis-à-vis China.

Developing non-debris-producing co-orbital counterspace systems emerges as a strategic imperative for India. A comprehensive set of non-debris-producing counterspace systems must be developed to ensure effective deterrence in space. This includes co-orbital KEWs that can de-orbit or damage a satellite through robotic grappling mechanisms, low delta-v kinetic kill vehicles that can damage/deorbit a satellite without causing fragmentation. As well as non-kinetic counterspace systems including RF jammers, High Power Lasers, High Power Microwaves, chemical sprayers and other evolving techniques, for effective deterrence in space are essential to meet the long-term security challenges posed by China.

ROLE OF INDIA'S SPADEX PROJECT IN DEVELOPING RPO SATELLITES

India's SPADEX (Space Docking Experiment) project spearheaded by the Indian Space Research Organisation (ISRO), focuses on demonstrating rendezvous, docking, and undocking capabilities using two small spacecraft. It is crucial for future space missions, including lunar sample returns and the development of a future Indian Space Station. The two constituent satellites, SDX01 (Chaser) and SDX02 (Target), equipped with a low-impact (approach velocity in the order of 10 mm/s), androgynous (identical) docking mechanism, have undergone the docking process twice.[24] The first docking took place on 16 January 2025 and was undocked on 13 March 2025.[25] The second docking was undertaken on 20 April 2025 and successful power transfer between the two satellites was undertaken on 21 April 2025.[26]

Success of the SPADEX mission also represents a crucial step in the development of indigenous Rendezvous and Proximity Operations (RPO) capabilities. This initiative demonstrates autonomous satellite docking and power transfer, paving the way for advancements in on-orbit servicing, space debris management, and national security applications besides. The success of the SPADEX will assist in the operationalisation of the following capabilities:

- **Autonomous Navigation and Guidance:** The project focuses on an autonomous approach, docking, and station-keeping between two spacecraft, a fundamental capability for future missions involving on-orbit servicing, refuelling, and repair. This aligns with global efforts by agencies like NASA and Roscosmos, which have successfully demonstrated RPO missions.[27]
- **Formation Flying and Proximity Manoeuvres:** SPADEX will enable controlled satellite movements in close proximity, critical for military reconnaissance, intelligence gathering, and counter-space applications. Similar technologies have been used by the United States Space Force and China's SJ-21 satellite, both of which have demonstrated satellite inspection and possible counter-space operations.[28]
- **In-Orbit Refuelling and Assembly:** A major application of RPO is extending the lifespan of satellites through in-orbit refuelling and servicing. SPADEX will develop docking systems that could support India's future space stations and deep-space exploration missions, akin to the modular assembly techniques used in the International Space Station (ISS) program.[29]
- **Counterspace Capabilities:** The ability to conduct RPO operations could enhance India's (SSA) and defensive counterspace capabilities. SPADEX could potentially enable inspections of adversarial satellites, space debris removal, or even active defence measures, a growing concern in contemporary space warfare.[30]

NAVIGATING THE FUTURE POSSIBILITIES

After the successful demonstration of SPADEX, India will be positioned to expand its space capabilities in multiple domains as under:

- **Military Surveillance and Space Security:** ISRO and DRDO (Defence Research and Development Organisation) may develop military-grade RPO satellites to monitor foreign satellites and space assets.[31]
- **Active Debris Removal (ADR):** SPADEX's docking technology could be applied to future space debris removal missions, allowing India to contribute to global sustainability efforts.[32]

- **On-Orbit Servicing and Space Robotics:** Future projects may include robotic servicing satellites capable of repairing, refuelling, and upgrading existing space assets.[33]
- **Quantum Communications and Secure Docking:** India is also exploring quantum satellite communication, which could be integrated with SPADEX to ensure secure docking and data transfer.[34]

WAY AHEAD

Besides developing resilient, agile satellites capable of withstanding or evading an electronic or kinetic attack, and a viable level of development (LoD) capability to enable reconstitution, India needs to quickly develop or even acquire a comprehensive spectrum of co-orbital counterspace capabilities in the kinetic and non-kinetic domain to retain a viable deterrent capability against any mala fide action by the adversary on its space assets. Beyond possessing a viable RPO capability, there is also a need to focus on other allied technology for development of operational counterspace systems that cause minimal harm to the space environment. Developing a potent SDA capability and the ability to ascertain attributability of space attacks through space forensics and electronic means is also a critical requirement for ensuring deterrence in space.

CONCLUSION

Space capabilities provide us with unprecedented advantages in both the civillian and military domains. Space systems provide our decision-makers with information and means to communicate, which are the two critical pillars of governance. Space systems are vital to monitoring strategic and military developments and are also critical in our ability to respond to natural and man-made disasters and monitor weather and environmental trends.

The ability to exploit the benefits afforded by space is central to our national security. However, the changing security environment in space increasingly threatens our capability to exploit space for our national interest. Space, one of the global commons like the high seas, is becoming increasingly congested, contested, and competitive. With its enhanced commitment in space in recent times and its dependence on space for critical civillian and military functions, space is now irrevocably entwined into India's strategic matrix.

The SPADEX mission represents a strategic step toward India's independent Rendezvous and Proximity Operations capabilities. By successfully demonstrating autonomous docking, SPADEX enables future advancements in co-orbital counterspace systems, besides debris management, and on-orbit servicing. It will also position India closer to leading space powers such as the US, Russia, and China, who have already demonstrated advanced RPO operations. The mission's success could mark the beginning of India's

capability to conduct independent space inspections, defend its space assets, and contribute to the growing field of space logistics. Developing a well-thought-out space security structure, with a viable deterrent capability to secure our space interests while carefully avoiding the maelstrom of a space arms race is sine qua non.

❖❖❖

Col (Dr) Kaushik Ray (Retd) served in the Indian Army for 26 years. He is currently an Assistant Professor at Amity University. Col Ray holds a PhD in Defence and Strategic Studies on Weaponisation of Space and Its Impact on India and an 'Advanced Certification in Space Technology' from IISc, Bangalore.

NOTES

1. "Frequently Asked Questions on Mission Shakti, India's Anti-Satellite Missile Test Conducted on 27 March, 2019", Ministry of External Affairs, Govt of India, accessed from https://www.mea.gov.in/press-releases.htm?dtl/31179/Frequently_Asked_Questions_on_Mission_Shakti_Indias_AntiSatellite_Missile_test_conducted_on_27_March_2019 on 20 March 2025.
2. Panda Ankit, Benjamin Silverstein, "The U.S. Moratorium on Anti-Satellite Missile Tests Is a Welcome Shift in Space Policy, Carnegie Endowment for International Peace" accessed from https://carnegieendowment.org/posts/2022/04/the-us-moratorium-on-anti-satellite-missile-tests-is-a-welcome-shift-in-space-policy?lang=en on 20 March 2025.
3. Ibid.
4. Sooi Ching Wei, "Direct-Ascent Anti-Satellite Missile Tests: State Positions on the Moratorium, UNGA Resolution, and Lessons for the Future | Secure World." accessed from https://swfound.org/news/all-news/2023/10/direct-ascent-anti-satellite-missile-tests-state-positions-on-the-moratorium-unga-resolution-and-lessons-for-the-future/ on 21 March 2025.
5. "Notice of the State Council on Issuing the 13th Five-Year National Science and Technology Innovation Plan_Science and Technology_China Government Network." accessed from https://www.gov.cn/zhengce/content/2016-08/08/content_5098072.htm on 23 March 2025.
6. Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, Space Threat Assessment 2018, Center for Strategic and International Studies, 01 April 2019, accessed from https://www.jstor.org/stable/pdf/resrep22469.6.pdf?refreqid=fastly-default%3Afaac5fcafa754d2ea1e25322523c1102&ab_segments=&initiator=&acceptTC=1 on 23 March 2025.
7. Matthew Mowthorpe, Markos Trichas, A Review of Chinese Counterspace Activities, The Space Review, 01 August 2022, accessed from https://www.thespacereview.com/article/4431/1 on 23 March 2025.
8. Chandrashekhar S, China's Space Program: From the Era of Mao Zedong to Xi Jinping. NIAS, 2021.Springer.
9. Matthew Mowthorpe, Markos Trichas, A Review of Chinese Counterspace Activities, The Space Review, 01 August 2022, accessed from https://www.thespacereview.com/article/4431/1 on 23 March 2025.

10. Chandrashekhar S, China's Space Program: From the Era of Mao Zedong to Xi Jinping. NIAS, 2021.Springer.
11. "SJ 21 - Gunter's Space Page." accessed from https://space.skyrocket.de/doc_sdat/sj-21.htm on 23 March 2025
12. "An In-Orbit Game of Cat and Mouse: Close Approaches Prompt Calls for Communications and Norms - SpaceNews." accessed from https://spacenews.com/an-in-orbit-game-of-cat-and-mouse-close-approaches-prompt-calls-for-communications-and-norms/ on 23 March 2025.
13. McCarthy Simone, "China is practicing 'dogfighting' with satellites as it ramps up space capabilities: US Space Force", CNN, 21 March 2025, accessed from https://edition.cnn.com/2025/03/21/china/china-space-force-dogfighting-satellites-intl-hnk/index.html on 23 March 2025.
14. "Geosynchronous Space Situational Awareness Program > United States Space Force > Fact Sheets." accessed from https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197772/geosynchronous-space-situational-awareness-program/ on 23 March 2025.
15. "GSSAP Surveillance Satellites - Airforce Technology." accessed from https://www.airforce-technology.com/projects/gssap-surveillance-satellites/ on 23 March 2025.
16. "Geosynchronous Space Situational Awareness Program > United States Space Force > Fact Sheets." accessed from https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197772/geosynchronous-space-situational-awareness-program/ on 23 March 2025.
17. "Space Delta 9 - Orbital Warfare > Space Operations Command (SpOC) > Display" accessed from https://www.spoc.spaceforce.mil/About-Us/Fact-Sheets/Display/Article/3878188/space-delta-9-orbital-warfare on 23 March 2025
18. "Kosmos-2499: Is It a Spy or an Assassin... or Both?" accessed from https://www.russianspaceweb.com/Cosmos-2499.html on 23 March 2025.
19. "Proton Successfully Returns to Flight Delivering a Secret Olymp Satellite." accessed from https://www.russianspaceweb.com/olymp.html on 23 March 2025.
20. Weeden Brian, Victoria Samson, Global Counterspace Capabilities 2024, Secure World Foundation, accessed from https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf on 23 March 2025.
21. "Secret Mission of Kosmos-2504." Accessed from https://www.russianspaceweb.com/Cosmos-2504.html on 24 March 2025.
22. Weeden Brian, Victoria Samson, Global Counterspace Capabilities 2024, Secure World Foundation, accessed from https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf on 23 March 2025.
23. "Soyuz-2-1v Launches Classified Payload." accessed from https://www.russianspaceweb.com/cosmos-2542.html on 24 March 2025.
24. ISRO 2025, "SpaDeX Mission", ISRO, 21 December 2024, accessed from https://www.isro.gov.in/mission_SpaDeX.html#:~:text=SpaDeX%20mission%20is%20a%20cost%2Deffective%20technology%20demonstrator,using%20two%20small%20spacecraft%20launched%20by%20PSLV.&text=The%20primary%20objective%20of%20the%20SpaDeX%20mission,Target%2C%20nominally)%20in%20a%20low%2DEarth%20circular%20orbit. on 24 March 2025.

25. ISRO 2025, “SPADEX Undocking Successful”, ISRO, 13 March 2025, accessed from https://www.isro.gov.in/spadex_undocking_successful.html#:~:text=The%20SPADEX%20satellites%20were%20successfully,orbit%20with%2045%2Ddegree%20inclination on 25 March 2025.
26. ISRO, “SPADEX Mission: Successful demonstration of Second Docking and Power Transfer”, ISRO, 21 April 2025, accessed from https://www.isro.gov.in/Spadex_Successful_demonstration_of_Second_Docking_and_Power_Transfer.html#:~:text=Home%20/%20SPADEX%20Mission:%20Successful%20demonstration%20of%20Second%20Docking%20and%20Power%20Transfer&text=ISRO%20successfully%-20demonstrated%20the%20docking,milestone%20in%20the%20SPADEX%20mission on 28 April 2025.
27. Sooi Ching Wei, “Direct-Ascent Anti-Satellite Missile Tests: State Positions on the Moratorium, UNGA Resolution, and Lessons for the Future” Secure World Foundation, October 2023, accessed from https://swfound.org/news/all-news/2023/10/direct-ascent-anti-satellite-missile-tests-state-positions-on-the-moratorium-unga-resolution-and-lessons-for-the-future/ on 24 March 2025.
28. “Rendezvous and Proximity Operations (RPO) – Space Engineering Research Center.”, Information Sciences Institute, University of South Carolina, accessed from https://www.isi.edu/centers-serc/research/rendezvous-and-proximity-operations-rpo/ on 24 March 2025.
29. Reesman, Rebecca, and Andrew Rogers. 2018. “Getting in Your Space: Learning from Past Rendezvous and Proximity Operations”, Center for Space Policy and Strategy, May 2018, accessed from https://aerospace.org/sites/default/files/2018-05/GettingInYourSpace.pdf on 24 March 2025.
30. Johnson Kaitlyn, Key Governance Issues in Space: Rendezvous and Proximity Operations, Center for Strategic and International Studies(CSIS), 2020, accessed from https://aerospace.org/sites/default/files/2018-05/GettingInYourSpace.pdf on 21 March 2025.
31. Dhillon Amrit, “India Attempts a Superpower Move: Docking Satellites in Orbit”, The Times,London, 31 Decemebr 2024, accessed from https://www.thetimes.com/world/asia/article/india-attempts-a-superpower-move-docking-satellites-in-orbit-rzmgs2tkl?region=global on 24 March 2025.
32. Komia Kantaro, Japan, India Startups to Study Laser-Equipped Satellite to Tackle Space Debris, Reuters, 17 December 2024, accessed from https://www.reuters.com/science/japan-india-startups-study-laser-equipped-satellite-tackle-space-debris-2024-12-17/ on 24 March 2025.
33. Barbee, Brent Wm, J Russell Carpenter, Scott Heatwole, F Landis Markley, Michael Moreau’, Bo J Naasz, and John Van Eepoel, “Guidance and Navigation for Rendezvous and Proximity Operations with a Non-Cooperative Spacecraft at Geosynchronous Orbit”, accessed from http://www.space.com/news/090225-wandering-spysat-danger.html on 24 March 2025.
34. ISRO, 2025, “SPADEX Undocking Successful”, March 13, 2025, accessed from https://www.isro.gov.in/spadex_undocking_successful.html on 01 April 2025.

❐❐❐

147-161

LOW EARTH ORBIT SATELLITE NETWORK FOR THE FUTURE WARFARE: NEED TO DEVELOP INDIGENOUS CONSTELLATION

Maj Gen AK Srivastava, VSM (Retd)

Abstract

Low Earth Orbit (LEO) satellites have ushered in a new dynamism in the rapidly advancing arena of satellite technologies. LEO satellites are greatly enhancing the capabilities of satellite based communications, earth monitoring and several other applications. Due to the huge potential it offers, the global leaders in the field have joined the race for launching big constellations of LEO satellites for providing high speed internet services globally. SpaceX's Starlink is, by far the largest constellation of LEO satellites with other players being Amazon (Kuiper), OneWeb and many more.

Starlink provided communications support to Ukraine during Russia-Ukraine conflict and proved its efficacy both for the civilian as well as military requirements. A military version of Starlink named Starshield, is also being developed by SpaceX, which will address the areas of communications and many more military applications.

Starlink is likely to make an entry into India, which is surely going to enhance the digital connectivity in the country. However, there are concerns regarding data security, monopoly and negative impact on the Indian space industry. India has proven capabilities in satellite technologies and is highly capable of joining the race for development of indigenous LEO satellite constellation.

This article aims to explore the developments in LEO satellites and assess the feasibility of an indigenous LEO satellite constellation to address both civilian as well as military requirements.

INTRODUCTION

The unprecedented growth of satellites in the recent past is revolutionizing the global telecommunications landscape by providing highly reliable, much faster and low latency services. These satellites are also playing a vital role in the field of Earth observation providing tremendous advantages like high resolution and frequent revisits. LEO satellites, orbiting at altitudes between 500 to 2000 km, provide clearer view of the Earth's surface, making them extremely suitable for satellite imagery and environmental monitoring.

Satellite internet based on Geostationary Earth Orbit (GEO) satellites is in use for a very long time. Now, LEO

satellites are scoring over GEO satellites in terms of low cost and simpler launches. Their proximity to Earth leads to higher throughput and faster internet access. The unprecedented increase in the demand for high-speed internet world over is leading to an exponential growth in LEO satellite internet market. This has led to a global competition for the deployment of LEO constellations with established companies like SpaceX, Amazon, OneWeb and many more joining the race. Elon Musk's Starlink is the world's first and largest LEO satellite constellation to deliver broadband internet capable of supporting streaming, video calls and more. Presently, it has more than seven thousand satellites in orbit.[1]

Starlink is being successfully used in the Russia-Ukrainian conflict for supporting military operations of Ukraine and has proved to be highly resilient against Russia's cyber and electronic warfare attacks. Also, large number of satellites provide inherent protection against anti-satellite weapons due to redundancy. A military version of Starlink named Starshield, has been developed, which will initially address the areas of communications, earth observation and hosting payloads. The future Starshield satellites will incorporate many more military applications. Other countries like Russia and China are also developing similar networks.

SpaceX is now planning to introduce the satellite network into India. It is widely felt that while India should avail of the Starlink services, the endeavor to develop indigenous satellite constellation must continue unabated.

This article aims to take a view of the enormous growth which is taking place in the field of LEO satellites and assess the viability of its indigenous development for civilian and military applications.

LEO SATELLITE NETWORK

A LEO satellite orbits relatively close to the Earth's surface at an altitude varying from 160 km to 2,000 km. LEO satellites are used for communication, observation, satellite imaging, transportation and International Space Station (ISS).[2] These orbits are lower compared to other orbits, but still quite far above Earth's surface. The GEO satellites always orbit along Earth's equator. The LEO satellites orbit in tilted planes and have more available orbits.[3]

The closeness of LEO satellites to Earth provides many advantages. Being at a lesser distance, these can capture images of higher resolution, thus very suitable for satellite imaging. The International Space Stations are also established in these orbits as it facilitates the travel of astronauts from and to Earth. These satellites are not stationary with respect to the Earth and travel in the orbit at a speed of around 7.8 km per second and make one circle of Earth in about 90 minutes. Thus, a single satellite in LEO is not useful for providing

communications. Hence, large constellation of these satellites are created for providing continuous coverage in such a way that some satellites are always covering a particular spot on Earth.[4]

These small LEO satellites, which are seamlessly connected to each other, act as moving mobile towers and provide broadband internet connectivity in all parts of the world. Many Global leaders are already deploying such mega constellations and have started providing the services. These communications are providing improved support to fields like the Internet of Things (IoT), aviation, maritime and emergency.[5]

Satellites are classified as small, medium, large, and cube satellite. Out of these, small satellites have the largest share and hold the dominant global LEO satellites market share. The LEO satellite market is presently very innovative due to being cost-effective, scalable, and flexible.[6]

Diagram 1, Cube Satellite. Source – Jet Propulsion Laboratory URL: https://www.jpl.nasa.gov/missions/m-cubed-cove-2/

A Cube satellites (CubeSats) is a class of small, standardised satellites, typically shaped like a cube measuring 10x10x10 cm (1U), often launched into low Earth orbit. CubeSats segment is growing at fastest pace due to their compact, modular design and low cost. Due to standardised sizes, CubeSats can be launched quickly as clusters for a quick response ability.

LEO SATELLITE CONSTELLATIONS FOR MILITARY OPERATIONS

Reliable, secure, robust and survivable communication networks are the backbone of digital battlefield and Network Centric Operations (NCO). The network is required to be all pervasive and must provide seamless interoperability, while having capabilities to work in adverse electromagnetic environment. LEO satellite networks are promising to meet most of the battlefield communication requirements. Their sheer numbers in the constellation considerably reduce

their vulnerability to anti-satellite weapons. The LEO satellites provide reliable and faster communications due their lesser distance from Earth and resultant lower latencies. This leads to seamless data connectivity across the battlefield including difficult and inaccessible areas. The ground equipment is lightweight which are suitable for quick deployment and re-deployment, thus providing seamless mobility. Their inherent capability to provide global connectivity makes it very suitable for large military operations. The availability of high capacity internet across the battlefield facilitates support to advanced applications like augmented reality and cloud services. Owing to various advantages offered by LEO satellite networks, leading armed forces of the world are aggressively pursuing for availability of such services for various applications.[7]

STARLINK

Starlink is currently the largest constellation of LEO satellites operated by US aerospace company SpaceX. Presently, it has around seven thousand operational satellites providing internet connectivity to more than one hundred countries. Starlink came into focus when it successfully provided communication support to Ukraine in the Russia-Ukrainian War.[8] Starlink System Characteristics are given in Diagram No. 2.

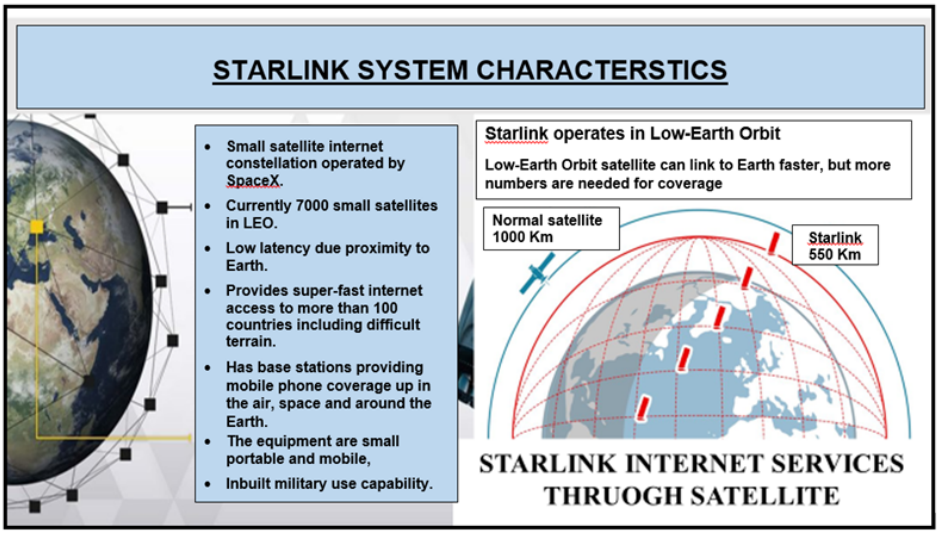


Diagram 2 – Starlink System Characteristics. Source: Author

TECHNOLOGY USED IN STAR-LINK

- **Satellite Hardware:** In first phase of deployment, 60 satellites, weighing around 227-260 kg, were launched in May 2019 at an altitude of 550 km. The satellites have flat-panel design with multiple high-gain

antennas and one solar array which maximizes space for dense launch configuration. They are equipped with krypton based Hall thrusters for orbit adjustment and deorbiting. The inter satellite links are based on specialised laser based communications. For links from the satellites to the ground stations, Ka band microwave is used with phased array antenna. The Starlink satellites, being closer to Earth, have low latencies of the order of 25 to 35 millisecond as compared to 477 milliseconds in case of GEO satellites. The later version V2 satellites are larger and more robust than the first generation, with upgrades including argon Hall thrusters, improved phased array antennas, and E-band backhaul capabilities.[9]

- **User Terminals:** In Starlink, the handsets do not directly connect with the satellites as it happens in Iridium, Thuraya Inmarsat and Globalstar. Here, the system is linked to flat user terminals, which track the satellites through phased array antennas. The terminals can be mounted on any platform including fast moving objects like trains.
- **Ground Stations:** The link between Starlink and ground stations is established on Ka-band microwave. With the introduction of V2 version satellites, E band frequencies from 60 GHz to 90 GHz have been added. The working of Starlink satellite is illustrated in Diagram No. 3.

Diagram 3, Starlink Working Process. Source - Carlos Placido, SpaceX-Raying Starlink Developments, Linkedin, 22 Sep 2022.URL:https://www.linkedin.com/pulse/spacex-raying-starlink-developments-carlos-placido/

SERVICES PROVIDED BY STARLINK

- **Satellite Internet:** Starlink makes available satellite-based, high bandwidth internet connectivity around the globe with particular emphasis on underserved areas and provides competitively priced services in developed areas.
- **Satellite Cellular Service:** T-Mobile US, has partnered with SpaceX and has started a beta service that permits smartphones to connect directly to Starlink satellites when they are out of range of cellular towers, thus providing seamless connectivity in unserved areas and in mobile dead zones using existing mid band PCS (1 GHz - 6 GHz) spectrum. The coverage has started with messaging, which later will expand to include voice and data services.
- **Military Satellites:** SpaceX has deployed customized military satellites which are improved versions of the Starlink satellite bus, in collaboration with Space Development Agency (SDA). SDA facilitates development of missile defence capabilities by utilising low-cost LEO satellite platforms procured from the industry. The program will also venture into launch of weapons into space for the US military.[10]

  SDA has signed a dual use contract to SpaceX, under which 4 satellites will be developed with capabilities of detecting and tracking hypersonic and ballistic missiles. The launching of satellites was done in April 2023. There will be a mesh network of large number of optically interconnected satellites forming its 'transport' layer. The application layers will include satellite navigation, missile tracking, weapons targeting, battle management and ground support.
- **Starshield Program:** Starshield program, which was started In December 2022, is to carry military payloads on board a customized satellite bus. These satellites are larger, with twice the area of a conventional Starlink satellite. To begin with, the services provided will include communications, Earth observation and hosting of custom payloads. This network by SpaceX is based on Starlink's technology focuses on national security and defence requirements.[11] It has been reported that, with the launch of 22 satellites in Janunary 2025, there are a total of 118 Starshield satellites already in orbit. Starshield is meant to provide its services mainly to US government agencies which include the Space Development Agency, United States Space Force and National Reconnaissance Office. Also, the future Starshield satellites will incorporate interceptor missiles, directed energy weapons and hypersonic projectiles.[12] The US government had awarded a large contract to Starshield in the year 2021 to manufacture large number of

satellites for the purpose of monitoring of targets across the globe.[13] These satellites became operational in May 2024.

Starshield is designed to provide three main services. These include; Provision of Communications, Remote Sensing and Custom Payloads. The communications function provides internet services across the globe based on network of satellites, similar to Starlink. Starshield enhances the technological features of Starlink in terms of higher levels of encryption and laser based interconnections to provide connectivity in remote and difficult areas. The Remote Sensing function enables the users to launch satellites fitted with sensors to capture data, like images of the Earth's surface. The data can then be used for variety of purposes like tracking movements on ground, monitoring of weather and disaster management. For the custom payloads function, SpaceX has built satellites capable of carrying specialized equipment made for certain specific missions. Military and government user can have their own sensitive equipment like sensors, which can be provided to SpaceX for integrating them into a specially designed satellite for quick deployment. This allows the users to develop their own classified equipment and avail of the satellite expertise of SpaceX.[14] With its tremendous potential and flexibility, Starshield is heading towards further expansion and growth and it is all set to revolutionize the conduct of space based operations. Starshield is likely to have a great impact in the strategic domain of national security.

CHINA'S VENTURE INTO LEO SATELLITES

Following up the development of Starlink and Starshield, China is rapidly developing its own constellations under Project SatNet named Guowang and Qianfan (Thousand Sails). China wants to follow the example of Starlink and Starshield for reliable and robust battlefield communications and their space based operations. China has given strategic priority status to its LEO mega constellation Guowang, which has been allocated to China SatNet company since 2021, and aims to launch around 13,000 satellites for global, military grade internet connectivity. It is also likely to support China's Beidou navigation system.[15]

Qianfan (Thousand Sails) is the next LEO satellite network being developed by China which is a commercial venture. It primarily focusses on broadband internet, but also aims to develop other applications like telecommunications, remote sensing and precision agriculture. Shanghai Spacesail Technologies Co. Ltd, (SPACESAIL) is implementing this project. China launched its first batch of satellites for Qianfan in August 2024 and now has 18 satellites in orbit,

with a final target of nearly 14,000 satellites by 2030. The aim of this project is to provide worldwide internet services similar to Starlink.[16]

RUSSIAN PROGRAMS IN LEO SATELLITES FOR MILITARY

Russia is in the process of developing LEO satellite network for military purposes which includes Satcom network, intelligence gathering, reconnaissance and for anti-satellite weapons. Russia is developing LEO satellite communications network. One such network is being implemented by Gazprom for government and business customers. This indicates that LEO satellites will be an important part of Russian communication network especially for the remote and underserved areas. Its utilisation for the Russian military is highly probable. In the ISR domain, LEO satellites are being widely used for intelligence gathering, reconnaissance and monitoring of other satellites in orbit. These have been inferred based on the observed movements of Russian satellites Resurs-P3 and Cosmos-2562. For Glonass steatite based navigation system, Russia is changing over from GEO to LEO satellites as it is facing various challenges in GEO satellites due to western sanctions. Thus, Russia will be using lower altitude, smaller satellites for its navigation capabilities. However, they will require larger number of such satellites for global coverage. Regarding potential anti-satellite weapons, the defence analysts have reported that the Russian LEO satellite programs may be linked to the development of anti-satellite weapons and nuclear space weapons and associated with Russian Cosmos. It has also been reported that Russian Starlink Killer system can detect and interfere with signals from Starlink satellites.[17]

STARLINK IN RUSSIA-UKRAINIAN WAR

Starlink services were provided to Ukraine during Russia-Ukraine conflict when their communication infrastructure was badly damaged due to Russian attacks. Ukraine's military and government very gainfully utilised Starlink to maintain Internet access in entire area of operations and also for other government services. Starlink is used by Ukraine for providing seamless communications to the civilians, the military and the energy infrastructure. The service is also used for the operational communications for supporting warfare. Starlink has proved to be very efficient for connecting different types of drones, fire coordination systems and supporting attacks on Russian positions.[18]

SATELLITE BASED INTERNET SERVICES IN INDIA

Satellite-based internet services are available In India, through satellites. These satellites are located at a distance of 35,786 km from the Earth and because of its large distance, the latencies are higher and data rates are significantly low. Such satellite based broadband services are already available to Indian Armed

Forces for coverage of remote locations through satellites such as GSAT 11 and GSAT 29 with peak bandwidth of 16 Gbps. Details of ISRO satellites managed by NSIL are given in Diagram No. 4.

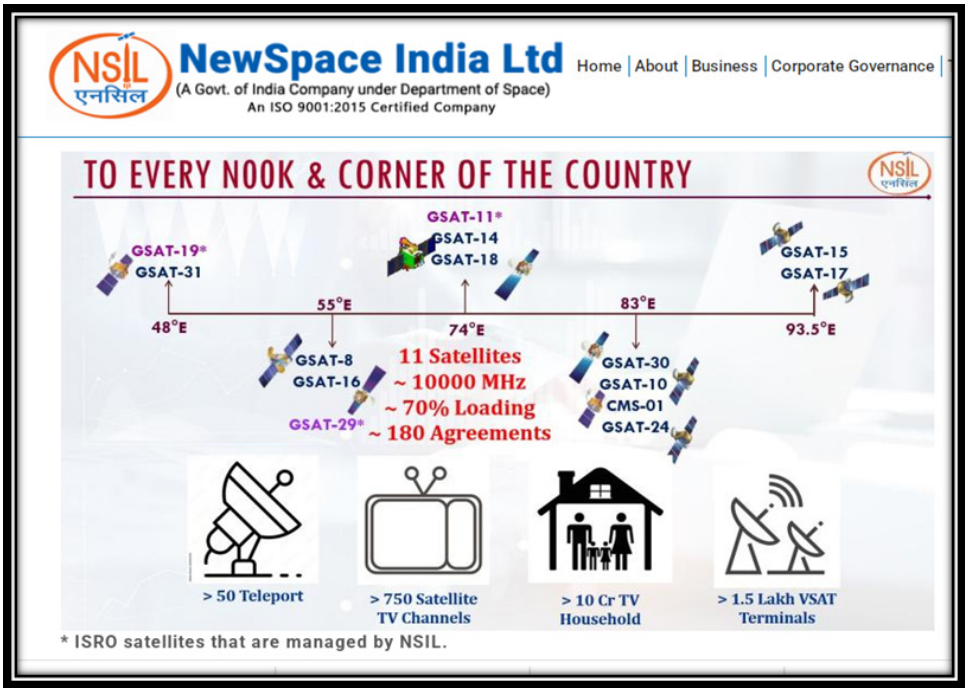


Diagram 4, ISRO Satellites Managed by NSIL. Source - Information, 'Satellite Fleet', New Space India Ltd (NSIL). URL: https://www.nsilindia.co.in/satellite-fleet

Indian state owned BBNL provides satellite-based internet services which includes coverage over remote and strategically important regions. However, LEO based satellite networks are offering tremendous advantages over the GEO based network, especially for the military environment. Hence a focused approach is required to acquire these capabilities and catch up with the technology with indigenous development.[19] India has great demand for connectivity as about half of its population is still not connected to the internet. Satellite internet will accelerate the provision of internet services to the unserved population and unserved areas. This being essential for civilian sphere, is also vital for strategic domain.

STARLINK'S ENTRY INTO INDIA

India is heading for a new experience in the area of internet as Starlink is planning to enter into its market through Bharti Airtel and Jio Platforms, who have signed agreements with SpaceX. The network promises to expand digital

connectivity in India to a large extent. However, there are certain concerns being expressed which need to be addressed holistically. What needs to be guarded against is establishment of monopoly and exploitation of data.[20]

INDIGENOUS DEVELOPMENT OF LEO SATELLITE CONSTELLATION

India has tremendously proven its capabilities in the satellite technologies. India has a successful space program, evidenced by missions like Chandrayaan-3, which successfully landed on the Moon's south pole, and other satellite launches.[21] At the present juncture, when foreign companies like SpaceX are entering into the India market, Indigenous development of LEO Satellite Constellation will be of strategic importance. It will be prudent for us to consume Starlink technology to our best advantage and parallelly continue our journey towards being a global leader in contemporary satellite technologies. It is only the indigenous LEO satellite technologies which can be utilized for strategic and military applications as foreign space-based internet solutions will have many vulnerabilities and cannot be trusted for such applications.

INDIGENOUS CAPABILITIES

India has tremendous strengths in satellite technologies including LEO, with ISRO being at the centre stage. It has demonstrated enormous capabilities in design and development of satellite systems and successful launches. The capabilities of its Polar Satellite Launch Vehicle (PSLV) in placing satellites in orbit has been appreciated world over. The point to be noted is that the cost of the launches is extremely low which can beat any other similar establishment.

India’s leading telecom operators, Airtel, Vodafone Idea, and BSNL, possess enormous capabilities in delivering the services to the customers spread over vast areas including remote and difficult terrains. The national efforts in space technologies are now being efficiently supported by large number of space technology start-ups. These dedicated entrepreneurs and innovators are capable of much wanted value additions by developing sophisticated satellite components and high-tech services. They are thus infusing tremendous dynamism in the overall ecosystem.

Other large industrial groups are also engaged in technological ventures which provide support in terms of software development, chip manufacturing, 3D printing etc. Such large entities possess technological capabilities to be a successful system integrator to coordinate the efforts

Large industry groups like TATAs are already making progress in LEO satellite technology. Tata Advanced Systems Ltd (TASL) launched an Earth observation satellite named TAST-1A into LEO on 7 April 2024. This was India’s first private sector satellite built in collaboration with Satellogic Inc, a US based company,

and assembled at TASL facility in Karnataka. It was launched by SpaceX from the Kennedy Space Center, Florida. It was part of the Bandwagon 1 mission.[22]

Another major initiative in LEO is by Bharti Global by acquiring the largest share in OneWeb, a LEO satellite communications company. OneWeb has now merged with Eutelsat, France to form Eutelsat Group. Bharti Enterprises remains the largest shareholder in the merged entity. This entity is engaged in providing global satellite operation and compete with Starlink and similar networks. OneWeb India has received authorization from the Indian National Space Promotion and Authorisation Centre (IN-SPACe) to launch commercial satellite broadband services in India.[23]

DEVELOPMENT OF CRUCIAL TECHNOLOGIES

There are several niche technologies which are essentially required for an LEO constellation. Such technologies include optical Inter-Satellite Links (ISL), advanced phased array antennas, Optical ISL handover, Ion Propulsion System, Advanced Satellite Tracker, Autonomous Collision Avoidance System etc. These technologies need to be developed indigenously through focused R&D efforts. India can exploit its unique capabilities in software development and manufacturing to create a place for itself in global arena. There is a need for a well-defined national vision to integrate the indigenous capabilities to make India a global leader in the LEO satellite industry. The entry of Starlink should be seen as an opportunity and we should not only be the consumers of Starlink, but it should inspire us to compete and have our own constellations in the sky.

RECOMMENDATIONS

LEO based satellite networks are offering tremendous advantages over the GEO based network, including for the military environment. Hence a focused approach at national level is required to acquire these capabilities and catch up with the technology with indigenous development. The recommendations are summarized below:

- **ISRO as Nodal Agency:** ISRO has completed close to 100 launch missions, 125 spacecraft missions and has planned missions like the Gaganyaan, Chandrayaan-4, Shukrayaan and Mangalyaan-2. Thus, ISRO has tremendous capabilities for spearheading this project.
- **Funding by the Government:** The project being large, needs focused approach by the Government and adequate funding for its implementation.
- **Participation by Various Stake Holders including MoD:** The constellation must address the requirements of Armed Forces, Government agencies as well as civilian usage.

- **Public Private Partnership:** It offers many advantages, including access to private capital, leveraging private sector expertise and innovation, and potentially reducing public sector costs and risks.
- **Involvement of PSUs and Large Industrial Groups:** PSUs and Large industrial groups undertaking satellite projects must be involved. They can act as capable system integrators.
- **Incorporating Space Technology Start-ups:** These dedicated entrepreneurs and innovators are capable of value additions by developing sophisticated satellite components and high-tech services.
- **Development of Critical Technologies:** Critical technologies highlighted in the article need to be developed indigenously through focused R&D efforts.
- **Gaining Experience by Partnering with Starlink and Similar Constellations:** In the interim period before own constellation is developed, network from Starlink and others can be utilized for permissible applications and gaining experience.
- **Technology Transfer and Sourcing of Components:** Technology transfer from global leaders and sourcing of components should be done from multiple sources so that there is no technology denial at a later stage.
- **Exploring Commercial Venture to Address the Huge LEO Satellite Market:** India's leading telecom operators who possess enormous capabilities in delivering the services to the customers spread over vast areas must be included for this purpose.

CONCLUSION

LEO satellites have brought in renewed traction in the field of satellite technologies. These satellites are promising to revolutionise communications, earth observation and many other applications. These satellites are going to play a key role in commercial, government and military applications. The global leaders in the field have joined the race for launching big constellations of LEO satellites for providing high speed internet services. Whereas the biggest constellation launched so far is that of Starlink of SpaceX, other projects like Kuiper of Amazon and OneWeb are making rapid advancements. These satellites are proving to be very useful for military applications due to their high throughput, greater mobility and better survivability. Starlink provided communications support to Ukraine and proved its usefulness both for the civilian as well as military applications. A military version of Starlink named Starshield, has been developed, which will initially address the areas of communications,

earth observation and hosting payloads. The future Starshield satellites will incorporate many more military applications.

Starlink is now planning to make an entry into India as SpaceX has signed contracts with Airtel and Reliance Jio. These services are going to hugely improve the digital connectivity in the country. However, certain concerns like data security, monopoly and challenges to Indian satellite industry need to be proactively addressed.

India has tremendous capabilities in satellite technologies. It is therefore necessary that the country joins the race and develops its own LEO satellite constellation. The indigenous network should be capable of addressing both civilian as well as military applications.

❖❖❖

Maj Gen AK Srivastava, VSM (Retd), has commanded a Signal Regiment in the sensitive Akhnoor Sector of Jammu and Kashmir, along the Line of Control. His staff exposures include DAA&QMG of a Mountain Brigade in the North East, Assistant Military Secretary (AMS) in Military Secretary's Branch, Colonel Adm of an Infantry Division in the desert sector during Op PARAKRAM and Planning Officer (Electronics) in MoD. His qualifications include M. Sc Physics (Electronics), Fellow, Institution of Electronics and Telecommunications Engineers, M. Sc. Defence and Strategic Studies, M. Phil Defence and Management Studies, M. Phil Social Sciences and Advanced Communications Course in Signals Academy Leningrad, USSR, (Now St. Petersburg, Russia).

NOTES

1. R. L. Rebach, "Large Constellations of Low-Altitude Satellites: A Primer", Congressional Budget Office, May 2023. https://www.cbo.gov/publication/59175
2. Boltz Christamas, "Low Earth Orbit", The European Space Agency, 03 Feb 2020. https://www.esa.int/ESA_Multimedia/Images/2020/03/Low_Earth_orbit
3. Lagunas, E., Chatzinotas, S. & Ottersten, B. "Low-Earth orbit satellite constellations for global communication network connectivity. Nat Rev Electr Eng 1", pgs 656–665 (2024). https://www.nature.com/articles/s44287-024-00088-9
4. Ed Fox, "Low Earth Orbit Satellite: Achieving Fast-Speed Connectivity", MetTel Blog, 10 Sep 2024, https://www.mettel.net/blog/low-earth-orbit-satellite/
5. John Burke, "How low Earth orbit satellite networks improve internet access", TechTarget: Nemertes Research, 25 Sep 2023, https://www.techtarget.com/searchnetworking/tip/How-low-Earth-orbit-satellite-networks-improve-internet-access
6. ibid
7. Philip Harlow, "The DoD and commercial SATCOM: Fashioning a true partnership", TELESAT Blog, 14 Aug 2024. https://www.telesat.com/blog/the-dod-and-commercial-satcom-fashioning-a-true-partnership/

8. Tereza Pultarova, “Starlink satellites: Facts, tracking and impact on astronomy”, Space.com, 27 Feb 2025. https://www.space.com/spacex-starlink-satellites.html
9. Sangeeta M Upadhye, “Starlink Technology”, International Advanced Research Journal in Science, Engineering and Technology, March 2025. https://iarjset.com/papers/starlink-technology/
10. Arushi Singh, “The Role of Starlink During Military Conflict”, Defence Research and Studies, 02 Mar 2024. https://dras.in/the-role-of-starlink-during-military-conflict/#:~:text=Meanwhile%2C%20the%20US%20military%20successfully,if%20the%20primary%20communication%20system
11. Mike Wall, “SpaceX reveals 'Starshield' satellite project for national security use”, Space.Com, 07 Dec 2022. https://www.space.com/spacex-starshield-satellite-internet-military-starlink
12. Article, “SpaceX Starshield: A New Frontier in Government Satellite Service”, New Space Economy, 01 Mar 2025. https://newspaceeconomy.ca/2025/03/01/spacex-starshield-a-new-frontier-in-government-satellite-services/
13. Erwin, Sandra, "NRO's first batch of next-generation spy satellites set for launch". SpaceNews. 01 May 2024. https://spacenews.com/nros-first-batch-of-next-generation-spy-satellites-set-for-launch/
14. Joey Roulette and Marisa Taylor “Musk's SpaceX is building spy satellite network for US intelligence agency, sources say”, Reuters, 16 Mar 2024. https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16/
15. Matt Swayne, “RAND Analysts: Chinese Military’s View Of Starlink As A Weapon Shapes Its Own LEO Strategy”, Space Insider, 28 Apr 2025. https://spaceinsider.tech/2025/04/28/rand-analysts-chinese-militarys-view-of-starlink-as-a-weapon-shapes-its-own-leo-strategy/
16. Andrew Jones, “Can China Challenge SpaceX's Starlink? New spaceports and rockets will launch the Qianfan megaconstellation”, IEEE Spectrum, 27 AUG 2024, https://spectrum.ieee.org/satellite-internet
17. Victoria Samson, “Russian Military and Intelligence Rendezvous and Proximity Operations” Secure World Foundation, December 2024. https://swfound.org/media/207995/fs24-03_russian-military-and-intelligence-rendezvous-and-proximity-operations.pdf
18. Laviniu Bojor, Tudorică Petrache and Cristian Cristescu, “Emerging Technologies in Conflict: The Impact of Starlink in the Russia – Ukraine War”, Research Gate: June 2024 Land Forces Academy Review 29(2):pgs185-194. https://www.researchgate.net/publication/381758551_Emerging_Technologies_in_Conflict_The_Impact_of_Starlink_in_the_Russia_-_Ukraine_War
19. } Report, “India Leo Satellite Market Size & Outlook, 2024-2030”, Horizon Grand View Research. https://www.grandviewresearch.com/horizon/outlook/leo-satellite-market/india
20. News Article, “Elon Musk’s Starlink signs deal with Bharti Airtel, Jio for high speed internet in India”, Economic Times, 12 Mar 2025. https://economictimes.indiatimes.com/industry/telecom/telecom-news/elon-musks-starlink-signs-deal-with-bharti-airtel-jio-for-high-speed-internet-in-india-check-likely-price-speed-plan-and-more/articleshow/118915938.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
21. Vinay Sarawagi, “Beyond starlink India Strategic Imperative in the LEO Satellite Race”, Times Now, 12 Mar 2025. https://www.timesnownews.com/technology-science/beyond-starlink-indias-strategic-imperative-in-the-leo-satellite-race-article-118920307

22. Kartik Bommakanti, “TSAT-1A marks progress, but challenges remain in US-India defence space ties”, Observer Research Foundation, Expert Speak Raisina Debates, Published on May 31, 2024. https://www.orfonline.org/expert-speak/tsat-1a-marks-progress-but-challenges-remain-in-us-india-defence-space-ties
23. News Article, “Eutelsat concludes OneWeb merger; Bharti Enterprises to be largest shareholder”, The Economic Times, 29 Sep 2023. https://economictimes.indiatimes.com/industry/telecom/eutelsat-concludes-oneweb-merger-bharti-enterprises-to-be-largest-shareholder/articleshow/104026802.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

❐❐❐

162-176

EVOLVING SPACE OPERATIONS AND THEIR IMPLICATIONS FOR FUTURE WARFARE

Gp Capt Puneet Bhalla (Retd)

Abstract

Space-enabled capabilities are becoming increasingly important for enhancing the effectiveness of domain-specific and joint operations. Space-enabled Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR), Missile Warning, SATCOM, and Position, Navigation and Timing (PNT) are providing force enhancement to terrestrial operations. Private space companies are investing heavily in the domain for commercial reasons, innovating and augmenting capabilities and capacities. The growing importance of space for military purposes is transforming it into a domain of conflict. Advanced space-faring nations are seeking to ensure freedom of action in the domain, while denying the same to their adversaries. These would involve both offensive and defensive measures, as well as measures to ensure space access. Warfare in space is going to be unique owing to the physics of orbits. Preparing for such an eventuality would not just require a technological edge, but doctrine and organisation changes. Equally important would be establishing corresponding force structures and skill development of combatants. India has an increasing dependence on space. There is a need to study these progressive changes, learn from global efforts and establish own set of responses in terms of policy, doctrine, strategy, organisation and force structure, while optimising utilisation through education and training.

INTRODUCTION

The dawn of space exploration was a result of military quest for gaining a vantage point to observe military deployments and missile sites of the adversary. It provided the advantage of freedom of overflight, while the high altitude ensured that they were secure from terrestrial weapons. Subsequently, satellites were also utilised to provide global communication and limited navigation assistance to terrestrial crafts, enabling both to undertake operations across the globe. During the First Gulf War of 1991, the US employed its space capabilities to provide disproportionate advantages to its forces at the operational and tactical levels. This transformed the strategic thought on modern warfare, and other nations also felt the need for space-enabled capabilities for their military operations. However, not many nations were able to achieve the technological prowess or had the economic strength needed for access to the domain. This has changed over the last decade with technology advancing at a rapid pace

and lowering of its costs, leading to its proliferation. There are now almost 70 nations that have a space program, with more participants showing interest in the domain in recent years. Increasing technology adoption has led to more monetisation of space-enabled services, resulting in greater private sector interest. These companies are investing in increasing their deployments and in research and development towards making these services more efficient, or coming up with innovative cost-cutting solutions.

Joint or integrated military operations, spanning the domains of air, land, sea, cyber and space, are being pursued by all advanced militaries. Efforts are being made to enhance the operational effectiveness of the forces through the optimum usage of each domain, coordination of action among the domains for joint, synergised operations and providing cross-domain support. Space-enabled capabilities have been making growing contributions towards the achievement of all these,[1] necessitating their integration and coordination across all levels of warfare and spanning all domains through a joint approach.[2] As space becomes ever more relevant to gaining advantages in conflict, nations would seek to negate these capabilities, and this would potentially transform the realm into a new domain for the conduct of warfare. Analysis of the advancements and the changing nature of the domain is necessary to prepare for the future of space operations.

SPACE SUPPORT TO OPERATIONS

Rapid technological advances and innovations are greatly enhancing the space-enabled functions supporting terrestrial forces and joint operations. Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) Satellites carrying sensors provide information on the adversary's deployments and their movements that help derive their plans and intentions. This information has been critical for planning own strategies and for planning and executing responsive military action, and for organising the logistics and communication support operations. Four types of resolutions define ISTAR, spectral, radiometric, spatial and temporal, and each is seeing major improvements. Hyperspectral (HR) and Synthetic Aperture Radar (SAR) satellites are broadening the spectrum of coverage, while overcoming the limitations of weather and time of day. Spatial resolutions are seeing improvements in terms of optical and digital enhancements. The ever-increasing number of sensors and imaging constellations being launched into orbit is ensuring shorter revisit times, enhancing persistence in coverage of given areas. Limitations of individual sensors are being overcome through digital advancements that allow processing and fusion of imagery from diverse sensor sources (space and terrestrial). Faster processing capabilities, onboard and edge computing, are further bringing down time for the provision of actionable intelligence to the commanders or

combatants. Space is becoming an important element of gathering information on the Electromagnetic Spectrum (EMS), with the US, Russia, China, and India having launched dedicated electromagnetic surveillance satellites. Satellites continue to provide meteorological and oceanographic information, affecting operations in all physical domains.

MISSILE WARNING

Early warning satellites deployed in Geosynchronous Orbits (GEO) have been providing global coverage of missile launches and tracking of missiles. As the plethora of recent missile attacks in the Russia-Ukraine war and West Asia conflicts have shown, unambiguous, timely, accurate and persistent missile warning and event characterisation remains strategically important for all nations and their security forces through all levels of conflict. Space-deployed capabilities and capacities would become ever more important contributors to the missile warning architecture being developed by nations.

MACHINE LEARNING (ML), ARTIFICIAL INTELLIGENCE (AI) AND DATA ANALYTICS

ML, AI and data analytics are being explored to provide critical insights, predictive analytics and decision support to commanders, greatly shortening the kill cycle. They could be further utilised for sensor prioritisation and data integration across all domains to ensure accessible, secure and standardised information.

SATELLITE COMMUNICATIONS (SATCOM)

Space-enabled communication is a critical enabling component of C4I2SR in all-domain operations, providing near real-time, beyond-line-of-sight communication links and redundancy in military communication architecture. SATCOM links have been gradually upgraded to provide both voice and data connectivity and are now enabling communication to rapidly mobile and geographically dispersed, diverse force elements. Nations and companies are exploring SATCOM for 6G communication, with security applications. Significant advancements in communication systems have been:

- **High Throughput Satellites (HTS):** Designed to deliver substantially higher data transmission, using techniques like multiple spot beams and higher frequency band capacity, is becoming the norm for all future SATCOM deployments to GEO.
- **LEO-based SATCOM Constellations:** They have already become a reality, significantly bringing down the latency and inspiring concepts like Internet of Military Things (IoMT), where multiple machines could be made part of an integrated grid for more prompt and autonomous

operations. The already operational US Starlink network, developed by the private spaceflight company SpaceX, is expected to have a 42,000-satellite constellation by 2030.[3] China is seeking its own Low Earth Orbit (LEO) based SATCOM service, with its 14,000-satellite Qianfan satellite constellation and 13,000-satellites 'Guo Wang' constellation planned at various orbital levels in LEO.[4] These constellations are being pursued for economic and military purposes, but would also serve political causes.

- **Free-space Optical Communication:** These use laser beams for wireless communication and are also experimenting to provide higher transmission bandwidth and speeds, and more secure communications. China has been at the forefront of this technology. In March 2025, one of its private commercial companies claimed a successful space-to-ground communication transmission of 100 gigabits per second using laser technology, ten times faster than previous achievements.[5] The breakthrough is particularly important to accommodate higher data flow associated with higher resolution imaging and sensing.
- **Data Relay Network:** Data relay satellites, positioned in GEO, enable near real-time data transmission by relaying transmissions between LEO-based ISR spacecraft and the ground stations. This also reduces reliance on the traditional network of terrestrial space Tracking, Telemetry and Control (TT&C) stations, making satellite control in orbit more responsive.
- **Quantum Communication:** Since August 2016, China has periodically demonstrated space-to-ground quantum key distribution. It remains the only nation to have achieved this ultra-long-distance, highly secure quantum SATCOM. This has inspired dedicated efforts in pursuance of this technology by other advanced space-faring nations.

POSITIONING, NAVIGATION AND TIMING (PNT)

Space-based PNT, enabled through Global Navigation Satellite Systems (GNSS), provides highly precise four-dimensional global positioning. Besides navigation, systems like the US's GPS, Chinese Beidou and Russian GLONASS provide highly accurate time reference to their security forces that help enhance the efficiency of their operations. China has introduced limited secure SATCOM services through their Beidou satellite network, and other nations are expected to follow. Increasingly, PNT satellites are being equipped for additional purposes, like providing limited SATCOM resilience. Cases of jamming against GNSS are increasing, compelling nations to constantly upgrade their systems, as well as to seek alternate space-enabled means of navigation. An example is China's CentiSpace-1, a futuristic LEO-based 160-satellite constellation,[6]

aimed at augmenting its Beidou GNSS, which also intends to employ a laser inter-satellite communication link. While the first satellite was launched in 2018, ten were added in January 2025.[7] U.S. experts have also proposed the use of highly accurate atomic clocks onboard Starlink satellites to provide terrestrial navigation inputs.[8]

SPACE SERVICE SUPPORT

- **Space Access:** All above services are dependent on assured and desired access to space through the launch services. These have seen incremental advancements in terms of payload capacity and the varied kinds of launch vehicles providing flexible launch options and reduced launch costs. Consequently, the number of launches has seen a tremendous increase, with smaller satellites resulting in more payloads being put in orbit per launch. SpaceX's reusable rockets have revolutionised the launch environment. Recently, it re-used a rocket after an astonishing nine-day turnaround.[9] This has been a game-changer for launches of satellites by the US and its allies, including military missions. China is trying to match up through its wide range of launchers and four launch bases, and has been second only to SpaceX in the yearly launch numbers.
- **Launch on Demand (LoD):** Militaries have benefited greatly from these, using the advanced capabilities to reduce development and deployment timelines. These developments are also enabling Launch on Demand (LoD) capabilities, being pursued by advanced space-faring nations to increase the resilience of their space operations. LoD would also support space combat operations through quick placement of satellites in orbit for various offensive and defensive tasks, to include enhancing incidental capacities or replacing damaged satellites at short notice.
- **Space Mobility:** Satellite manoeuvring through TT&C is being resorted to within and in-between orbits for initial deployment, station keeping and end-of-life disposal. This capability is now advanced to precise Rendezvous and Proximity Operations (RPO) to enhance mission effectiveness, but could equally be employed for inspecting satellites of adversaries, to respond to evolving space conflict scenarios and for co-orbital anti-satellite (ASAT) missions.
- **On-Orbit Sustainment:** While smaller replaceable satellites with shorter in-orbit life are becoming the norm, measures to extend the lifetime of spacecraft are also being explored. Software of modern sensors and satellites can be remotely upgraded through network links, ensuring longevity. Other measures being pursued by governmental and commercial entities include on-orbit RPO measures to maintain, service,

refuel or replace components of spacecraft. All these capabilities have co-orbital ASAT potential, and the threat would continue to rise as more nations or entities gain proficiency in these operations.

NEAR EARTH AND VERY LOW EARTH ORBIT (VLEO) SPACE

As the traditional space environment gets congested and vulnerable, space-faring nations and commercial entities are exploring this 'closer to Earth' region to augment or provide alternate capabilities for ISR, communication, missile warning and for other innovative uses. Within the aerospace environment, there is no clear demarcation in terms of the physicality of the atmosphere/space that could delineate various bands. While 100 km above the Earth's surface has been broadly accepted as the lower boundary of space, there is no consensus on the exact delineations of these two bands. Near Earth generally denotes the high-altitude atmospheric belt beyond that used by commercial and military aircraft, and VLEO is taken as the orbital area below approximately 450 km altitude. Both offer advantages, as well as challenges for regular operations.

COMMERCIAL AND ACADEMIC CAPABILITY INTEGRATION

The commercial space sector has grown exponentially in the past decade, with active commercial spacecraft now substantially outnumbering active government-owned spacecraft in orbit. Commercial space initiatives span the breadth of space operations, to include launch vehicles, high-definition imagery, optical communication and, for the future, on-orbit servicing and maintenance and space debris clearance. More nations, including major space farers the US and China, are exploring and supporting their commercial and academic entities to support space operations. The 'whole of nation' approach, entailing cooperation and coordination among multiple government and non-government entities, for their capability and capacity expansion, including national security applications, is the emergent norm. The US supports SpaceX programmes, including Starlink LEO-based communication constellation and have established a Commercial Integration Cell, for sharing of information from private sector space assets with their defence counterparts.[10] China follows its Civil-Military Fusion (CMF) strategy at capability and capacity enhancement. Interestingly, most commercial private players in the domain remain heavily dependent on government agencies for technology development and testing and for selling their services.

The dual-use nature of these services has raised concerns about their use. Recent examples include the open declaration of use of privately owned Starlink satellite internet constellation by Ukraine against Russia. Some Chinese commercial satellite imagery companies were sanctioned by the US for providing satellite imagery and assistance to Russian forces.[11] Other space

capabilities being pursued by private entities also have dual-use potential. Private commercial assets available for hire or bought out by nations could be used to enhance capacities or provide resilience during conflicts. For example, in the US, a space startup has been contracted by its Air Force Research Laboratory to develop orbital warehouses to store payloads in orbital space and deploy them promptly at the desired time and place.[12] Such developments further underscore the increasingly indistinguishable roles of commercial and military operations in space and raise concerns about the legitimacy of targeting civilian assets during conflicts.

THE EVOLVING NATURE OF SPACE CONFLICT

Established spacefaring nations, who have relied on freedom of operation in the domain, feel concerned about a significant increase in the potential to interfere or disrupt their operations by adversaries, by targeting their vulnerabilities. Their space doctrines have thus evolved from majorly force enhancement/ multiplier functions to defining both defensive and offensive measures and actions towards securing their interests in space. Space operations to promote security and stability, as defined by the US, involve preventing conflict in, from and to space, including all activities to deter an adversary and to provide space combat power in the event of conflict to prevail over the adversary.

As in other terrestrial domains, combat power in space is to achieve and preserve freedom of action and reduce prohibitive interference from adversary forces, while simultaneously impeding or denying the adversary from use of its space-enabled capabilities. Although the orbital physics makes space a unique operating environment, the fundamental principles while formulating the space doctrines have continued to follow the terrestrial ones, gaining and exploiting the position of advantage within the space domain, seizing space dominance/ superiority at the time and place of choosing and denying the same to the enemy. The measures include involving both kinetic and non-kinetic means to deny, disrupt, damage, or destroy adversary space capabilities in all domains and manoeuvring and concentrating space-based power.

THREATS TO SPACE OPERATIONS

Space operations have always had to cater to a naturally hazardous environment. Unintentional threats emerging from more space operations and participation are congestion in the domain and space debris. However, warfare in space would be concerned with intentional man-made actions against any of the three segments of space operations, orbital, terrestrial or the communication links. The effects achieved could either be reversible (temporarily neutralisation to achieve specific denial effects), which would be plausibly deniable and hence

potentially non-escalatory, or non-reversible, which could lead to proportional responses, escalating the level of conflict.

ELECTROMAGNETIC SPECTRUM (EMS) AND CYBERSPACE

As the space assets are remote and distributed and must be controlled through networks, they depend on the EM spectrum and on cyber capabilities. As numbers in space have increased, both the spectrum and cyberspace have also become congested and competitive. Several instances of Electronic Warfare measures, like jamming and spoofing of GNSS signals, as well as cyberattacks on the digital infrastructure, have already been reported against space assets. Nations would take measures to secure their assets and services through protection and deterrence measures. In case of escalation of threat, or in case of conflict, they would resort to offensive action, including Electronic Warfare measures and cyberattacks against the link segments.

EMPLOYMENT STRATEGY

Sustained military enablement operations and space power projection would be achieved through a comprehensive concept of operations, involving both defensive and offensive measures.

- Defensive space operations are to protect space assets against the evolving threats and challenges, preserve space combat power in support of operations in all domains and neutralise or reduce the effectiveness of adversary actions. Spacecraft protection measures would involve planning and deployment measures to ensure that capabilities are disaggregated, distributed and diversified among orbital spaces and spacecraft. Deception measures would also be employed, and satellite constellations would add to these resilience measures. Satellites could themselves be protected through hardening and provision of onboard defensive suites, and manoeuvring could be resorted to avoid imminent threats. However, all these would add to the satellite weight and complexity of the mission and adversely impact mission life through the consumption of fuel. Nations are now seeking deployment of small and cheap ‘bodyguard’ satellites, co-orbital assets that could be pre-positioned or launched at short notice to protect high-value satellites. Positioned close to the ‘client’ satellites, they could ‘nudge’ co-orbital threats away or could be equipped specifically with defensive suites or offensive capability to neutralise emerging threats.[13] Coordination among different agencies would be necessary to protect the terrestrial infrastructure and to secure the network segment against electronic warfare and cyberattacks.

- Offensive operations are now being planned and prepared to negate an adversary's use of military or hostile space capabilities to reduce the effectiveness of its forces in all domains. Both the US and China have developed and deployed space planes, with defensive and offensive action potential.

SPACE REGULATORY ENVIRONMENT

The current space regulatory regime, while being broad, is not sufficient to cater to the evolving activities in space or the technologies involved, making it ever more incapable of ensuring the preservation of space as a peaceful domain. Efforts at diplomatic solutions to the evolving threats to the space environment have not borne results, owing to vested interests of the participants. Equally, there have been no sustained efforts at agreements on defining what constitutes irresponsible and aggressive behaviour in space or the penalties for when the red lines are crossed. There is no consensus on the rules of acceptable behaviour or the acceptable response to any adverse action in space. Unless new agreements are put in place, the space environment will remain volatile, compelling nations to develop deterrence and conflict capabilities.

WARFARE IN ORBIT

Despite multiple demonstrative tests of anti-satellite (ASAT) capabilities by leading space-faring nations, including India, nations have refrained from actions that could disturb this relatively sanctuaried environment. This is not because of altruism, but orbital dynamics that would cause any destructive action to result in the creation of space debris, limiting access to certain orbital altitudes by all participants. Therefore, the preferred route being pursued by nations in case of space conflict would be disruption through non-kinetic capabilities like cyberattacks, electronic warfare and directed energy weapons (lasers and microwave), to cause reversible or irreversible effects. Ground-based neutralising weapons are severely restricted in their ranges owing to the large power requirements. Orbital placement overcomes this limitation, but putting sufficient power on small-sized satellites remains a challenge. Advanced space-faring nations are now using their RPO proficiencies to test co-orbital deployment and manoeuvring. Such capabilities have been demonstrated in both LEO and GEO, raising concerns about the sanctity of the space environment. Dual-use assets make such deployed capability difficult to discern, track or protect against in advance. In addition to the satellites being targeted, their ground stations also become a lucrative target.

Orbital peculiarities also define how action will take place in orbit. Dictated by physics, satellites cannot make sudden avoidance manoeuvres. Their movement requires precise and timely application of energy. Even then, the

change takes its own time to reach full effect. In March 2025, the US reported 'dogfight' manoeuvres conducted in LEO by five Chinese satellites. Categorised by the US as a show of tactical and technological advancement in space capabilities, these did not involve harsh movements, but slow, steady, deliberate manoeuvres relative to each other.[14] Hence, co-orbital abilities, both defensive and offensive, would have to be achieved through calculated pre-positioning and subtle moves that could delay detection and hence the response. Thus, dominating the conflict in space would not be defined by numbers or firepower, but would be dependent on foresight, planning and timely action achieved through efficient command and control.[15]

DOCTRINE

Operational doctrines are constantly being evaluated and updated to cater to the evolving conflict landscape. Space doctrines have remained nebulous due to the distant nature of the domain, scarcity of assets and terrestrial centrality of conflict. An increasing dependence on space-enabled abilities, along with greater interdependencies among domains, is necessitating the redefinition and rehashing of doctrines to align with multi-domain, hi-tech, joint operations. Costs associated with access to and sustained operations in space are extremely high, and a common framework for the employment of space-enabled resources as part of joint operations would be necessary to optimise their use. Technological advantage is not sufficient, and gaining operational advantage would necessitate skill development through organisational and training measures. The rapidly evolving capabilities, conflict scenarios and threats would require testing through training and exercises, leading to regular review of these documents.

COMMAND AND CONTROL (C2)

The distinctive character of space operations, the unique attributes of the domain's physical dimension, the global and remote nature of space operations and their relevance to domain-specific as well as joint operations, make their Command and Control (C2) difficult. Space-based assets will continue to be in short supply and will be split between the military-specific and dual-use assets. This would entail a persistent understanding of the capabilities and effects of terrestrial, link and orbital segments to attain operational efficiencies, achieve positions of advantage and attain resilience.

ORGANISATIONAL ADAPTATION

The vacillation on military space operations has been most evident in the inconsistent organisational changes made over the years by major space farers to cater to the altering realities. The most prominent have been the cases of US

Space Command (USSC) and the Chinese People's Liberation Army Strategic Support Force (PLASSF). The US first established the Space Command in 1985, but disestablished it in 2002, placing its space assets and operations under its Strategic Command. Advancing capabilities and increasing challenges to its space operations and dominance have compelled it to re-establish the Space Command as a combatant command in August 2019. Aiming to integrate various high technology elements, China established PLASSF in 2015, bringing together electronic warfare, space and cyber under a common command. However, in April 2024, the decision was revoked, and the People's Liberation Army Aerospace Force (PLAASF) was set up, separate from a Cyberspace Force and Information Support Force. With this, it became only the second nation, after the US, to have established an independent space force. Both nations are heavily dependent on the domain for their national economic and security interests and need to deter interference in their space operations. Having dedicated organisations would consolidate their space-based assets and infrastructure under a singular command and integrate people, processes and technologies to ensure optimisation of resources. A dedicated force would better help organise, train and equip and present a dedicated, specialist cadre that would be more adept at utilising the domain in support of joint objectives, as well as plan and train for future space conflict scenarios.

SPACE DOMAIN AWARENESS (SDA)

All measures aimed at ensuring a safe and secure space environment, as well as to respond to any aggression in the domain, must begin by having the requisite domain awareness. Conventional Space Situational Awareness (SSA) involves the ability to detect, track, characterise, discriminate between and maintain comprehensive knowledge about spacecraft and debris in the orbital segment of the space environment, to ensure safe and sustainable space activities. Space Domain Awareness (SDA) is a broader function that encompasses SSA, along with awareness of the terrestrial and link segments. In military terms, SDA is the timely, relevant and actionable understanding of the operational environment that allows military forces to plan, integrate, execute and assess space operations. SDA thus requires not only collection, integration and processing of observational data from multiple, diverse sensors and sources, but also the ability to identify anomalies in behaviours and patterns that could affect, or potentially affect, any aspect of space operations and present it in timelines that would allow adequate responses at all levels of operations: strategic, operational and tactical. Clearly, SDA would be contributory to all space mission planning.

Very few nations possess ample resources to create adequate SSA. SDA entails much more investment in terms of material and manpower, and unity of

effort among various military and non-military agencies for optimisation. SDA efforts would also benefit through the sharing of assets and information among allies. Private companies are integrating their capabilities and capacities to provide a complementary sensor network involving both terrestrial and space-based sensors to contribute to SDA. Use of ML and AI would greatly enhance monitoring prioritisation, anomaly detection and reporting and decision-assist to facilitate more responsive courses of action. Introducing clearly defined rules of engagement, pre-determined plans and pre-established priorities into the software would help in decision support. The US Space Force is currently experimenting with a new AI-based software dubbed R2C2 (Rapid and Resilient Command and Control), which aims to automate the detection of threats and data collection and organisation.[16] The China National Space Administration (CNSA) is reportedly developing its own AI-driven satellite imagery analysis alongside capabilities to track space debris.[17]

RECOMMENDATIONS FOR THE JOINT FORCES

Among the capabilities and innovations listed above, India has achieved success in some and is diligently pursuing others. These would need to be followed up and evolved for national security purposes. Some of the recommendations are covered below:

- **Military Utilisation:** Heightened awareness among the armed forces in recent years has given impetus to efforts towards capability and capacity enhancement, integrating and leveraging capabilities from the domain and for optimally employing their effects. An integrated approach to include all space-linked organisations, DRDO, commercial entities and academia towards technological development and deployment.
- **Doctrine:** A dedicated Defence Space Agency (DSA) has been a positive step towards the integration of space into terrestrial military operations. The same now needs to be reflected adequately and appropriately in joint doctrines. Future strategies and plans need to incorporate explicit space capabilities in support of operations. These would form the basis for defining and planning the Space Force structure in orbit and on Earth, in terms of human and other resources. In a volatile global environment, doctrines would require periodic review based on technological and environmental changes, lessons learnt from global campaigns and local exercises and training.
- **Space Specialists:** Optimal utilisation of assets within the armed forces would necessitate trained space operations specialists having essential skills and exposure. Such specialists would better provide definite perspectives on capabilities and capacities and be able to interact more productively for procurements and deployments. Going

forward, they would also be more competent to handle space control operations and to respond to a denied, degraded and disrupted space operating environment.

- **Space Security:** As space gets more contested and hostile, tangible measures would be required to ensure access to the domain and the security of assets and operations. These would entail the development and operationalisation of offensive and defensive capabilities, as well as appropriate command and control structures for these assets. Selected declarations of these capabilities could be considered for deterrence. Persistent enhancement of indigenous and collaborative SDA, space-based and terrestrial, is imperative.
- **Private Participation:** While military and 'combat' operations in the domain, as they emerge in the future, would be purely military functions, increasing hybrid exploitation of civilian assets in space for expanding capabilities and capacities has gained tacit global acceptance as the way forward. Institutional initiatives already in place should be utilised for proactive engagement and providing ample support to all such indigenous efforts to pursue national security objectives. Enabling policies and organisational evolution is necessary to enable exploration of technology developments in other domains for improving and optimising operations in space.
- **Educating the Combatant:** Joint space education and training strategies are essential to promote comprehension among the commanders and achieve applicable requisite skill levels among specialists and non-specialists of all branches of the armed forces. Incorporation of space capabilities needs to be part of all training exercises. These need to keep up with the technological and doctrinal changes.

CONCLUSION

India has been among the leading space-faring nations, and its dependence on the domain for national progress continues to increase. There is also greater awareness and acceptance of the advantages extended by space-enabled capabilities towards national security tasks and missions. The national space sector has thus seen greater vigour in recent years in terms of policy evolution and budgetary support, leading to enhanced capability building and innovation. The government has recognised the value of a 'whole of nation' approach, and this is amply reflected in the National Space Policy and some of the institutional initiatives for commercialisation and private participation.

❖❖❖

Gp Capt Puneet Bhalla (Retd) is a former helicopter pilot and has been a Senior Fellow at Centre for Land Warfare Studies (CLAWS) and Centre for Joint Warfare Studies (CENJOWS). He has authored a book, "Space Security: Emerging Technologies and Trends," and has contributed mltiple articles on technology and national security to reputed think tanks and publications.

BIBLIOGRAPHY

1. "Space Doctrine Publication 3-0, Operations, Doctrine for Space Forces", Space Training and Readiness Command (STARCOM), 19 July 2023, https://www.starcom.spaceforce.mil/Portals/2/SDP%203-0%20Operations%20(19%20July%202023).pdf
2. "Joint Doctrine Publication 0-40, UK Space Power," UK Space Power, September 2022, https://assets.publishing.service.gov.uk/media/653a5261e6c968000daa9b8a/JDP_0_40_UK_Space_Power_web.pdf
3. Henry Sokolski, "A China-US War in Space: The After-Action Report," Bulletin of the Atomic Scientists, 17 January, 2022, https://thebulletin.org/premium/2022-01/a-china-us-war-in-space-the-after-action-report/
4. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," U.S. Department of Defense, 2024, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF

NOTES

1. "Space Doctrine Publication 3-0, Operations, Doctrine for Space Forces", Space Training and Readiness Command (STARCOM), 19 July 2023, https://www.starcom.spaceforce.mil/Portals/2/SDP%203-0%20Operations%20(19%20July%202023).pdf
2. "Joint Doctrine Publication 0-40, UK Space Power," UK Space Power, September 2022, https://assets.publishing.service.gov.uk/media/653a5261e6c968000daa9b8a/JDP_0_40_UK_Space_Power_web.pdf
3. Tereza Pultarova, "Starlink satellites: Facts, tracking and impact on astronomy," Space.com, 28 March, 2025, https://www.space.com/spacex-starlink-satellites.html
4. Garretson et al, "Thousand Sails: Why Low Earth Orbit is the Next Frontier for Great Power Competition between the U.S. and China", American Foreign Policy Council, 3 February, 2025, https://www.afpc.org/publications/policy-papers/thousand-sails-why-low-earth-orbit-is-the-next-frontier-for-great-power-competition-between-the-u.s-and-chinathum
5. "Chinese Breakthrough in Laser Data Transmission to Shake Up Telecom Industry," Policy Circle Bureau, 24 March, 2025, https://www.policycircle.org/industry/laser-data-transmission-china/
6. "Centispace 1 S4", NASA Space Science Data Coordinated Archive, National Aeronautics and Space Administration, 04 April 2025, https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=2022-108B
7. "CentiSpace-1 S1, ..., S5", Gunter's Space Page, 04 April 2025, https://space.skyrocket.de/doc_sdat/centispace-1.htm

8. Mark Harris, “Starlink signals can be reverse-engineered to work like GPS—whether SpaceX likes it or not,” MIT Technology Review, 21 October, 2022, https://www.technologyreview.com/2022/10/21/1062001/spacex-starlink-signals-reverse-engineered-gps/
9. Doug Cunningham, “SpaceX Sets Rocket Re-Use Record Friday with a Nine-Day Turnaround,” SpaceDaily, 21 March, 2025, https://www.spacedaily.com/reports/SpaceX_sets_rocket_re-use_record_Friday_with_a_nine-day_turnaround_999.html
10. Alan T. Dugger, “Space as a Gray Zone: The Future of Orbital Warfare,”, Modern War Institute at West Point, 14 February 25, https://mwi.westpoint.edu/space-as-a-gray-zone-the-future-of-orbital-warfare/
11. Kelly Ng, “Ukraine: US sanctions Chinese firm helping Russia's Wagner Group”, BBC, 27 January 2023, https://www.bbc.com/news/world-asia-china-64421915
12. Alan T. Dugger, “Space as a Gray Zone: The Future of Orbital Warfare,” Modern War Institute at West Point, 14 February 25, https://mwi.westpoint.edu/space-as-a-gray-zone-the-future-of-orbital-warfare/
13. “Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China,” U.S. Department of Defense, 2024, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF
14. Courtney Albon, “China demonstrated ‘satellite dogfighting,’ Space Force general says,” Defense News, 19 March 2025, https://www.defensenews.com/space/2025/03/18/china-demonstrated-satellite-dogfighting-space-force-general-says/
15. Alan T. Dugger, “Space as a Gray Zone: The Future of Orbital Warfare,” Modern War Institute at West Point, 14 February 25, https://mwi.westpoint.edu/space-as-a-gray-zone-the-future-of-orbital-warfare/
16. Greg Hadley, “Space Force Is Testing AI to Automate Ops—and Eyeing More”, Air and Space Forces Magazine, 12 December, 2024 https://www.airandspaceforces.com/
17. Pentagon’s annual report on the “Military and Security Developments Involving the People’s Republic of China”

❐❐❐

177-188

PROLIFERATION OF 'WEAPONISED NON-GEOSTATIONARY SATCOM' VIA NON-STATE ACTORS AMIDST CHALLENGES TO TELECOM SOVEREIGNTY

Dr Chaitanya Giri

Abstract

India has the highest 5G telecommunications network penetration in the world and is engaged in multi front asymmetric and hybrid war. It is becoming evident that countries, motivated by necessity and the influences of digitally buoyant populations, are transitioning from terrestrial to satellite-based telecommunication systems, which is viewed positively. Artificially created positive sentiments for these transitions, purported to eliminate the digital divide, may come at the expense of national telecom sovereignty, particularly for those nations that adopt them without due diligence. This consequence could be leveraged by non-state actors and secessionist forces exploiting these systems for nefarious purposes, even in regions with weak telecom connectivity. A strict check by tri-services on the use of satellite phones has so far prevented such exploitation. With the advent of global satellite telecom services, regulations must be revisited to deter nefarious actors from using satellite telecommunications to undermine India's national sovereignty and global interests, especially when its neighbourhood is in geopolitical flux. Such transition from terrestrial to terrestrial-space satellite internet require the tri-services to carry out strategic bulwarking, with an emphasis on telecommunications sovereignty much above communications security.

INTRODUCTION

In 2021, the Institute for Security Studies, a South African think tank focused on African security issues, revealed that the Islamic State West Africa Province (ISWAP), a terror group active in the conflict zones of the Lake Chad Basin, was utilising satellite-based Wi-Fi services to facilitate real-time data sharing and communication.[1] The Lake Chad Basin[2] is a large conflict-ridden area spanning Nigeria, Cameroon, Niger, and Chad, which are not entirely connected by satellite-based Wi-Fi across their geography. Chad, which is severely impacted by terrorism, has since long banned the possession and use of satellite phones.[3] Since 2013, Nigeria has implemented a similar ban in its Borno region, which is affected by ISWAP-led terrorism.[4] ISWAP is believed to be using these satellite-based services, particularly through Thuraya satellites,

to communicate with international Islamic State terror groups and other partner organisations, reaching as far as the Levant, Afghanistan, and the Philippines. ISWAP is thought to be using satellite-based communications systems and is thought to involve the sharing of finances and strategic advice with various factions and partners.

ISWAP is not the only terror group using satellite-based services. In 2022, following the withdrawal of the US armed forces from Afghanistan, multiple satellite phone signatures and Wi-Fi-enabled thermal imaging devices, originally used by the US forces, were detected in the hands of terrorist groups in Kashmir, India.[5] It is not fully clear which all terror groups had laid hands on these instruments and smuggled them via Pakistan into Kashmir. Pakistan is complicit in the smuggling of such satellite phones and also in aiding telecommunication services. The Pakistani Ministry of Information Technology and Telecommunication's company, Special Communications Organization, whose director general is touted to be a former Inter-Services Intelligence (ISI) official, has worked to increase telecom signal strength in Pakistan-occupied Jammu and Kashmir. While doing so, Pakistan has facilitated a cocktail of highly-encrypted You-Send-My-Message (YSMS) services that involve pairing smartphones with very high-frequency radiosets, LoRa (low-power-long-range) technology for ensuing alerts, for security systems at terror bases, and detonating explosives, and satellite phones, especially serviced by Thuraya, to ensure secure communications in regions with low-internet connectivity.[6] The Pakistani establishment's aiding of terrorists and interfering with the Indian telecommunications network was a gross violation of Article 45 of the constitution of the International Telecommunications Union, which has close to 200 member states, including Pakistan.[7]

In several recent cases, tourists and backpackers have also been detained in India for possessing such prohibited communication devices.[8] Indian security and intelligence agencies are acutely aware that satellite-based communication devices can be utilised even by non-state actors with limited technical expertise. In January 2025, the Indian Directorate General of Civil Aviation mandated that civilian airliners operating in India inform passengers that carrying satellite phones is legally prohibited.[9] India has permitted only INMARSAT satellite phone handsets (also known as user terminals), exclusively serviced by Bharat Sanchar Nigam Limited (BSNL), as the country's authorised Global Satellite Phone Service (GSPS).[10] However, services provided through Iridium and Thuraya satellites are not allowed.[11] Nevertheless, the new security challenge that now arises is the malicious use of 'satellite-direct-to-cell' services offered by modern satellite internet and telecommunications service providers and how creatively terrorist groups, proxies, informal armies, and non-state actors might exploit them within India.

THE SECURITY ATTRIBUTES OF NON-GEOSTATIONARY SATCOM BUSINESS

Iridium, Thuraya, Globalstar, and INMARSAT are some of the satellite telephony service providers that have classically used geostationary satellites and operate in the L-band or S-band in accordance with the Radio Regulations of the International Telecommunications Union.[12] The use of satellite phones is highly regulated globally, and in India, it is prohibited because their use makes it difficult for homeland security agencies to intercept satellite signals. Satellite phones are less vulnerable to local interference, but on the downside, they are not user-friendly, have low latency, and are expensive to use.

The technological maturity attained by Non-Geostationary Satellite (NGS) constellations has assuaged several disadvantages of satellite telephony. While classical satellite phone handsets require the device to be oriented towards the satellites, this is not the case with the new-generation 5G cellular phones or even data-receiving terminals of direct-to-customer NGS constellation-based service providers like SpaceX's Starlink, Amazon's Kuiper, Hughesnet and Viasat. The latency is extremely low, the bandwidth is extremely high in gigabytes per second ranges, and the issue of staying connected with one satellite, in the case of the earlier generation satellite phones, is eliminated.

Terror groups have started exploiting the government agenda focused on last-mile connectivity by allowing satellite internet services. The unregulated and unchecked distribution of user terminals in areas where these services are available can enable nefarious actors and terror groups to use them without restraint. The Malian government was among the first to recognise this fact.

In March 2024, the Malian government banned Starlink from selling its direct-to-customer kits, citing concerns about their misuse by armed factions and terrorist groups, particularly those linked to the Islamic State and Al Qaeda. In October 2024, Mali resumed Starlink kit sales in a regulated manner for a six-month trial period to establish a regulatory framework and a platform for registering users and identifying all equipment sold in the country.[13] While equipment can be identified, malicious actors may still engage in identity fraud, identity theft, and using fake identities at the point of sale and during the Know-Your-Customer (KYC) process. The concerns raised by the Malian government for satellite internet services are echoed by several other governments in Africa grappling with terrorism, insurgency, and homeland security challenges.

UNAUTHORISED AND UNREGULATED SATELLITE INTERNET SCARE IN GEOPOLITICALLY SENSITIVE REGIONS OF INDIA

During joint operations in Kagpokpi, Imphal East, Chandel, and Churachandpur, the Indian Army's III Corps (Spear Corps) and the Assam Rifles uncovered a

significant arsenal of conventional weaponry. They also discovered a cutting-edge technological device, a Starlink user terminal marked RPF-PLA, which has raised concerns among strategic communities and security agencies.[14] The RPF-PLA marking suggests it belonged to the Revolutionary People's Front, the political wing of the People's Liberation Army Manipur, a group running a self-proclaimed government from Sylhet, Bangladesh.[15] It is crucial to now determine how a starlink terminal came to be in the hands of RPF-PLA militants in Manipur.

In April 2024, before the political coup, Bangladesh experienced a major internet disruption. This outage happened due to a rupture in the SEA-ME-WE-5 submarine cable, one of Bangladesh's two primary international connections, which occurred adjacent to the Malacca Straits. The cause of the rupture, whether accidental or premeditated, remains unsettled.[16] At the same time, the Bangladesh Telecommunication Regulatory Commission had begun making guidelines for non-geostationary satellite providers seeking to offer broadband services within Bangladesh. This was a big boost for service providers who were interested in commencing their commercial operations in Bangladesh.[17] Starlink, which has regulatory approval now, is expensive for a common Bangladeshi. Its terminal kits cost around USD 600, and monthly services are around USD 120 for unlimited data. The current Bangladeshi broadband rates are much more affordable at USD 5 for a 5 Mbps monthly subscription. Unfortunately, before the formal commercial services began in Bangladesh, anti-India militant and terrorist groups began to use Starlink. In November 2024, the Indian Coast Guard seized a Myanmarese boat smuggling 6000 kg of methamphetamine, worth USD 4.25 billion, that was in possession of Starlink terminal in Indian waters around Andaman and Nicobar Islands.[18]

CHALLENGES WITH THE MARKET OF SATELLITE-BASED INTERNET KITS

Countries with limited digital penetration due to economic struggles, political turmoil, authoritarian regimes, and sectarian or armed conflicts often have populations yearning for secure and on-the-go internet connectivity. This desire quickly manifests into a strategic use-case for such connectivity during distress to extend SOS calls, communicate basic situational awareness during Humanitarian Assistance and Disaster Relief (HADR), mobilise basic defence to escape to safer zones, and raise some degree of resistance when a critical mass of motivated individuals connects. All kinds of powers in such countries could desire control over such networks, be it a legitimately elected government, a faction aiming a coup, a military junta, or even non-state actors aiming to exploit the volatile geopolitical circumstances.

Any government or regime aims for telecom sovereignty and control over networks during peacetime and more vigorously during wartime. However, volatile geopolitical circumstances create a demand emerging from customers that would push their governments to bypass terrestrial networks that are more susceptible to disruption and sabotage. Even in peacetime, if existing national terrestrial telecommunications networks are infrastructurally poor and hence provide poor network coverage, especially in the rural and remote regions, when the populations do not have access to reliable internet with satisfactory bandwidth, latency, and other technical factors, the populations could demand organically, and through pressure groups and lobbies, the introduction of satellite-based internet services.

If the government denies satellite-based internet services, certain unrelenting customers, like non-state actors or terror groups, would desire to bypass the telecom services controlled by the government to access the internet uninhibitedly. If the government permits the introduction of any global satellite internet service provider, that would eliminate or diminish any existing terrestrial telecom service provider from the market. It could also create a situation for rapidly creating a regulatory framework in favour of satellite internet services, which, if not framed effectively, can be deleterious from a national security standpoint.

In under-developed economies with persistent security challenges, certain non-state actors, terrorist groups, and smuggling networks are likely to proliferate user terminals illegally. These terminals are sold at exorbitant prices in the black market, significantly higher than those in legitimate markets. Consequently, the eventual customers of these terminals are typically powerful actors with ample resources, driven by strong motivation and a meticulous agenda to use these terminals across various regions while also avoiding legal repercussions for using foreign and prohibited telecom devices. Secessionist political parties, military factions, and groups in conflict over specific geographic areas are likely to promote satellite-based services to advance their separatist geopolitical goals. However, this usage will remain restricted to certain regions where satellite-based internet coverage is available, even if only temporarily.

The proliferation of transnational black market satcom user terminals begins with point-of-sale purchases made by individuals acquiring terminals in countries where the government formally permits sales and services. These terminals are then transported or smuggled into countries where sales and services are unavailable, particularly in geopolitically sensitive regions. These devices can be traded with non-state actors through clandestine proliferation routes or informal supplies in large consignments. Numerous open-source intelligence references indicate that terminal kits have been discovered in countries where

they were not officially sold or where services were not provided. In 2022, a notable technology vlogger from a particular country was seen unpacking such a kit in their country where sales and services were unavailable at that time and still are. Even if the kit was purchased legally in a third country and remains in the vlogger's possession, it suggests that the customs police at the entry airport either did not comprehend the nature of this instrument or intentionally allowed it entry, unlike in a well-regulated nation where such an instrument would be considered contraband equipment.

Western think tanks have made detailed reports of such kits making their way into Iran[19] and Russia.[20] It is said that the Russian forces, too, have derived tremendous gains from the use of terminal kits purchased by Eastern Europe and thereafter going into the large void of mushrooming black markets.[21] Starlink has been involved in providing humanitarian services from Poland to Ukraine since the early days of the Russia-Ukraine conflict. However, along with the Russian and Ukrainian forces laying their hands on the user kits in a geography where the satellite internet services were kept active, the kits also fell into the hands of several smaller non-state actors along with the well-acknowledged use of Starlink services by the Ukrainian Armed Forces and the Azov Battalion.[22] However, the Western mainstream media does not mention how such service providers are entering into civil war-ridden Mali or Sudan with partisan support. In Sudan, internet service is being offered at exorbitant rates by the Rapid Support Forces militia, while terrestrial internet networks have been disrupted due to the conflict.[23] Sudan has many priorities to be attained before opting for costly internet; peace is one such priority.

In January 2025, Kazakhstan, after several months of indecision on allowing satellite-based internet services, unearthed grave security threats emanating from satellite communication instruments, particularly Thuraya, Iridium, Inmarsat and Starlink. Kazakhstan's Ministry of Digital Development cited its 2012 National Security Law that prohibits the establishment and operation of any communication instrument whose control centres are not located in the country and calls for the prohibition of the use of instruments by the above service providers.[24] Kazakhstan is mulling over focusing on ramping up its national digital penetration through the use of its indigenous geostationary satellites of the KazSat series and also considering the Kazakh-Chinese joint venture Spacesail Kazakhstan Limited and Eutelsat-OneWeb, all of whom quench the stipulations laid by its national security law.

The conflict in Ukraine has helped create several new companies that have now become vitally important in the downstream value chain of Starlink. The Ukrainian company Adaptis has gained an important breakthrough for the Ukrainian Armed Forces, as it is now able to repair the user terminal, which

was earlier considered non-repairable. This would help Ukraine and its various armed units maintain uninterrupted communications via the 24000 plus terminals that it has received from Starlink. Adaptis would also be in a position to explore several other markets where such repairs are warranted.[25] The Ukrainian non-governmental organisation Aerorozvidka was also called the 'war startup' by the US think tank Atlantic Council.[26] It eventually merged as a unit of the Ukrainian Armed Forces. The drone operators of Aerorozvidka's aerial reconnaissance unit have claimed to have used Starlink terminals to carry out precision artillery strikes against Russian equipment and positions.[27]

Many unique autonomous drone technology platforms are attempting to connect their devices to satellite constellations. One such example is the 'Eagle Nest Off-Grid' solution built by the Canadian drone-tech company 'RDARS'.[28] The Eagle Nest Off-Grid solution is a solar-powered technological system comprising the 'Eagle Watch' a drone, 'Eagle's Nest' a drone parking station; Eagle Rover, an indoor robotic system; and 'Eagle Watch' a command and control software system. This entire solution can be operated off-grid where the electric power source is absent and can be connected to the global networks through Starlink, which has been successfully integrated into the system. Overall, this solution acts like a situational awareness system with military tactical intelligence gathering applications. Such satcom-empowered applications can give tremendous military advantages to users. However, they are still under the threshold of not using satcom for long-range precision strikes, which is currently the unsaid but commonly understood limit of space militarisation.

TRI-SERVICE ASSESSMENT OF THREATS, VOIDS AND OPPORTUNITIES

India is currently witnessing a cascading conflict scenario emerging in several theatres of Asia, which is culminating eventually into a war between the US and China. The tri-service war preparedness calls for telecom sovereignty and indigenity of components as it works on India's conventional war fronts. However, the bigger issue would be the Communication Security (COMSEC) power differential created by countries deliberately arming non-state actors and proxies in geopolitical hotspots with secure satcom user terminals. Where dense terrestrial networks, in times of war, can be damaged and quickly salvaged, the same cannot be said for satcom networks.

Non-geostationary satellite communications are at the crux of the emerging contours of future 'mosaic warfare', a military concept originating from the Pentagon that underlines adaptable, distributed and resilient military systems relying on interconnected and modular components for enhanced flexibility and survivability. Such satcom systems have interconnectivity, flexibility,

and survivability features.[29] The fact that the tri-services would eventually be using such satcom technologies for mosaic warfare is more of an impending reality, making it a technological void for militaries to fill through innovation and evolution. The threat, however, lies in possessing a limited and innocent understanding of such non-geostationary satellite systems as last-mile civilian connectivity providers.

India's Blue Water Navy ambitions, the Air Force's global outreach, and the Army's operations in highly challenging geographies would depend on secure satcom networks. However, if equivalent satcom networks are available to proxies and non-state and terror actors, of course, that would be possible only through patronage. Such patronage would keep the tri-services overwhelmingly engaged with such actors, with the patrons keeping the desire to exhaust the tri-services to make a consequential assault later at a time of choosing. These kinds of threats are not emerging from adversarial platforms, but from adversarial use of commercially available technologies.

Satellite-based internet services are increasingly beneficial and valuable worldwide, appealing equally to governments and their citizens. The last-mile connectivity offered by such services helps in digital penetration. If they are operated in a well-regulated, enabling, and constructive environment, they have the potential to bring economic dividends and socio-economic progress. Such a service can create severe geopolitical complications if made operational in countries with deficient regulatory and legal fundamentals as well as defunct military threat perception and intelligence; those lacking terrestrial telecommunications networks will find it difficult to keep track of direct-to-customer communications networks operating in their countries, leading to situations threatening national security. Furthermore, the same LEO satellites, if not regulated well for the ubiquitous internet services that they can provide, can be surreptitiously used by politically, socially, and economically motivated nefarious actors to meet their goals.

From the perspective of sentiment analysis,[30] it is crucial to understand that when a dual-use technology is excessively admired, such admiration can hinder the critical review and regulation of its operators and end-users. The review and regulation become even more complex when militias, non-state actors, and intelligence and counter-intelligence agencies employ the same technology for grey-zone activities. It is important to understand India's immediate solution to the geopolitical issues arising around India's neighbourhood, including Bangladesh, Myanmar, Nepal and Pakistan and the need to ensure if these countries are capable of keeping an eye on anti-Indian activities in the interest of shared peace, prosperity, and progress. Another concern is that will proxy and non-state actors residing in these countries, overtly or covertly, thrive on

conflict and secession at the behest of their extra-territorial masters by using such telecommunications networks to further their agenda. Such proxies usually thrive on non-interceptable and disruption-resilient communication lines that help them in guerrilla operations, even in the most network-deficient geographies.

Indian tri-services have been articulating its threats through the prism of fighting asymmetric, unconventional, and hybrid wars. One techno strategic development the Indian tri-services should not miss in factoring is their net assessment is the growing role of under-regulated, uncontrollably proliferated, and weaponised non-geostationary satellite communications systems and their use by proxies, secessionist political parties, terror groups, armed militia and mercenary groups and non-state actors.

There are two ways, in which a constructive solution to the advertent and inadvertent conflicts arising from such satcom systems can be arrived at. They are:

- **Operational Front:** On the operational front, the tri-service would need to emphasise the cumbersome vigil and neutralisation of every nefarious entity's use of such systems on a case-to-case basis and make any necessary and stronger reforms in satellite telephone prohibition that are already in place.
- **Judicatory front:** On the judicatory front, the tri-service, and more importantly, the Indian strategic planners, including those sitting in the National Security Council, could focus on rapid assuaging of the crux of the problem by meticulously extending 'arms control' clauses to the deficient Outer Space Treaty and in the ITU convention toward preventing the weaponisation of satellite communication systems and preventing its use by unrecognised actors.

CONCLUSION

Such global rule-making has become exceedingly crucial, as the words of Everett Dolman, from his famous book Astropolitik "Who controls low-Earth orbit controls near-Earth space. Who controls near-Earth space dominates Terra. Who dominates Terra determines the destiny of humankind.", [31] are becoming tantalisingly real. The real fomenting reason for the imminent conflicts is the failure of the global rulemaking to regulate the weaponisation of satcom and one that stands for national sovereignties and their strategic autonomies. The tri-services would have to work on both warfare and lawfare.

❖❖❖

Dr Chaitanya Giri is a Fellow at the Centre for Security, Strategy and Technology at the Observer Research Foundation. He sits on the Advisory Board of the Satcom Industry Association.

NOTES

1. Malik Samuel, "ISWAP's use of tech could prolong Lake Chad Basin violence," *Institute for Security Studies*, 13 April 2023, https://issafrica.org/iss-today/iswaps-use-of-tech-could-prolong-lake-chad-basin-violence
2. African Union, "Boko Haram and other terrorist groups activities in Lake Chad Basin region suppressed in a joint forces operation," 8 August 2024, https://au.int/en/pressreleases/20240808/boko-haram-and-other-terrorist-groups-activities-lake-chad-basin-region
3. Sylvia Duroson (2024), "Satellite Technology to Transform Internet Access in Chad," Tech in Africa, URL: https://www.techinafrica.com/satellite-technology-to-transform-internet-access-in-chad/
4. Gaetano Sicolo, "Dark Signals: The Growing Threat of Satellite Internet in Extremist Networks," *Global Network on Extremism & Technology*, 18 December 2024, https://gnet-research.org/2024/12/18/dark-signals-the-growing-threat-of-satellite-internet-in-extremist-networks/
5. The Hindu, "Militant groups in Kashmir now have Iridium satellite phones, Wi-Fi-enabled thermal imagery tools," 17 April 2022, https://www.thehindu.com/news/national/militant-groups-in-kashmir-now-have-iridium-satellite-phones-wi-fi-enabled-thermal-imagery-tools/article65329539.ece
6. Aparna Rawal, "Pakistan boosts Telecommunication towers in POJK to aid terrorists," *Indian Defence Review*, 22 February 2024, https://indiandefencereview.com/pakistan-boosts-telecommunication-towers-in-pojk-to-aid-terrorists/
7. "Constitution of the International Telecommunications Union," International Telecommunications Union, Accessed on 20th March 2025, https://www.itu.int/en/council/Documents/basic-texts/Constitution-E.pdf
8. Toby Antony, "Satellite phone seized from Canadian national at Kochi airport," *The New Indian Express*, 5 December 2024, https://www.newindianexpress.com/cities/kochi/2024/Dec/05/satellite-phone-seized-from-canadian-national-at-kochi-airport-4
9. Jagriti Chandra, "Airlines to inform foreign travellers not to carry satellite phones," *The Hindu*, 30 January 2025, https://www.thehindu.com/news/national/airlines-to-inform-foreign-travellers-not-to-carry-satellite-phones/article69159915.ece
10. Sandhya Dangwal, "BSNL, INMARSAT launch satellite phone service in India, Here's how it will give a push to Digital India initiative," *India.com*, 25 May 2017, https://www.india.com/business/bsnlinmarsat-launch-satellite-phone-service-in-india-heres-how-it-will-give-a-push-to-digital-india-initiative-2166965/
11. Consulate General of India, San Francisco, "Important Notification for Travellers to India - Ban on Import or Use of satellite phones in India," Ministry of External Affairs, 10 February 2025, https://www.cgisf.gov.in/alert_detail/?alertid=89
12. Alexander Pastukh et al. (2023), "Challenges of Using the L-Band and S-Band for Direct-to-Cellular Satellite 5G-6G NTN Systems," *Technologies*, Vol. 11 (4), 110. 10.3390/technologies11040110

13. Osamu Ekhator, "Mali temporarily lifts Starlink ban for 6 months to develop new regulatory framework," *Techpoint Africa*, 11 October 2024, https://techpoint.africa/news/mali-lifts-starlink-ban/
14. Bidhayak Das, "The mystery of Starlink devices in Manipur's conflict landscape," *The Borderlens*, 19 December 2024, https://www.borderlens.com/2024/12/19/starlink-devices-in-manipur/
15. "People's Liberation Army (PLA) - Insurgency North East" South Asia Terrorism Portal, https://www.satp.org/terrorist-profile/india-insurgencynortheast/people-s-liberation-army-pla
16. John Tanner, "Bangladesh's internet slowdown persists as SEA-ME-WE-5 repairs delayed," *Developing Telecoms*, 26 April 2024, https://developingtelecoms.com/telecom-technology/optical-fixed-networks/16615-bangladesh-s-internet-slowdown-persists-as-sea-me-we-5-repairs-delayed.html
17. BSS, "Could Starlink redefine internet connectivity in Bangladesh?" *Dhaka Tribune*, 16 February 2025, https://www.dhakatribune.com/bangladesh/development/373860/tech-experts-starlink-could-redefine-internet
18. Kaushik Deka, "Why Modi govt initiated probe into unlawful use of Elon Musk's Starlink," *India Today*, 7 January 2025, https://www.indiatoday.in/india-today-insight/story/why-modi-govt-initiated-probe-into-unlawful-use-of-elon-musks-starlink-2660913-2025-01-07
19. Babak Taghvaee, "How Starlink's Direct-to-Cell Service Could Help Iranians Overthrow Their Regime," Middle East Forum, 3 February 2025, https://www.meforum.org/mef-observer/how-starlinks-direct-to-cell-service-could-help-iranians-overthrow-their-regime
20. Ellie Cook, "Russian Army Hit by Mass Starlink Outages on Ukraine Frontline: Reports," *Newsweek*, 5 February 2025, https://www.newsweek.com/russia-ukraine-starlink-outage-elon-musk-spacex-2026614
21. Malin Hunziker, "Can Europe replace Elon Musk's Starlink in Ukraine?" *Neue Zürcher Zeitung*, 17 March 2025, https://www.nzz.ch/english/can-europe-replace-elon-musks-starlink-in-ukraine-ld.1875460
22. Nick Booth, "SpaceX is Starlinking Nazis says Russian space agency chief – then calls for Musk to 'answer in adult way'" Mobile Europe, 9 May 2022, https://www.mobileeurope.co.uk/spacex-is-starlinking-nazis-says-russian-space-agency-chief-then-calls-for-musk-to-answer-in-adult-way/
23. Digital Rights Lab, "Starlink in Sudan: A lifeline or war facilitator?" *Global Voices Advox*, 20 August 2024, https://advox.globalvoices.org/2024/08/20/starlink-in-sudan-a-lifeline-or-war-facilitator/
24. Bruce Pannier, "The Twilight of Starlink in Kazakhstan?" *The Times of Central Asia*, 7 February 2025, https://timesca.com/the-twilight-of-starlink-in-kazakhstan/
25. Militarnyi, "Ukrainian Adaptis Company Masters Repair of Starlink Terminals," 7 March 2025, https://mil.in.ua/en/news/ukrainian-adaptis-company-masters-repair-of-starlink-terminals/
26. Patrick Tucker, "The War Startup," *Government Executive*, 6 May 2015, https://www.govexec.com/magazine/magazine-analysis/2015/05/war-startup/111943/
27. Militarnyi, Aerorozvidka demonstrated how they are destroying the tanks with the help of R18 drones," 15 April 2022, https://mil.in.ua/en/news/aerorozvidka-demonstrated-how-they-are-destroying-the-tanks-with-the-help-of-r18-drones/

28. Newsfile - A TMX Company, “RDARS Completes Initial Development of Drone Eagle Nest and Watch "Off-Grid" System Solution Using Solar Power and SpaceX Starlink Communications,” 27 June 2023, https://www.newsfilecorp.com/release/171367/RDARS-Completes-Initial-Development-of-Drone-Eagle-Nest-and-Watch-OffGrid-System-Solution-Using-Solar-Power-and-SpaceX-Starlink-Communications
29. David Fryer, “Aligning Emerging Concepts and Capabilities With Mosaic Warfare,” *Contemporary Issues in Air and Space Power*, Vol. 2(1), bp41567496.
30. Sardin et al. (2024), “Sentiment Analysis of Starlink on Twitter Using Support Vector Machine Algorithm,” *Journal of Computer Networks, Architecture and High Performance Computing*, Vol. 6(3), 10.47709/cnapc.v6i3.4348.
31. Everett Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (Frank Cass Publishers, London, 2005), 6-7.

❐❐❐

189-205

TRANSFORMING AIR DEFENCE FOR MULTI-DOMAIN WARFARE: STRATEGIC RESPONSES TO EMERGING THREATS

Col Abhishek Bharti

"In the ever-changing skies of conflict, the true strength lies not in denying the evolution of threats, but in our readiness to innovate and adapt, ensuring our defence is as dynamic as the dangers we face."

-Author

Abstract

The nature of aerial threats is undergoing a seismic shift-moving from conventional, manned engagements to a complex ecosystem of unmanned systems, hypersonics, cyber-electromagnetic disruption, and coordinated, multi-domain strikes. Legacy air defence doctrines and technologies, designed for predictable and linear threats, are increasingly ineffective in this evolving battlespace. This paper analyses the transformation of air threats, identifies key vulnerabilities in traditional air defence postures, and argues for a strategic pivot towards air denial, multi-domain integration and technological agility. Drawing insights from recent conflicts and China-centric developments, it proposes a layered, networked, and artificial intelligence-enabled air defence model tailored to India's unique threat environment. It also offers a blueprint for doctrinal evolution, indigenous innovation, and operational restructuring, necessary to secure India's airspace in an age of non-contact, synchronised warfare.

INTRODUCTION

As the character of warfare undergoes a seismic transformation, the ascendancy of non-contact kinetic operations has emerged as a defining pillar of modern conflict. Airpower - unmatched in speed, precision, scalability, and reach continues to serve as the preferred instrument of strategic response. Whether executing stand-off strikes or enabling synchronised, Multi-Domain Operations (MDO), it offers flexible, timely, and scalable engagement options across a broad range of scenarios and the full spectrum of threats, positioning it at the forefront of future battle doctrines. Once marked by a degree of predictability, the battlespace has evolved into a crucible of innovation and adaptation. The previously well-understood domain of aerial combat-long dominated by

conventional fighter aircraft and rotary-wing platforms, has been fundamentally disrupted by the proliferation of unmanned systems, stealthy cruise missiles, advanced ballistic missiles, and Hypersonic Glide Vehicles (HGVs).[1] These emerging threats, often characterised by agility, affordability, and low Radar Cross Section (RCS) areas, reveal critical vulnerabilities in traditional Air Defence (AD) architectures.[2] Consequently, it is imperative to reimagine AD strategies and technologies to address the 'grey rhino' of emerging air threats -visible, pressing, yet dangerously under-addressed. In an era where the cost of complacency is measured in vulnerability, the consequences of inaction may prove as disruptive as the threats themselves.

AIR THREAT TAXONOMY

The contemporary aerial threat landscape is no longer confined to conventional platforms alone - it now spans an expansive and complex continuum of manned, unmanned, kinetic, and non-kinetic vectors. From traditional threats such as fighters, bombers, and attack helicopters to unmanned systems like Unmanned Aerial Vehicles (UAVs), Unmanned Combat Aerial Vehicles (UCAVs), loitering munitions, and autonomous drone swarms, the battlespace is increasingly getting saturated and contested. The missile domain itself has evolved, encompassing cruise missiles, ballistic missiles, Multiple Independently Targetable Reentry Vehicles (MIRV)-capable systems, Anti-Radiation Missiles, the emerging class of HGVs and hypersonic waveriders, all designed to compress decision timelines and bypass layered defences.[3] Tactical-level saturation now includes rockets, artillery shells, and mortar rounds, while advanced stand-off threats such as precision-guided munitions and decoy drones add layers of deception and complexity. At the strategic level, high-altitude platforms, stratospheric balloons/ airship platforms, and pseudo-satellites provide persistent Intelligence, Surveillance and Reconnaissance (ISR) and jamming capabilities, while future-forward concepts like space to air kinetic threats and orbital bombardment remain within the adversary's doctrinal calculus.

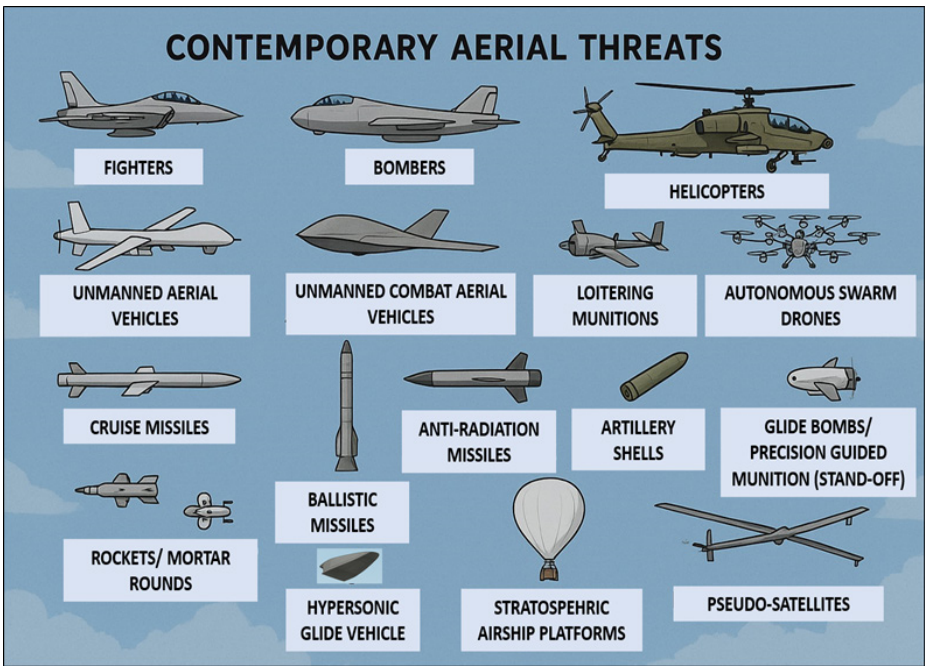


Image 1: Contemporary Aerial Threat Landscape. Source: Author

EVOLUTION OF THE BATTLESPACE AND AIR THREATS

The modern battlespace has undergone a fundamental reconfiguration - both in its physical dimensions and its conceptual underpinnings. Once defined by linear engagements involving manned aircraft and ballistic missiles, today's battlespace is marked by saturation, asymmetry, and simultaneity. Threats now emerge across multiple domains and altitudes, leveraging speed, ambiguity, and affordability to overwhelm traditional AD constructs.

Unmanned Aerial Systems (UAS) have emerged as one of the most disruptive elements in this transformation. Ranging from commercial-grade quadcopters to High-Altitude Long Endurance (HALE) platforms, these systems combine low RCS with persistent surveillance and kinetic capability. In the 2020 Nagorno-Karabakh conflict, Azerbaijan's use of loitering munitions and Turkish-supplied Bayraktar TB2 drones devastated Armenian armour and Surface to Air Missile (SAM) systems.[4] Similarly, in the Russia-Ukraine conflict, both sides have extensively employed UAS for ISR, artillery spotting, and precision strikes - illustrating the operational centrality of drones in both attrition and disruption roles.[5]

This evolution has introduced the notion of 'cheap mass' in warfare, where swarms of low-cost, attritable systems challenge expensive, exquisite platforms.

Russia's deployment of Iranian-origin Shahed-136 drones and precision stand-off munitions reflects a strategy of overwhelming defences through volume and persistence, while Ukraine's use of commercial drones to direct fires has redefined tactical initiative at the lowest levels.[6]

Complementing these developments is the maturation of cruise missile technology. Terrain-hugging profiles and stealth features render systems like Russia's Kalibr and Kh-101 difficult to intercept. Their deployment in conjunction with ballistic missiles such as Iskander and hypersonic platforms like Kinzhal compresses reaction timelines and complicates engagement geometry.[7] The Russian Oreshnik missile, reportedly equipped with MIRVs, represents a significant escalation in the complexity of the threat matrix and its deployment introduces both quantitative saturation and qualitative unpredictability into the battlespace. These weapons are designed to exploit the seams between detection and response, between sensor and shooter.

China's doctrinal and technological developments add another layer of complexity. The People's Liberation Army (PLA) Rocket Force's expanding inventory of short to intermediate range missiles, integrated with Cyber and Electromagnetic Activities (CEMA) and space-based ISR, demonstrates the reality of multi-domain convergence. Concepts like 'System Destruction Warfare' reflect an approach that targets AD ecosystems holistically, degrading command and control nodes, sensors, and shooters before kinetic engagement even begins.[8] Russia's use of Global Positioning System (GPS) spoofing, satellite communication jamming, and Electronic Warfare (EW) enabled drone strikes in Ukraine demonstrates how defenders can be blinded or deceived at critical moments. The need for electromagnetic resilience is now as essential as kinetic hardening.

Traditional threats have also evolved. Rockets, mortars, and artillery shells, once relegated to indiscriminate area fire, now operate within ISR-linked digital kill chains. Their improved guidance and precision make them effective tools in multi-vector saturation attacks, especially when synchronised with missile and drone salvos.

Crucially, airpower is no longer confined to battlefield effects. Recent conflicts have illustrated its expanded strategic function: targeting power grids, oil depots, transport hubs, and industrial capacity to erode war-sustaining infrastructure and break national will. The spectrum of what must be protected has grown broader and sharper, with rising numbers and strategic weight. Civil-Military fusion has rendered the national infrastructure a legitimate and lucrative target set.

The cumulative effect is a battlespace contested in both depth and time, where detection does not guarantee survivability, where distance does not offer

sanctuary, where saturation defeats precision, and where legacy AD systems risk irrelevance without rapid adaptation. The challenge before modern militaries is not simply to detect and shoot, but to operate within a fluid, contested, and multi-domain battlespace, one that is increasingly defined by convergence, disruption and complexity.

CHALLENGES TO LEGACY AD POSTURES

Legacy AD postures, designed for a more predictable and linear threat environment, are increasingly misaligned with the demands of contemporary warfare. The foundational assumption, that air threats would arrive in discernible patterns and in manageable numbers, has been upended by the emergence of low-RCS drones, swarm attacks, hypersonic systems, and non-contact, cross-domain capabilities.

In today's battlespace, missile launches have become increasingly domain-agnostic, blurring the once distinct boundaries of land, sea, air and even space. A ballistic missile can now be launched not just from terrestrial silos, but from submarines, surface warships, strategic bombers, or transporter erector launchers.[9] Cruise missiles, too, have evolved into modular weapons, deployable from airborne platforms, naval vessels, sub-surface assets, and mobile ground vehicles. With rapid advancements in dual-use space technologies, tomorrow's missiles may well descend from orbit, compressing reaction times and disrupting traditional detection protocols. This cross-domain versatility of launch platforms introduces a new and complex threat calculus for air defenders, demanding a paradigm shift in surveillance, cueing, and interception strategies.

One of the most pressing challenges lies in the static deployment philosophy that governs much of India's existing AD network. Fixed-site radars, siloed command and control centres and geographically predictable deployments are particularly vulnerable in an age where adversaries possess persistent surveillance, long-range precision fires and rapid-reaction strike capabilities. These vulnerabilities are magnified in mountainous or urbanised terrain, where mobility and concealment become operational imperatives. In the Indian context, the operational environment is further complicated by diverse terrain.[10] Current doctrines inadequately reflect these realities, often assuming the availability of space and infrastructure for fixed deployments.

Equally problematic is the continued dependence on legacy communication protocols and GPS-based synchronisation, which severely limits the resilience, adaptability, and survivability of AD networks in a contested battlespace.[11] In a high-end conflict scenario particularly one involving peer adversaries like China such vulnerabilities can lead to command fragmentation, delayed engagement cycles, fratricide risks due to unreliable Identification Friend or Foe (IFF) mechanisms, and severely disrupted kill chains. Additionally, legacy systems

often operate on narrow-band, easily saturated communication channels that lack the bandwidth to support real-time multi-sensor data fusion, AI-enabled threat prioritisation, and autonomous engagement loops. Compounding the issue is the insufficient focus on encryption and transmission secrecy, which leaves communication links susceptible to interception, signal manipulation, and deception. Resilience to jamming, spoofing, signal denial, and cyber intrusion is no longer optional, it is foundational.

India's AD architecture continues to be somewhat constrained by the need of more inter-service fragmentation and doctrinal synergy.[12] While newer systems have been inducted, they frequently operate in isolated data loops, with limited real-time fusion across Army, Air Force, and Navy domains. In the absence of a unified command structure and integrated sensor-shooter network, decision-making slows and resource optimisation suffers. Technological upgrades alone are insufficient without parallel reform in training, doctrine, and command philosophy. Training curricula have not yet evolved to simulate electronic warfare environments, rapid target reassignment, and real-time cross-domain integration. Rigid engagement protocols and compartmentalised decision-making impede responsiveness in high-tempo, multi-domain scenarios. Sustained efforts have already fielded in near seamless integration of control and reporting arrangements of all the three services which was demonstrated during Operation Sindoor.

THE SHIFT FROM AIR SUPERIORITY TO AIR DENIAL

The long-standing military aspiration of achieving and sustaining air superiority is increasingly being challenged by the complexity of modern warfare. In peer or near-peer conflicts, especially where technological parity is narrowing and Anti-Access/ Area Denial (A2/AD) capabilities proliferate, the ability to completely dominate the air domain, even temporarily, is no longer assured. The cost, risk, and resource demands associated with traditional air superiority campaigns may outweigh their operational benefits in many contemporary scenarios.

This shift is exemplified by recent conflicts where technologically inferior forces have successfully contested airspace using integrated AD, electronic warfare and distributed strike networks. In the Russia-Ukraine conflict, for instance, neither side has achieved uncontested access to the air domain.[13] Instead, both rely heavily on ground-based air denial strategies, combining mobility, redundancy, and survivability to constrain the adversary's options rather than seek dominance. Air denial, as a doctrine, emphasises disruption over ownership. It involves deploying layered and resilient systems that impose operational friction, degrade mission success, and raise the cost of air access.[14] Rather than aiming to eliminate enemy air capabilities outright, the objective is to deny them freedom of action at critical times and places.

This concept holds particular relevance for India. The People's Liberation Army Air Force's (PLAAF) numerical superiority and China's deep industrial base provide it with a far greater tolerance for attrition. Attempting to match sortie rates or platform counts would be neither feasible nor strategically prudent. In a prolonged air campaign, China's ability to absorb and replenish losses far outpaces India's, making a like-for-like contest unsustainable. A denial-focused posture, centred on mobility, concealment, multi-domain integration, and survivability, offers a cost-effective and operationally realistic alternative. Within this framework, concepts such as the 'Blue Sky', a transient window of airspace cleared of hostile threats, become pivotal for enabling manoeuvre and safeguarding critical assets. Unlike permanent air superiority, it reflects a condition of temporary air denial achieved through synchronised AD action. Equally vital is the 'Air Littoral', the contested vertical zone between ground forces and high-altitude platforms - where drones, loitering munitions, cruise missiles, and low-flying aircraft operate with increasing lethality.[15]

Dominance in these layers demands dynamic targeting, agile deployment, and redundancy across sensors and shooters. The ability to impose persistent doubt, delay, or disruption on enemy air planners not only degrades their tempo but also acts as a potent deterrent in its own right.

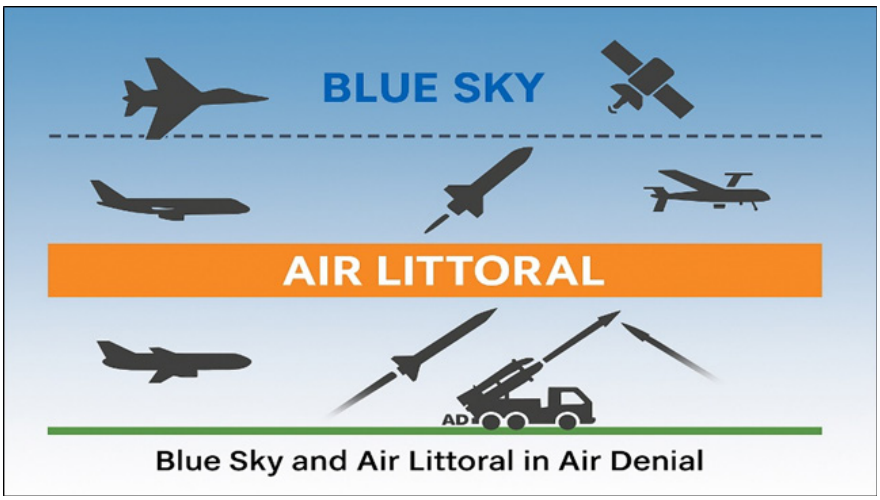


Image 2: Blue Sky and Air Littoral Concept. Source: Author

Ultimately, air denial does not signify doctrinal compromise; rather, it reflects strategic adaptation to the realities of contested, multi-domain warfare. It enables nations with limited air dominance capacity to shape the air environment in their favour through intelligent defence, calculated disruption, and integrated deterrence.

THE IMPERATIVE FOR MULTI-DOMAIN INTEGRATION

Modern warfare no longer respects the boundaries between land, sea, air, cyber, and space. Aerial threats increasingly unfold as cross-domain constructs, launched from one domain, guided through another, and striking with precision coordinated by a third. This domain convergence introduces complexity in trajectory, timing, altitude and signature, compressing detection-to-intercept cycles and overwhelming traditional, siloed responses. Addressing such threats through isolated service-centric postures risks fragmentation, latency, and operational breakdown.[16]

For air defenders, domain-agnostic awareness and response have become essential, not optional. When adversaries such as China design campaigns to synchronise electromagnetic, kinetic, and space-based effects, integration is no longer a doctrinal aspiration, it is a survival imperative. Multi-domain integration ensures that sensing, decision-making, and action are synchronised in real time, across domains, thereby preserving not only target protection but the functional integrity of the entire defence ecosystem. It also ensures that every sensor contributes to the fight, every shooter is part of a network, and every engagement decision is informed by a comprehensive, real-time operational picture. In a battlespace where threats manoeuvre fluidly across domains, only a unified, integrated response can deny the adversary the advantage of speed, scale, and surprise.

The adversary already operates with domain convergence in mind. China's ‘System Destruction Warfare’ model envisions coordinated strikes across the electromagnetic spectrum, space-based surveillance, and kinetic actions, all aimed at paralysing an opponent’s decision-making and response cycles.[17] Modern air campaigns will likely begin with cyber incursions that spoof, jam or degrade detection systems before kinetic salvos commence. The hybridisation of domains now blurs the boundaries of initial engagement.

If threats manoeuvre across domains, then the response must be forged through multi-domain integration, because in modern warfare, single-domain answers invite multi-domain defeats.

STRATEGIC RESPONSES AND TECHNOLOGICAL PATHWAYS

AD must evolve from static, platform-centric constructs to dynamic, adaptive networks designed for multi-domain operations. In a battlespace defined by speed, saturation, and synchronised threats, survivability and agility, not sheer firepower, must become the operational metrics. This transformation requires more than technological modernisation; it demands a doctrinal shift that places cross-domain integration and distributed resilience at the core of India’s AD strategy.

At the heart of this shift lies the development of tiered, vertically integrated architectures capable of engaging threats across altitude bands and threat types. These should seamlessly combine long-range interceptors, medium-range SAMs, and close-in defence systems, reinforced by Counter-Rocket, Artillery, and Mortar (C-RAM) and Counter-Unmanned Aerial Systems (C-UAS) capabilities.[18] Operating in vertical depth enables simultaneous engagement of high-altitude ballistic missiles, mid-altitude cruise missiles and UAVs, and low-flying loitering munitions and First Person View (FPV) drones, all within a single, responsive network.

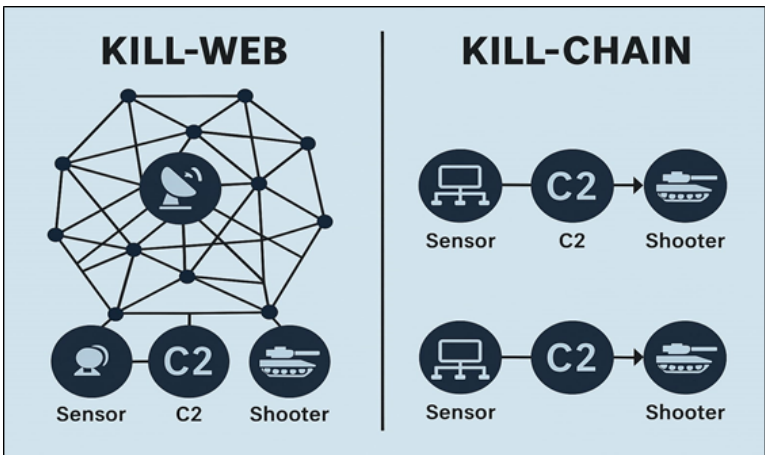


Image 3: Kill Web and Kill Chain Concept. Source: Author

To counter massed aerial attacks, particularly those enabled by AI-coordinated drone swarms, India must adopt distributed kill-web architectures, resilient, real-time targeting ecosystems that link sensors to shooters across domains. These networks should integrate Directed Energy Weapons (DEWs) such as high-energy lasers and high-power microwaves for rapid, low-cost per shot neutralisation of low-RCS threats, especially in inner defence rings.[19] Complementing these are '3P' airburst munitions (Pre-fragmented, Programmable, Proximity-fuzed) for legacy gun systems like the L-70 and ZU-23-2B, and Close-In Weapon Systems (CIWS) or Gatling platforms offering high-rate, terminal-phase interception. Together, these technologies form a responsive, cost-efficient buffer and offer scalable, low-latency interception against massed, low-RCS threats operating within the air littoral.[20]

At the platform level, hybrid C-UAS systems integrating hard-kill and soft-kill options, such as jamming, spoofing, and DEWs, must become the norm. Mounted with Electro Optical (EO)/Infrared (IR) sensors and radars, and cued by AI-enabled threat classification algorithms, these systems compress decision timelines and enable autonomous response against fast, low-cost

drone threats. To be effective, such platforms must be fielded in density across all critical Vulnerable Areas (VAs) and Vulnerable Points (VPs).

Image 4: Directed Energy Weapons Against Drones. Source: Author

Deployment philosophy must also shift. Inspired by the Agile Combat Employment (ACE) model, AD units must emphasise dispersion, frequent repositioning, deception, and rapid modularity to minimise targetability. This becomes particularly urgent in the face of China's Air–Artillery–Missile–Drone (A2MD) campaigns, which rely on multi-vector saturation to dislocate both static and mobile assets. Even mobile AD units, if predictably employed, remain vulnerable to ISR-enabled precision strikes. Hence, mobility must be paired with emission control and tactical unpredictability.

Underpinning this architecture is the requirement for a cyber-hardened, AI-enabled command and control system. It must be capable of autonomously ingesting multi-sensor inputs and directing shooters, even in GPS-denied and EW-contested environments. Alternate navigation solutions, such as Inertial Navigation Systems (INS), terrain-matching algorithms, and emerging quantum positioning - must be integrated to ensure uninterrupted functionality.[21]

However, technological advancement without context-sensitive adaptation remains hollow. Systems optimised for the desert or plains may falter in high-altitude terrain or island theatres. Therefore, doctrine, equipment, and tactics must be tailored to India's diverse operational environments, supported by modular procurement strategies and robust indigenous research and development. A robust public–private innovation ecosystem, with targeted support to defence start-ups and Micro, Small and Medium Enterprises (MSMEs), will be critical to driving iterative upgrades, rapid prototyping, and battlefield-specific customisation.[22]

Ultimately, these strategic and technological pathways must be anchored in a forward-looking doctrine, one that anticipates, adapts, and integrates, rather than reacts, stagnates or compartmentalises.

RECOMMENDATIONS FOR THE INDIAN CONTEXT

While the Russia–Ukraine war has become a touchstone for modern AD thinking, its lessons, like those from the Israel–Iran confrontation and the Azerbaijan–Armenia conflict must be doctrinally contextualised.[23] For India, adopting foreign templates wholesale risks strategic misalignment. India's AD must, therefore, be tailored to its own geography, adversaries, and doctrinal imperatives.

India's AD posture must evolve in both capability and philosophy to meet the unique challenges posed by the strategic complexities of operating across multiple, distinct theatres. Along the northern borders with China, the high-altitude environment imposes severe constraints on radar visibility, mobility, and electronic system reliability. This demands an architecture capable of rapid adaptation, autonomous decision-making, and sustained functionality under degraded conditions. In contrast, the western front, characterised by close-proximity threats, frequent provocations, and densely populated areas, requires rapid-response systems, seamless command and control, and minimal reaction timelines. Meanwhile, the maritime domain, particularly around the Andaman and Nicobar Islands, faces mounting pressure due to increased Chinese activity in the Indian Ocean Region. Here, domain awareness, real-time sensor fusion, and integration of naval and space-based assets are essential.

Across all these fronts, the imperative is clear, AD cannot remain service-bound or reactive. It must be anticipatory, layered, and networked, anchored in jointness and resilient against multi-domain saturation. This evolving challenge demands a strategic leap, India must rapidly enhance its early warning architecture, including space-based surveillance assets capable of detecting even MIRV separation events in real time. Simultaneously, investment in AI-driven threat classification and prioritisation algorithms will be critical to manage saturation scenarios where multiple threat vectors descend simultaneously.[24] Interceptor stockpiles must be diversified and scaled up, while command structures need doctrinal flexibility to enable simultaneous, multi-vector engagements. To counter the next-gen threat decisively, India must also fast-track its efforts on futuristic technologies, ranging from boost-phase interceptors to DEWs and AI-enabled kill-webs that compress decision timelines and impose layered deterrence at scale.[25]

The foremost priority is to move from fragmented, service-specific deployments to an Integrated Air and Missile Defence (IAMD) structure, interconnected across services, synchronised in real time, and managed through joint theatre

commands. This is essential not only for operational synergy but also to reduce redundancy, close response gaps, and improve sensor-to-shooter timelines. In a potential Indo-China conflict scenario, China may exploit the region's geographical contiguity to manoeuvre near, around, or through the sovereign airspace of neighbouring states such as Nepal, Bhutan, Myanmar, and Bangladesh. This reality underscores the need for India to incorporate extended air corridors, regional airspace dynamics, and cross-border trajectory mapping into its integrated AD planning. Central to this is the establishment of -from low-flying drones to high-altitude missiles, to ensure no layer of the aerial spectrum remains unmonitored or vulnerable.

Image 5: Multi-Domain Integrated Air Defence Concept. Source: Author

The complexities of multi-domain warfare necessitate a paradigm shift in airspace management, from static, procedural control to dynamic, AI-assisted orchestration. In a battlespace saturated with manned aircraft, drones, loitering munitions, and hypersonic vectors, traditional deconfliction protocols are inadequate. India must develop an autonomous, real-time airspace governance framework capable of adaptive prioritisation, seamless tri-service coordination, and layered decision authorisation. AI-driven airspace controllers, fused with EO/IR and radar feeds, can enable predictive engagement zones, thereby

reducing fratricide risk and improving time-sensitive targeting. This capability is central to ensuring operational fluidity and survivability in future high-velocity, contested air environments.

A resilient, sovereign satellite communication network is vital for sustaining AD operations in a contested battlespace. As adversaries increasingly target ground-based command and control links through cyber and electronic warfare, the absence of a Starlink-like Low-Earth Orbit (LEO) constellation leaves India exposed to operational paralysis.[26] Such a constellation would ensure uninterrupted sensor-shooter connectivity, precision navigation, and secure, low-latency command and control, even in a GPS-denied environment. While India's Indian Regional Navigation Satellite System (IRNSS) also known as Navigation with Indian Constellation (NavIC) provide crucial regional positioning support, it must be integrated with future LEO constellations to enhance redundancy, resilience, and coverage. Integrating this space-based layer into India's IAMD architecture is no longer optional, it is a strategic necessity for autonomous operations, real-time data fusion, and resilient defence across altitudes and domains.

Technological integration without organisational transformation risks partial effectiveness. India's fragmented service-specific AD structure must evolve into a unified, jointly staffed ecosystem. Institutionalising tri-service AD cells, cross-posting of AD specialists, and integrated planning mechanisms within theatre commands can bridge doctrinal gaps and harmonise sensor-shooter operations across services. Doctrinally, India must institutionalise red-teaming, wargaming, and threat forecasting into its AD planning cycle. Exercises should routinely simulate cyber-EW contested environments, GPS denial, and saturation strikes, not as exceptional scenarios, but as baseline conditions. Training programmes, war games, and doctrinal simulations must reflect this joint ethos. True synergy lies not just in hardware, but in shared thinking, planning, and execution. An integrated institutional culture will ensure India's IAMD architecture is not just connected, but cognitively coherent across all levels of war.

On the industrial front, the emphasis must be on creating a domestic AD ecosystem. Platforms like Akash and Akash-NG must be rapidly iterated and exported. Indigenous development of AI-integrated fire-control systems, Long Range SAM (LRSAM), Medium Range SAM (MRSAM), modular launch platforms, C-UAS systems, Man Portable AD Systems (MANPADS) and smart munitions should be prioritised under Make in India and Innovations for Defence Excellence (iDEX) initiatives.

Recent conflicts have positioned AD as the battlefield's 'first responder' - bearing the brunt of the initial aerial assault and setting the operational tempo for survival.

No longer a supporting actor, AD now defines the opening moves of warfighting. For India, this paradigm shift demands not just recognition but resolute action: accelerated procurement, focused modernisation, and institutional prioritisation of AD must now be treated as national strategic imperatives. In light of increasing cross-domain and trans-theatre threats, there is a compelling case for establishing a unified structure under Theatre Command, an institution that harmonises planning, operations, and procurement across the services. Embracing a 'One Nation-One Airspace-One Shield' philosophy would ensure seamless coordination, eliminate response gaps, and enable faster decision-making in high-tempo conflict environments. As airspace becomes increasingly contested, ownership must give way to orchestration.

Image 6: One Nation-One Airspace-One Shield Concept. Source: Author

CONCLUSION

The character of aerial threats has undergone a seismic transformation. From manned aircraft and ballistic missiles, the battlespace has shifted to one dominated by drones, hypersonics, cyber-electromagnetic effects and saturation-style attacks coordinated across domains.[27] In such an environment, legacy AD systems, static, fragmented, and platform-centric - risk obsolescence unless fundamentally reimagined. This reimagination cannot

be confined to equipment upgrades or incremental acquisitions. It must be doctrinal, institutional, and technological. Survivability, agility, and multi-domain integration must replace firepower and mass as the defining principles of AD efficacy. The ability to disrupt, delay, and degrade adversary aerial operations, rather than seeking total air dominance, will determine operational success in future conflicts. India's AD forces must evolve into an intelligent, adaptive ecosystem: networked across domains, hardened against electronic and cyber warfare, and tailored to operate across diverse terrain profiles. Red-teaming, AI-driven command systems, DEWs, and modular procurement strategies must become the norm rather than the exception. The threats are clear, the lessons are vivid, and the cost of inertia is steep. What remains is the will to transform. In an age of contested skies and converging domains, it is not superiority but strategic resilience that will secure the airspace of the future.

In such a dynamic and multi-vector threat environment, AD must be reimagined, not as a platform-centric function, but as a seamless, anticipatory shield capable of responding across altitudes, domains, and intensities. For India's AD transformation to succeed, it must decisively break from the inertia of peacetime proceduralism and embrace a mission-first, threat-informed doctrine. The tyranny of the '3 Ps', Policies, Processes, and Procedures, must not be allowed to throttle innovation or delay capability induction. In an era where adversaries are fielding disruptive technologies at speed, doctrinal adaptability, operational flexibility, and rapid experimentation must override bureaucratic rigidity. AD modernisation is not merely a matter of acquisition, it is a mindset shift, where responsiveness, integration, and survivability become the new strategic currency. The time to prioritise purpose over process is now.

❖❖❖

Col Abhishek Bharti is an Army Air Defense officer who has vast operational experience. An avid reader and prolific writer, he contributes regularly to various military journals and his academic pursuits include five different Master's degrees in defence/military technology domain. The officer commanded his unit along Line of Actual Control on Northern borders. After undergoing Higher Defence Management Course, he is currently serving as a Directing Staff at Defense Services Staff College, Wellington.

NOTES

1. Paul Scharre, The Coming Swarm: The Evolving Art of Drone Warfare (Washington, DC: Center for a New American Security, 2015), 10–18.
2. Hunter Stoll, John Hoehn, and William Courtney, "Air Defense Shapes Warfighting in Ukraine," RAND Corporation, February 22, 2024, https://www.rand.org/pubs/commentary/2024/02/air-defense-shapes-warfighting-in-ukraine.html.

3. Dr Jack Watling and Nick Reynolds, “Tactical Lessons from Israel Defense Forces Operations in Gaza, 2023,” RUSI, July 11, 2024, https://rusi.org/explore-our-research/publications/occasional-papers/tactical-lessons-israel-defense-forces-operations-gaza-2023.
4. Mark Massa, “The TB2: The Value of a Cheap and ‘Good Enough’ Drone,” Atlantic Council, August 30, 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/the-tb2-the-value-of-a-cheap-and-good-enough-drone.
5. Kartik Bommakanti, “The Military Lessons of the Russia-Ukraine War,” Observer Research Foundation, January 18, 2024, https://www.orfonline.org/research/the-military-lessons-of-the-russia-ukraine-war.
6. Nakul Dev, “Exploitation of Air Power in Russia-Ukraine Conflict and Lessons for IAF,” Centre for Air Power Studies, 2024, https://capsindia.org/wp-content/uploads/2024/10/Nakul-Dev-1.pdf.
7. Kartik Bommakanti, “The Military Lessons of the Russia-Ukraine War,” Observer Research Foundation, January 18, 2024, https://www.orfonline.org/research/the-military-lessons-of-the-russia-ukraine-war.
8. Sherrill Lingel et al., Joint All-Domain Command and Control for Modern Warfare, RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RR4408z1.html.
9. John Tirpak, “Air Superiority is Still the Key to Winning. Achieving It Is Getting Harder,” Air & Space Forces Magazine, March 4, 2025, https://www.airandspaceforces.com/air-superiority-key-to-winning/?utm_source=perplexity.
10. UNI India News Service, “AD: Lessons for India from Russia-Ukraine War,” February 28, 2025, https://www.uniindia.com/air-defence-lessons-for-india-from-russia-ukraine-war/india/news/3402350.html.
11. Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It (New York: HarperCollins, 2010), 112–117.
12. UNI India News Service, “AD: Lessons for India from Russia-Ukraine War,” February 28, 2025, https://www.uniindia.com/air-defence-lessons-for-india-from-russia-ukraine-war/india/news/3402350.html.
13. Lieutenant Colonel Herbert Bowsher, “Air Denial Lessons from Ukraine,” U.S. Naval Institute, September 2023, https://www.usni.org/magazines/proceedings/2023/september/air-denial-lessons-ukraine.
14. Maximillian Bremer and Kelly Grieco, “Air Denial: The Dangerous Illusion of Decisive Air Superiority,” Atlantic Council, August 30, 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/air-denial-the-dangerous-illusion-of-decisive-air-superiority.
15. ibid.
16. Joe Goodwin, “Allied Air Command Lessons from Ukraine,” Joint Air Power Competence Centre, May 2024, https://www.japcc.org/articles/allied-air-command-lessons-from-ukraine/?hl=en-GB.
17. Sherrill Lingel et al., Joint All-Domain Command and Control for Modern Warfare, RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RR4408z1.html.
18. CZDEFENCE, “Lessons Learned from the Deployment of AD in Ukraine,” Czdefence.com, February 13, 2023, https://www.czdefence.com/article/lessons-learned-from-the-deployment-of-air-defence-in-ukraine.
19. P.C. Katoch, “Lessons from the Israel–Hamas War,” Sps-Aviation.com, October 31, 2023, https://www.sps-aviation.com/experts-speak/?h=Lessons-from-the-Israel-Hamas-War&id=771.

20. P.C. Katoch, “Lessons from the Israel-Hamas War,” Spslandforces.com, May 2023, https://www.spslandforces.com/story/?h=Lessons-from-the-Israel-Hamas-War&id=880.
21. Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It (New York: HarperCollins, 2010), 112–117.
22. UNI India News Service, “AD: Lessons for India from Russia-Ukraine War,” February 28, 2025, https://www.uniindia.com/air-defence-lessons-for-india-from-russia-ukraine-war/india/news/3402350.html.
23. Kartik Bommakanti, “The Military Lessons of the Russia-Ukraine War,” Observer Research Foundation, January 18, 2024, https://www.orfonline.org/research/the-military-lessons-of-the-russia-ukraine-war.
24. Hunter Stoll, John Hoehn, and William Courtney, “Air Defense Shapes Warfighting in Ukraine,” RAND Corporation, February 22, 2024, https://www.rand.org/pubs/commentary/2024/02/air-defense-shapes-warfighting-in-ukraine.html.
25. Sherrill Lingel et al., Joint All-Domain Command and Control for Modern Warfare, RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RR4408z1.html.
26. Nakul Dev, “Exploitation of Air Power in Russia-Ukraine Conflict and Lessons for IAF,” Centre for Air Power Studies, 2024, https://capsindia.org/wp-content/uploads/2024/10/Nakul-Dev-1.pdf.
27. John Antal, 7 Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting (Philadelphia: Casemate, 2022), 123-145.

❐❐❐

206-218

JOINT TRAINING NEEDS FOR FUTURE WARFARE

AVM (Dr) M S Rama Mohan, VSM (Retd)

"*Training must evolve to face the unique security challenges and fight future wars in an integrated manner as a theaterised force*."

General Anil Chauhan, Chief of the Defence Staff 35th TSTTC, 13 November 2024

Abstract

Future wars are complex, ambiguous and unpredictable. A sure way of fighting and winning future wars is to train well and in time so that the variables in the winning proposition are minimised. As future warfare will be technologically advanced, the training needs will differ from the traditional training requirements. The skill levels, knowledge and experience required of a joint fighter where the response time is less than a second, the decision matrix is complex, and the domain is little known. The solution is identifying the training attributes and skills required to fight future wars. Technology can address the technology-using this maxim, the paper identifies the key training needs, namely skills, knowledge and outcomes required to train the joint fighter for future warfare. The paper also recommends an approach for joint training for future warfare.

INTRODUCTION

The theory of Warfare has two components, namely nature and character. While the nature of warfare is immutable, its character is changing owing to the dynamic security environment, the advent of niche technologies, and the blurring of boundaries between conventional domains of land, sea, and air. These changes require future military leaders to be prepared to fight and win on technologically advanced battlefields. The preparation starts with training the soldiers, sailors and airmen for future warfare in an integrated environment. The training outcome will depend on a firm understanding of the attributes of future warfare and the skills and knowledge required to survive and win future wars. Future wars have always been more violent, complex, and disruptive than present ones. Military history is replete with examples where lethality, ambiguity and unpredictability have progressively increased between wars. At the same time, it needs to be understood how the present forecast of future wars is different. The answer will lead to the attributes of future warfare, which will set the basis for the training outcomes.

LITERATURE REVIEW

Most of the literature reviewed on future wars asserts that future warfare will be highly automated, and its effects cannot be predicted.[1] The literature predicts that the wars will be fought at the cognitive level, involving several domains that are not conventional. Future warfare will be technologically driven to bring about kinetic and non-kinetic effects. The 'Joint Doctrine of the Indian Armed Forces 2017' broadly covers future wars. The doctrine covers the requirement of integrated human resources development.[2] The Joint Training Doctrine 2017 emphasises jointness in the training and is silent on the attributes or qualities a joint war fighter must be trained in.[3] Most of the literature reviewed mentions various technologies used in future warfare.[4] The literature is silent on the human element and the attributes of the joint war fighter in future warfare. In some cases, a bold argument of replacing human beings in future wars is made.[5,6] In 2018, the US Army Training and Doctrine Command hosted a conference called Learning 2050, which alludes to skill sets and training for the future soldier.[7] However, a gap in the knowledge of future warfare is perceived insofar as the joint war fighter's specialist skills and expertise are required to operate technologically advanced equipment in different domains.

The paper analyses future warfare and the capabilities a joint force must develop. The capabilities are mapped to the joint war fighter's desirable skills and knowledge attributes. The paper concludes with proposed skills and knowledge that a joint war fighter must be trained in and recommends a strategy for achieving the training for future warfare. The paper assumes that the integrated training environment to fight as a theaterised force is a given variable. The present pattern of teaching prevalent in the three services or joint training institutes or the organisational aspects related to the theorised environment of the Indian Armed Forces has neither been included in the analysis presented in the paper nor compared with the joint training attributes, as such an objective could be the theme of another paper, probably a follow-on paper.

WHAT IS FUTURE WARFARE?

The available literature shows that future warfare has been widely commented on in detail. The prognosis of future warfare by the futurists ranges from the next five years to nearly two decades. The future warfare is ambiguous, uncertain, short, swift, lethal, intense, precise, non-linear, unrestricted, unpredictable and hybrid.[8] Each characteristic of warfare introduces a new dimension to the war. To sharpen the analysis, the characteristics are grouped into four distinct attributes of warfare, Syncretic, Sophisticated, Spontaneous and Synergistic, which are called the 4S model of future warfare. The details of which are as

under:

- **Syncretic:** The present wars are waged in the conventional domains of land, sea, air, space and cyber. The challenge comes when warfare uses multiple domains to achieve an effect, thus defeating the defences meant for the domain. The capture of the US drone RQ-170 by Iran in December 2011 is a case where cyber warfare was used to block the data link of the drone and then spoof the GPS signal to divert the drone to the location Iranian forces desired.[9] Thus, the cyber domain was used to create an effect in the air domain. Examples abound where the multi-domain operations in future warfare will be the norm. A joint force must aim to achieve the capability of integrating all domains of the operations, among other things, through a unified C4ISR protocol and standard rules of engagement. Various systems of each domain must seamlessly exchange the common operational picture and data across multiple domains without any degradation. Towards this, the common operational picture must be domain agnostic.[10] The uni-domain thought process of each service must move to a multi-domain or an integrated domain approach to generate an effect. The joint fighter must operate equally skilfully in all domains, which is challenging. From the training point of view, understanding, adapting, and proficiently operating in a domain-agnostic environment is an essential skill for surviving in multi-domain warfare.
- **Sophisticated:** The future warfare will be complex. Advanced concepts and disruptive technologies will be used in future warfare.[11] Every method, technology, and strategy will be more complicated than the last warfare.[12] Therefore, complexity cannot be rejected as a convention in future warfare. In the present context, sophistication exponentially increases with the emerging technologies to produce novel war-fighting equipment. The infusion of artificial intelligence in target detection, identification, and tracking, as in the case of weapon sensors, is a case in point. STM Kargu attack drones equipped with advanced machine-learning algorithms were used in the Nagorno-Karabakh Conflict in 2020.[13] Several emerging technologies are shaping future wars. The time taken for emerging technologies to be adopted by militaries is progressively reducing from a few decades to a few years. A faster infusion rate of the technologies has resulted in an unprecedented increase in the complexity of the battlefield. From the joint force capability point of view, contemporary technology must be acquired, adopted and applied in warfare. The technology must bring unconventional effects and exploit the weakness of the adversary's defences. A word of caution, technology alone or sophistication alone cannot bring about

success in a war. The judicious employment of technology at the three levels of war, tactical, operational and strategic, determines the war's success, which comes from integration.[14] The integration of information, its processing and decision-making at three levels of warfare is key for the sophistication to have a meaningful effect. Therefore, the joint war fighter must easily navigate complex and disruptive technologies at all three levels.

- **Spontaneous:** Spontaneity is a function of the commencement of war, its duration, and the effects the war generated. All three parameters of war are volatile. The effects of the war are unpredictable to a fair degree of accuracy.[15] Considering multiple orders of damage mechanisms, the deterministic models of the effects will fail in future wars, as small weapons can bring about a disproportionate effect. The attack by Houthis on Abqaiq-Khurais oil facilities in Saudi Arabia by drones in September 2019 is an example of the disproportionate effect created by a small weapon.[16] A top-level analysis of effects shows that the first-order damage was on the oil facility infrastructure, the second-order effect was on the oil production of Saudi Arabia, and the higher-order effects were on the Saudi Arabian economy and world oil markets. A detailed analysis will bring out higher-order effects that require large prediction models and computational power. The deterministic nature of warfare gives way to a non-deterministic nature. The strategic parts are non-deterministic, while the operational and tactical aspects provide several probable options (not fully deterministic). Similarly, predicting the duration or cessation of war is challenging given the innumerable physical and virtual variables. In the ongoing Ukraine-Russia conflict, Russia stated on 22 February 2022 that it invaded Ukraine for a peace-keeping function. The conflict is now a full-scale, all-domain war that has been ongoing for over two years. The prediction of the conflict and its effects is an example of the recent past, where the prediction of the cessation of the war was incorrect from the beginning. The ongoing Middle East crisis of the Israel-Palestine conflict is a sterling example of the unpredictability of the effects of war. The Yemeni Houthis and Iran joining the conflict is another example of the spontaneous escalation of the war. Therefore, spontaneity in future warfare is an important characteristic. To respond to the spontaneity of future wars, the joint force must be agile, and its fighters must be adaptable to the evolving scenarios. Towards this, the joint fighter must be trained on the cognitive skills of adaptability to dynamic situations and different domains.
- **Synergistic:** The warfare is syncretic and sophisticated, so a high level of functional coordination for seamless and continuous operation

between owners of land, sea, air, space, and cyber domains will be imperative. The boundaries will be blurred, and operations will be uninterrupted. A domain-agnostic approach is essential for a smooth transition from the uni-domain approach. A smooth transition of command and control across the blurred boundaries of the domains without losing operational efficiency and ethical standards will be a challenge. The novelty of technology has never ensured success in its own right it is the integration of innovation into effective methods and means that gives a strategic or tactical edge.[17] Therefore, a joint force must be equipped with an integrated architecture where the operational picture flows freely in the near-simultaneous time frame. Secure, high-speed information highways transcending the domains are a part of the integration. From the training point of view, the joint fighter must be aware of the common operational picture, the peculiarities and operational rules of engagement of the domain.

4S - CAPABILITY MAP

The 4S characteristics of future warfare must translate into the capability of a joint force. Such a correlation between characteristics and capabilities is gross, as the ultimate objective of correlation is to derive the skills and expertise expected from the joint war fighter.

S. No	Characteristic	Capability
1.	Syncretic	• Operations in a single network battlespace integrating all the domains. • Real-time data exchange of assets and operations on secure digital infrastructure.
2.	Sophisticated	• Data-driven equipment using AI/ ML techniques for efficiency, precision and effectiveness. • Hypersonic weapons, human-machine teaming concept, robotics and high-level automated systems.
3.	Spontaneous	• Decentralised C2 structures. • Agile small teams instead of large formations. • Edge computing environment. • High-speed, autonomous decision support systems.
4.	Synergistic	• Digital battle space. • Well-defined rules of engagement. • Common equipment/ interfaces/ data formats.

Table 1. 4S- Capability Map, Source: Author

CORRELATION BETWEEN CAPABILITIES AND TRAINING ATTRIBUTES

The 4S Capabilities mapping at a gross level has identified capabilities that must be progressively built over time. As future warfare evolves, the desired capabilities will also change. Therefore, the mapped capabilities are based on the current understanding of future wars. In addition, the mapping is restricted to the technologies/tools that are available/known today. A blend of existing technologies or a specific emerging technology may provide an effective capability to address future warfare. A summary of the correlation of capabilities of future warfare with the training attributes

S. No.	Future Warfare Capability	Skills Required	Knowledge Required	Experience Gained Through Training
1.	Multi-dimensional, single network battlespace	High-level situational awareness, cross-domain coordination. Digital literacy.	Understanding operations and ROE of multi-domain.	Joint and coalition exercises across domains.
2.	High-speed decision support systems	Rapid threat assessment without information overload, decentralised command execution.	Expertise in decision-making at tactical levels in real-time based on the decision support system output.	Crisis simulation and war games.
3.	Asymmetry and Unpredictability	Adaptive thinking in grey and hybrid situations.	Hybrid warfare tactics deal with unconventional threats.	Training in ambiguous and dynamic environments.
4.	Network-Centric and Coordinated Operations	Exchange of data and information and collaborate in problem-solving.	Joint operations planning, battlefield live and virtual networking.	Multi-force integration exercises.
5.	Psychological and Cognitive Warfare	Influence operations, counter-disinformation, develop empathy, collaboration, and intuition.	Psychological operations (PsyOps), under high stress conditions.	Red teaming, cognitive warfare scenarios.

S. No.	Future Warfare Capability	Skills Required	Knowledge Required	Experience Gained Through Training
6.	Greater Autonomy in Execution	Independent problem-solving, tactical leadership.	Mission command philosophy, operational autonomy.	Field training exercises with minimal oversight.
7.	Resilience and Adaptability	Stress management, recovery planning.	Operational resilience, risk mitigation.	Training under high-pressure scenarios.
8.	Blurring of War and Peace	Strategic ambiguity handling, crisis response.	Grey zone conflict, hybrid warfare theory.	Exercises involving the gradual escalation of conflicts.
9.	Precision and Minimal Collateral Impact	Target discrimination and ethical decision-making.	Laws of armed conflict, rules of engagement.	Live-fire exercises, ethical warfare training.
10.	Complexity and Interoperability	Immersion with the advanced technologies, Cross-cultural teamwork, and inter-agency coordination.	Exploitation of state-of-the-art equipment, International security policies, and joint force doctrine.	Joint and multinational training operations.

Table 2. Future Warfare Capability and Training Attributes. Source: Author

Training for future warfare involves acquiring complex skills and advanced knowledge, besides operating in a joint environment. The training outcome must aim to impart specific skills, knowledge, and experience to joint warfighters through targeted training. From Table 2 above, the following is a summary of skills that a joint warfighter must acquire:

- **Digitalisation and Technological Literacy:** The joint war fighter must know the technology domain and its interconnectedness with various domains and their interactions. The war fighter must proficiently navigate the maze of digital technologies and use them to create desired military effects. The following imperatives must be considered for training:
  - Awareness of technology and its utilisation aspects.
  - Knowledge of one's domain and awareness of other domains.
  - Network architecture, information exchange and access controls.
- **Cognitive Skill Proficiency:** Developing the mental capacity to arrive

at reasonable and ethical decisions with many inputs under a dynamic situation is a skill that will be required in future warfare. The cognitive ability development in joint war fighters is achieved through immersive extended reality training, gaming, and man-unmanned teaming. The imperatives for training are:

- Decision-making in an information overload situation.
- Critical thinking and adaptability to evolving situations.
- Discern the fake input from the real input.

The topics/ subjects as given in Table 3 could be introduced to the joint war fighters through applied learning and experiential learning for advanced knowledge and improvisation. Advanced-level expertise on the topics/ knowledge could be imparted based on the individual's aptitude, ability to absorb the knowledge, and doctrinal requirements.

S. No.	Topic	Learning Level	
		Applied	Experiential
1.	AI and Machine Learning Algorithms	✓	×
2.	Robotics and Automation	✓	✓
3.	Quantum Computing, Cryptography and Post-Quantum Cryptography	✓	×
4.	Decision Support Systems	✓	✓
5.	Data and Information Fusion	✓	✓
6.	Computer Vision	✓	✓
7.	Communication and Data Networks- All domains	✓	×
8.	Cybersecurity	✓	✓

Table 3. Topics for Applied Learning and Experiential Learning. Source: Gilli, A., Gilli, M., and Grgić, G. (2025). NATO[18] URL: https://www.tandfonline.com/doi/full/10.1080/01495933.2024.2445491

SPECIFIC JOINT TRAINING OUTCOMES

Having seen the training attributes for future warfare, various subjects mentioned earlier in the paper for joint training are further developed. Each subject focuses on the joint warfare scenarios and expected capability. Traditional joint training approaches are restrictive for AI-driven combat, cyber warfare, multi-domain operations, data-driven decision support systems, and space operations, as the subjects are complex and inter-disciplinary. The trainees develop a barrier to accepting the discourse on the subjects, as the trainees do not immediately see the utility of the subjects. Simulation and gaming must be practised to help the trainees cross the barrier. Advanced technologies of extended reality,

simulations, and blockchain must be extensively used to impart joint training. Some important aspects are covered below:

- AI-driven Personalised Military Training for imparting joint training across multi-domains helps acquire the basic skills and knowledge to meet the individual service's learning pace and role in joint operations. DARPA's adaptive learning systems are an example of AI-driven personalised military training.
- Extended Reality (XR) training encompassing virtual, augmented, and mixed reality techniques provides immersive training, creating joint training situations. The training enhances situational awareness, tactical decision-making, and the feeling of the equipment/operations. The US Army's IVAS (Integrated Visual Augmentation System) is an example that creates high-risk combat scenarios.
- Wargaming and AI-driven simulations enable joint warfighters to immerse themselves in the different tactical scenarios and assess the validity of their responses in real-time. Such as immersive experience develops and asses the cognitive skills of the war fighters and thus preparing them for dynamic combat environments.
- Cyber Warfare and Ethical Hacking Training is essential to defend critical information infrastructure, prevent data breaches, and execute cyber operations. NATO Cyber Security Exercises and Israel's Cyber Gym are some examples. The training enhances cyber resilience, electronic warfare capabilities, and digital defence strategies.
- Space Warfare and Satellite Operations Training in surveillance, missile defence, and communications and space warfare is critical. The training prepares the joint war fighters to handle the threats from the space/ near space domain.
- Gamification of Military Training enhances engagement, improves strategic thinking, and makes training more effective. Improves problem-solving, decision-making, and battlefield strategy formulation.
- Digital Twins for Battlefield Readiness creates real-time battlefield replicas to train, test strategies, and predict outcomes without deployment. The technique reduces training costs, enhances decision-making, and provides real-world combat readiness.

DISCUSSION

Technology will drive future warfare. The battlefield will be overwhelmed with gadgets that extend the joint warfighter's depth and breadth of situational awareness. The decision support systems will assist the warfighter in sifting

through the myriad information provided to him at the aural, visual, and cognitive levels. The information may be authentic or malicious. The decision dilemma will give way to the cognitive dilemma. The shortened OODA loop affords little reaction time for the joint warfighter. The uni-domain, multi-domain or all-domain will result in a domain-agnostic warfare, where a joint warfighter's offensive action in one domain will create a first-order military effect in another unrelated domain. Higher-order effects will be far more impactful and unintended than first-order ones. The above narrative, though futuristic, is viable. The training must prepare the joint warfighter to survive the stated operational environment.

While the joint fighter must be trained on technologically advanced war equipment and cognitive skills, the joint fighter must be grounded in the foundational values and abilities. The cognitive dilemma that the war fighter will face often in future warfare must be overcome by the foundational values and skills that differentiate humans from machines, empathy, collaboration, intuition and judgment.[19] The warfighter must depend on foundational values to survive future wars and avoid decision fatigue. The training must strengthen these attributes in a joint warfighter and encourage their applications in high-stress and dynamic situations, volatile, uncertain, complex and ambiguous.[20],[21] Such a training will ensure that warfare control does not drift from humans to machines, from ethical to unethical, from responsible to unaccountable application of military effects.

The future warfare capabilities will be effective only if the technologies have diffused to an extent that the doctrine and tactics are aligned entirely to exploit the full potential of the technologies. The training of the joint warfighter to develop suitable skills must follow the doctrinal principles, beliefs and guidelines. The joint doctrine must be updated for future warfare. The training doctrine must evolve the various patterns to absorb the technologies of future wars.

The need is to fight future wars in an integrated and joint environment. The joint doctrine has laid out a broad perspective towards training for battle in an integrated and joint environment. The joint training doctrine now must elaborate on the training needs as brought out in the paper. Advanced training concepts can bring the joint warfighter's skill level in line with the aspirations of the joint doctrine. A US Army War College team conducted a study between October 2022 and May 2023 to answer the question "What will Intelligentised warfare look like in 2035, and what skill sets will leaders need to win in this environment?".[22] The study brought out several recommendations that range from pragmatic to fantastical. Whether the study report will be accepted by the planners/ futurists is a different aspect. But such a study unleashes the imagination and prepares the fertile mind to start the training for future warfare.

RECOMMENDATIONS

Advanced technologies in future warfare require advanced training techniques to understand the employability of the technologies, harness the maximum potential of the technologies and develop counter techniques to technologies. Traditional joint training techniques need to be augmented and, if need be, give way to advanced techniques. The following recommendations are made for the joint training for future warfare:

- Joint doctrine document (Joint Training Doctrine JP-02/2017, HQ IDS) may include a section/chapter to include the preparation and training for future warfare, covering the training attributes and outcomes.
- Advanced training/education technologies may be adapted to meet the joint training scenarios/simulations to achieve skill upgradation and technological proficiency.
- A joint services task force may be constituted to recommend an optimum training architecture for future warfare. Curriculum, content, delivery modes, aids, and outcomes must be among the architecture deliverables.
- A project may be commissioned to evolve the joint training needs for future warfare with a time perspective of 25 years. Technologies, capabilities, training attributes, patterns, and a broad scope of the content must be project deliverables.
- Learning techniques in the Joint Services Training Institutes of the Indian Armed Forces to move towards applied and experiential learning to imbibe complex future warfare skills, knowledge and experience.

CONCLUSION

The future warfare will be technologically advanced and unprecedented in terms of the skills and knowledge required to fight and win jointly. The training needs for future warfare should be derived from the 4S model. The training needs thus derived require a novel approach different from the traditional one, such as digitalisation and technological literacy, and cognitive skills proficiency. A mission-mode approach is required to address the changes to the training doctrine to align it with future warfare. Training/ education technology must be harnessed to fight future wars in an integrated environment.

❖❖❖

AVM (Dr) M S Rama Mohan, VSM (Retd) is a qualified Flight Test Engineer and an airpower technologist. His areas of interest include emerging technologies, air power, flight testing and strategic trade controls.

NOTES

1. Raphael S. Cohen et al., "The Future of Warfare in 2030: Project Overview and Conclusions," RAND, May 11, 2020, https://www.rand.org/pubs/research_reports/RR2849z1.html . Accessed on 05 Apr 2025.
2. Joint Doctrine Indian Armed Forces, 2017, HQ IDS, Chapter 5, Sec VII, pp 46-47.
3. Joint Training Doctrine-JP-02/2017, HQ IDS, Chapter I and Chapter II, cover mostly the organisational and operational part of the joint training. The doctrine is silent on training methodology, content, and delivery. Considering that the doctrine was published in 2017, the scope, range and depth of the training for future warfare may not have been enshrined in the doctrine.
4. Njall Trausti Fridbertsson, "Technological Innovation for Future warfare", 025 STCTTS 22 E rev.1 fin – Original: English – 20 November 2022, https://www.nato-pa.int/download-file?filename=/sites/default/files/2022-11/025%20STCTTS%2022%20E%20rev.1%20fin%20-%20THE%20FUTURE%20OF%20WARFARE%20-%20FRIDBERTSSON%20REPORT.pdf, Accessed on 05 Apr 2025; Rajeswari Pillai Rajagopalan and Sameer Patil, eds, Future Warfare and Critical Technologies: Evolving Tactics and Strategies, New Delhi: ORF and Global Policy Journal, 2024,https://www.orfonline.org/research/future-warfare-and-critical-technologies-evolving-tactics-and-strategies, Accessed on 05 Apr 2025.
5. Thea Riebe, Anja-Liisa Gonsior, Lilian Reichert & Christian Reuter (07 Dec 2024): Envisioning Human-Machine Interaction in Future Warfare: Defence Industry Narratives on Human Control of Autonomous Weapon Systems, Global Society, DOI:10.1080/13600826.2024.2436966, Accessed on 05 Apr 2025.
6. Michael P. Ferguson, "Ghost In The Machine: Coming To Terms With The Human Core Of Unmanned War", The Scholar, Vol 8, Issue 2, Spring 2025, Texas National Security Review, University of Texas at Austin, pp 27-46, https://tnsr.org/2025/03/ghost-in-the-machine-coming-to-terms-with-the-human-core-of-unmanned-war/, https://hdl.handle.net/2152/63836, Accessed on 05 Apr 2025.
7. Ian Sullivan, Matthew Santaspirt, Luke Shabro, Marie Murphy, Mad Scientist Conference: Learning in 2050, Georgetown University, 9 August 2018. https://community.apan.org/wg/tradoc-g2/mad-scientist/m/learning-in-2050/256954, Accessed on 05 Apr 2025.
8. Joint Training Doctrine -JP-02/2017, HQ IDS, pp 10.
9. Exclusive: Iran hijacked US drone, says Iranian engineer, Scott Peterson Staff writer, Dec. 15, 2011, The Christian Science Monitor.
10. Gilli, A., Gilli, M., & Grgić, G. (2025). NATO, multi-domain operations and the future of the Atlantic Alliance. Comparative Strategy, 44(1), 73–91. https://doi.org/10.1080/01495933.2024.244549 1. Accessed on 05 Apr 2025.
11. Lt Gen Ashok Bhim Shivane, "Future Wars: Emerging Perspective", Rakhsa-anirveda, 08 Jul 2024, https://raksha-anirveda.com/future-wars-emerging-perspective/ . Accessed on 05 Apr 2025.
12. Kent, Randolph. (2015). The future of warfare: Are we ready?. International Review of the Red Cross, 97(900), pp. 1341–1378. doi:10.1017/s1816383116000412. Accessed on 05 Apr 2025.
13. Cole Livieratos, "From Complicated to Complex: The Changing Context of War",Modern War Institute, West Point, 14 Jun 02, https://mwi.westpoint.edu/from-complicated-to-complex-the-changing-context-of-war/ . Accessed on 05 Apr 2025.
14. Mark GilChrist, "Emergent Technology, Military Advantage, and the Character of Future War", Strategy Bridge, 26 Jul 2018, Emergent Technology, Military Advantage, and the Character of Future War. accessed on 05 Apr 2025.

15. Ibid 1.
16. “Attacks on Saudi Oil Facilities: Effects and Responses”, CRS Insight, 01 Oct 2019, Congressional Research Service, IN11173, https://crsreports.congress.gov, Accessed on 05 Apr 2025.
17. Robert A. Johnson, "Predicting Future War," Parameters 44, no. 1 (2014), pp 69, doi:10.55540/ 0031-1723.2801, Accessed on 05 Apr 2025.
18. Applied Learning is a structured and guided learning process that generally happens in a classroom environment. The learning is prescribed for imparting functional knowledge of combat systems, such as pilot training in the simulator. Experiential learning is a real-world-based, self-paced learning process. Military commanders participating in war games and exercises learn advanced concepts through experience. Experiential learning is prescribed for advanced training and for innovation/ improvisation
19. Nandan Nilekani, “Leadership in AI”, Microsoft AI Tour, https://www.youtube.com/@microsoftindia/videos, Accessed on 05 Apr 2024.
20. Sorin Topor, “The Future of Warfare in the Volatility, Uncertainty, Complexity and Ambiguity Context,” Revista Academiei Forţelor Terestre 29, no. 2 (June 1, 2024): 227–36, https://doi.org/10.2478/raft-2024-0024 . Accessed on 05 Apr 2025.
21. The VUCA framework, proposed by Bennis, Warren, Nanus, and Burt in 1985 and later adopted by the US Army War College in 1987 to describe the post-Cold War situation, is applied. The future warfare will be volatile, uncertain (unpredictable), complex and ambiguous. The VUCA framework proposed for strategic leadership is still relevant in so far as the characteristics of future warfare are concerned and is adopted to describe future warfare. Cross-domain strategies and warfare methodologies are added to the VUCA framework to describe future warfare in its entirety. Further, the scope of volatility in the VUCA be expanded to mean the speed of operations and 5 Vs with which the big data is generated and processed in future wars. Further reading Bennis, Warren ; Nanus, Burt (1985). Leaders: Strategies for Taking Charge . Harper & Row. ISBN 9780060152468 .Strategic Leadership (1985).A complete history of the terms since its first usage in US Army documents cn be seen at U.S. Army Heritage and Education Center (February 16, 2018). "Who first originated the term VUCA (Volatility, Uncertainty, Complexity and Ambiguity)?" . USAHEC Ask Us a Question. The United States Army War College.
22. COL Leslie Carlson, et al, “Techno Warfare 2035”, USAWC, May 2023, https://madsciblog.tradoc.army.mil/450-what-skill-sets-will-leaders-need-for-warfare-in-2035/, Accessed on 05 Apr 2025.

❐❐❐

ADVISORY BOARD & EXECUTIVE COUNCIL CENJOWS

Printed and published by Maj Gen (Dr) Ashok Kumar, VSM (Retd) on behalf of Centre for Joint Warfare Studies (CENJOWS), 301, B-2 Wing, 3rd Floor, Pt Deendayal Antyodaya Bhawan, CGO Complex, Lodhi Road, New Delhi-110003, and printed by Adroit Publishers, New Delhi, India.

Editor: Maj Gen (Dr) Ashok Kumar, VSM (Retd)

CENJOWS

CENTRE FOR JOINT WARFARE STUDIES

(Web site: https://www.cenjows.in - Email: cenjows@cenjows.in / cenjows@yahoo.com)

APPLICATION FOR MEMBERSHIP FOR INDIVIDUALS/ORGANISATIONS

(EFFECTIVE WEF 01 MAY 2025)

(TO BE SUBMITTED ONLINE ONLY, ONLY APPLICABLE DETAILS AS PER CATEGORY TO BE FILLED)

To,
The Director General
Centre for Joint Warfare Studies (CENJOWS)
301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi-110003

Dear Sir,

1. Please register me as a **Life☐/Annual☐** member of the Centre for Joint Warfare Studies (CENJOWS).

2. I undertake to abide by the Rules and Bye Laws of the Institution.

3. **Life Membership/ Annual Membership (Individuals).**

(a) **Common to All.**

(i) Name in full (in Capitals)……

(ii) **Address:-**
Office/Unit……

……

Pin Code …… Phone No …….…….... Mobile No. ……..

Email ……

(iii) **Permanent/Residential Address**

……
Pin Code…….. Phone No …… Mobile No……..……

Email ……..

(b) **Additional Inputs (in case of Serving/Retired Defence Personnel)**

(i) Parent Service Army/Navy/Air Force/Civil Services ……
(ii) Personal Number…….…… (iii) Rank/ Designation……
(iv) Name in full (in Capitals) …… ……..
(v) Decorations ……..…….... (vi) Appointment ……
(vii) Date of Commission ……
(viii) Date of superannuation……
(ix) Date of Seniority (if different form date of Commission) ……..
(x) Date when qualified in DSSC/TSOC ……..

(c) Areas of expertise or interest:-

(i) ……..……

(ii) ……..

(d) Any other information that may be of interest to the CENJOWS (including important exposures):-

……
……

(e) Name of College and University where Studying (in case of students) ……

……..

(f) The current membership rates for Individuals are as under:-

(i) Life membership:-

(aa) Serving/Retired Officers (For 20 years) - **Rs 5000/-**

Note: 50% discount will be given to the following categories:-

(aaa) Officers qualifying in DSSC /TSOC if apply prior to completion of the course. All service HQs will be intimated for this provision.

(aab) Officers applying within two years of commissioned service.

(aac) Officers applying within two years of superannuation.

(ab) Civilians (For 15 years) - Rs 15,000/-

(ii) (aa) Annual Membership (For one year) - Rs 1000/-

(ab) For University/ College Students (For one year)- Rs 500/-

(iii) Institutional Membership (For 15 years):-

(aa) Non Corporates Membership - Rs 30,000/-

(ab) Corporates Membership - Rs 50,000/-

(g) Proof of my identity (Copy of passport/Voter ID Card/Adhaar Card) is attached for approval of membership **(JPG/ PNG Format).**

(h) Two stamp sized photographs for Life membership card (Individuals) **(JPG/ PNG Format)**.

(j) Payment by NEFT/ Digital as per details given below:-

Name of Organisation	: CENJOWS
Bank Name	: CANARA BANK
Branch Address	: **KASHMIR HOUSE**, NEW DELHI-110011
IFSC Code	: CNRB0019122
A/c Type	: SAVING
A/c No.	: 91222160000046

(Please attach the proof of payment)

4. **Institutional Membership (Institutions/ Organisations)**
(Provision of Lifetime Membership only)

(a) The particulars of our Institution/ Organisation are given below:-

(i) Name of the Institution/ Organisation ……

(ii) Nature of Activity/ Scope of Work ……

(b) Address:-
……..……..……..
……
Pin Code …… Phone No ……..... Email……

(c) Name of Head of the Institution ……..

Phone No **……** Mobile No ……....Email ….....

(d) Name of Administrative Officer (for Correspondence purposes) ……
……
Phone No …… Mobile No ……. Email ……..

(e) Areas of expertise or interest:-

(i) ……..……
(ii) ……..
(iii) ……..

(f) The current membership rate for Institutional Membership are (For 15 years):-

(aa) Non Corporates Membership - Rs 30,000/-

(ab) Corporates Membership - Rs 50,000/-

(g) Payment by NEFT/ Digital as per details given below:-

Name of Organisation	: CENJOWS
Bank Name	: CANARA BANK
Branch Address	: **KASHMIR HOUSE**, NEW DELHI-110011
IFSC Code	: CNRB0019122
A/c Type	: SAVING
A/c No.	: 91222160000046

(Please attach the proof of payment)

(h) Two membership cards will be issued to the Institution/Organisation.

5. I Certify that the details forwarded above are correct. I shall follow the amended rules and regulation as intimated.

Place : **……** Yours faithfully,

Date : **……...**

FOR OFFICE USE ONLY

Identity Card/Document No: **.....** To be verified by Secretary (Secretary to speak on telephone to confirm the credentials).

New Delhi

Date …….. Secretary, CENJOWS

Accepted/Rejected

Membership Number **.....**
(Interaction to be held with DG, CENJOWS for Institutional Life Time Memberships)

Place: New Delhi

Date: …….. Director General CENJOWS
