MULTI DOMAIN OPERATIONS: CREATING CAPABILITY OVERMATCH

Lt Gen (Dr) N B Singh, PVSM, AVSM, VSM (Retd)

Abstract

Multi-domain operations (MDO) encompass the synchronized employment of land, sea, air, space, and cyberspace capabilities to achieve strategic and operational objectives. It involves a holistic approach to warfare, integrating different domains to create a unified and synergistic effect. MDO emphasizes the interconnectedness of these domains, recognizing that adversaries can operate across multiple environments. This concept necessitates joint and combined forces, advanced technology, and innovative strategies to counter complex threats and achieve decisive outcomes. The Indian military has to strategize and aim at generating military effectiveness by embracing the inter connectedness of different domains. Leveraging these capabilities synergistically it can gain a decisive advantage in any conflict in the Himalayas.

Introduction

The war in Ukraine has entered the third year and both sides continue to come out all guns blazing after periods of consolidation operations that enable regenerating and repositioning of military capabilities. The war has become an industrial scale war, demonstrating the power of technology to generate capability overmatch and create decision dilemmas for the adversary. One crucial lesson is the emergence of connectivity as an indispensable military resource. Forces without connectivity could be constrained to suffer enormous costs in blood, hardware and morale. Mass, a fundamental principle of war need not be achieved through concentration of forces but also through delegation and decentralisation. The idea of combined arms is going down to lower formations and units where soldiers will need to possess more initiative, technical knowledge and skills. A small team with satellite link can see and strike targets that were once the preserve of higher echelons. Due to increased battlefield transparency, troops will have to be constantly on the move, disperse to survive and hence demands for physical and mental toughness will be extreme. Militaries without the resilience to absorb massive losses of men and material may not remain viable on the battlefield. Ukraine war is teaching all militaries to strategize and train differently.[1]

The Indian military is confronted with an adversary that is aiming and arming to achieve technological parity with the mightiest military. It is modernising it forces at a fast tempo, attempting to transform into a world class force. It is refining its command and control structures to conduct dynamic, fast tempo joint, multi domain operations. Its military industrial base is home grown, resilient capable of introducing new technologies in the stride and maintaining industrial surges that could wear out the enemy. These technologies are enabling sharing of information, intelligence, battlefield, logistics, weather predictions on robust, survivable communication links to enhance situational awareness that could facilitate decision making and buoy up military effectiveness. The emergence of a Strategic Support Force responsible for electronic warfare, space and cyber space demonstrates the growing focus of the adversary on conducting multi domain operations (MDO).[2]

Regional Developments

The security landscape in the subcontinent is historically prone to political and military stand off by our adversaries and could result in blunting military effectiveness in multiple domains particularly cyber, information and electromagnetic spectrum (EMS). MDO are conducted across multiple domains and contested spaces to neutralise an adversary's warfighting capabilities by creating several dilemmas at operational and tactical levels through application of capabilities and resources across domains (land, air, maritime, space, cyberspace and electromagnetic spectrum) to achieve military effectiveness and create an operational overmatch. Key components of MDO are :-

- **Integration.** MDO emphases seamless integration of capabilities across different domains, breaking down of organizational silos and fostering collaboration amongst branches and units.

- **Convergence.** MDO seeks to achieve convergence where actions in one domain complement and reinforce actions in other e.g. air strikes may be coordinated with EW and cyber attacks to degrade enemy's defences before a ground attack.

- **Information Assurance.** Information superiority is crucial in MDO. Effective collection, analysis and dissemination of information enable commanders to make informed and timely decisions giving the forces a decisive edge.

- **Agility and Adaptability.** MDO requires flexibility and adaptability to respond rapidly to changing circumstances. Commanders must be able to shift resources and adjust tactics dynamically to exploit emerging opportunities or counter adversary actions.

China is aiming to achieve near technological and military parity with the US and has the economic and industrial base to make this vision a reality. It has repeatedly demonstrated the intent to dominate, challenge its neighbours and fracture existing cordial relations between them. It continues to make investments in India's immediate and strategic neighbourhood in order to deny access, breed ambiguity and bring smaller nations under its influence. It is already made rapid strides towards building a modern, world class military that can project power universally. In its pursuit of informatization considered to be an important lever of modernisation, it has developed unique capabilities in the fields of microelectronics, AI, quantum computing, EW, EMP, space and counter space technologies. It has streamlined processes of acquiring, transmitting, analysing and employing information to conduct joint military operations in multiple domains and developed capabilities to provide field commander near real-time shared situational awareness that would enable quick and unified efforts to exploit fleeting opportunities. It expects future wars to be fought outside its geographical borders encompassing maritime domains too.[3] For the Indian military it will prudent to use these developments as a pacing threat to develop own capabilities. Vulnerable fault lines have to be identified and addressed else these will be the first principal targets. The war in Ukraine has amply demonstrated this.

The PLA has moved ahead with the creation of theatre commands in place of regional commands and established joint operations command centre manned by persons from all services. It is working towards expanding the operational environment in a number of ways; time, domains, geography and constituents. The battlefields stands expanded with the inclusion of cyber, space, information and electronic warfare (EW) becoming key components of their operations. The battlefield has expanded geographically too with increased ISR and deep strike capabilities. Its capabilities to collect information on military and other strategic targets, detect changes in force postures, assess predictability in conduct of military operations, special operations, signal intelligence, survivable communication networks and sensor shooter links are rising through a well crafted modernisation plan backed with liberal funding.[4]

Its well developed indigenous defence industrial base (DIB) rolls out increasingly sophisticated platforms that give it an escalation advantage in not only geographical terms but also duration of conflict, constraining its adversaries to react and divert resources to address the capability overmatch. Take the case of the light tank. The Indian Army was the first to move light tanks into J&K region in 1948 (Zoji La) and 1962 (Chushul), yet over the years it never could foresee the advantages of deploying a bespoke light tank for its forces till the positioning of the Chinese light tank Type 15 at Line of Actual Control (LAC). It can conduct unconventional warfare to generate instability through proxies, activists, terrorists and subverts. Its capabilities in the information, cyber and space domains are being repeatedly honed through pilot runs and periodic launches to assess effectiveness. These actions create ambiguity and inhibit retaliation due to denial about origin.

Information Assurance

What the Adversary can do

The all round capability development of PLA has given operational approaches to it to fracture and severely impede the warfighting abilities of any force that still operates on predictable and templated operational concepts; specially those based on attrition oriented, slow tempo trench warfare. The emphasis on winning high tech wars has led to creation of core military capabilities in the following areas:--

- **Power projection** – using a combination of long range air power, aircraft carriers, bases and economic connectivity through BRI initiative.

- **NBC Forces** – Possesses full spectrum expertise, combat units and equipment for such operations. Nuclear forces are being optimised to enhance peace time readiness levels and responsiveness.

- **Space and Counterspace** – Continues to develop capabilities to effectively use space based systems for civil and military use and deny an adversary the use of space based assets during crisis and conflicts.

- **Cyberspace** – Has invested in developing cyber reconnaissance, cyber attack and cyber defence capabilities for controlling the information domain comprising not only networks but also electromagnetic spectrum (EMS), intelligence and psychological domains.

- **Deception** – Designated as a form of combat support it aims to create asymmetric advantages, achieve technological surprise and paralyse the adversary through deception.

- **Logistics** – Originally organised on the Russian push model of logistic support, it is being transformed into a precision logistic support system that is agile, digitised, based on high speed transportation with skilled human resource to support high tempo operations.

- **Defence Industrial Base** – This perhaps is the most significant capability of the People's Liberation Army (PLA) that gives it the wherewithal to aspire for technological parity with US and in the bargain technological dominance in the region. Its network of science cities, industrial parks and high tech zones can provide the industrial and maintenance surge needed for prolonged combat operations to wear out an adversary. The growing cooperation between China and Russia could help plug gaps in industrial capabilities of its DIB. This provides strategic assurance, consolidates national resilience and the ability to pursue its national security strategy both at regional and global level.

- **Underground Assets** – A versatile military underground assets programme has been pursued to create hardened facilities to protect command and control centres and missile assets. Such a technologically advanced tunnelling and construction programme can be used at LAC to throw up new capability surprises for the Indian military like the reported employment of Eletro Magnetic Pulse (EMP) weapons to disable men and machine during the LAC stand off.

The extent and spread of this planned modernization have given PLA a Western style command and control capability in which theatre command can develop varied force packages to meet mission needs. The Strategic Support Force is equipped for operations in the EW, space and cyber domains. In summary, close integration of information warfare, unconventional actions and conventional warfare capabilities gives PLA a very strong competitive advantage and if employed with balance it provides the ability to calibrate the tempo of conflict and exploit weaknesses of adversary as these unfold. Its cross domain synergy can give it layered options across domains enabling it to observe and strike vulnerabilities both during close and deep manoeuvres.[5]

Own Response: Incubating Military Effectiveness

Military effectiveness refers to the competitive advantage that a military possesses over its adversary i.e. the operational and technical overreach, the agility and depth with which a military can paralyse its adversary in all warfighting domains. It entails the performance of similar military activities better than the adversary. Highly skilled human resource, technological superiority, ability to innovate on the fly, new warfighting concepts are key to military effectiveness, as these enable launching of technological surprise. Militarily effective forces possess the resilience to overcome new threats posed by a determined enemy.

To be able to in demonstrate military effectiveness to stymie the intentions of an adversary the military needs to look at force postures much beyond mirroring. It has to create capabilities across most domains; critical being survivable communications and sensor shooter links in a contested EM environment. It has to develop battle procedures that very effectively utilise the terrain to its advantage. It has to be agile enough to integrate capabilities in all domains and be prepared for deep operations that go beyond the LAC. Deep operations will be needed to ensure effective battle field interdiction of extended lines of communications and inhibit logistic sustainment. Some Key Response Areas (KRAs) could be:-

Integrated Capability Development

The fundamental requirement for the Army is to develop combat capabilities in multiple domains to stymie the adversary’s intentions and manoeuvres, neutralising its capability overmatch and creating multiple dilemmas. The IBGs need to be versatile enough to integrate, synchronise and converge all elements of combat power including space, cyber, EMS, information to carry out Blip Krieg alongside physical manoeuvres. In the face of any capability surprise sprung by the adversary, real-time situational awareness using a constellation of low earth orbit satellites (LEOS) could provide communication connectivity and intelligence to forward troops in the form of a live feed. FPV drone/ precision rounds available at IBGs could be then dispatched to neutralise the threat. Data driven combat can add precision and speed of the kind frontline troops have not been used to. Electronic Warfare (EW) could scale up survivability.

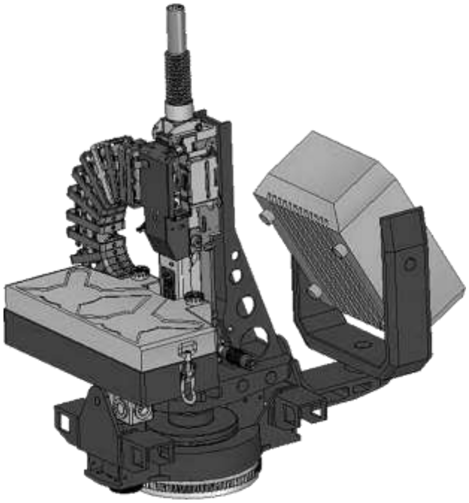
FPV Drone: Despatching an Explosively Formed Projectile

A special focus on countermeasures that denude capabilities of drones and precision weapons like EW is needed. Sensors, precision weapons and the connecting networks all can be rendered ineffective by EW as the War in Ukraine has shown.[6] Excalibur rounds, drones and missiles have been largely neutralised by Russian EW. However the flop side is that jamming can impact own communications and also interfere with other electronic devices. So the attempt is to enhance encryption and introduce malicious software in the drone communication links, use other guidance means like terrain matchingetc. In summary the side that achieves EMS supremacy and can prosecute Blip Krieg along side Blitzkrieg will retain the competitive advantage. EW and Cyber warfare have now become indispensable.

Integrated Capability Deployment

Operational Innovation

Ukraine war has demonstrated how even infantry men in positional defences have become vulnerable to drone warfare. What happens to trench warfare that has been so effective employed by the Army in the mountains in the past. Even a small body of men can be effectively found by a drone if the stay at a place for too long. It can then attack the target or bring in precision fires. Agility and dispersion could help but would create gaps in the defences. Hence positional defence will have to be multi layered employing technology. A technological counter using platoon weapons needs to be improvised at the defended locality level. Jamming as an anti drone measure at times may not be feasible. Global Positioning System (GPS) can be supplemented by signals from LEOS, or ground based communication, terrain matching or magnetic field navigation to overcome jamming.[7] A possible kinetic solution using an AGS enabled device can be an answer. A radar can be integrated to the grenade launcher to create a 150-200 metre saturation area around the trenches to destroy anti personnel drones. Similar improvisations need to be developed at platform level for artillery batteries and tank squadrons to effectively counter adversary's capability overmatch at tactical level.



AGS based Anti Drone System

Combat Force Regeneration

An issue that normally gets overlooked by the Army in prolonged forward deployments is equipment capability degradation when platforms are warehoused and operated in the open. It is one thing to move heavy weapon platforms in close proximity of the LAC and another to keep them going once they arrive. The US Army maintained an operation readiness rate (ORR) of 95% in Iraq and operational availabilities below 90% had commanders being questioned. Such high rates were feasible mainly because of its large indigenous DIB and a very agile logistics delivery system.[8] In Ukraine both sides are struggling to sustain equipment readiness rates of above 50% as the density of ISR and firepower delivered by FPV drone has created a sticky battlefield with very high attrition.[9] The development of the domestic defence manufacturing industry and local supply chains of vintage platforms has to be taken up on a war footing to avoid a scramble for spare parts and ammunition in times of need. In the extremely difficult terrains of Himalayas, equipment stress is much more intense than the OEMs expectations and could silently erode readiness of units. New norms for wartime sustainment of platforms have to be evolved. A forward sustainment base (FSB) for in service engineering needs to be created in Ladakh. Two and a half decades ago this outcome had surfaced during combat exploitation of Bofors, but the localised nature of the conflict did not impact the crisis adversely. Hence no lessons learnt. Continuous combat force regeneration through seamless integration between Army's FSB, Navy, IAF, DPSU, OEMs and MSMEs has to be aimed at, to support MDO at the LAC since losses of equipment both due to terrain and battle damage could be overwhelming.

Distributed Logistics

One important lesson in Ukraine has been that logistics is too important a subject to be left to generalists. The push or pull model needs to be replaced by distributed logistics. In Ukraine, the Russian Army depended on logistic sustainment from rear areas and mainland to move food, fuel, ammunition and spares by rail, road and air. It then had to be transported in soft skinned fuel carriers and logistic vehicles. Troops that moved South from Belarus towards Kiev in Feb 2022, had the supplies cut off and were destroyed piecemeal with artillery and other fires.[10] The use of HIMARS rockets later on by Ukraine to target fuel and ammunition replenishment areas threw a spanner in the wheels of the Russia's warfighting machine,starving it of fuel and ammunition. This enabled Ukraine to launch successful counter offensives in Kherson and Kharkiv.[11] Ukraine's supply lines have proved to be more resilient, reliable and agile may be due to the fact that it fighting the war on its own territory[(7)] ;something that the Indian military has to take note and work upon. Ukraine has managed to support its diverse arsenal of tanks, guns, rockets and missiles by pioneering new forms of operational sustainment. 3D printing of spare parts, condition based monitoring of key systems, use of algos to decide what to push and when are some innovative procedures.[12] Stocks need to be positioned well forward by creation of FSBs. Deep engineering support and agile logistics is sine qua non for the kind of long duration combat, an intelligent, technologically advanced adversary can resort to. The repeated attempts to optimise 'tooth to tail ratios' by downsizing the tail can have serious consequences --- loss of face of a vaunted force. Logistic has had a stellar role in military history—the Army needs to re- learn this.

Addressing Pre-emption

The Indian military has a history of repeated pre-emption by the adversary both at LAC and LC. Today the bandwidth to deliver surprise over an expanded battlespace has increased covering cyber, EMS, space, information, NBC besides classical domains. It has become increasingly feasible for adversaries to develop counters to known capabilities. Dependence on foreign systems has created new vulnerabilities, as specifications get shared if similar systems are acquired by others e.g. Sukhoi, S400, T90/T80 tanks. Counters get developed in quick time as they no longer have to wait for systems to be deployed and learn how to counter capabilities. This fast-tracked cycle of measure/countermeasure/ counter-countermeasure will continue to add surprise to future conflicts. Ukraine's war at sea has succeeded due to technological surprises.[13] In the new era of aspiring power competition, PLA could employ many layers of stand off in multiple domains to deliver surprise. Non- kinetic effects like disruption of communications, denial of tracking & navigation capabilities, fakes, information overload could precede kinetic operations. Achieving technological parity in game changing technologies would be an enabling step towards a comprehensive MDO capability.[14] This calls for employment of the military's intellectual firepower to think beyond the algorithm and evolve doctrine, organizations, training, leadership, systems, human resource and processes for sustained military effectiveness. Exercises must follow thereafter, replicating the future battlefield -- expansive, lethal and hyperactive with increased strategic ambiguity and entropy. The capability of early warning and launching own surprises across the Himalayas must be silently incubated and honed

Total War

Future engagements in the sub continent could be remain at the diplomatic, information, economic, industrial level and escalation to armed conflict may not be the end state. Besides developing unconventional warfare capabilities and synergising, land, air and maritime operations with space, cyber, EMS there is a need to look at two critical area of national resilience; firstly, industrial surge and secondly concept of total war. Besides modernization of hardware and munitions, the industrial base has to gear up to manufacturing combat enabling systems and technologies at a pace that outpace daily losses of platforms or helps regenerate battle damaged platforms. Acquisition process has to become more accommodative towards indigenous solutions even if these are not fully mature using the Buy and Try model so that feed back from the military can help improve performance of indigenous systems. The role of local population in and around the country's borders will be very crucial in future conflicts. Cross society networks and resistance of the kind witnessed in Ukraine can add to national resilience. Smart phones and the available uploads, volunteer hackers, civilian drone manufacturers, commercial imagery providers and AI analysts, can all end up civilianising the digital battle field and add to national effort and military effectiveness.

Conclusion

Future wars in the Indian context could have a very unique dimension. Besides being multi domain, it could have an uncanny resemblance with the war in East Europe. Apart from the fact that most platforms on either side of the LAC are from the Russian stable and hence equipped with similar technologies, the sheer losses of men and material could be very high. This is because of the formidable industrial might of the northern adversary and its ability to deploy large number of formations, hardware and ammunition in the areas of interest. In a stalemate situation, its ability to quickly generate overmatch through its integral industrial base and limited reliance on foreign supplies could be a differentiator. Long duration conflicts with periods of consolidation operations like the one being seen in Ukraine will give advantage to Red and has to be avoided at all costs. In addition, the possibility of Pakistan acting in concert with PLA cannot be ruled out. It could raise the tempo of its unconventional warfare extending it to other parts of the country specially the NE, create ambiguities using automated "bots" to influence domestic and foreign audiences and delay decision and reaction. In short, from our western neighbour one can expect all actions including terrorism, subversion, criminal activities, reconnaissance, information warfare and direct strikes at lines of communication and industrial infrastructure using techint and hardware supplied by China and some others; all in support of a joint strategic objective. With both sides having access to technology, the side with capability to fight in a technologically contested environment is likely to have an advantage. The Indian military has to strategize and aim at generating military effectiveness by embracing the inter connectedness of different domains. Leveraging these capabilities synergistically it can gain a decisive advantage in any conflict in the Himalayas as the terrain is in support. A calibrated force posture with focus on capability consolidation and generation may be better to prevent onset of human and equipment fatigue. Combat resilience, industrial resilience and resilience of the human resource could form the core strands of this strategy.

****

Lt Gen (Dr) N B Singh, PVSM, AVSM, VSM (Retd) is a former DGEME, DGIS and Member Armed Forces Tribunal. He writes on technology related operational subjects, space and green energy initiatives.

NOTES

1 The Intelligence: "Ukraine's War two years on". Podcast by The Economist 23/02/24

2 Defence Intelligence Agency, US Department of Defence , "China Military Power" 2019. www.dia.mil/military-Power -Publications

3 TRADOC Pamphlet 525-3-1, "The US Army in Multi- Domain Operations 2028".Dec 2018

4 Ibid

5 Ibid

6 The Intelligence : "Russia pushes back on Kharkiv". Podcast by The Economists 13/03/24.

7 The Economist, "The Future of War" July 8 2023.

8 "Army Equipment After Iraq"; Lawrence J. Korb, Loren B Thomson, Caroline P Wadhams,2006 Center for American Progress www.americanprogress.org

9 The Intelligence : "Russia pushes back on Kharkiv". Podcast by The Economists 13/03/24.

10 The Economist, "The Future of War" July 8 2023.

11 The Intelligence : "Russia pushes back on Kharkiv". Podcast by The Economists 13/03/24.

12 The Economist, "The Future of War" July 8 2023.

13 The Intelligence: "Stalemate in Ukraine". Podcast by The Economist 02/11/23.

14 Vivekanand International Foundation, "Indian Armed Forces in 2047", Pentagon Press LLP, New Delhi, 2023.

TECHNOLOGY DRIVEN MULTI DOMAIN OPERATIONS (MDO) FOR JOINT WARFIGHTING

Lt Col Gaurav Kumar Singh

"It seems probable that once the machine thinking method had started, it would not take long to outstrip our feeble powers… They would be able to converse with each other to sharpen their wits. At some stage, therefore, we should have to expect the machines to take control." —Alan Turing

Abstract

MDO converges effects across the domains of land, air, maritime, space and cyber to achieve advantage for friendly forces. These domains must incorporate niche technologies for disruptive impact on the battlefield. This article focuses on the impact of niche technologies in MDO and its overall impact on Joint Warfighting. The paper also lays out suggested road map for implementation of niche technology in MDO.

Introduction

The MDO concept of United States (US) is aimed to exploit its technological edge with its adversaries and compensate the developments in Russian and Chinese military capabilities. It unequivocally targets the integrated systems and the anti-access strategies of Russia and China. Similarly, Chinese recognise technology as a determining factor to structure their military science and strategy. China insists on the non-kinetic aspect of