Aligned with the Future

Victory through Joint Knowledge

SYNERGY

Journal of the Centre For Joint Warfare Studies (CENJOWS)

VOLUME 3 ISSUE 2 ISSN: 2583-536X AUGUST 2024

IMPACT OF NICHE TECHNOLOGIES ON JOINT WARFIGHTING

SYNERGY

JOURNAL OF THE
CENTRE FOR JOINT WARFARE STUDIES

Volume 3 Issue 2 Online ISSN : 2583-536X August 2024

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 : 2024
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
Editor : Maj Gen (Dr) Ashok Kumar, VSM (Retd)
(dg@cenjows.in)
Deputy Editor : Dr Ulupi Borah, Senior Fellow
(ulupi.borah@cenjows.in)
301, B-2 Wing, 3rd Floor
Pt. Deendayal Antyodaya
Bhawan, CGO Complex,
Lodhi Road
New Delhi-110003

Editorial Board :
Col AP Tripathi
(secy@cenjows.in)
Col KJ Singh (Retd), Col Coord
(kj.singh@cenjows.in)
Wg Cdr Vishal Jain, Senior Fellow
(vishal.jain@cenjows.in)
Capt (IN) Nitin Agarwala
(nitin.agarwala@cenjows.in)
Dr Ulupi Borah, Senior Fellow
(ulupi.borah@cenjows.in)
301, B-2 Wing, 3rd Floor
Pt. Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi-110003

Secretary : Col AP Tripathi
Publications Manager : Ms Arijita Sinha Roy

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

© Centre for Joint Warfare Studies

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system without permission from the Director General, Centre for Joint Warfare Studies, New Delhi.

Price : **Rs 750/- INR or US 25$**
RNI No: DELENG/2022/82424
Print ISSN : 2583-5378
Online ISSN : 2583-536X

IMPACT OF NICHE TECHNOLOGIES ON JOINT WARFARE

CONTENT

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.

MESSAGE

Technology has been a strategic enabler that has had a revolutionary impact on the conduct of warfare. Wars, from its inception till the middle of 19th Century were fought on a single battlefield. But today, technological advancements have enabled wars to be fought concurrently, displaced by both '**Time and Space**'. Technological innovations have expanded warfare into newer arenas like the space, cyber and the cognitive domains. Yet, it has shrunk the combat environment through real-time net centricity and battle space transparency.

Introduction of new technologies like Artificial Intelligence (AI), Machine Learning (ML), Big Data, Edge Computing, Robotics, Cyber capabilities are heralding new concepts in warfare like Manned – Unmanned Teaming (MUMT), Autonomous and Unmanned Systems and a gradual shift from Net Centric to Data Centric Warfare. The latter will focus on decision superiority during combat than information superiority of the former.

There is an emergent need for our Armed Forces to embrace niche capabilities and remain ahead of the technology curve as these would increasing affect the manner in which Integrated Joint Operations would be conducted in the future. Judicious and timely inclusion of these technologies are a sine qua non.

Contd…..2/-

75 आज़ादी का अमृत महोत्सव

प्रमुख रक्षा अध्यक्ष
CHIEF OF DEFENCE STAFF

The Indian Government and the Services have taken several initiatives to ensure that these niche technologies are not only absorbed but also developed within the country so as to be self-reliant. The involvement of Private industries and entrepreneurs have provided greater boost to this national endeavour.

This edition of '**Synergy**' themed "**Impact of Niche Technologies on Joint Warfighting**", therefore comes at an appropriate time to trigger thoughts and debates in the communities of thinkers and practitioners alike. I am certain that this edition will encourage further ideation towards bolstering the fighting prowess of the Indian Armed Forces.

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

Jai Hind!

(Anil Chauhan)
General
Chief of Defence Staff

Lt Gen Johnson P Mathew,
PVSM, UYSM, AVSM, VSM

FOREWORD

The relationship between technology and war is as ancient as warfare itself. Historically, many technologies first developed for military purposes have eventually found civilian applications. Innovations in materials, explosives, propulsion, electronics, and energy often originated within military contexts before transitioning to the private sector. In fact, it could be argued that technology epitomizes the adage, "necessity is the mother of invention".

Technology has continually reshaped the character of war. The Industrial Revolution significantly accelerated this transformation, granting modern militaries unprecedented mobility, lethality, and reach. The 19th century saw innovations like the rifle, the railroad, and the telegraph, revolutionize warfare, while the 20th century was marked by the advent of the machine gun, the airplane, and the tank. More recently, the rise of information technologies has profoundly influenced modern conflicts, demonstrating how technological advancements can alter the course and nature or war.

Today, the onset of the Fourth Industrial Revolution and the emergence of new technologies, present an unprecedented confluence of capabilities, each with the potential to dramatically impact warfare. The synergy created by integrating diverse technologies may prove more transformative than any single innovation, potentially redefining the character of future conflicts.

However, technology is not a cure-all. The mere novelty of technology does not guarantee success in warfare. What matters is the integration of innovation into coherent strategies, effective warfighting concepts, and methods tailored to specific operational environments. Ultimately, victory is forged in the outcomes of arduous battles; while the tools of war evolve, the fundamental nature of war remains unchanged.

This comprehensive issue of Synergy on 'Impact of Niche Technologies on Joint Warfighting', therefore, is timely and relevant to provide an insight into the technological advances being made in the field of military technology. The varying idea and viewpoints of the authors are sure to generate constructive debates to help shape policies, doctrines and practices while providing innovative ideas to bolster the national military security of India.

Jai Hind!

(Johnson P Mathew)
Lt Gen
CISC

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

FROM THE DIRECTOR GENERAL'S DESK

The Geo-politics as well as the Geo-economics are changing with unprecedented rapid pace and in the process, they are challenging the existing world order. These disruptions are being now led by Technological advances. These technological advances in the form of Niche Technologies are disrupting the battle fields every passing moment. The conventional military superiority has been challenged beyond doubt be it during Russia - Ukarine War or during Israel Hamas Conflicts. This holds equally true for other conflicts in the different parts of the world as well.

These Niche Technologies will also play a pivotal role for India's future wars/ conflicts if they are necessitated in the national interest. These assume larger importance when China is already leading the technology space not only with reference to India but has become a lead country in the world in some of the technologies affecting the warfighting.

India possesses immense intellectual wealth which needs to be harnessed for preparing the defence forces to remain battle ready. This is most important when joint warfighting is the need of hour. The country cannot move forward in 'coordinated way' of warfighting and has to adopt to the symphony of 'integrated' war fighting. This edition of 'Synergy Journal' covers a vide spectrum of Niche Technologies which are critical for modern day Joint Warfighting.

It is not only that these Niche Technologies are adequate to meet our challenges, there are many more and these are evolving with every passing day. An attempt has been made to highlight some of the Niche Technologies so that all the stake holders start thinking towards this critical area of national importance.

Indian defence forces have already initiated multiple steps to adopt the usage of Niche Technologies in policy and doctrine formulation for Joint Warfighting. It is hoped that the content of this Journal will fastrack all such processes. The adoption of these Niche Technologies will not only change the equipment profile of the defence forces but will impact every aspect of warfighting. The country has to adopt to these changes fast to be on the 'winning curve'.

Jai Hind

(Ashok Kumar)
Maj Gen (Retd)
Director General

IMPACT OF NICHE TECHNOLOGIES ON JOINT WARFIGHTING

Gp Capt Ved Prakash Singh, VSM

Abstract

Since times immemorial, technology has permeated warfighting and has shaped the conduct as well as the outcome of wars. This paper aims to bring out some of the niche technologies which could have an impact on joint warfighting. Based on a review of the literature, the paper has adopted a framework of first identifying some of the emerging technologies affecting joint warfighting, thereafter identifying the factors affecting warfighting (space, time, force, decision making) and finally the impact of the identified technologies on factors affecting warfighting. The analysis based on this framework brings out that technology increases the space of operations, reduces the timeframe to act, enhances the effectiveness of forces and reduces the decision-making timelines. This impact eventually enhances the chances of a technologically adept side to win a war.

Introduction

Technology has a permeating effect on warfighting, hence technological superiority will have a prominent place in future wars. Revolution in Military Affairs (RMA) is deeply influenced by technology through changes in strategy and doctrine. Stirrups were an innovation or technological advent which led to RMA and the Mongols utilized it fully to establish one of the largest empires in the history. Technology has always been capable of dual use that is for civilian use as well as military use; for example, during the metal age implements made of metal were used for agriculture and tamed animals who were used for assisting humans in daily chores including agriculture. However, with passage of time, the same implements were tweaked to be used as weapons for war along with the animals like horses and elephants, also being used for war. In modern parlance, the use of chips is an apt example. It is used in domestic equipments like washing machine etc. and the same chip can also be used for drones Similarly, computers used in civilian domain find a lot of use in military domain. In the recent times, evolution of warfare has also brought out the ability of technology to fill in for numbers, leading to the paradigm of technologically advanced forces getting the better of larger low-tech forces. This has been proved by the Europeans in their conquest of the world with the help of numerically inferior forces but equipped with superior technology. The gulf war also elucidated the dominance of niche technology on battlefield whereas recent examples highlighting the same are Nagorno-Karabakh conflict, Russia-Ukraine war and Israel-Hamas war. Technological advancements may not always be eureka moments in the history of its evolution, but may also include amalgamation of available technologies to foster a niche technological output.

Framework of the Paper. To elucidate the theme that is "impact of niche technology on joint war fighting", the paper would follow the following frame work:

- First, it would identify emerging technologies for joint warfighting (including technologies in various stages of maturity or on the horizon).
- Thereafter it would identify the factors affecting war fighting.
- Lastly it would bring out the impact of the identified technologies on the factors affecting war fighting.

Emerging Technologies. The appointment of Chief of Defence Staff (CDS), creation of Department of Military Affairs (DMA) and buzz about integrated theatre commands, has ushered jointness, integration and joint warfighting to the center stage of Indian military, academic and policy discussions. Technology is an important cog in the warfighting wheel, therefore, out of plethora of technological developments, the following technologies have been selected, keeping in mind their impact on joint warfighting.

Artificial Intelligence (AI). Russian President Vladimir Putin said "Artificial intelligence is the future, not only for Russia but for all humankind. Whoever becomes the leader in this sphere will become ruler of the world."[1]

In India NITI Aayog defines it as a constellation of technologies that enable machines to act with higher levels of intelligence and emulate the human capabilities of sense, comprehend and act.[2]

AI employment in the military is in the fields of autonomous navigation (swarm drones), image recognition (ISR), threat recognition by integrating multiple sensors, simulation, cyber security etc. Army Design Bureau, using Computer Vision[3] has developed an AI powered night vision device which is connected to a wristband that vibrates and silently notifies a sentry on duty in case of any suspicious activity. Another achievement is the implementation of real-time translation of Chinese audio into English/ Hindi by a homegrown company called Cogknit.[4] This can be used by troops deployed on the border, grasping of ISR data and enhance situational awareness of pilots flying near the border. AI can be gainfully employed in detecting changes by observing photos over a period by employing 'Image correlation'. AI can also be used for enhancing maritime domain awareness (MDA), predictive maintenance, data analytics, text mining and cybersecurity.[5] Anshuman Narang in his book "China's Strategic Deterrence" brings out that AI would impact "acoustic signal processing, underwater target recognition, electronic warfare, enhanced C4I2SR making battle space more transparent through data fusion, info processing, intelligence analysis, military planning and deductions, intelligent autonomous systems for swarm, missile intelligentisation, simulation, wargaming, training, expansion of human stamina, precision logistics, deep semantic analysis, maritime robots and unmanned AI enabled submarines[6] to change the current informatized warfare to intelligentised warfare".

Quantum Technology (QT). Quantum is a dual use technology with a possibility of changing the world and concept of warfare completely in the future.[7] QT is rooted to quantum physics which is probabilistic in nature, counterintuitive and predicts phenomena which classical physics cannot predict.[8] QT uses the properties of superposition and entanglement for a wide range of applications.

Quantum technology promises manifold use for the armed forces. It is used for Quantum Computing[9] (harnesses the laws of quantum mechanics to solve problems too complex for classical computers), Quantum-encryption[10] (more secure than classical protocols and will make encryption impermeable), Quantum positioning system (navigation in GPS denied environment), Quantum Radar[11] (operates in high background noise and can detect stealth aircraft), Quantum Sensing (sense around the corners and small size) and Quantum Communication[12] (creates secure channels for information transfer and is resistant to eavesdropping). These applications have the capability of starting another revolution in military affairs.

5G/6G/ Internet of Military Things (IoMT) Devices. 5G and 6G refers to the 5th and 6th generation of mobile wireless network. 5G has data transfer speed 10 times greater than 4G and 6G is predicted to have data transfer rate 10 times greater than 5G.[13] The substantially high frequencies of 6G have two key effects, first is substantial low latency (time taken by data to travel from source to end user) and second is the higher bandwidth which determines the amount of data that can travel over the network at a time. Unmanned machines would play a stellar role in the future warfare and 6G would provide the operators better control on them[14] because of their properties of high data handling capability and low latency. 6G would be an intelligent as well as adaptive network and its exploitation can reduce sensor to shooter time by shortening the OODA loop. Another application of this technology could be in providing last mile connectivity to units or elements that are not directly connected with OFC network, either because of their remote locations or due to their high mobility roles. A battlefield C4ISR grid can be formed using 5G private network technology. Various elements like ground vehicles (GV), Low Earth Orbit (LEO) satellites, HAPS and UAVs can be used to form a 5G/ 6G network. The technology can also be used to provide tactical 5G Adhoc Networks[15] of various sensors at tactical level to provide more accurate firing solutions to the AD weapon system. Here**,** a wireless sensor network or a device-to-device network can be formed using nearby ELINT sensors, ISR platforms like UAV, SIGINT ground stations and any other passive sensor component. This information can be fed to AI enabled aggregator software at AD Command post to help generate firing solutions with minimum use of active transmission. 5G/ 6G networks can provide low latency that would be required for such operations.

The integration of AI and 6G would optimize network resources, predict user demands, dynamically allocate bandwidth and unlock new possibilities for an array of IoMT applications. IoMT is a class of heterogeneously connected devices employed for future warfare[16]. It allows real-time connection between devices like unmanned vehicles and command station. For such connections 5G/ 6G would be a prerequisite because of their high bandwidth and low latency. Sensors of IoMT in battlefield enhance surveillance capability and thereby increase the situational awareness (SA) of commander. This enhanced SA ultimately leads to shortening of own OODA loop and a holistic response to the adversary.

Robotics. Robotics is a branch of engineering and computer science that involves manufacture and operations of robots[17]. The objective of the field is to create intelligent machines which can assist humans in performing their work. Coupled with AI and machine learning, robotics products can handle repetitive, dull and dangerous tasks without any mistakes, without getting sick and working 24 X 7.

Robotics could be used in developing and fielding 'unexploded bomblets handling robots' (UXBR). With the threat of bomblets in SEAD/DEAD and runway denial missions by the enemy, the UXBR would be a highly effective and life saving option. The second application could be developing and fielding 'weapon handler robots'. This will not only aid in performing the mission critical task of weapon handling but also tide over the perennial problem of manpower shortage in the armed forces. The third application could be 'cargo handler robots' for use by armed forces in lugging around load and free up troops for combat duties. The fourth application could be for 'guard robots', enabled with AI (computer vision and natural language processing) these robots could be used for guarding infrastructure and scanning of incoming personnel before granting them access to military stations.

Drones/ Unmanned Surface Vehicles (USVs)/ Unmanned Ground Vehicles. The wars of the 21st century have highlighted the utility of drones/ USVs/ UGVs from ISR to combat roles. The incorporation of advanced sensor, edge processing and AI has enhanced the 'God Mode' of these platforms[18] with likely upgradation from 'remotely piloted' to 'autonomous' drones/ USVs/ UGVs and swarms.

Drones can be employed for ISR, EW, logistics, communications and Kinetic roles. The tedious and time-consuming analytical work of interpreting the data from various EO/IR, ELINT/COMINT/SIGINT sensors in these drones could be automated using AI to shorten the OODA loop. Drones have proven their mettle in Armenia- Azerbaijan war, Russia - Ukraine conflict and Israel- Hamas war.

Man-Unmanned Teaming (MUM-T). MUM-T refers to combining manned and unmanned vehicles/ aircraft/ boats etc. to undertake integrated missions complementing each other's capabilities.[19] This team could perform 'networked' Kinetic (including absorbing enemy fire), ISR, EW, roles with the manned system providing 'human in the loop' for ethical warfighting. With AI in the swarm drones, the sensor data will be processed faster and lead to shortening the OODA loop and reducing the combat decision making time.

MUM-T platforms have form fit function of a manned aircraft, but utilise AI to fly the mission.[20] The employment philosophy consists of one manned leader along with 6-7 unmanned aircraft. By swapping mission specific modules, a MUM-T airframe could be prepared for prosecuting any mission (SEAD/ CSFO/ Interception/ ISR/ BDA).[21] Additionally, the onboard AI coupled with sensors would enable the combat drones to execute missions even in a contested/ denied environment with no GPS, no waypoints and no communications.[22]

Directed Energy Weapons/ Counter Drone System. Directed Energy Weapons (DEWs) are a type of electromagnetic or particle technology which use energy, as opposed to a physical projectile, to strike a target.[23] DEWs encompass three distinct technologies. First, Laser including High Energy Laser (HEL) and low energy laser, second Radio Frequency

Systems involving high powered microwaves (HPM) as well as millimetre waves and third Particle Beam systems.

HEL and Particle Beam Systems, can lead to disruption and destruction of equipment, whereas low-energy lasers can dazzle systems including sensors on satellites. HPM can degrade and damage electronics, thus can be used to counter threats of unmanned aerial system as well as a wide range of electronics. The DEWs would be used for security of static bases and Naval ships from drones. They can also be used to dazzle satellites and engage missiles.[24] DEWs use energy fired at the speed of light, making them faster and potentially less costly per shot than missiles. HEL based DEWs can engage incoming missiles at a greater range than existing CIWS systems with matching rate of fire with lesser logistical requirements than CIWS. Laser based DEW suffer from atmospheric factors and line of sight range limitations. It can be mitigated through Microwave based DEW which is yet to materialise in India. DEW technology, once fully matured and weaponised, will be crucial enabler in neutralisation of both air and space based threats at various ranges. Indian companies like BEL and Zen technologies have taken nascent steps into developing Counter Unmanned Aerial System (CUAS).[25]

Hypersonic Weapon Technology. Hypersonic flight is defined as flight over Mach 5/ 6172 kmph and can penetrate advanced Ballistic Missile Defence (BMD) and Air Defence.[26] Hypersonic weapons being developed are of two types: Hypersonic Glide Vehicles (HGVs) and Hypersonic Cruise Vehicles (HCVs).[27] The HGVs lack propulsion and are referred to as boost-glide types. They are connected to a booster rocket and propelled to an altitude of roughly 100 kilometres. At this height, the craft separates and descends to earth on a somewhat flat trajectory while utilizing the height to accelerate to hypersonic speeds of Mach 8 to 10. The HCVs can be launched either via booster rockets or a mother aircraft. A propulsion system that would ignite after separation would supplement cruise phase, giving the descending projectile extra speed and permitting greater manoeuvrability.

With their characteristics of high speeds, compressed timelines, extended ranges and manoeuvrability; hypersonic weapons could provide various strategic and military benefits. They might supplement ballistic choices, but what would spur interest and investment in the future would be their capacity to defeat conventional missile defences,[28] thereby influencing adversary's A2AD plans. These weapons may be employed against Air Defence targets, strategic targets, maritime targets such as Aircraft Carrier, Command and Control Centres and Interdiction targets.

Near Space Platforms. Near space is defined as the region which is between 20 Km (Armstrong limit altitude) and 100 Km (Von Karman line), that is between air-space and outer space.[29] The development of lightweight solar cells, high-energy-density batteries, miniaturization of electronics, exponential increase in computing power and lightweight, strong, flexible materials that can resist degradation under strong ultraviolet illumination with impermeability to gases have made near space platforms possible. Graphene is a material made from graphite using Nano Technology (discussed later in the paper) is the strongest material ever measured. It is 200 times stronger than steel, can stretch like rubber, completely impermeable to liquid as well as gases and is very light weight.[30] The convergence of these technological advances has led to the development of Near Space Platforms. Two such Near Space platforms are Near Space Balloon and Near Space Unmanned System also called High Altitude Pseudo Satellites (HAPS).[31]

Near Space balloons and HAPS can be used for persistent ISR, communication, position, navigation, time and maritime domain awareness. The advantages accrued are persistence over point of interest, better resolution due proximity to point of interest, wide and easily adjustable footprint for ISR/ communication role and cost effectiveness.[32]

Virtual Reality (VR). Virtual reality is defined as 'any set up that aims to elicit human neural responses using externally and intentionally created synthetic environments, such as that obtained during interaction with the physical world.'[33] It uses specialized equipment to create a virtual environment which stimulates one's senses by introducing changes in the virtual environment.

Virtual reality would be used for realistic training through high fidelity simulation thereby providing the forces with better trained individuals. VR may also be used for stress testing of individuals for various assignments and also training them culturally before any foreign duty or exercise with foreign forces.

Augmented Reality (AR). VR equipment is bulky and creates a virtual environment which is removed from the actual environment. These limitations of VR are solved by another technology called Augmented Reality.[34] AR doesn't require a person to wear any equipment, instead it overlays information on the real world.

This technology makes it possible to simulate flying/ driving/ sailing in various scenarios without a functional flying simulator. It can also be used to enhance existing low grade simulators with immersive experience for realistic training. AR allows even more realistic training with the person being aware of the surrounding.

Nano technology and Materials Science. Nano technology is the field of science that involves manipulation of matter on atomic scale to design new structures, materials and devices[35]. This technology can be used for reducing the size and weight of equipment carried by soldiers and also developing new materials for military purposes e.g. light weight material for making battle dress of soldiers, ability to stop bullets and protection against toxins. The technology may also be applied to aerospace for making nano satellites, nano sensors and nano drones, wherein the technology would be used to change the micro structure of aluminium to make it akin to titanium sans the weight penalty.

Elucidating Factors Affecting War. Milan Vego in his seminal work 'Joint Operational Warfare' has brought out that 'the art of warfare is to obtain and maintain freedom of action- the ability to carry out critically important, multiple and diverse decisions to accomplish assigned military objectives. One's freedom of action is achieved primarily by balancing the factors of space, time and forces. These factors and, increasingly, information are pivotal for making sound decisions at all levels. The higher the level of war the larger the factors of space, time and force and hence the more critical for the commanders and their staff to properly balance these factors.'[36] The essence being that war fighting is impacted by control of the following factors: -

Space. Milan Vego brings out that 'factor of space encompasses land, sea and airspace including outer space with all their features which influence the employment of land, sea and air forces"[37]. In the present scenario of technological advances and presence of attack vectors of all kind of ranges the "physical space in which friendly and enemy forces move and manoeuvre will probably be much larger than it is today. The lines separating the rear zone and combat zone will be further blurred and the zones increasingly difficult to differentiate.'[38]

Time. Milan Vego brings out that 'any military action or measure requires a certain amount of time to plan, prepare, conduct and sustain. Large forces do not just suddenly appear in a theatre. They sometimes need several days or even weeks to complete movement from one area to another.'[39] Technological advances made in the field of ISR and secure communication of the same to commanders would compress the factor of time involved in sound decision making for movement and action by forces.

Force. Milan Vego brings out that 'force in its narrowest meaning pertains to military forces of power. Properly understood, however, the factor of force includes not only troops, naval forces and air forces but also the forces of all services with their logistical support.'[40] The technological advances would redefine the factor of force from massing to concentration of effects. Hence the force effectiveness would depend on quality rather than quantity.

Decision Making. Colonel John Boyd of USAF developed a decision making framework in the form of Observe, Orient Decide, Act (OODA) loop.[41] The cycle begins with an observation (provides situational awareness), which leads to situational orientation (contextualising the observation) of the commander. The commander then decides on appropriate course of action and finally acts (executes) on that decision. Thereafter the results are observed and the cycle is set in motion again. The aim being to go through the OODA loop faster than the enemy and disrupt his decision cycle.

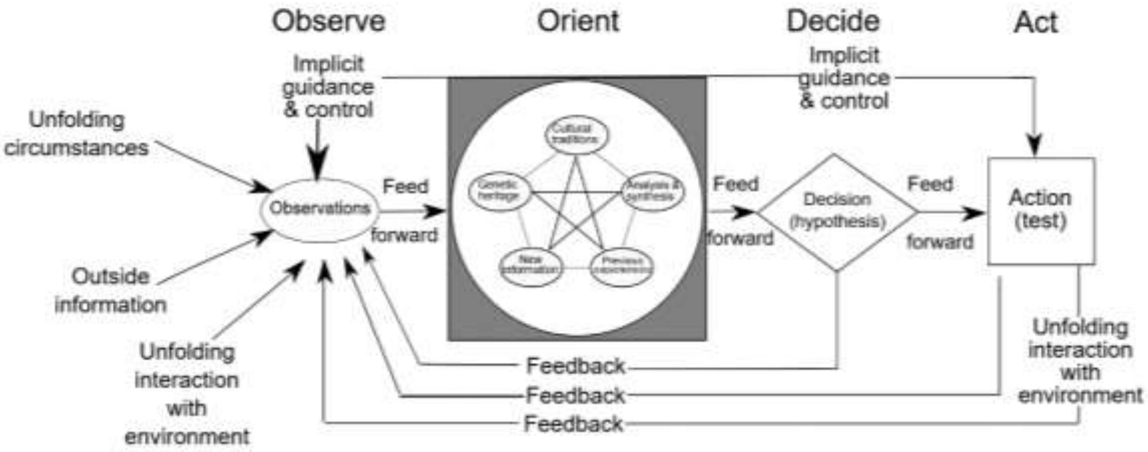


Fig 1: OODA LOOP[42]

Impact of Technologies on Factors of Space, Time, Force and Decision Making

Space. The intelligence data obtained through near space platforms, Drones, MuMT would be securely communicated to the commander using 5G/ 6G/ Networks/ IoMT, AI and QT. The commander would then use QT, AI, decision algorithms and his experience to take a holistic decision and act at a place of his strength and enemy's vulnerability using precision hypersonic weapons. In effect technology provides data and also empowers the commander to decide the area for mobilization and action thereby increasing the factor of space for operations.

Time. The ISR data obtained through near space platforms, Drones, MuMT, and its instant communication to the commander using 5G/ 6G/ Networks/ IoMT along with utilization of QT, AI and decision algorithms assist him in taking a decision faster. This gives the commander extra time to mobilise his forces. Apart from this, missile including hypersonic weapons can be used to stop access as well as deny an area to the enemy. The timeframe required to prepare the missile vis a vis the distances it affects is much less than the time required to mobilise forces to similar distances. Hence technology would help a commander to act proactively in lesser timeframe.

Force. The precise knowledge of enemy through ISR technologies, its instant communication to the commander and sound decision making with the help of AI, QT and decision algorithms enhances the effectiveness of any force under a commander. This assisted by hypersonic weapons (low probability of intercept), UCAVs, MuMT, Robotics etc. further increase the offensive effectiveness of the forces. DEW and Robots would be used for safety and security of bases. Nano technology would be used for enhancing the safety of combatants and AR/ VR would be used for their realistic training. The holistic effect of all these would be to enhance the effectiveness of the forces in war.

Decision Making. The technologies affecting the observe part of OODA loop are UAVs, Satellites and Airship. They assist in enhancing situational awareness about the enemy through ISR missions. This feed would be given to the orient part of the cycle through the technologies of SDR, Quantum Communication, Quantum Encryption, Sensors, 5G, 6G and IoMT. These technologies assist in communicating the observations about the enemy to the commander and enhancing the orientation of the commander of the likely battle space. The technologies of Quantum Computing along with decision making algorithms fed by big data, AI, ML would assist the commander in making a decision about the plan of action. These technologies assist the commander in taking a sound decision with the help of science and history amalgamated with his experiences and understanding/ appreciation of the situation. Hypersonic, MIRV, Precision munition, AI, Nano technology and material, UCAVs, MuMT and robotics along with other conventional forces assist the commander in executing the decision in a faster time frame. It is evident that the technologies reduce the time to go through own decision cycle and provide an opportunity to the commander to disrupt enemy's decision cycle.

Conclusion

Technology is an important part of any revolution in military affairs and this has been elucidated succinctly by Sir Frank Whittle as "A nation's ability to fight a modern war is as good as its technological ability." However, technology alone is not an end all therefore to accrue maximum advantage of technological advancement, the doctrine of the Armed Forces must be open to advantages offered by the technology and evolve to amalgamate it into the central belief of the forces. Milan Vego is very prescient in sounding the same sentiment as "To fully exploit the potential of new technological advances such as netting of forces, operational concepts incorporating and integrating the new technologies must be developed into coherent doctrines."[43]

*****

Gp Capt Ved Prakash Singh, VSM, is a flying branch officer of IAF and has over 6800 hours of flying. He is a Qualified Flying Instructor, an Instrument Rating Instructor and Examiner. The Officer was member of the pioneer team for induction of C-130J aircraft in the IAF and has also undergone the Pilot Instructor Course on C-130J in USA. He has commanded a C-130J special ops unit and is currently posted to 4Wg as COO.

NOTES

[1] Anshuman Narang, *China's Strategic Deterrence* (New Delhi, 2019).

[2] Aayog, N. I. T. I. "National Strategy For Artificial Intelligence# AIFORALL.

niti.gov.in/writereaddata/files/document_publication." NationalStrategy-for-AI-Discussion-Paper. pdf (2018).

[3] AI-enabled night vision device is being used by the Indian Army. Indiaai Case Study 30 May 23. Accessed at https://indiaai.gov.in/case-study/ai-enabled-night-vision-device-is-being-used-by-the-indian-army

[4] Army uses AI to break through the Chinese language barrier. Indiaai Case Study 30 May 23. Accessed at https://indiaai.gov.in/case-study/army-uses-ai-to-break-through-the-chinese-language-barrier

[5] "Indian Armed Forces Push for Integrating Niche Technologies - Defence News | The Financial Express," accessed June 1, 2024, https://www.financialexpress.com/business/defence-indian-armed-forces-push-for-integrating-niche-technologies-2630428/.

[6] Narang, *China's Strategic Deterrence*.

[7] Narang, *China's Strategic Deterrence*.

[8] "What Is Quantum Physics? Quantum Physics in Simple Terms | Caltech Science Exchange," accessed June 10, 2023, https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-physics.

[9] Narang, *China's Strategic Deterrence*.

[10] Narang.

11 Narang.

12 Narang.

13 "CHINA'S 6G TO POWER AI ARMY OF THE FUTURE," accessed June 1, 2024, https://www.scmp.com/news/china/military/article/3080235/chinas-military-draws-6g-dream-.

14 "CHINA'S 6G TO POWER AI ARMY OF THE FUTURE."

15 "Development of 5G Mobile Ad Hoc Networks for DoD - Defense Advancement," accessed June 2, 2024, https://www.defenseadvancement.com/news/development-of-5g-mobile-ad-hoc-networks-for-dod/.

16 Shafeeq Maheen, "Internet of Military Things (IoMT) and Future of Warfare" (Center for Aerospace and Security Studies, 2022).

17 "What Is Robotics? | Definition from WhatIs," accessed June 3, 2024, https://www.techtarget.com/whatis/definition/robotics.

18 "Indian Armed Forces Push for Integrating Niche Technologies - Defence News | The Financial Express."

19 "Indian Armed Forces Push for Integrating Niche Technologies - Defence News | The Financial Express."

20 Kratos Defence,"XQ 58A Valkyrie:, "https://www.kratosdefense.com/-/media/k/pdf/usd/xq-58a-valkyrie.pdf , Jan 25, 2018, accessed on Jun 11,2023

21 SAE, "The future of Collaborative Combat Aircraft",https://www.sae.org/highlights/the-future-of-collaborative-combat-aircraft, accessed on Jun 11, 2023

22 Shield AI, Worlds best AI pilot Hivemind", https://shield.ai/hivemind/, accessed on Jun 11,2023

23 "Directed-Energy Weapon - Wikipedia," accessed June 2, 2024, https://en.wikipedia.org/wiki/Directed-energy_weapon.

24 "Science & Tech Spotlight: Directed Energy Weapons | U.S. GAO," accessed June 10, 2023, https://www.gao.gov/products/gao-23-106717.

25 "Indian Military Orders Anti-Drone Systems from BEL and Zen Tech. - Bharat Shakti," accessed June 3, 2024, https://bharatshakti.in/indian-military-orders-anti-drone-systems-from-bel-and-zen-tech/.

26 Narang.

27 Kelley M Sayler, "Hypersonic Weapons: Background and Issues for Congress," accessed June 2, 2024, https://crsreports.congress.gov.

28 Sayler.

29 Narang, *China's Strategic Deterrence*.

30 Ric Edelman, *The Truth About Your Future* (New York: Simon & Schuster , Inc, 2018).

[31] Lt Col Edward B. Tomme, D. Phil. *The Paradigm Shift to Effects-Based Space:*

Near-Space as a Combat Space Effects Enabler (Air University : Maxwell AFB 2005) Page 5

[32] Narang, *China's Strategic Deterrence*.

[33] "Military Applications of Virtual Reality and Beyond | Manohar Parrikar Institute for Defence Studies and Analyses," accessed June 1, 2024, https://idsa.in/issuebrief/military-applications-of-virtual-reality-and-beyond-aupadhyay-140923.

[34] Edelman, *The Truth About Your Future*.

[35] Edelman.

[36] Milan Vego, *Joint Operational Warfare Theory and Practice*, Revised Se (Rhode Island: US Naval war College, 2009).

[37] Vego.

[38] Vego.

[39] Vego.

[40] Vego.

[41] "The OODA Loop Explained: The Real Story about the Ultimate Model for Decision-Making in Competitive Environments | OODA Loop," accessed May 31, 2024, https://www.oodaloop.com/the-ooda-loop-explained-the-real-story-about-the-ultimate-model-for-decision-making-in-competitive-environments/.

[42] "The OODA Loop Explained: The Real Story about the Ultimate Model for Decision-Making in Competitive Environments | OODA Loop."

[43] Vego, *Joint Operational Warfare Theory and Practice*.

FUSION OF NICHE TECHNOLOGY IN BRO WORKS TO SUPPORT JOINT WAR FIGHTING

Lt Gen Rajeev Chaudhry, VSM (Retd)

Abstract

Border Roads Organisation (BRO) with its new found potential has accelerated its projects through infusion of new technologies post Galwan clash and reduced the road head differential considerably with China on its Northern Borders. BRO by taking the roads right up to the most forward posts all along the LAC has not only ensured operational optimisation of Armed Forces but also provided them with much desired strategic extension specially in Eastern Ladakh and Arunachal Pradesh. Its contributions to mobility, logistics, force multiplication, and inter-service synergy are vital for maintaining a strategic advantage in high-altitude and remote warfare scenarios. With this momentum, BRO is better poised to adopt niche technologies which can revolutionise the infrastructure development on our borders by not only better construction quality but also expediting project timelines and assured sustainability in environmentally sensitive areas. Integrating these newly adopted techniques and other niche technologies by BRO with joint war-fighting efforts by the Armed Forces will ensure that India is better prepared to address the strategic challenges posed by China and to maintain the security and integrity of its borders.

Introduction

The geopolitical global landscape is transforming rapidly due to increasing tensions in Eastern Europe and Middle East. Sooner or later it is certainly going to spread eastward to South China Sea thereby activating Indian Ocean as future hotspot for China and United States jostling in the power game. India has to gear up its doctrines, force structures and war fighting capabilities to meet challenges of backlash of such conflicts by guarding its maritime and land borders strongly. China has tested Indian responses through local skirmishes at Dokala, Galwan and Yangtse[1] during last seven years with a view to provoke India to take such local conflicts to next higher levels. India and China both have significant military capabilities and are positioned strategically along the Himalayan frontier. Given the rising tensions and the potential for conflict, it is imperative to understand how the Indian Armed Forces along with its other essential components could effectively engage in joint warfighting operations against China. This paper explores the niche technologies in use and which more can be infused by Border Roads Organisation (BRO) to optimise the potential of our war fighting mechanism.

Rapidly evolving technologies are changing the character of warfare[2], and we are yet to understand the impact of these changes. Adapting to this evolving landscape requires the joint force to integrate capabilities and synchronize effects fluidly across all domains. The opportunity for the Joint Force, as it looks ahead to a future still unclear by the long term impact of rapid changes, is to get ready for the warfare of the future.

India is rapidly moving towards theaterisation of its regional commands[3] to subsequently enunciate its Joint War-fighting Concept & Doctrine (JWCD). JWCD will act like a beacon for integration of Armed Forces with industry and other components to support the joint war-fighting effort and would offer a shared vision of the terrain and common destination. In this complete process, BRO is going to play a bigger role by creating a robust infrastructure network to enable the Joint Force extend its reach, options to manoeuvre and strike designated targets with increased accuracy and impunity. It would be BRO’s endeavour to maximise the strength of Joint War – fighting mechanism during critical combat situations.

Strategic Context

The 1962 Sino-Indian War and subsequent skirmishes along Line of Actual Control (LAC), underscore the volatility of our Northern frontier. China's infrastructural development in Tibet, including roadways, railways and airbases started much before India raised BRO in 1960 with two projects deployed in Srinagar and Tezpur to develop strategic roads in J&K and Arunachal Pradesh, crucial for the rapid mobilization of troops and military equipment.[4] China has been focused and consistent in enhancing this infrastructure considerably all along the LAC, whereas India lagged behind due to its regressive strategic thinking and provision of meagre funds for connecting its posts right upto LAC.

Force Multiplication through Infrastructure

In modern warfare, infrastructure acts as a force multiplier. The BRO's efforts in constructing and upgrading road networks not only facilitate the movement of military personnel and equipment but also support the establishment of advanced bases and logistics hubs.[5] These infrastructures serve as staging areas for joint operations involving the Indian Army, Air Force, and other paramilitary forces.

For instance, the development of roads leading to forward airbases allows for the quick transportation of fuel, ammunition, and other critical supplies, ensuring that air operations can be sustained for longer periods. In the event of a conflict with China, the ability to sustain prolonged air operations and provide air support to ground troops can be a decisive factor in achieving military objectives. In addition, vital inputs are also taken from the respective state administrations while planning all projects so as to factor in the local socio-economic requirements and internal security compulsive concerns.

Building Construction Synergy in Armed Forces

The BRO's infrastructure projects also foster synergy between various branches of the armed forces. The coordination required for the construction and maintenance of roads and bridges in challenging terrains necessitates close collaboration between the BRO, the Indian Army Corps of Engineers, and other defence agencies. This collaboration ensures that all branches of the military are familiar with the infrastructure capabilities of BRO available to them.

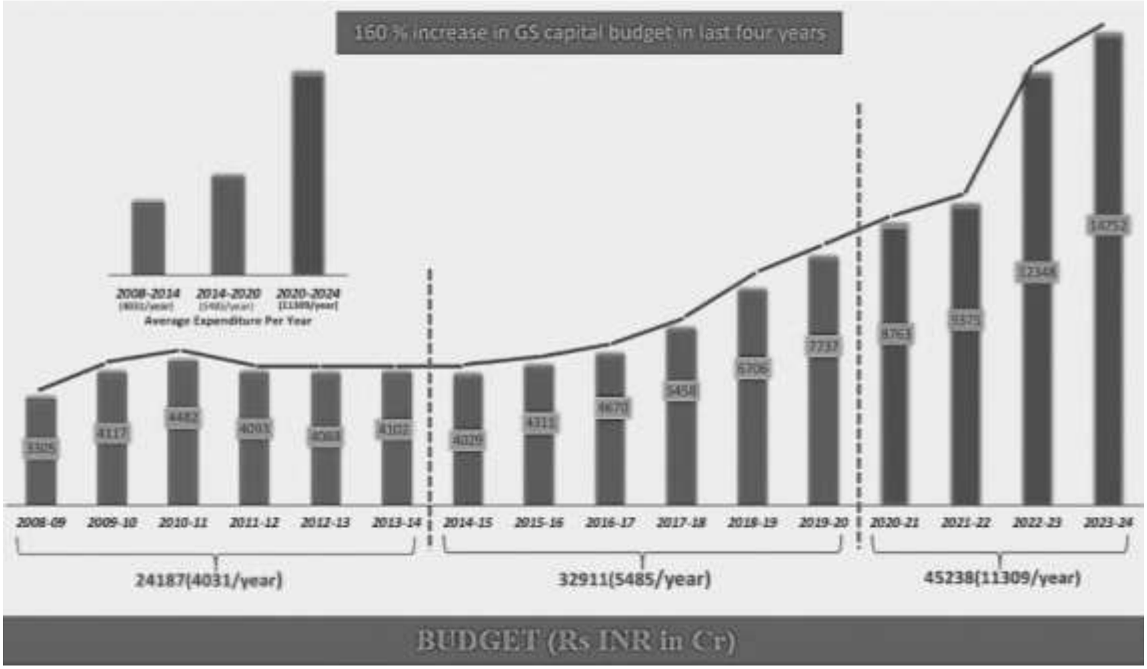
Moreover, the BRO's projects have been using advanced engineering techniques and technologies during past few years to accelerate the work pace, which provide valuable learning opportunities for military engineers. The experience gained from these projects enhances the technical and operational expertise of the armed forces, contributing to their overall war-fighting capabilities.

Psychological and Strategic Significance

The development of strong infrastructure on our borders has a psychological and strategic impact on both our forces and the adversary. For our troops deployed in remote and difficult areas, the availability of extensive road matrix boosts morale and ensures better logistics lines, medical evacuation routes and communication links. This logistical assurance is crucial for ensuring the effective readiness of troops in critical combat situations.

On the other hand, the development of infrastructure on our inhospitable Northern Borders sends a strong message to adversaries like China about India's steadfastness to defend its territorial integrity. Accelerated pace of work by BRO on our borders post Galwan conflict has sent a strong signal to China dissuading it to avoid any misadventure with India.[6]

Incremental budgetary support over the last four years, infusion of new technologies and products besides the latest equipment and machines, worked like a magic potion in consuming Rs 45238 Cr in the past four years vis-a-vis Rs 45,194 Cr which was spent in nine years of pre-Galwan period.[7]



Source: Author

Challenges and Future Prospects

BRO while ensuring last mile connectivity on our Northern Borders has been braving the challenges of the harsh and often unpredictable weather conditions, coupled with difficult terrains. Additionally, budgetary constraints and bureaucratic hurdles can also impede the timely completion of projects.

Looking ahead, the BRO's role is expected to become even more critical as geopolitical tensions with China persist. The ongoing strategically important border infrastructure projects, are set to further bolster India's defensive and offensive capabilities. Additionally, the BRO's involvement in the development of dual-use infrastructure, which can serve both civilian and military purposes, will enhance the overall strategic depth and resilience of India's border regions.

Modernisation of BRO post Galwan

New and emerging technologies are redefining the methodology of road construction with a transformed focus on sustainable development. Technological advancements made in this area have quickened the speed of construction and lowered the project lifecycle costs.[8] Some of the areas of modernisation and use of new technologies/equipment and innovative ideas by the BRO, specifically adopted and introduced post Galwan conflict, have been deliberated upon in subsequent paragraphs.

- **Digitisation and Automation.** BRO is first Govt department and presumably the only one to digitize all its roads and put it on Geographic Information System (GIS) for ease of better future planning and integration with other ministries working in the same domain. Almost all roads except few have also been uploaded on 'Gati Shakti Sanchar Portal' to ensure that all departments have visibility of each other's activities providing critical data for planning and execution of their projects in an absolute manner. By doing this, different departments will be able to prioritize smooth and optimal execution of their projects. Also, through use of 11 new software, specifically created to meet BRO's ground requirements, executives and staff are in better position to monitor progress of all its projects deployed in 11 states and 3 UTs.

- **Fixing Alignments.** BRO has already started use of drones and Light Detection and Ranging (LiDAR) for preparation of the DPRs for its road projects. With the advent of high-resolution satellite imagery, BRO can conduct detailed topographical assessments with unparalleled precision.[9] This data forms the foundation for designing routes that are not only cost-effective but also minimize environmental disruption. The imagery can reveal potential geological hazards, allowing BRO to proactively design mitigation strategies, which is particularly crucial in areas prone to landslides and earthquakes and prevent crucial disasters akin to Silkyara tunnel in Uttarakhand.

- **Monitoring Construction Progress**. BRO has already projected its demand for a dedicated LEO Satellite for pseudo real-time multi-sensor data acquisition for road alignment and earth work requirement planning to support the preparation of Detail Project Report (DPR) along with support to track ground-based assets in remote locations.[10] Satellite imagery can be used to monitor the progress of road construction in remote areas, providing real-time updates and helping in better project management. This not only ensures adherence to timelines but also allows for the rapid reallocation of resources to areas where progress may be lagging or where unforeseen challenges have arisen.

- **Satellite Communications**. Operating in the world's most isolated regions, BRO utilizes satellite phone communication to forge dependable connections between its ground teams and the Headquarters. Sufficient satellite phones have been procured for its remotely located detachments working on formation cutting and snow clearing tasks.

- **Geocells in Sub Base/Base Courses.** During last 3-4 years, BRO has come out of its old mindset and experimented with new materials to stabilize pavement structures by using many new stabilization techniques that improve pavement structural strength and reduce repair and maintenance by using on-site or recycled materials. Geocells have proved to be one of the latest stabilization techniques for sub-grade improvement and base reinforcement. These are three-dimensional honeycombed cellular structures made with polymeric materials such as High Density Polyethylene (HDPE) that form a confinement system when in-filled with compacted soil or aggregates.[11] In many stretches of BRO roads, Geocells have increasingly been used to increase bearing capacity of sub base and base courses.

Hapoli-Sarli-Huri Road in Arunachal Pradesh, Source: BRO images

Balipara-Charduar-Tawang Road in Arunachal Pradesh, Source: BRO images

Sasoma-Saserla Road in Ladakh, Source: BRO images

- **Cementitious Sub-Base/Base Courses.** For road bases, there are a variety of soils or granular materials available for construction, but they may exhibit insufficient properties (e.g. low bearing capacity and susceptibility to frost action), which then results in substantial pavement distress and reduction of the pavement life. However, addition of a stabilizing agent can improve the properties of soil. Among all these stabilizing materials, cement-bound agents show quite high stiffness and strength values, and display good performance for serviceability and durability for pavements.[12] Construction of large number of roads post Galwan has been undertaken by BRO in Ladakh, Uttarakhand, Sikkim and Arunachal Pradesh using this technology.

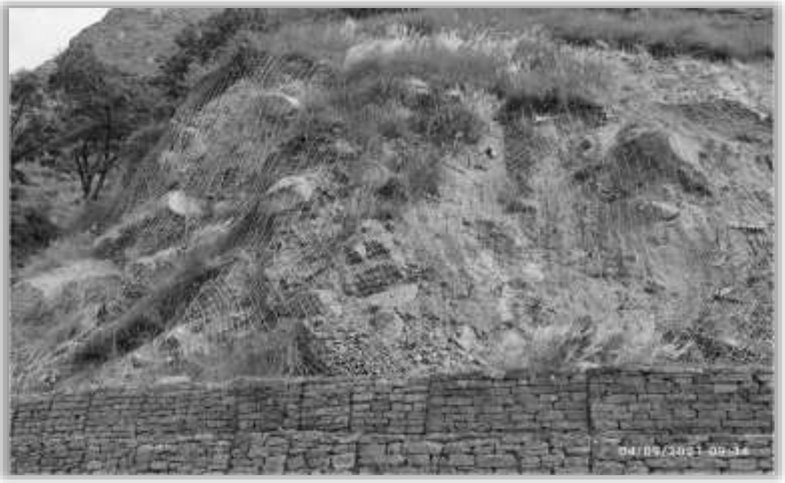
Mahe-Debring Road in Ladakh, Source: BRO images

Sumna–Rimkhim Road in Uttarakhand, Source: BRO images

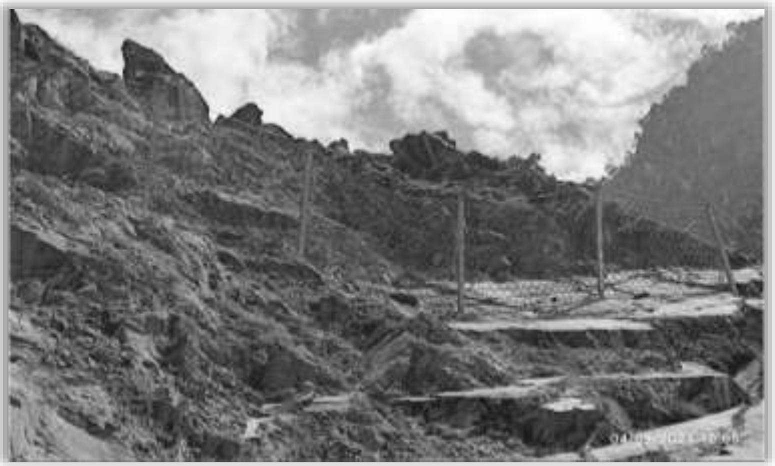
Hapoli-Sarli-Huri Road in Arunachal Pradesh, Source: BRO images

- **Slope Stabilisation to Mitigate Landslides.** The biggest challenge during construction of mountain roads are the fragile hill/valley side slopes created during formation cutting, which come down due to their own weight or get weakened during rains thereby causing considerable damage to roads, bridges and allied structures. Slope stabilisation refers to any implemented technique that aims to stabilize an unstable or inadequately stable slope through use of pre–stressed anchors, rock bolts, piles, soil nailing geosynthetics reinforcement, retaining wall, shotcrete etc.[13]

  A considered decision was taken by DGBR in 2022 to include slope stabilisation in the original scope of road construction as part of the DPR, in order to minimise damage to roads during rains and also to protect the fragile ecosystem as a major preventive measure at places where BRO is constructing roads.



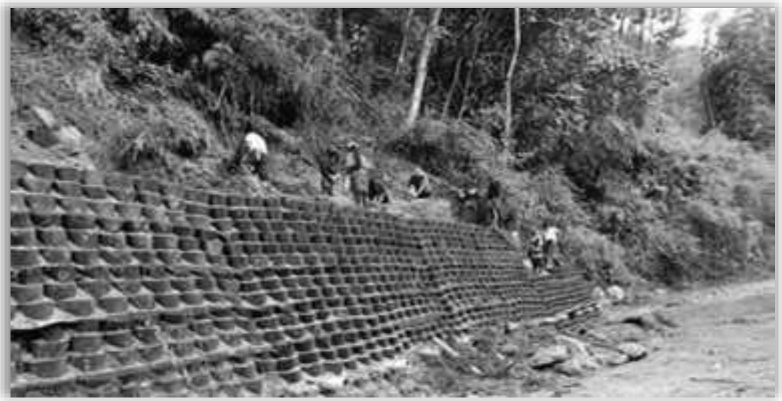
Drapery with Hill Side Gabion Wall on Joshimath-Mana Road in Uttarakhand, Source: BRO images



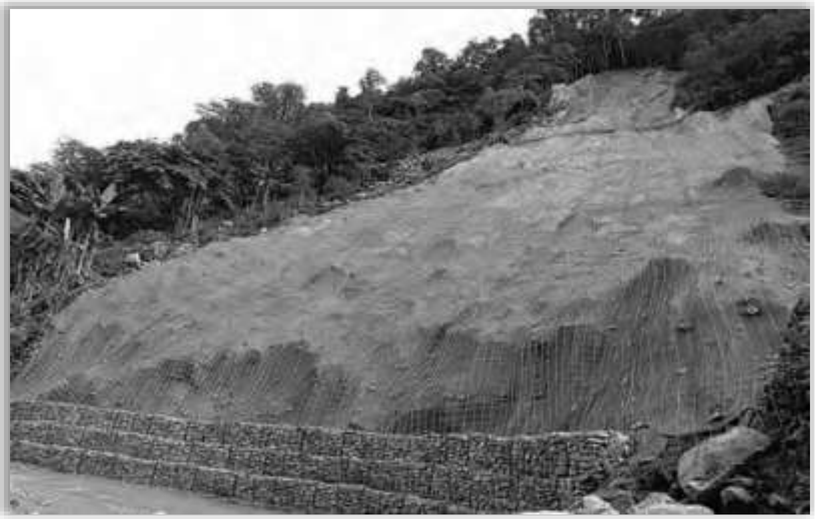
Dynamic Rockfall Barrier on Joshimath-Mana Road in Uttarakhand, Source: BRO images

Secured Drapery with Micro Piling Work on Joshimath-Mana Road, Source: BRO images

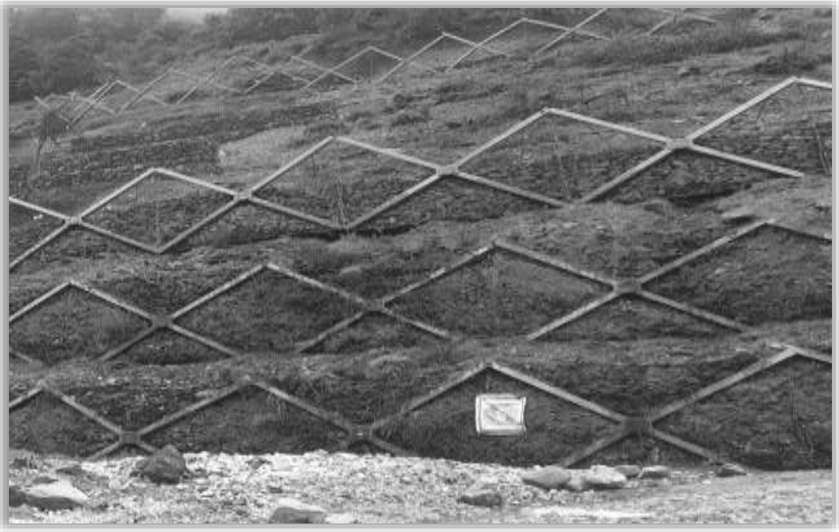
Rockfall Embankment on Joshimath-Mana Road, Source: BRO images



Geo Breast Wall on Sangklang-Toong Road in Sikkim, Source: BRO images



Biodegradable Coir reinforced with Gabion Wall on TCC-Maza Road, Source: BRO images

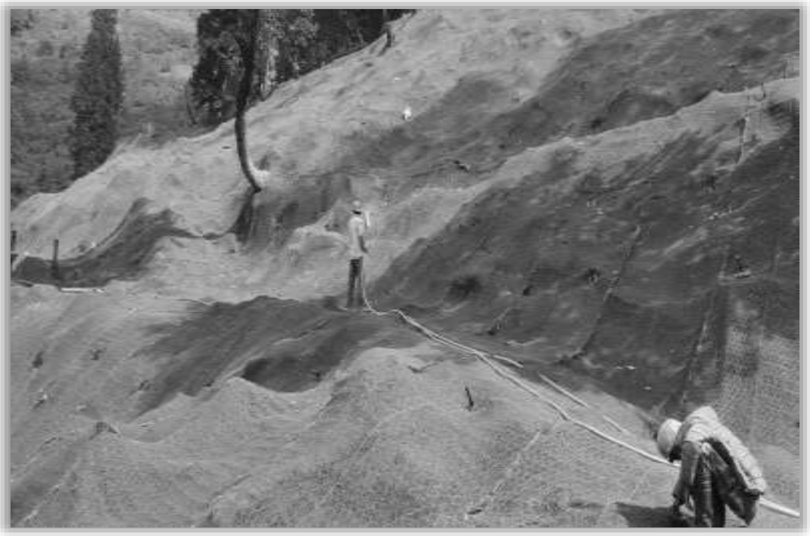


Geotextile Material with Erdox-Cruciformon Road Kyachee GG– Nasar GG–Lungro GG (K-N-L), Source: BRO images

Geo Synthetics on Balipara-Charduar-Tawang Road, Source: BRO images

Geo Synthetics on TCC-Taksing Road, Source: BRO images

Pre-Stressed Cable Anchor on approach to South Portal of Atal Tunnel, Source: BRO images

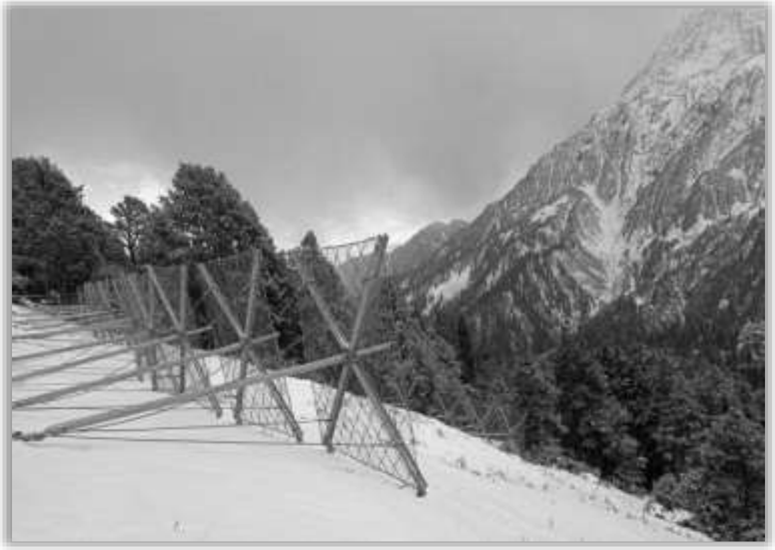


Reinforced Geomat on approach to South Portal of Atal Tunnel, Source: BRO images

Hydro Seeding on approach to South Portal of Atal Tunnel, Source: BRO images

- **Avalanche Protection Structures.** Avalanche protection structures considerably downscale the risk to life and property posed by avalanches. Road from Palchan to South Portal of Atal tunnel experiences heavy snow fall[14]. To make this axis all-weather road, avalanche protection structures have been provided by BRO. Many such snow protection structures have been constructed by BRO on road leading to South Portal of Atal Tunnel.

  - **Snow Erodox**. The Snow Erodox is low cost, light, easy and fast to install structure with low environmental impact and can withstand dynamic impacts (rock/ice falls).



Snow Erodox System at South Portal of Atal Tunnel, Source: BRO images

  - **Snow Galleries**. Snow Galleries are direct defense measures for roads or highways in the middle zone of avalanches where snow removal becomes almost impossible.

Snow Gallery near South Portal of Atal Tunnel, Source: BRO images

- **Geosynthetic Cementitious Composite Mat.** Geosynthetic Cementitious Composite Mat (GCCM) is a new product, which is mainly used to line small drainage channels. BRO utilized the technology to construct lined drain on Road TCC – Taksing.[15]

GCCM being prepared to make drains along road TCC- Taksing, Source: BRO images

- **State-of–the-art Runway Drainage System.** There is an essential technical requirement to ensure draining out of surface and subsurface water for the long service life of the airstrip and safety of aircraft. In the runway at Barrackpore, a state-of-the-art sub-surface drainage system has been constructed by BRO. The runway was dedicated to the nation by Hon'ble Raksha Mantri on 12 Sep 23.

Sub-Surface Drainage System at Barrackpore Runway, Source: BRO images

- **Plastic-Coated Aggregates.** Safe disposal of waste plastic continues to be a very serious environmental concern across the globe. As an initiative to reuse the plastic waste, BRO has started using waste plastic extensively in bituminous road construction not only in India but also in Bhutan.[16]

Mixing of dry plastic waste with aggregate, Source: BRO images

Resurfacing using plastic waste on Phuentsholing–Thimphu Road in Bhutan, Source: BRO images

Resurfacing using plastic waste onBalipara-Charduar-Tawang Road, Source: BRO images

Black Topping using plastic waste on Hapoli-Sarli-Huri Road, Source: BRO images

Resurfacing using plastic waste on Hnathial-Sangau-Saiha Road in Mizoram, Source: BRO images

- **Inter Locking Concrete Block (ILCB) Pavements.** ILCBs are pre casted concrete blocks of varied dimensions and can be interlocked horizontally and vertically as per use. BRO has started using ILCBs since 2021 on pavement of roads at all mountain passes it maintains where heavy snowfall takes place and snow clearance operations by tracked Dozers lead to damage to bituminous layers. The damage caused by snow clearance operations to upper layers of roads leads to interruption in smooth traffic flow and also increases road maintenance cost exponentially. Overall, adoption of this technology will result in considerable cost reduction in construction and cyclic maintenance of roads at mountain passes.[17]

ILCB Pavement at Changla Pass on Karu–Tangtse Road, Source: BRO images

ILCB Pavement on Balipara-Charduar-Tawang Road (Sela Top) , Source: BRO images

ILCB Pavement on Bumla-Bumla PP Road, Source: BRO images

- **Precast Concrete Technology (Cut & Fit Technology).** BRO is working in one of the most difficult and harsh terrains of the world. These areas typically have very limited working season, completion of road projects in a time bound manner is therefore a huge challenge for BRO. In order to overcome these challenges and fast pace of construction of road, BRO is working on Cut & Fit technique in road construction. To telescope construction activities, all the elements of road are casted at a site ideal for casting process, while the formation cutting is under progress at higher reaches. With this technique, sequential construction is replaced with parallel construction activity to reduce the overall project duration and costs. Lot of work has been done on the pre cast culverts, pavements, reinforced earth walls, drains and breast walls during past few years.[18]

BRO has executed a pilot project on Along-Yingkiong Road in Arunachal Pradesh in 2022 at Panging with all the pre cast elements i.e. protective structures, culverts, drains and pavements. This technique turns out to be economical, if cyclic maintenance cost and escalation due to typical time over run of conventional road construction is taken into account.

Similarly, it has also been adopted in Ladakh for construction of pre-cast box culverts, which has been found to be extremely useful in speeding up construction and averting/reducing disruptions to traffic. Such culverts can be casted even in winters under suitable conditions when no work is possible at site. Each pre cast culvert is cheaper by approximately Rs 11 Cr as compared to conventionally constructed culvert.

Pre-cast Breast Wall & Drain on Along-Yingkiong Road, Source: BRO images

Construction of Precast Box Culvert in Ladakh, Source: BRO images

- **White Topping Technology**. A PCC layer is constructed on top of the existing bituminous layer. This layer imparts additional structural strength during rehabilitation of roads. A pilot project of white topping in BRO has been undertaken successfully at a heavy rainfall area for rehabilitation of road Tuting–Bona in Arunachal.[19]

- **Modular Bridges of Load Class-70.** Garden Reach Shipbuilders & Engineers (GRSE) in a Joint Venture with BRO has produced a CL-70R double lane modular bridge at 1/3rdthe cost of imported bridges with similar specifications. One such bridge of span 140 ft was launched on Flag Hill-Dokala road at an altitude of 11000 ft in Feb 2021.

  In view of cost effectiveness and time saving in construction, BRO and GRSE signed a MoU in March 2022 which was extended for 60 bridges in May 2023.[20] More than 30 of these bridges have already been constructed at most critical forward locations. This initiative by BRO will certainly be a game-changer in road infrastructure development in the country making this initiative a major step towards Atmnirbhar Bharat. These prefabricated structures are easy to transport and assemble, significantly reducing construction time and labour costs.

CL-70 Double Lane Modular Bridge on Flag Hill-Dokala Road in Sikkim, Source: BRO images

- **Cold Mix Asphalt Technology.** Cold mix asphalt technology has been a game-changer for the BRO, especially in remote and high-altitude areas where hot mix plants are not feasible. This technology uses bitumen emulsion at ambient temperatures, which significantly reduces energy consumption and greenhouse gas emissions[21]. The BRO has utilized cold mix asphalt for constructing and maintaining roads in Ladakh and Arunachal Pradesh, ensuring all-weather connectivity with minimal environmental impact.

- **Route Guidance System**. In past, BRO used to lose many operators and machines during snow clearance operations over high mountain passes, due to difficulties in estimating the correct road alignment due to heavy snow accumulation. To overcome this, BRO has identified sensor-based Route Guidance System after extensive trials, in which GPS server fed with road alignment data is attached to snow clearance equipment to obtain precise location of the road.[22] This has ensured enhanced safety to the operators during snow clearing operations. The equipment has been found to be very effective in identification of the road alignment during snow clearance.

Sensor Based Route Guidance System, Source: BRO images

- **Use of Steel Slag.** A pilot project has been undertaken by BRO on road Joram - Koloriang in Arunachal Pradesh by using steel slag in Nov 2022, which will be able to withstand heavy rains and harsh climatic conditions. The road constructed by use of steel processed slag not only increases the durability but also helps in reducing the cost of construction as slag-based materials have better properties than natural aggregates. This technology will reduce greenhouse gas emissions and in turn carbon footprint in fragile ecosystems where BRO is constructing roads on forward areas. BRO is now working out a long-term logistic arrangement for construction of steel slag roads in strategic areas.[23] This initiative taken by BRO has also been lauded by the Hon'ble Prime Minister. Construction cost of steel slag road is 30% less than the conventional road with 3 to 4 times higher strength than the conventional one.

THIS ROAD STRETCH HAS BEEN
CONSTRUCTED USING STEEL SLAG AGGREGATE

Road Stretch of Joram-Koloriang Road constructed using Steel Slag, Source: BRO images

- **Carbon Neutral Habitat at Hanle.** BRO has taken lead in construction of carbon neutral habitat for its newly inducted Task Force at Hanle to undertake many strategically important projects in Chumar sector.[24] Also to enhance induction of men, machines and material at faster rate in Ladakh, BRO has also taken major initiative to undertake construction of 3D printed complex at Chandigarh to house its detachment and storage facility. It is going to be world's largest 3D printed building complex soon.[25]

Carbon Neutral Habitat at Hanle (15000 feet), Source: BRO images

World's largest 3D printed complex in final stages of completion for BRO Ladakh Air Despatch establishment at Chandigarh, Source: BRO images

- **Green Construction.** BRO has co-opted environmental conservation practices in an institutionalised manner into the scope of its infrastructure projects thereby considerably extenuating the adverse ecological consequences of road construction activities. Few examples are given below:
    - Use of Steel Slag in lieu of aggregate in Arunachal Pradesh.
    - Use of Plastic in road construction in a big way.
    - Use of Geo textiles, Hydro Seeding, Bio Mass as slope stabilisation techniques on roads.
    - Use of Cut and Fit Technology at Panging in Arunachal Pradesh thereby all components of road from drains, breast walls, pavement members etc to be pre casted and fitted at location.
    - Energy Efficient Buildings at Leh.
    - Carbon Neutral Habitat at Hanle.
    - Use of Green Diesel in collaboration with IOC.
    - Use of pre fabricated culverts in Ladakh.
- **Mobile Containerized Accommodations.** Snow clearance has been one of the major tasks by BRO in the border areas to facilitate the movement of security forces and their logistic requirements. Mobile containerized accommodation is a prefabricated container mounted on a vehicle and it serves as moving shelter for persons working under harsh climatic conditions, thus reducing the movement of men and machine to detachments/nearest units and increasing efficiency. It is fitted with heating arrangements to provide immediate relief from harsh winters. Snow clearance of Leh-Manali highway was completed using this mobile accommodation, due to which snow clearance operations could be completed in faster time and with enhanced safety.

Conveyance of Mobile Containerized Accommodation in Ladakh, Source: BRO images

- **Induction of New Equipment/Vehicles.** Many new generation equipment/vehicles have been identified for induction post Galwan to achieve better efficiency in BRO.
  - **Tele-Operated Dozer**. A remotely operated Dozer BD-50 developed by CVRDE/DRDO is under the process of induction. It is equipped with Human Machine Interface (HMI) which can be carried out by any person or mounted on any B-vehicle. It will certainly reduce the casualty rate during formation cutting in most treacherous locations.
  - **Direct Methanol Fuel Cell (DMFC)**. DMFC is a green energy power generating device which converts chemical energy to electrical energy by using Methanol as the fuel. It has extremely low fuel consumption and will lead to major savings in fuel and related costs of logistics.
  - **JCB Tele-handler**. JCB Tele-handler machine is highly manoeuvrable equipment with a Telescopic Boom which can be fitted with numerous attachments at its end to enable several operations at extended height or reach with requisite safety and ease. The tele-handlers have huge applications in road construction and tunnelling operations as multi-utility construction equipment.

- **Super Long Front Excavator.** BRO has gone for 12 numbers, 65 Ton super long front excavators with 23.5 m long boom as a replacement of vintage draglines, which has been specially made by TATA Hitachi for BRO.
- **Other Multi tasking Equipment**. Equipment such as multi utility tractors, spider excavators, flat bed trucks, self loading concrete mixers, backhoe loaders with concrete mixture etc have been inducted to achieve economy of resources.

BRO has ensured adoption of multitude of innovative technologies, which are environment friendly and safe, during last 3-4 years. The priority for BRO now is construction of robust and maintenance free roads. There would be compelling requirement of dedicated R&D with special focus on permafrost soils in Ladakh and regions with heavy rainfall conditions.

Infusion of Niche Technologies

BRO is presumably the only Government organisation which has prepared and published 'BRO VISION 2047', its vision document to cover the period of Amrit Kaal.[26] In envisioning future development and reforms, several strategic initiatives, including infusion of niche technologies, have been suggested to enhance the construction capabilities of BRO.

Given the increasing complexity of modern warfare and the strategic challenges posed by China along LAC, it is imperative for the BRO to leverage niche technologies to enhance its capabilities. By integrating advanced technologies such as additive manufacturing, smart materials, sensor fusion, big data analysis, 5G/6G networks, the Internet of Military Things (IoMT), artificial intelligence (AI), quantum computing and green construction, the BRO can significantly improve its efficiency, effectiveness and synergy with the Armed Forces in joint war-fighting scenarios.

- **Additive Manufacturing.** Additive manufacturing or 3D printing can revolutionize the way the BRO constructs and maintains infrastructure. An initiative has already been taken in this direction by constructing world's largest 3D printed complex at Chandigarh to support construction of various strategic projects in Ladakh on mission mode. Also, Cut and Fit technology pilot project has successfully been undertaken to prove that use of pre cast components would revolutionise road construction not only by saving time and costs but also reduce carbon footprint in the fragile ecosystems of Himalayan ranges.

- **Smart Materials.** Smart materials have properties that can change in response to environmental conditions, offering numerous benefits for the BRO. These materials can repair minor damage on their own, extending the lifespan of roads and bridges and also reducing maintenance costs. Smart materials can adapt to changing conditions, such as temperature fluctuations or mechanical stresses, increasing the strength and longevity of border infrastructure. Adoption of such technology by BRO would certainly transform the work culture and practices in field thereby making its field units more effective and efficient.

- **Sensor Fusion.** Through sensor fusion BRO can increase situational awareness and decision-making in various ways at its most challenging construction locations. By integrating data from satellite imagery, ground-based sensors and UAVs, the BRO can monitor its work along LAC in real-time. This capability is crucial for assessing road conditions and planning critical construction activities. This fusion can also assist in evaluating weather and terrain conditions to simplifying designing and maintaining roads and bridges in remote locations.

- **Big Data Analysis.** Big Data analysis can be utilised to analyse historical data obtained from various sources to discern patterns and trends thereby predicting future challenges to enable efficient execution process through right climatic windows by optimisation of men, machines and materials on work sites. Advanced analytics would be able to support decision-making by providing actionable information into factors such as terrain suitability, risk assessment, and project prioritization.

- **5G/6G Networks.** BRO small detachments are sprung all along our land borders involved in construction and maintenance activities at remotest locations. Next-generation communication networks such as 5G and 6G can significantly enhance BRO's operations by providing backward and lateral real-time communications to these small detachments thereby reducing the risk factor to BRO Karmyogis working in harshest conditions. Such networks would also support telemedicine centres recently introduced by BRO in far flung areas. Three such centres were inaugurated by Hon'ble Raksha Mantri on 03 Jan 23 from Siyom in Arunachal Pradesh, located at remote and difficult locations of Project Vartak, Pushpak and Himank.[27]

- **Internet of Military Things (IoMT).** The IoMT enabled roads, bridges and tunnels would be able to monitor their own condition and report any discrepancies in real-time, reducing the need for manual inspections and enabling proactive maintenance. IoMT devices can track the location and status of construction equipment, materials and personnel, improving logistics and optimising dynamic allocation of all kind of resources thereby cutting down on costs and construction time considerably.

- **Artificial Intelligence (AI).** AI can revolutionize the BRO's operations by automating complex tasks of infrastructure planning, enhancing decision-making and improving predictive maintenance activities. Such initiative would not only make construction activities seamless but ensure reduction of downtime of machines and extend lifespan of roads and bridges. AI can also analyze surveillance data to predict natural calamities like landslides and avalanches to prevent loss of precious lives and damage to roads.

- **Quantum Computing.** Quantum computing can ensure significant benefits for the BRO in optimising resource allocation and construction schedules thereby cutting on project slacks and ensure avoidance of cost and time overruns. It can also assist in studying the terrain data to develop better quality and durable infrastructure along the borders.

Dignity and Social Security to CPLs

BRO employs approximately 70,000 casual paid labourers (CPLs) whose efforts are pivotal in executing the daunting tasks in inhospitable terrains. In a transformative move to uplift the living standards of CPLs, the organisation has provided an array of amenities designed to cater to both their professional and personal well-being. Prefabricated shelters, Porta Cabins, and Bio Toilets have been introduced to improve living conditions. Recognising the extreme weather they often face, the BRO has equipped CPLs with Super High-

Altitude Clothing, while recreational facilities have been established to bolster morale, leading to increased productivity and the ability to work for extended periods.

This comprehensive welfare approach was bolstered by a landmark decision in January 2024, when the Raksha Mantri approved a term insurance scheme for CPLs. Additionally, in September 2023, a policy was introduced to repatriate the mortal remains of deceased CPLs to their native places and cover funeral expenses, alleviating the burden on their families. Also, Raksha Mantri has approved a proposal to waive the requirement of completing 179 days at the time of accident for the payment of ex-gratia lump sum compensation to CPLs working in BRO. The combined effect of these welfare initiatives has been substantial, fostering a sense of dignity and security among CPLs.

Conclusion

BRO is an essential component of Indian Armed Forces, playing a crucial role in reinforcing Indian joint war-fighting capabilities, specifically in the context of potential conflicts with China. Through constant upgradation and maintenance of strategically critical border infrastructure, BRO facilitates swift movement of troops and switching of formations at the point of conflict to ensure moral ascendency, effective dominance and sustenance of military operations in the most harsh terrains and climatic conditions. Its contributions to quick military response supported by sustained logistics, force multiplication and decisive strategic extension to joint war-fighting mechanism are pivotal for maintaining an operational edge in high-altitude and remotely spaced conflict situations. Here are certain specific recommendations to facilitate the acquired momentum by BRO and assist it to further accelerate the development of infrastructure on our Northern borders to offset the existing roadhead differential in next 5-6 years.

There is a need for financial reforms in the BRO to ensure incremental fund flow and their efficient utilisation. This would involve greater budgetary oversight, improved financial management practices and better monitoring and evaluation of ongoing projects. There is compelling need to revise existing archaic norms for authorisation of equipment and allotment for funds for procurement of machines to undertake ensuing works. Infact the power to decide the type of equipment and machines required to undertake the strategic works should be delegated to the DGBR to avoid delays in prevalent procurement cycle.

The new technology and products not only enhance the quality of projects but also reduce time of construction and long term costs. There is a need to look at this aspect with open mind in the larger national interest while creating strategic roads and other projects. The BRO workforce needs to be equipped with the necessary skills to operate modern equipment effectively and adopt the latest technologies and construction methodologies to ensure effective execution of strategic works specially tunnels.

BRO is an integral part of Indian Armed Forces under Article 33 of the Indian Constitution and BRO is also probably the only uniformed organisation which is not governed by an exclusive Act. GREF cadre is governed by CCS (CCA) Rules, 1965; whereas Army component of the organisation is dealt by Army Act, 1950 and Army Rules, 1964. It is strongly recommended that BRO Act should be brought in for curtailing anomalies in the pay structure, to deal with disciplinary cases in just and fair manner and bring in more transparency and accountability in functioning of BRO towards Nation building. There have been too many agencies constructing roads in the same space. Such arrangement creates confusion of duplication of connectivity due to lack of inter-ministerial coordination and final accountability of poor quality or speed of work as at time 3-4 agencies are allotted patches of stretch on the same road. It is recommended that there should be “One Border- One Agency” policy promulgated to have clear demarcated areas of operation. Till that happens at least we must ensure “One Axis – One Agency” principle to ensure speed and accountability. Also roads built by BRO should not be handed over to state PWDs but continued to be maintained by BRO itself.

There is an urgent need to create a foreign wing of BRO to enable it to undertake infrastructure projects in friendly foreign countries to establish sub regional connectivity to promote trade, commerce and strengthening diplomatic ties. The government plans to set up BIMA for planned and comprehensive development of infrastructure on borders. One of the aims is to enhance the ongoing development of specific areas by increasing public-private partnership (PPP) and allocation of funds for completing works.[28] BIMA can be created initially as one of the verticals of BRO, because of a robust structure already existing at its Headquarters in Delhi. Subsequently it can be moved directly under MoD, to facilitate better and seamless integration with stakeholder ministries.

As border tensions continue to shape our continued deployment all along LAC, the BRO's role in strengthening security matrix and supporting joint military operations will remain preeminent. Post Galwan conflict, the BRO has embraced several niche technologies in its construction methodology. These advancements have not only enhanced construction quality but also expedited project timelines and ensured sustainability in environmentally sensitive areas. Integrating these newly adopted techniques and other niche technologies with joint war-fighting efforts by the Armed Forces will ensure that India is better prepared to address the strategic challenges posed by China and to maintain the security and integrity of its borders.

*****

Lt Gen Rajeev Chaudhry, VSM (Retd) on 30 Sep 2023 after 40 years of selfless service in Army. During his last assignment of DGBR for three years, he doubled the pace of work to meet stringent targets post Galwan clash and worked to get an incremental budget allocation of 160% for GS roads. He was honoured with Award of Construction World Person in Year-2021, CIDC Vishwakarma Award for Year 2022 and Institution of Engineers India Eminent Engineer Award for Year 2023 for his exemplary contribution towards infrastructure development on our land borders. He brought transparency in expenditure through increased use of GeM and ensured timely payments to the firms (90% of payments were made within nine days) for which BRO was awarded Gold Certificate for two consecutive years.

NOTES

1 Brig (Dr) Pathak, Ashok (Retd). "India ChinaBorder Dispute Packets of Information to Continuous Spectrum". Vivekanand International Foundation", January 27, 2023.

2 Junaid, Khola. "Emerging Technologies and their Impact on Warfare". Modern Diplomacy, June 11, 2024.

3 Kumar, Bhaswar. "Indian Military Theaterisation plans gather Pace…". Business Standard, May 15, 2024.

4 Lt Gen Chaudhry, Rajeev (Retd). "BRO : Looking Ahead, Going Beyond". Indian Aerospace & Defence Journal, May 2024, pp 20-26.

5 Maj Gen Chaturvedi , Ajay Kumar(Retd). "Infrastructure Development as a Force Multiplier". Vivekanand International Foundation, November 04, 2020.

6 Lt Gen Chaudhry, Rajeev (Retd). "Border Roads Organisation: Strategic Surge in Infrastructure". Destination India, May 2024, pp 52-55.

7 Lt Gen Chaudhry, Rajeev (Retd). "BRO : Looking Ahead, Going Beyond". Indian Aerospace & Defence Journal, May 2024, pp 20-26.

8 Lt Gen Chaudhry, Rajeev (Retd). "Surging Surface Infrastructure in Border Areas: Necessity as well as Asset for the Nation". Centre for Joint Warfare Studies, Issue Brief, April 08, 2024.

9 Mohan, Vijay. "BRO to employ Drones for faster, accurate Geological Survey in Road Construction". Tribune, October 07, 2023.

10 Lt Gen Chaudhry, Rajeev (Retd). "Surging Surface Infrastructure in Border Areas: Necessity as well as Asset for the Nation". Centre for Joint Warfare Studies, Issue Brief, April 08, 2024.

11 Singh, Rahul. "India moves to secure Key Flashpoint at LAC". Hindustan Times, September 29, 2023.

12 Choubey, Jitendra. "Steering Connectivity and Inclusion on the Frontiers". Geospatial World, October 18, 2022.

13 Dighe, Sandeep. "Border Roads Organisation Blazes a Trail in most Testing Conditions". Times of India, November 18, 2022.

14 Manta, Dipender. "Soon, Avalanche Protection Structures near Atal Tunnel". Tribune, June 27, 2021.

15 Choubey, Jitendra. "Steering Connectivity and Inclusion on the Frontiers". Geospatial World, October 18, 2022.

16 Dighe, Sandeep. "Our Focus is on Strategic Roads on Indo-China Border: BRO Director General Lt Gen Rajeev Chaudhry". Times of India, May 07, 2023.

17 Singh, Mayank. "More Boost for Infrastructure Development along LAC as BRO aims to make roads sturdier". New Indian Express, August 23, 2022.

18 Natam, Karda. "BRO Spearheading Road Construction along LAC". Arunachal Times, January, 2021.

19 Faridi, SA & Maria, R. "Everything is Possible through Hard Work". NBM&CW Magazine, March 2023.

20 TNN. "GRSE to Build 30 Modular Steel Bridges". Times of India, May 10, 2023.

21 Deb, Pinki & Singh, K Lakshman. "Mix Design, Durability and Strength Enhancement of Cold Mix Asphalt: A State-of-the-art Review". Innovative Infrastructure Solutions, February 2022.

22 Faridi, SA & Maria, R. "Everything is Possible through Hard Work". NBM&CW Magazine, March 2023.

23 Global Slag Staff. "Indian Border Roads Organisation using Steel Slag to Build Roads near Border with China". Global Slag News, September 29, 2023.

[24] Team India Sentinels. "BRO's First Carbon Neutral Habitat in Ladakh…". India Sentinels, October 28, 2022.

[25] Goyat, Ramesh. "The World's Largest 3D Concrete Printed Campus Built by BRO and L&T at Chandigarh". Daily Guardian, September 25, 2023.

[26] Lt Gen Chaudhry, Rajeev (Retd). "BRO : Looking Ahead, Going Beyond". Indian Aerospace & Defence Journal, May 2024, pp 20-26.

[27] Shukla, Ajai. "Rajnath Singh dedicates Rs 724 Crore Infra Projects to the Nation". Business Standard, January 03, 2023.

[28] Times of India, "Eye on China, Govt plans Border Infra Management Authority", May 02, 2022.

DATA: THE NEW MUNITION FOR JOINT WARFARE

Gp Capt Ankur Mathur

Abstract

Sometimes, existing technologies converge, mutate, or get creatively applied on battlefields to create a unique winning concoction. The fusion of big volumes of digital data and its assured transmission through battle networks is a crucial element of the modern battlefield. The side that manages it better, wins. Many emerging military technologies have data management integral to them. At the heart of emerging concepts of Multi-Domain Operations (MDO) is the ability to seamlessly transfer data across various domains. Cross-domain data transmissivity is therefore going to become an important capability, in ruggedized devices and networks. To overcome these, the Indian Armed Forces must implement modern data management concepts based on cloud computing and edge computing. To navigate the digitally connected battlefields, there is a need to formulate a Defence Data Policy framework. For establishing a tri-service data cloud and network protocol of cross-domain connectivity. IAF can be the lead service.

Introduction

Technology has always impacted warfighting. With emerging technologies, new concepts of warfighting emerge. Some of these concepts and their application on the battlefield profoundly impact the outcome of wars. Scholars refer to them as the Revolution in

Military Affairs (RMA). The human History of Warfare is replete with such examples. Whether it was the horse-driven chariots of the Indus Valley, or the Huns, Turks and Mongols who graduated from chariot to horse-riding, or the Chinese gunpowder that enabled a Musketeer to fire bullets from a distance, it was soon realised that when men of equal worth fight on unequal terms, the side with better weapons win[1]. However, it was not always the latest or the most advanced technology of the era that tilted the balance on the battlefield. Sometimes, it was the synthesis of existing technologies, their mutations, their creative application, or their convergence that created a unique winning concoction. A case in point was the success achieved by the 'great ships' of the European mariners of the 16th Century, who successfully combined their ship-building prowess with broadside firing cannons using gunpowder; shipbuilding, cannons and gunpowder being commonly known technologies at that time. Their convergence on a battleship changed the course of the history of naval warfare, and that of European Colonialism.

It is the converging technologies of today that have prompted some scholars to believe that 'The Future is Faster' than we think.[2] Converging technologies have transformed businesses, industries and even our daily routines. A case in point is the smartphone in our pockets which is fast, compact and much more powerful than a decade ago. Technology, in the military, will continue to have a huge impact. However, when it comes to forecasting warfare-based technology, the task becomes complicated. War tests technology to the hilt. War is also the testbed of technology. Hamish McRae, in his book 'The World in 2050' offers his advice on how to think about technology and its impact on the future[3]. As per him, the advancements in technology can be incremental or revolutionary. Incremental advancements, he says, are generally bounded by the Laws of Physics. But when human desires get added, which is what warfare has been all about, then revolutionary changes may also occur. Revolutionary technologies belong to the realm of 'unknown unknowns' and therefore are being left out of the scope of this paper.

The incremental rise in digital data across all facets of humanity and its processing has so far been following 'Moore's Law'[4]. The fusion of big volumes of digital data that gets generated by today's platforms and its assured transmission is one such arena that can potentially tilt the balance of force application towards the side that manages it better.

Data: The new Munition

Information and Communications Technologies (ICT), 5G/6G Wireless Networks, Artificial Intelligence (AI), Big Data Analytics, Machine Learning (ML), Autonomous Unmanned Vehicles, Sensor Fusion, C4ISR grids, and many more such emerging technologies have data management integral to them. In fact, at the heart of emerging concepts of Multi-Domain Operations (MDO), Joint All Domain Command and Control (JADC2) and Advanced Battle Management Systems (ABMS) is the ability to seamlessly transfer data across various domains[5]. Cross-domain data transmissivity is therefore going to become an important factor in any future battlefield.

Data has a crucial role to play in Defence Intelligence and ISR. Large datasets are generated by various ISR platforms, Satellites, the Internet, Social Networks and Digital Communications. For Defence Intelligence Agencies, sifting through this data becomes a challenge. Other hurdles of quality assurance, inter-agency security and legal compliance must be crossed before data can be presented for Command and Control (C2) functions or for the sensor-shooter loop. Of course, data needs to be tagged with a time stamp. Intelligence data in today's Information Age has a limited 'Shelf Life'. Hence, customised and intuitive products at the speed desired by modern wars are possible only through employing techniques of data sciences[6].

Artificial Intelligence (AI) promises to help Defence Intelligence Agencies overcome the '3V Challenge' (volume, variety and velocity) and reduce the risks concerning '2V' (veracity, value).[7] However, we now know how algorithms can be misinterpreted, what is now referred to as artificial stupidity.[8] Algorithms, if revealed to the adversary, can also be exploited. Better algorithms, apart from logic, require bigger data sets. Thus, as AI evolves from stupidity to intelligence, the need for big data is going to be insatiable.

Information Technology is transforming modern Air Defence architectures as well. The requirement of a robust air defence is well known. John Warden once remarked that "since the German attack on Poland in 1939, no country has won the war in the face of enemy air superiority."[9] To deny air superiority to the adversary, all modern air forces have been integrating their air defence elements across domains to achieve an Integrated Air Defence

System (IADS). Modern IADS include air surveillance, weapon control and battle management functions. By integrating various Surface Air Missile (SAM) systems, these IADS follow a 'System of Systems' approach.[10] As a C2 function in Battle Management, they enable seamless passage of data even to the last echelon, thereby improving redundancies, depth of communication and span of control. Multi-domain integration and multi-effect approach with malleable communication are key ingredients of modern IADS.

For an effective 'kill chain', these IADS are increasingly relying on functions like Threat Evaluation and Weapon Allocation (TEWA) to act as a decision assistance tool. Apart from technical data, a large quantity of historic dataset is required to provide the predictive modelling capability to these tools. As air defence threats expand into near-space (20-100 km), the role of these IADS will also expand to include Ballistic Missile Defence (BMD) capability and Space Domain Awareness (SDA) features. Data integration, correlation, distribution and dataset-based decision-making will therefore become quintessential.

All this is only possible if cross-domain data transmission protocols are well established. Data, its storage and analytics, and its transmission through associated battle networks are thus the new munition of warfare, ready to be employed effectively in 'Informationized' warfare. Likewise, its denial to the adversary, and disruption/ destruction of its associated networks, make it a legitimate target throughout the full spectrum of warfare.

Data: In Military Matters

Military Data and its associated ICT devices have certain attributes. Military organizations devote a large chunk of their ICT resources to ensure the secrecy of data. In the contested battlespaces, they also need to ensure that data transmission remains jam-resistant. Use of spread-spectrum techniques along with encryption are used to ensure data security and data assurance to the end user. Along with the digitisation of sensors, processing and decision elements, communication elements are increasingly becoming digitised. For communication links, apart from requirements of resilience to jamming, spoofing, interception and disruption, latency becomes an important factor. The need for near real-time data transfer of communication networks is an important factor in designing communication architecture. High latency makes communication ineffective. A case in point is a high latency of 0.5 seconds achieved by satellite-based communications operating through Geostationary Earth Orbits (GEO).[11]

Ruggedization of ICT devices and associated networks is a prerequisite that all military organizations must cater to. In addition, ICT devices in various domains viz land, sea, air and space, need to have ruggedization features suited to their medium. For example, land-based devices must cater to high temperatures and dust resistance, those at the sea would require saltwater protection while those in the air must cater to high vibrations and temperature variations up to several degrees sub-zero. Space ICT devices requires a special type of hardening, one that caters to a hostile space environment. Thus, unless ruggedized, most commercially off-the-shelf (COTS) ICT devices are unsuitable for military needs.

Military, unlike its civil counterparts, has no choice in deciding its workplace. The 'Work from Home' feature is ruled out. Moreover, their 'offices' vary from icy peaks to remote jungles, thousands of feet above the terra firma to meters deep in the oceans. These 'offices' are also prone to frequent relocation as per the needs of the situation. Their remoteness, and thus lack of a readymade ICT infrastructure leads to low data transfer rates at the end user. Hence, many of the existing ICT solutions, currently employed by Global Businesses and Industry, need tweaking to make them compatible to military use. To overcome the challenge of end point connectivity, militaries across the globe are trying to employ WiFi and SATCOM (Satellite communication) links. Both however have low bandwidth as compared to Optical Fibre Cable (OFC) enabled networks. However, as the incremental technologies progressively evolve, 5G/6G WiFi networks and Low Earth Orbit (LEO) satellite-constellation-enabled StarShield network (military version of Elon Musk's StarLink) are promising high-speed low latency data throughput rates as high as 610 Mbps.[12]

Information Technology (IT) in the 21st Century has continued on its upward trajectory. As storage, networking and data processing speeds improve; this along with the falling manufacturing costs and increased miniaturization of chips are paving the way for new IT products each year. Cloud Computing is one such technology that has shown promising results. With a Cloud, it is possible to back-source the processes of data storage, applications, services, security, management and even infrastructure[13]. Private Enterprises benefit from it as these Cloud services are available for hire, thereby reducing the cost of maintaining and sustaining them. The idea has caught the attention of the Defence Industry as well, with many well-known companies like Thales offering Defence Cloud services for Military use.[14] US Dept of Defence (DoD) has issued detailed guidelines in the form of the DoD Cloud Strategy in 2018 to leverage the technology for US Military.[15] The US Army, in 2020 has come out with its independent document in the form of The Army Cloud Plan.[16]

It therefore seems that Cloud Computing may have all the answers to the challenges of Military data handling. Not quite so. Cloud Computing has solved the problem of data processing and storage by obviating the size, weight and power requirements of the equipment required at the tactical end of the battlefield. However, Cloud strategies rely heavily on long-distance high throughput low latency data links, which are hard to establish in remote areas and a highly contested IEW (Information and Electronic Warfare) environment[17]. On the other end of the computation spectrum are the promises given by another technology, that of Edge Computing.[18] The difference is in the place where computation is being carried out. In this case, it is as close to the place where data is being generated. Such a concept can be applied to sensors that do not suffer from limitations imposed by size, weight and power. Pre-processed or presentable data can therefore be transmitted to the end user, thereby shrinking data processing times as well as the overall quantum of data to be transmitted.[19] Edge Computing is being extensively used in the Space domain, with India-based Space startups like KaleidEO and SkyServe demonstrating such capabilities.

New and transformative architectural technologies like Cloud Computing and Edge Computing have their inherent advantages. Their applicability to the needs of military battle networks will vary across domains. Since the panacea is yet to be found, data optimisation will be the key to the 'Data Centric' approach to military networks.[20]

Data: A Joint Strategy

Large datasets generated by today's digital platforms become a strategic asset. Its sovereignty, standardisation, security, storage and exploitation as per the needs of the country therefore assume great importance. In the Armed Forces, thousands of gigabytes of digital data is generated every day by various sensors and weapon platforms. Irregular storage management, insufficient format standardisation, undefined data access protocols and lack of data accountability may lead to a large amount of this crucial data being lost. There may be a lack of recognition across the Armed Forces that data is important. Data is a critical component of all analytical tools, Machine Learning (ML) algorithms and AI-based software. Predictive modelling based on Neural Networks, where pattern recognition is the key, requires a large amount of training data. Quality of data also plays a crucial role in providing high assurance rates to predictive modelling. Hence, digital data archiving, storage, format standards and quality, all become important.

Interoperability of battle networks is a crucial area which the Armed Forces must consider holistically. Interoperability has costs associated with it. Interoperability will require data standardisation across sensors, shooters, backend servers, processing units, networks and more, which eventually may not be feasible. However, interoperability is not binary. It is possible to define the degree of interoperability.[21] It will also be worthwhile to understand that interoperability at different levels of the network will have different challenges. Data sharing at the backend will be fundamentally different from data sharing at the tactical edge. Hence, the Armed Forces may look at data-specific access protocols instead of an overly ambitious all-out interoperability.

Interoperability of Defence Communication is another emerging data-driven environment. With the ubiquitous presence of digital communications, Armed Forces across the globe are now opting for Software Defined Radios (SDR). These SDRs have inherent flexibility, interoperability, security and spectrum efficiency advantages.[22] In India too, Armed Forces across the domains are procuring SDRs as per their service needs. Indigenisation of SDRs is also underway at Defence Research and Development Organisation (DRDO). SDR technology requires a standardised operating software environment and associated applications, known as waveform. Portability and interoperability among the SDRs are only possible with such standardisation[23].

With so much reliance on data and its associated networks, Counter Battle Network Operations are going to be the first among the target list of the adversary's most probable Courses of Action (COA). Armed Forces therefore need to formulate strategies to mitigate the effects of both the kinetic and non-kinetic weapons that the adversary may employ actions against their battle networks. However, this threat perception must not lead to actions bordering paranoia. An overly sensitive approach to the security and secrecy of data and networks becomes counter-productive to battlefield efficiency. It is therefore important to segregate data and networks according to their merit. Encryption standards across networks must therefore vary depending on the data type, thus enhancing the required degree of interoperability for non-critical data.

United Kingdom Ministry of Defence in their document titled 'Data Strategy for Defence' describe data as their second most important asset, only behind their People. Consequently, this document describes the journey to formulate 'rules of the road' for Defence related data.[24] The US Dept of Defence (DoD) has also come up with its own DoD Data Strategy. The key focus areas of the document are Joint All Domain Operations, Decision support to Senior Leadership and Business Analytics. It aims to make defence data visible, accessible, interoperable, trustworthy and secure.[25]

Indian Armed Forces also need to formulate a Joint Defence Data Policy framework. This framework should include Defence Data Management Strategy, Defence Data Network Protocols, Defence Data Encryption Standards, Defence Data Storage and Retrieval Policy, Defence Data Analytics and AI Tools Application Protocols, to name a few. These can flow from an overarching Defence Data Strategy. Such a document can become the guiding light for future ICT procurements, networking and software designing, defence industry standards for partnership, collaborations, and even promoting indigenization.

Data: The India Way

The Ministry of Electronics and Information Technology (MeitY), under the Government of India (GoI), is entrusted with the issuance of data policies in the public domain. Consequently, the Ministry has issued the India Data Accessibility and Use Policy in 2022.[26] For data management, the Ministry has announced the setting up of the India Data Office (IDO). For data management, each ministry is to nominate a Chief Data Officer, who in turn will be responsible for the implementation of policy, data access and sharing, data quality and metadata standards. This policy, along with the National Data Governance Framework Policy, aims to provide the much-needed standardisation and allocate responsibility for data management across ministries under GoI. However, the real success story of Digital India has been the combined power of UIDAI (Unique Identification Authority of India), open APIs (Application Programming Interfaces) and UPIs (Unified Payment Interfaces), which together have transformed the digital landscape of the country[27]. This is an apt example of how to set up required digital protocols under a policy framework, provide centralised regulation, while at the same time, allowing enough latitude for public-private innovation to be fostered.

The Ministry of Defence (MoD) has also taken certain positive steps in this direction. To enable waveform interoperability among SDRs provided by various vendors, the Ministry has developed a reference implementation of India specific operating environment called India Software Communication Architecture (SCA) profile or Indian Radio Software Architecture.[28] Artificial Intelligence has been given a big push by the formation of the Defence AI Council (DAIC). Consequently, a list of AI-based products that can be tailored exclusively for Defence needs has been created. Both public and private companies are being encouraged to partake in the development of AI-based products for Defence.[29]

In the past few decades, the Indian Armed Forces have been trying to achieve Net-Centricity. Since 2010, The Indian Air Force (IAF) has created its secure pan-India networks in the form of AFNET. The Integrated Air Command and Control System (IACCS) that also rides on AFNET has undergone various upgrades and today supports one of the most robust and secure Air Defence (AD) architecture. The Indian Navy has been constantly upgrading its Trigun Network to achieve Maritime Domain Awareness (MDA) by integrating various inputs from coastal surveillance radars, Automatic Identification System (AIS) equipped vessel data through satellites, and vessel traffic management systems, among others.[30] Under project Akash Teer, the Indian Army aims to integrate all its sensors and shooters through a network.[31] While service-specific Net-Centricity is being achieved rapidly, interoperability is on the back burner.

To overcome this shortcoming, a tri-service Defence Communication Network (DCN) is being established.[32] However, by adding another network layer, the problem of interoperability of networks and cross-domain data access remains as it is.[33] The fact of the matter is that interoperability of networks and seamless data transfer is a worldwide challenge, with leading militaries like that of the US still grappling with it. Many of their previous efforts, like the Joint Tactical Radio System (JTRS) and Joint Enterprise Defence Infrastructure (JEDI) went awry.[34] Despite the buzzwords of MDO and JADC2, even today, each of their services continues to pursue independent service-specific network solutions. Hence, the Indian Armed Forces must quickly abandon an overambitious approach to cross-domain transmissivity. Instead, a more pragmatic approach is advocated.

One such pragmatic approach involves nominating a 'Lead Service'. This lead service is to formulate the standards of network protocols, encryptions and security across all domains within the Armed Forces. Such an approach will benefit from the existence of an already established IT infrastructure, a networking architecture, a trained human resource, and institutional experience in the implementation of policies, thereby reducing costs and accelerating success. While following such an approach, however, the lead service needs to take cognizance of the domain-specific needs of other services and must be able to tailor its network accordingly. Here, it is suggested that the well-established net-centricity of the IAF or any other service can be harnessed to conceptualise a tri-service data cloud and network protocol of cross-domain connectivity. The end-point data connectivity to remote users across domains may be provided by using secure WiFi networks and Satellite links. Also, as has been mentioned earlier, services must jointly choose which data needs to be shared within the sub-layers of the network, thereby optimising the data bandwidth requirements of the entire network. Domain-specific Net-Centricity efforts must be continued concurrently.

Along similar lines, another practical approach may involve nominating a 'Lead Command'. Since the contours of the Joint Commands have started to emerge, one among the newly formed Joint Theatre Commands can be entrusted with the task of quick implementation of a new Joint Network. Defence Cyber Agency (DCyA), under Headquarter Integrated Defence Staff (HQ IDS) can help in this endeavour. Thus, the Lead Command becomes the test bed for creating a larger tri-service interoperable network in the near future. A *de-novo* approach that leverages existing data science technologies and ICT expertise, available through public-private collaboration, can produce exciting results. Implementing modern data management concepts based on cloud computing and edge computing in the short term, and wideband wireless networks and Space-based LEO constellations in the long term, can be used to meet the data needs of the 'digital' soldier/ sailor/ airmen.

Conclusion

So far, it has been discussed that in war, it is not always the newest technology that provides the edge to one side. At times, it is the amalgamation of several existing technologies that can create conditions necessary for victory. With terms like Data-Centricity, Multi-Domain Operations and Informationised War entering the military lexicons, more is being demanded from data and their battle networks. Data management in the Armed Forces needs urgent attention. It will be the lifeblood of many emerging technologies. Formulating a Joint Data Strategy is a good approach to data management across all domains. The success of Digital India has provided the much-needed ray of hope in formulating a nuanced Defence Data policy. Indian Armed Forces must abandon the over-ambitious tri-service integration of networks. Instead, a more pragmatic approach needs to be taken. With the formation of Joint Structures in the Indian Armed Forces moving from the planning to implementation stage, the jointness in 'hearts and minds' needs to progress to jointness in 'bits and bytes'.

*****

Gp Capt Ankur Mathur was commissioned in the Fighter stream in June 2001. He has 2600 hours of flying experience on various fighter aircraft like MiG 21, MiG 29 and Hawk Mk 132. He is Qualified Flying Instructor and an alumnus of Defence Service Staff College, Wellington. He has undergone Higher Air Command Course and Warfare and Aerospace Strategy Program at College of Air Warfare. He is presently posted as Chief Operations Officer of an operational base in Eastern Air Command.

NOTES

[1] John Keegan, A History of Warfare, (Pimlico ed. 2004), pp 38,161,328

[2] Peter H. Diamandis & Steven Kotler, The Future is Faster than You Think, (Simon & Schuster,2020).

[3] Hamish McRae, The World in 2050, (Bloomsbury Publishing, 2022), pp 139-141

[4] www.investopedia.com, "What Is Moore's Law and Is It Still True?", available at https://www.investopedia.com/terms/m/mooreslaw.asp, accessed on 03 Jun 24.

[5] RAND Corp, "What Is JADC2, and How Does It Relate to Training?", available on https://www.rand.org/pubs/perspectives/PEA985-1.html, accessed on 03 Jun 24.

[6] Paul B. Symon and Arzan Tarapore, "Defense Intelligence Analysis in the Age of Big Data", (Issue JFQ 79, October 2015, National Defence University Press), available on https://ndupress.ndu.edu/Media/News/Article/621113/ defense-intelligence-analysis-in-the-age-of-big-data/, accessed on 03 Jun 24.

[7] István Szabadföldi, "Artificial Intelligence in Military Application – Opportunities and Challenges", (Land Forces Academy Review Vol XXVI, No.2(102), 2021), available on https://sciendo.com/article/10.2478/raft-2021-0022, accessed on 03 Jun 24.

[8] Sydney J. Freedberg Jr., "Artificial Stupidity: Learning To Trust Artificial Intelligence (Sometimes)", (2017, Breaking Defense), available on https://breakingdefense.com/2017/07/artificial-stupidity-learning-to-trust-the-machine/, accessed on 03 Jun 24.

[9] John A. Warden, III, The Air Campaign: Planning for Combat, (toExecl,2000), pp 13

[10] Peter W. Mattes, "Systems of Systems: What, Exactly, is an Integrated Air Defense System?", The Mitchell Forum (No 26, June 2019), available on https://mitchellaerospacepower.org/wp-content/uploads/2021/02/a2dd91_2f17e209f90f4aaab80b116e4d139eb4.pdf, accessed on 03 Jun 24.

[11] Todd Harrison, "Battle Networks and the Future Force: Part 1", (Center for Strategic & International Studies, August 2021), available at https://aerospace.csis.org/battle-networks-and-the-future-force/, accessed on 04 Jun 24.

[12] Max Polyakov, “The Future of Starlink: Hidden Military Potential”, (Max Polyakov News Space, August 2023), available at https://maxpolyakov.com/hidden-military-potential-of-starlink/, accessed on 04 Jun 24.

[13] https://www.geeksforgeeks.org/cloud-computing/, accessed on 04 Jun 24.

[14] News report, “NATO selects Thales to Supply Its First Defence Cloud for the Armed Forces”, (Express Computer, Jan 2021), available at https://www.expresscomputer.in/news/nato-selects-thales-to-supply-its-first-defence-cloud-for-the-armed-forces/72213/, accessed on 04 Jun 24.

[15] DoD Cloud Strategy, 2018, available at https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF, accessed on 04 Jun 24.

[16] US Army’s The Army Cloud Plan (2020), available on https://api.army.mil/e2/c/downloads/2020/09/11/81bb912e/the-army-cloud-plan-2020-final2.pdf, accessed on 04 Jun 24.

[17] Todd Harrison, “Battle Networks and the Future Force: Part 1”, (CSIS) pp7

[18] Stephen J. Bigelow “What is edge computing? Everything you need to know”, available on https://www.techtarget.com/searchdatacenter/definition/edge-computing, accessed on 04 Jun 24.

[19] Todd Harrison, “Battle Networks and the Future Force: Part 1”, (CSIS) pp 6-7

[20] Jerome Dunn, “What “Network-Centric to Data-Centric” Really Means”, (Booz Allen Hamilton), available on https://www.boozallen.com/insights/defense/defense-leader-perspectives/what-network-centric-to-data-centric-really-means.html, accessed on 04 Jun 24.

[21] Todd Harrison, “Battle Networks and the Future Force: Part 2”, (Center for Strategic & International Studies, November 2022), pp 6, available on https://aerospace.csis.org/battle-networks-and-the-future-force-part-2/, accessed on 04 Jun 24.

[22] Dinesh Kumar Pandey, “Software Defined Radio: Enhancing Communication Capabilities”, https://capsindia.org/software-defined-radio-enhancing-communication-capabilities/

[23] News report, Economic Times, “Defence ministry accords high priority to Indigenisation of Software Defined Radios”,(26 July 2022), available at https://government.economictimes.indiatimes.com/news/technology/defence-ministry-accords-high-priority-to-indigenisation-of-software-defined-radios-for-armed-forces/93130708, accessed on 04 Jun 24.

[24] UK Ministry of Defence, Data Strategy for Defence (2021), available at https://assets.publishing.service.gov.uk/media/614deb7a8fa8f561075cae0b/Data_Strategy_for_Defence.pd, accessed on 03 Jun 24.

[25] US DoD, DoD Data Strategy 2020, available at https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF, accessed on 04 May 24.

[26] India Data Accessibility and Use Policy, (MeitY ,GoI, 2022), available at https://www.meity.gov.in/writereaddata/files/India%20Data%20Accessibility%20and%20Use%20Policy.pdf

[27] Divya Goel, "From Platforms to Protocols: India's Story of Leapfrogging Financial Inclusion ", (MEDIUM, 2022), available on https://medium.com/digitalhks/from-platforms-to-protocols-indias-story-of-leapfrogging-financial-inclusion-c5c127ec57a2, accessed on 04 Jun 24.

[28] PIB Delhi, "Aatmanirbhar Bharat': MoD accords high priority to indigenisation of Software Defined Radios for the Armed Forces", (26 Jul 2022), available at https://pib.gov.in/PressReleasePage.aspx?PRID=1844825

[29] Dept of Defence, MoD India, "AiDef" (2022), available at https://www.ddpmod.gov.in/sites/default/files/ai.pdf, accessed on 04 Jun 24.

[30] Anil Chopra, "Towards an Integrated Military Future", (Anirveda,2021), available at https://raksha-anirveda.com/towards-an-integrated-military-future/, accessed on 04 Jun 24.

[31] Ibid

[32] Ibid

[33] Sunil Srivastava, "JOINT C4ISR FOR THE INDIAN ARMED FORCES- QUO VADIS?", (CENJOWS, Vol I, Issue 1, O t 2022), available at https://cenjows.in/wp-content/uploads/2022/10/1-Joint-C4ISR-for-The-Indian-Armed-Forces-by-Lt-Gen-Sunil-Srivastava-Retd.pdf, accessed on 04 Jun 24.

[34] Ibid, pp 6

INFORMATION DOMINANCE: KEY ENABLER IN MULTI DOMAIN OPERATIONS

Brig Rajeev Ohri, VSM (Retd)

Abstract

Various erstwhile domains which were isolated but contributing to national power have been synergised through Information Domain. This has resulted in a paradigm conceptual shift with emergence of concepts like MDO and its contribution to CNP. The paper attempts a full spectrum understanding of information domain i.e. what all does it encompass, impact of compute and communication fusion and high speed wireless technologies, information domain sovereignty, niche and emerging technologies convergence, impact on new world order and civil military fused organizations and structures required to seamlessly absorb, manage and utilize these technologies to be ahead of the conflict/ competition curve in MDO scenario. The key to successful conduct of MDO is realignment from a technology centric to Protection, Control and Denial (PCD) based capability centric approach. Convergence of national resources in Information domain is the key to conduct MDO of the future.

Introduction

The world is transitioning from a bipolar to a multi polar geo strategic arena with aggressive competition in multiple domains other than military. Our national endeavour to restructure world organisations and realign international power structures is also based on emergence of multiple domains which are contributing not only to Comprehensive National Power (CNP) of a nation but also a new world order. The traditional way of power evaluation, has also undergone a transition with emergence of multilple domains other than military playing a major role in national power projection. National Security, a subject which was considered a military exclusive and limited to land, air and sea domains has now graduated to a multi domain 'Whole of Nation' approach. Equally important is the synchronization of military capabilities with nationally integrated Instruments of Power.[1] The reasons for this shift need to be understood to identify core areas which have a direct bearing on national power and security. Emergence of concepts like Multi Domain Operations (MDO) (see Figure 1) are conceptually linked to CNP. MDO existed from ancient warfare times, but ability to conduct MDO through combination of Kinetic and Non-Kinetic means is a paradigm shift in recent times. The Non-Kinetic component is fundamentally everything other than the land air and sea domains. Since information domain plays a key role in synergising this capability it has become a major binding component of MDO and National Power. Information domain impacts efficiency of all domains. Ability to influence, convince and persuade beyond national boundaries has tremendously enhanced due to Information and communication technology transformation. Capabilities in niche technologies in Information domain need to be strategically synergised for Information dominance in MDO scenario. It will not be an exaggeration to say that concept of MDO has emerged because of Information domain.

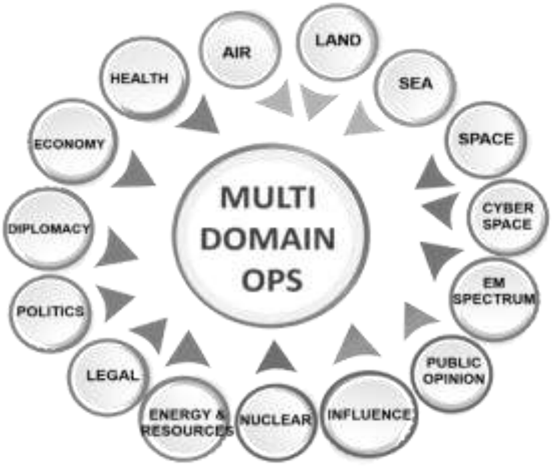


Figure 1 : Multi Domain Operations

Information Domain Emergence and Its Implications on MDO and CNP

The developments in Information domain in last few years has globally transformed war fighting and conceptually changed the security paradigm of many Armies and countries. A careful look at the multiple domains clearly brings two aspects viz each domain has an information domain backbone on which it is surviving and secondly the synergistic impact and linkage of each domain towards national power is made possible through information domain. Therefore, information has become an all encompassing domain which is critical for not only day to day successful operation of all domains but ability to share information across domains is the main enabler for synergizing multiple domains resulting in comprehensiveness in National Power.[2]

In order to catalyze MDO, strategic culture along with information domain awareness within each ministry/ department handling each domain needs to be built. The traditional national organizational structures which evolved with evolution of technologies, now need to realign to the converged information domain reality. Certain ministries like Ministry of Electronics and Information Technology (MEITY), Communications and I&B need convergence at National level for synergizing information domain for efficient MDO capability. Organisations need realigning from a technology centric to capability centric approach. Accordingly, regrouping of technology based organisations into capability based structures will be step in right direction for effective MDO capability.

Each domain requires three major capabilities viz Protection, Control and Denial (PCD). Protection is basically defence of the assets. We can also categorise it as Resource Enabler. Denial is offensive capability to deny the resources to adversary, or Resource Disruptor and Control is asset management or Resource Management to utilize the domain resources efficiently. Enhancing capabilities to protect own critical assets and deny these to the adversary in all domains have become vital to the National Security construct. Since Information Domain is the key to MDO, PCD concept template is recommended to be applied on this domain to generate national capabilities. It is important to not only handle the domain holistically but also have dedicated national level agencies for Protection, Denial and Management of Critical Information Infrastructure. Since Defence Networks are an important asset of this Information Infrastructure, national expertise in both Civil and Military holds the key towards building capacities in securing, management and denial of not only defence networks but also information domain involved in national capability building. Erstwhile concept of segregating military from civil is no more relevant in 21st century multi domain whole of nation approach to conflicts / competition. Each domain organization needs to create a PCD capability within itself, besides the national level information domain PCD capability.

It is important to understand full spectrum understanding of information domain i.e. what all does it encompass, what is the new paradigm and emerging red lines on information domain sovereignty, where are niche and emerging technologies converging towards impact on new world order and finally the organisations and structures required to seamlessly absorb, manage and utilize these technologies to be ahead of the conflict/ competition curve in MDO scenario.

Information Domain : Emerging Technologies and Imperatives

Major technologies which have transformed the concept and conduct of operations in 21st century are primarily in Information domain. Core technology pertaining to Information and Communications Systems, Cyber,[3] EW and Space has majorly impacted our C4ISR (Command, Control, communication, Computer, Intelligence, Surveillance and Reconnaissance), degradation capability, OODA (Observe, Orient, Decide, and Act) cycles, Non-contact warfare through autonomous platforms, predictive analysis through AI and Big Data and overall ability to impose will on adversary with better perception management capability. The paradigm shift of flow of Info from wired to wireless domain has brought convergence of Cyber and EW domains. Accordingly, concepts on Cyber & Electro-Magnetic Activities (CEMA) have evolved in major Armies of the world.

The two major technology disruptions which are impacting Information domain and MDO are convergence of compute and communications and high data rate communication capability from wired to wireless domain. The erstwhile Combat Net radios which were the only means of exercising Command and Control are now getting replaced by Software Defined Radios, 4G/5G mobile communications, high bandwidth capable Satellite handsets with inbuilt information processing capability for Navigation, Decision Support and military utility applications. This has resulted in major enhancements in Mobility, precision, battlefield transparency, shared situation awareness and overall shortening of OODA loop. If UAV (Unmanned Aerial Vehicle) / drones have revolutionised warfare, then the backbone of this revolution is Electromagnetic Spectrum (EMS) domain. From a spectrum perspective, all flow of info takes place in the EM Spectrum which has expanded from HF (High Frequency) / VHF (Very High Frequency) to the extremities of Light Waves. Therefore, denial of spectrum to adversary, control of vital Info flow, electromagnetic sovereignty and extraction of vital data and intelligence from spectrum have become synonymous with national power. In other words, spectrum has become a important sub domain of information warfare as is evident from organisation changes carried out by leading armies of the world. The EMS aspects need to be understood from Indian defence forces context in conjunction with existing pillars of our information philosophy. Creating CEW (Cyber and EW convergence) enabler and disruption capabilities is the recommended technology way ahead in Indian context.

Since synergy of MDO in modern warfare is enabled by Info domain, it is imperative that ministries like Railways, Telecom, Space, Air and Surface Transport, Power, Finance, Information and Broadcasting etc which are directly or indirectly involved towards defence capability, create strategic verticals for better planning, coordination and execution of projects for understanding impact of their overall capability to defence and CNP. Their information networks and data are vital targets for adversary information offensive and have a huge impact on our national defence capability. It is evident that this information domain linkage amongst ministries or domains requires a strategic infusion in all relevant ministries. Civil Military Fusion holds the key to this infusion and conduct of successful MDO.

Creation of National Critical Information Infrastructure (NCII) was a felt need in cyber domain and accordingly a protection centre was created. The NCII includes everything from financial systems and energy grids to transportation networks and government operations. Criticality of these domains for not only military but also for national power make them vulnerable to adversary info attacks. In order to protect the NCII from malicious actors, it is important to have a robust security strategy in place. Cyber and EM sovereignty is gaining more importance than our traditional borders. There are large number of stake holders, as far as the NCII is concerned.[4] These include Transport, Telecom, Power and Energy, Banking and Financial Institutions, Strategic and Public Enterprises and Government offices (see Figure 2). Each one of these sectors / organ has a charter to protect its assets. The role of the military in protecting NCII is limited to the protection of their own assets, just like every other stakeholder. With Info and Spectrum becoming key components of National Power, creating capabilities for its defence along with denial of this capability to adversary have become imperative for any nation.

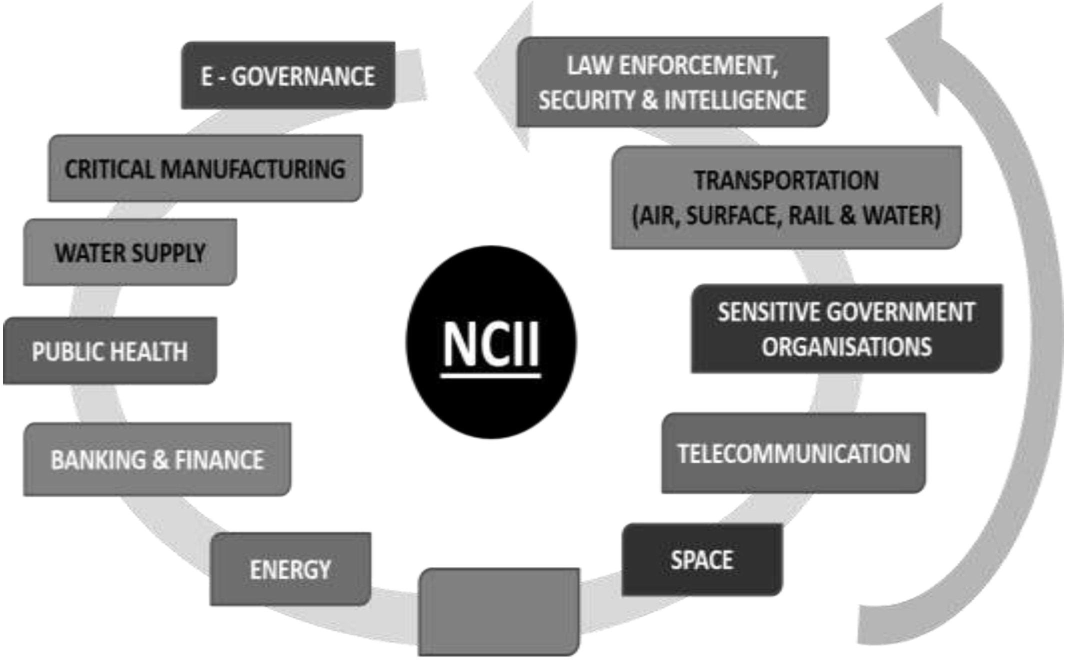

E - GOVERNANCE
LAW ENFORCEMENT, SECURITY & INTELLIGENCE
CRITICAL MANUFACTURING
TRANSPORTATION (AIR, SURFACE, RAIL & WATER)
WATER SUPPLY
NCII
SENSITIVE GOVERNMENT ORGANISATIONS
PUBLIC HEALTH
BANKING & FINANCE
TELECOMMUNICATION
ENERGY
SPACE

Figure 2 : National Critical Information Infrastructure

Capability Development in Information Domain

Lack of CMF has resulted in Indian Armed Forces lagging behind in terms of technology. This is inspite of India being a superpower in the fields of information communication technology (ICT) and space. While the IT sector is booming, with new startups and businesses emerging every day, the Armed Forces are still struggling to evolve into an agile eco system at par with national industry with adaptive capability for technology absorption.

Spectrum is the domain that needs major attention due to shift from wired to wireless and the convergence of Cyber and Electro Magnetic Spectrum operations. However, it is also the domain where expertise lies with the Academia, R&D and Industry. Synergy between the Armed Forces, Research and Development (R&D), Academia and Industry would prove to be a powerful engine of innovation and is a must for achieving the desired end state of Info Domination through CMF.

The Indian Armed Forces can benefit immensely from this synergy. The industry has the required expertise and experience to help the armed forces modernize their capabilities specially in areas of non kinetic warfare. The two can also cooperate in research and development to develop new technologies that can be used by the armed forces. It would also go a long way in fueling the dreams of “Make in India” and “Atmanirbhar Bharat”.

However, for this synergy to be effective, the CMF in the Info Domain has to follow a whole of nation approach, with an Umbrella Information Organisation (see Figure 3) at the National level. This has to be an empowered Info domain organization, with cross ministerial linkage with MeitY, Information and Broadcasting (I&B), Finance and the Industry ministries. Such an umbrella org is the solution to handle Info domain holistically and create synergy amongst all stakeholders. This will also provide a template for capability based organization rather than technology centric approach. Convergence of national resources in Information domain is the key to conduct MDO of the future. All domains also need to build PCD capability around this template, so that there is a seamless connect between various ministries and MDO agencies. Since defence domain is one of the main components of MDO, need for Information Command (Figure 4) on similar capability based organization is imperative. This will synergise our national resources for suitable national MDO capability on lines of developed nations and counter response to northern adversary information domain organization.

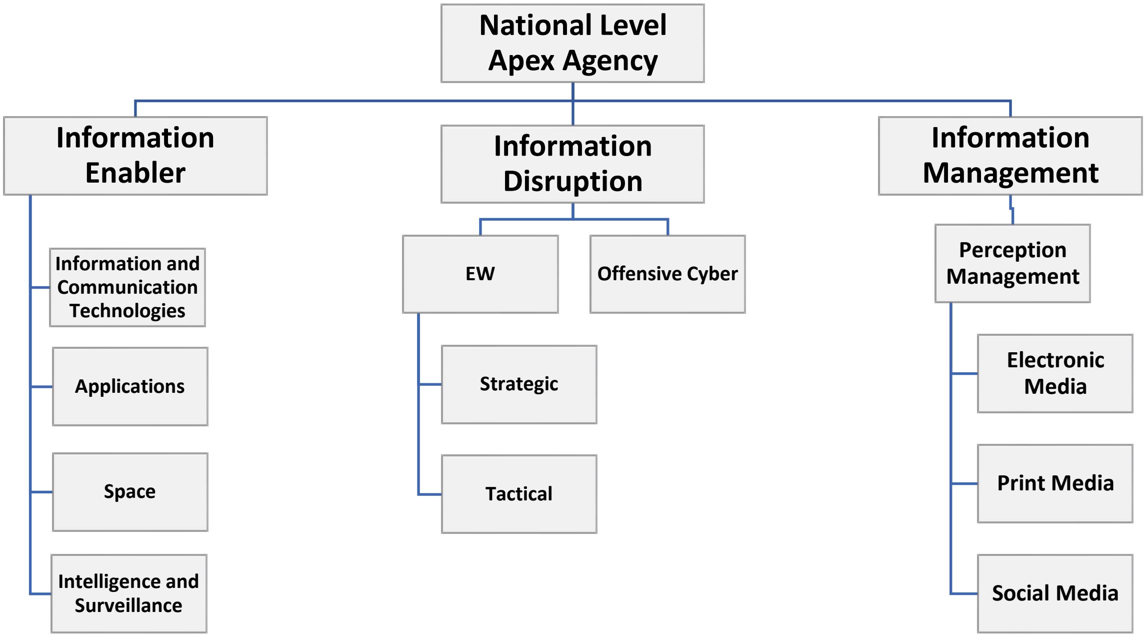


Figure 3 National Information Umbrella

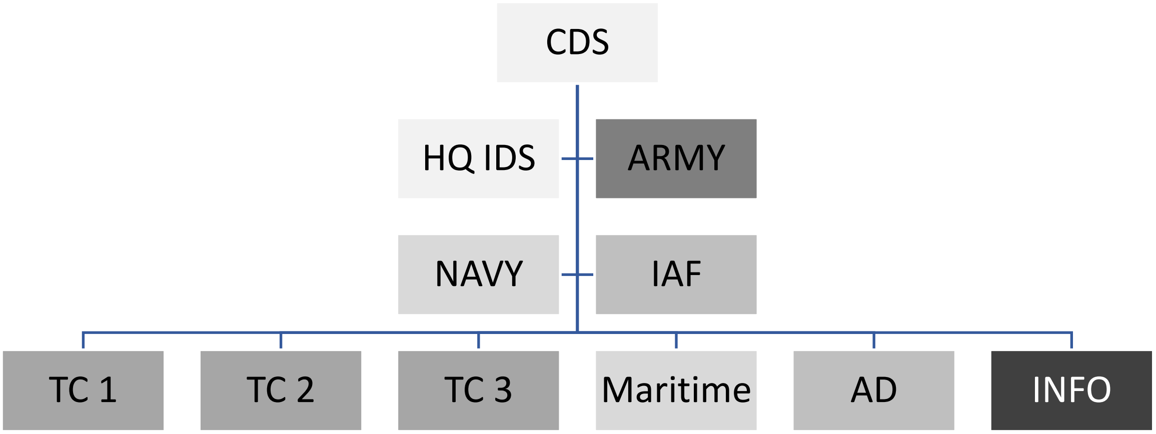


Figure 4 : INFORMATION COMMAND - KEY TO MDO

Further sub division of Info enabler verticals needs to be based on synergy of various niche emerging technologies based on logical grouping given in Figure 3 above. This will pave the way for futuristic coherence of emerging technologies into tangible operational capabilities. It is important that capability development in these verticals / technologies is handled by appropriate agencies / organisations which have the ability to synergise stakeholders and take it to logical conclusion. Adhoc tasking and piecemeal actions will result in time and effort dissonance. Therefore, formulation of appropriate logical structures based on technology convergence and CMF is the way forward.

Recommendations : Defence capability, CMF, MDO and CNP

- **Military Information Service**. Information and EMS domain requires a specialisation oriented de novo look at HR management. In view of the limited HR availability and major capability thrust required to create and sustain evolving defence information infrastructure, there will be a requirement to induct non-combatant subject matter experts for effective management of the backend infrastructure and processes. This will enable combatants to handle the challenges in combat zone. Creation of a non-combat Military Information Service will be a step-in right direction. This will assist in not only taking on backend Information domain tasks but also bring Civil Military Fusion to a logical conclusion.

- **EM Spectrum Operations**. Since Information exchange is shifting from wired to wireless mode, Electromagnetic spectrum domain is the defining domain for MDO. National PCD capability in this domain is imperative to conduct Electromagnetic Spectrum Operations (EMSO). Spectrum is key Information enabler through Spectrum intelligence and Surveillance. In order to build a national EMS capability, it is important that there is seamless exchange of spectrum intelligence exchange between national agencies and field formations. This capability is recommended on lines of Geo Intelligence framework. The huge spectrum intelligence gathering capability of field units can be utilised by multiple agencies through this framework. This will also facilitate in removing overlaps in multiple agencies undertaking similar spectrum related tasks but also overcome the technology challenges faced by field formations. In Information Security area, high capacity data transfer capability shift from wired to wireless has brought to fore the requirements of over the air security protocols. Security development and testing agencies need to find de novo solutions for this evolving dimension. Moreover, in a joint force concept, interoperability will hinge on seamless information security.

In the Spectrum Management. area, demand for this premium resource from multiple agencies is going to increase by the day. Evolved solutions will facilitate a collaborative and deconflicted spectrum usage philosophy. R&D in this domain will pay rich dividends in future. Electro Magnetic Interference (EMI) / Electro Magnetic Compatibility (EMC) aspects will also gain prominence with enhanced density of emitters and intense dependence on EM radiations by multiple stake holders in combat zone. Expertise in combat zone spectrum management is a requirement which will gain prominence. In Information Denial capabilities, spectrum will play a key role in strategic target degradation. Therefore, need for a strategic EW capability under national info umbrella is imperative for MDO and CNP.

- **Navigation Technologies.** GIS and Geo location has emerged as key technology for not only military but also civil agencies. It is imperative, that the vulnerability of these technologies be minimized by indigenous terrestrial solutions rather than global space based solutions.

- **Mobile Technologies**. The form factor, processing capability, data capacity and multi utility applications of mobile segment has direct relevance in military domain. Somehow, in absence of a military grade mobile technology with inbuilt Electronic Protection features, this high utility, relatively low-cost technology has not been exploited for military purposes. It is time this challenge is thrown open to industry to make this technology available to military for C4ISR in a contested EM space in the form required. This will be a good alternative to SDR technology since, infrastructure for creating military mobile in Indian context with non-expansionist ideology is relatively easy to implement.

- **Training Transformation**. In order to leap frog in Info domain, there will be requirement of training transformation based on CMF. While the leadership has to adapt to hybrid approach of handling kinetic and non-kinetic domain, the execution has to adopt a specialisation approach. Multinational collaboration and cooperation will be key for a faster transition.[5] Collaboration with appropriate civil agencies based on core strength, infrastructure sharing, common training protocols need consideration.

Conclusion

The evolving global conflict scenario indicates a clear shift from pure kinetic to MDO scenario, where nation states need to evolve from traditional kinetic attrition concepts to developing PCD capabilities in multiple domains. This transition has been catalysed by information domain which itself is gravitating towards electromagnetic spectrum capabilities. Concepts like Information and Electromagnetic sovereignty are taking centre stage. Multiple technologies primarily in information domain are evolving rapidly. The solution space for information dominant conflict lies in finding indigenous, simple workable solutions. The ever-evolving technology poses challenges of fast obsolescence and high cost. Tendency to run after every new technology needs to be curbed. Nation states need to follow capability based approach to converge technologies towards developing PCD capability in each domain. Since information domain is the binding force for MDO, it is imperative that a national information umbrella organisation created which converges national capabilities towards an efficient structure which provides a template for all domains. Civil Military fusion hold the key for bringing strategic culture in all domains and enhancing technical capability of defence domain. Nation states with ability to synergise all stake holders of this domain through CMF have better probability of success in dominating info and EMS space.

****

Brig Rajeev Ohri, VSM (Retd) is an alumnus of IMA, Dehradun. His operational assignments include Signals Intelligence during OP VIJAY, Commanded Signal Regiment in OP HIFAZAT, Deputy Brigade Commander of Strike RAPID Brigade in Deserts and Chief Signal Officer on Line of Control in OP RAKSHAK J&K. The officer has done UN tenures in Rwanda. Brig Ohri has had staff tenures in WARDEC, MS Branch, GSO1 (Ops) in new raising HQ IGAR (S), Col (Ops & Plg) in Information System & Brig PMO SURAJ where he was awarded VSM for his contribution to EW capability building.

NOTES

1 Multi Domain Operations in NATO https://www.act.nato.int

2 Chapter: 1 The Multi-Domain Operations and the 2035 Operational and Technology Environment National Academies of Sciences, Engineering, and Medicine. 2021. Powering the U.S. Army of the Future. Washington, DC: The National Academies Press. https://doi.org/10.17226/26052.

3 Domain Operations in Future High-Intensity Warfare in 2030 https://codcoe.org

4 The Italian Defence Approach to Multi-Domain Operations https://www.difesa.it

5 Unlocking Training Technology for Multi-Domain Operations https://www.rand.org

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.

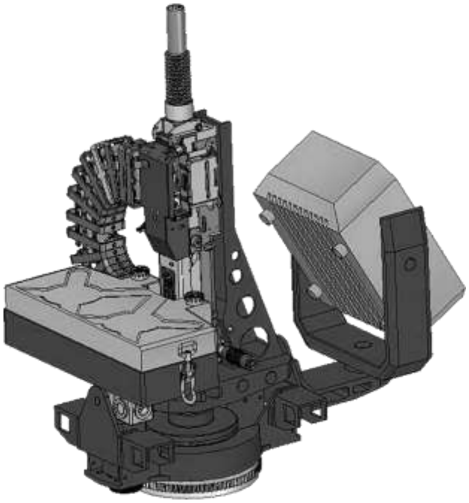
FPV Drone: Despatching an Explosively Formed Projectile

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 future warfare, for which the objective of annihilating opposing forces would have given way to a system-to-system confrontation (体系对抗, tǐxì duìkàng). The outcome of the struggle would be determined by a side's ability to generate, exploit, and protect information, which for armed forces would be a source of "integrated whole effectiveness" which would thus improve their ability to conduct precise strikes on C4ISR nodal centers and weak links in the adversary posture. Denial of information, through isolation, decapitation, or sabotage, achieved through kinetic means or influence actions, is hence the major effect of the new Chinese doctrine. It is no longer just a matter of coordinating its forces, but of unifying them in "integrated joint operations" (体化联合作战, tǐhuà liánhé zuòzhàn), increasing their mechanization through information enhancement.[1] Recent developments in the Chinese literature further emphasize that this modernization is likely to undergo a new stage with the implementation of "intelligentization" (智能化, zhìnénghuà) described by American authors as an algorithm-to-algorithm confrontation, with the incorporation of automated decision-making into the planning, conduct, and even execution of maneuvers.[2]

Multiple Domains of Warfighting

Pre-requisites for War fighting in MDO in Indian Context

The essential components of MDO includes the traditional domains of land, sea & air and the additional domains of cyber, space, electromagnetic and psychological warfare. Indian Armed Forces have already initiated steps towards multi-domain capability development by creation of the Integrated Theatre Command, Cyber and Space Agencies, Armed Forces Special Operations Division and IBGisation. The transition in MDO based joint warfighting requires addressing basic pre-requisites as under:-

- **Integration.** Efficient joint integration, across multiple domains at multiple levels of warfare, within military as also civil domains with security implications is imperative. An integration of domain and capability forms the foundation of an MDO approach.

- **Civil Military Fusion.** This involves integration and leveraging civil resources, such as commercial satellites, logistics infrastructure, cyber expertise, niche technologies and academia to support MDO. Civil entities must be encouraged to contribute to the development and implementation of Multi-domain Precision Warfare strategy.

- **Command and Control (C2) Structures.** The present joint warfare operation focusses on joint operations at operational level. MDO command-and-control structures require digital air-land integration with increased ranges of decision-making architectures to manage a complex battlespace.

- **Cross-Domain Skills.** MDO would require departure from bottled approach of respective domain to expertise in intelligence based operations to cross-domain knowledge and skills to understand capability of systems across multiple domains. Commanders within respective domains will require instinctive ability, to operate in multiple domains.

Technological Domains in Multi Domain Operations

Niche Technologies

Niche technologies in civil applications can be suitably modified for application into the military such as Lethal Autonomous Weapon Systems (LAWS), Internet of Battlefield things (IoBT), hypersonic weapons and nano technology in defence applications. For the purpose of general understanding, these technologies can be broadly categorised as under:-

- **Perception, Processing and Cognition.** Cloud computing, Artificial Intelligence, unmanned sensors, Big data analytics, robotics, Internet of things etc.

- **Performance Enhancing Materials.** Quantum computing, bio materials, meta technologies, composites for airspace etc.

- **Communication, Navigation and Targeting.** Directed energy weapons, EM weapons, visible light comn & optical satellite links.

- **Manufacturing & Logistics.** Additive manufacturing, logistics drones, 4D printing & VR/ AR.

Crystal Gazing – Niche Technologies in MDO

By 2035, nations with advanced technologies will absorb present niche technology in ambit of MDO by metamorphosis of quantum computing and artificial narrow intelligence to augment emerging technologies supporting semi-automated warfare. In such Joint Warfighting, systems will interact with systems to make complex decisions by adapting to changing situations with limited human input and evolving its collective experiences. Increasingly conflicts in MDO, military will increasingly operate beyond the traditional domains while conducting the "grey zone warfare," with decreased human involvement.

Future conflict will encompass the cyber, space, electromagnetic and cognitive domains thereby blurring the peacetime and wartime boundaries. In such joint warfighting, niche technologies designed to augment human performance combined with technological advancements will enable autonomous systems to accelerate the pace of warfare. Digital communication and tracking technologies will enable decision support systems in dispersed operations duly supported by long range kinetic strikes along with non-kinetic domain strikes to gain a positional advantage.

The envisaged scenario of MDO using Niche Technology is as under:-

- **Shaping of Battlefield.** The battle of systems is expected to occur before physical human engagement by ubiquitous computerized sensors supported by automated call-for-fire. Simultaneously, Cognitive Warfare will focus on influencing and manipulating the thoughts, beliefs, attitudes, and behaviors of targeted individuals to gain a decisive advantage over the opponent by controlling human behavior’s mental and emotional aspects, otherwise known as the cognitive domain.
- **Commencement of Hostilities.** Enhanced humans paired with robot armies and autonomous uncrewed vehicles will launch physical operations to achieve desired end state.
- **Linear and Simultaneous Decision Making.** Integration of quantum computing to enable the processing of complex data sets from multiple domains for accelerated wargaming and decision-making.

Niche Technologies in MDO. Cutting edge disruptive technology has been utilised to invent highly effective and high precision weapon systems which will drive the Joint Warfighting in MDO. A few notable technologies for Joint Warfighting are as under :-

- **Artificial Intelligence (AI) in Decision Support Systems.** This is probably the most disruptive technology as the use of AI is an enabler in the field of big data analytics to analyse large data of the battlefield sensors and as the driver of autonomous weapons. Most notably, AI driven military decision support systems are technologies which will augment the capabilities of a combat forces commander manifold in fast paced MDO. It will empower the commanders to process phenomenal amount of battlefield data and make speedy and efficient decisions to employ critical assets effectively.

- **Directed Energy Weapons.** High energy lasers can counter small and fast moving weapon systems such as missiles, aircraft, drones and also space based targets. The inherent advantage of laser weapons to precisely target and disable a weapon platform with minimal collateral damage makes it an ideal niche technology. In addition, powerful ship and ground based systems can effectively target even space assets with the strike speed of light, leaving virtually no response time with the target.

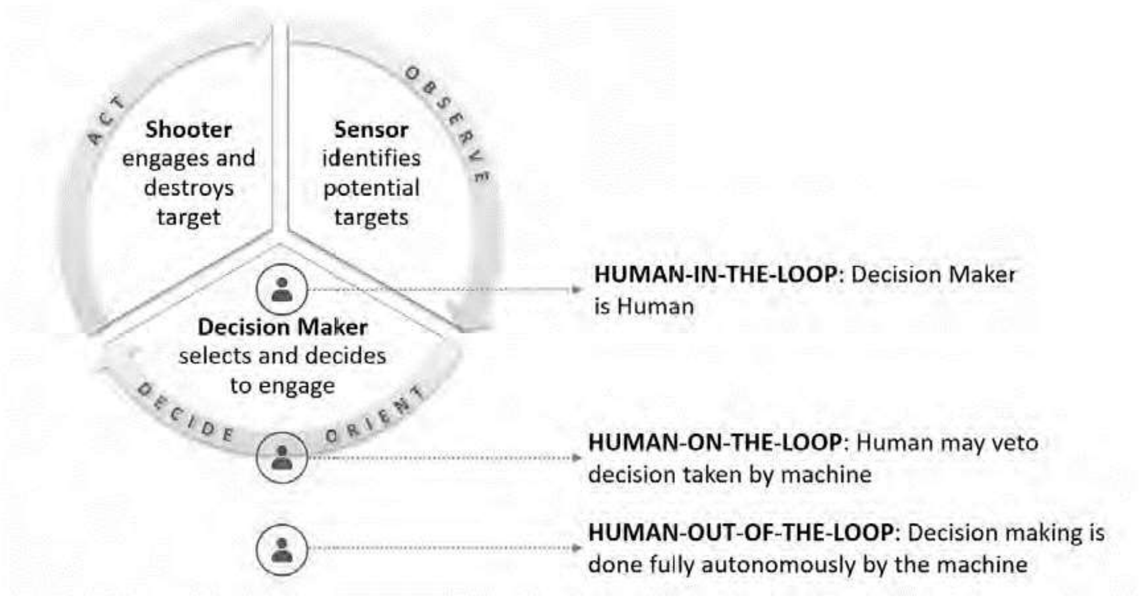
- **Hypersonic Weapons.** Hypersonic Weapons generate high kinetic energy to cause phenomenal damage. Also countering such a weapon system is also highly difficult. It is important to note that speed is not the only characteristic that makes hypersonic weapons effective, in fact ballistic missiles are all hypersonic at the re-entry stage, however what is special in the next gen hypersonics is the maneuverability which makes them very difficult to counter.

- **Quantum Technology.** Quantum technologies will revolutionize computing power, encryption, and sensing. Current encryption is built to be so complex that a modern computer would take thousands of years to crack it by force. Quantum computers would be able to break asymmetric encryption in minutes.[3] Quantum sensors, meanwhile, take advantage of the sensitivity of tiny particles to measure subtle changes in an environment, including rotation, electromagnetic signals of any frequency, and temperature.[4] Quantum sensors could enable a navigating system that can operate even in GPS-denied environments.[5]

- **Quantum Brain Networks (QBraiNs).** Quantum Brain Networks (QBraiNs) is a new interdisciplinary area of study described by Cornell University as integrating knowledge and methods from neurotechnology, artificial intelligence, and quantum computing. The objective is to develop enhanced connectivity between the human brain and quantum computers for various disruptive applications. QBraiNs technology aims to use a brain-machine interface (BMI) to create a computing platform that can help individuals analyze complex data sets and detect patterns or anomalies to support rapid decision-making in real-time.[6]

- **Autonomous Unmanned Aerial System (UAS).** Autonomous UAS are suitably poised to occupy significant airspace as compared to manned air missions due to cost effectiveness, versatility, endurance and human life factor. Manned air missions will in future be used mainly to control UAS swarms or to augment the efficiency of unmanned autonomous missions in scenarios where survivability chances are high. Its employment is gradually occupying the vacant space in kinetic battlespace which is not covered by rockets, missiles or aircrafts due to factors like cost to effect ratio, cost of human lives and deniability. In such threat scenarios, autonomous and AI enabled UAS present different employability options based on its capability and suitability of mission. These can be utilised in battlefield based on dividends accrued from its employment.

- **UAS Swarms.** Swarms of loitering UAS with capability of coordinated action using AI is a very effective way of defeating Air Defence systems and causing phenomenal damage to vital installations while remaining undetected from traditional radar systems.


ACT
OBSERVE
DECIDE
ORIENT
Shooter engages and destroys target
Sensor identifies potential targets
Decision Maker selects and decides to engage
HUMAN-IN-THE-LOOP: Decision Maker is Human
HUMAN-ON-THE-LOOP: Human may veto decision taken by machine
HUMAN-OUT-OF-THE-LOOP: Decision making is done fully autonomously by the machine

Degree of Autonomy in OODA Loop[7]

- **Nano Sensors and Materials.** Nano sensors have the capability to embed in the ubiquitous computer network and make the battlefield a highly connected place. Use of nano materials in military uniforms, gear and hardware have the potential to revolutionise sustenance and survival capability of soldiers and effectiveness of weapons with the use of stronger lighter and requirement specific material fabrication.

- **Exoskeletons.** Exoskeletons are external frames which are developed to fit the physiology of a human body and to enhance its capabilities. These suits will increase the load carrying capacity and physical strength of a soldier by more than 50 percent and probably even more. Such super soldier suits have already been designed in concept by many nations such as the US - TALOS, ONYX and Russian RATNIK projects.

- **Robotics.** Robots are already in limited use in fields such as the Bomb Disposal, logistics mules etc. The capability of such machines can be phenomenally enhanced using AI which will enable removal of the human element from critical tasks in operations.

- **Advanced Communication Technologies.** Joint operations between disparate forces and tactical coordination between dispersed units depend on secure and ubiquitous communications. Long-range engagements will make communications even more critical, from providing warning of incoming fire to coordinating with far-flung elements. High-end sensor suites and real-time targeting data are only as effective as the communications network used to transfer information from sensor to shooter.[8]

- **Bioengineering.** Bioengineering applies engineering principles of design and analysis to biological systems and biomedical technologies. Bioengineering includes synthetic biotechnology, which is a subfield focused on creating biological processes or biological compounds not found in nature.[9] Bioengineering incorporates genetic engineering, modifying organisms in a way that produces a different behavior or outcome, and enhanced human biology.[10] Bioengineering has varied application from fuel production to creating bio-weapons with genetically modified pathogens.

Challenges – Technology Driven MDO

- **Nascent Self Reliance in Critical Battle Domains.** MDO is directly linked to situational awareness for an effective response by Indian Armed Forces in the face of rapidly evolving, nebulous and ambiguous security challenges across the spectrum of conflict. In contemporary times, strategic and operational situational awareness will largely depend on defensive and offensive cyber capabilities, information dominance and persistent stare space situational awareness (SSA), which translates into the creation of maritime, high-altitude, and electronic operational mosaics.[11] Although 'technological leapfrogging' is prophesised by commentators to reduce the widening technological asymmetry with adversaries, the advances in critical technologies lack pace and definitive strategies to convert technology into military grade products. Thus, support from India's strategic partners is essential for developing indigenous capability and self reliance both non-contact and non-kinetic fields such as cyber and space domains.

- **Lack of Joint Operational Culture for Leapfrogging to MDO.** In previous conflicts like Kargil War 1999, Doklam Standoff 2017 and Galwan Standoff 2020, Indian operational approach has remained land-centric and infantry dominated rather than a technology-enabled manoeuvre approach. A critical analysis of these conflicts reveal that although the joint mobilisation and response of three services has been forced due to the crisis and not a result of an integrated or joint integrated structures and organisations. In addition, each service has its own set of weapon platforms, which are integrated during operations thereby leading to reduced technological compatibility and overall efficacy in battlefield.

- **Joint Structures and Strategies.** In the future wars, Indian Armed Forces will deal with adversaries conducting orchestrated and integrated MDO where sum will be greater than the whole. However, Indian Armed Forces lack structures and strategies to jointly develop and innovatively leverage the existing niche technologies in future battlefields.

- **Latency in Technological Absorption.** Indian Armed Forces suffer from slow pace of technological absorption to effectively leverage the potential of niche and disruptive technologies. It is imperative that the Indian Armed Forces must transform beyond the current superficial initiatives towards integration and jointness. Three services are yet to induct a combat cloud (an indigenous technology regime for ubiquitous and seamless connectivity of all sensors and shooters). An AI-enabled battlespace was one of the initial capabilities sought from the Defence Communication Network (DCN) deployed in 2016.[12] Ensuring the resilience of this network by continuously maintaining and updating hardware and software infrastructure would be vital. The hardware would include a constellation of satellites in different orbits, high-altitude pseudo satellites, terrestrial elements and manned/unmanned aircraft that can be launched quickly to cover gaps should the need arise. The newly formed Defence Space Agency has much ground to cover in this realm.[13] After setting up the combat cloud, the next step will be to equip sensor/shooter elements with software-defined radios (SDRs) compatible with datalinks, thereby creating an IoMT.[14] Currently, only IAF aircraft are equipped with SDR.[15]

Recommendations

- **Tri-Service Armed Forces Coordination Cell.** Headquarters Integrated Defence Staff must establish an Armed Forces Coordination Cell for National Development - to derive maximum benefits from national infrastructural projects and Government developmental Initiatives. This Cell will coordinate, as a single point agency on behalf of the armed forces, with concerned Ministries, military requirements that can be incorporated into national infrastructural projects and developmental Initiatives.

- **Agreements with Academic Institutions for Technology Development.** Premier training establishments of the armed forces, field army and Services think-tanks must establish formal academic relationships with reputed technological institutions to develop a technological development roadmap in sync with the national strategic environment. These agreements must include exchange of faculty and students and joint conduct of research on technology and national security issues.

- **Regular Discussion for Mutual Understanding.** To align indigenous defence industry with future technological and strategic requirements of the Indian armed forces, it is imperative to organise regular interaction with industry to course correct the strategic direction of capability development of Indian armed forces. The aim of such interactions must be to identify key disruptive technologies instead of diluting efforts in multitudinous technologies, to lay out roadmap for innate indigenous capabilities for tangible operational benefits and coordinate practically acceptable timeframe for development of these technologies for armed forces.

- **Technology Capability Development Perspective.** Indian Armed Forces need to identify critical/ core technologies where the progress with urgency under direct supervision of DMA is quintessential. The remaining technologies to be developed from core technologies can be called as analogous technologies, where private sector efforts desire encouragement. A suggested list of such technologies is as under:-

  - **Critical/ Core Technologies.** These are high priority technologies and include Quantum Technologies, Bio-engineering, Secure and Redundant Communications.

  - **Analogous Technologies.** These are priority technologies requiring research & development by private sector and include Space Based Technologies, High Performance Batteries, AI/ ML, Big Data Analytics and Robotics (including Autonomous Systems).

- **Technology Development Roadmap.** A vision document must be prepared to spell out capabilities and technologies required to be developed, specific to the national security requirements. The domestic scientific and academic community must form part of the evolution of this document so as to ensure that it is rooted in practical and achievable parameters. This roadmap must be published with perspective for a decade and be updated every five years, for it to remain current and relevant.

- **Compendium of Problem Statements.** Technology Perspective and Capability Roadmap must be accompanied by a Compendium of Problem Statements, elaborating on specific weapon systems and platforms required by each military service, and spelling out essential Qualitative Requirements. These problems, once formally stated, will enable private defence industry, including start-ups, to evolve concrete design proposals and facilitate identification of research areas for the future. This process must be participative between the military, DRDO, scientific institutions and private industry.

- **Lateral Absorption of Domain Specialists in Armed Forces.** Indian Armed Forces must explore direct absorption of technology specialists through Domain Expert Induction Scheme. Technology Expert Induction Scheme. Initially, a pilot project by inducting experts for each Service can be commenced along with a pool of 15-20 experts for technologies of common interest. Necessary orientation training must be imparted to inducted experts so as to impart holistic understanding of the armed forces perspective along with their operational and technological requirements. These inductions must aim is to augment Services expertise in niche and emerging technologies. Selection criteria must be based on technological job requirements elucidated as under:-

  - **Identify Technology Streams.** It is imperative that Service specific requirements and common usage technologies are identified by each service based on specific technological fields. Concurrently, an in house domain expert team of three services must explore common usage technologies as also dominant technological fields for concerted research and funding.

  - **Establishment of Services based Centre of Excellence.** Suggested technological centres of excellence of three services are as under:-

    - **Common Defence Technologies.** Cyber warfare, Electronic Warfare, Network Centric Warfare, Communication, Navigation, Drone warfare, Smart Weapon Delivery systems, AI, Quantum Computing, Big Data Analysis, etc.

    - **Land Dominant Technologies.** Battlefield Management Systems, Robotic Surveillance, Autonomous Weapons, Smart Anti-Tank Missiles, etc.

    - **Air Force Dominant Technologies.** Avionics, Beyond Visual Range technologies, Airborne Early Warning systems, Aero-engines, long range communications etc.

    - **Maritime Dominant Technologies.** Propulsion systems, Maritime Domain Awareness systems, Electronic Warfare suites for Naval vessels, Anti-Submarine systems, etc.

- **Mandate of Domain Experts.** Technological domain experts must be mandated to collaborate with the scientific community, academia and industry so as to provide armed forces perspective while developing niche technologies. These experts must be associated with conceptualizing, development, testing, manufacture and induction of these niche technologies in armed forces.

- **Establish Civil Military Collaborated Technology Research Centres.** Technology based Civil Military Collaborated Technology Research Centres must be established at national level technological institutes such as IISc or IITs, for focused research in area of specific niche technology. The funding of these Research Centres must be through the Services to encourage focused domain specific research in emerging and disruptive defence technologies.

Roadmap for Capability Development in Niche Technology

The MDO will be driven by disruptive niche technologies to achieve incremental dominance. This requires well thought strategy for tri services joint warfighting capability development. The suggested roadmap for capability development in niche technology for Armed Forces are discussed in succeeding paras.

- **Short Term Capability Development (2-5 Years).** A Tri Service Common Operating Picture and Real-time Situational Awareness for optimal intelligence and operational management of battlefield is imperative to gain ascendancy in MDO. This requires development of secure Information and Communication Infrastructure to include data cloud and servers for a central Data Repository; secure network connectivity and data management; big data analytics with blue and red force tracking capability, augmented and artificial intelligence for informed decision making based on autonomous data analysis inputs. It requires geospatial mapping of troops, equipment and operational resources for a real-time Decision Support system.

- **Mid Term Capability Development (5-10 Years).** A dedicated and concerted research needs to be achieved in directed energy weapons, long range vectors, guided missiles and loitering ammunition with terminal guidance for enhanced precision, based on information superiority gained through developments in Decision Support system. This phase must focus on improvements in Decision Support system to augment the capability of manned unmanned technology systems in Tri Services weapon system platforms. Force Protection through research and developments in stealth technologies, adaptive camouflage, advance materials and active armour technology will be imperative coupled with precision based firepower.

- **Long Term Capability Development (10-15 Years).** In this phase of development, Autonomous Weapon Systems will transition from basic functions to Advanced Fully Autonomous Weapon Systems by retaining the ability to achieve specified objectives as also dynamically make limited decisions using distributed algorithms. Thus, the developments in the fields of cloud computing, block chain, big data analytics, IoT and AI, must ensure a decisive technological transformation from automation to autonomy in this phase. It is essential that by 2040, Indian MDO graduates into non-contact domain through offensive cyber, space based weapons and lethal autonomous weapon systems. In addition, it is also prudent to devise a Tri Service approach to mitigate the threat emanating from Swarm of Unmanned Autonomous Systems with payloads for surveillance, electronics suppression and other weapon platform including manned unmanned autonomous combat missions.

Conclusion

Indian Armed Forces needs to evolve a technology driven MDO for joint warfighting so as to stay ahead of the curve and achieve deterrence in the complex security environment. The start point of this Tri Service integration leading to interoperability in niche technology landscape must be the raison d'etre of operational jointness in warfighting. A culture of civil military fusion in niche technologies so as optimize research in Tri Services centres of excellence is quintessential. The induction of domain experts is essential to lead technological absorption in armed forces, achieve understanding of nuances of technology development and devise employment philosophies for these niche technologies. As major global powers adopt MDO as its future military doctrine, it is imperative for India to initiate actions to achieve convergence and coherence through incorporation of niche technologies in joint warfighting. The transformation needs change in strategic mindset, to adapt to the changing conceptual, technological, and cultural military needs and sensibilities, as also to adjust to the speed at which the niche technologies are absorbed.

****

Lt Col Gaurav Kumar Singh is an alumnus of NDA and was commissioned into 129 Air Defence Regiment in December 2010. The officer is a graduate of Long Gunnery Staff Course and Defence Services Staff Course. He was awarded CDS Medal at DSSC. He has served as GSO – II of an Infantry Brigade on LC and Instructor Cl 'B' at Army AD College.

NOTES

[1] T. Fravel, Active Defense - China's Military Strategy Since 1949. Princeton: Princeton University Press, 2019.

[2] K. McCauley, "People's Liberation Army: Army Campaign Doctrine in Transition", FMSO, 9 January 2020.

[3] World Economic Forum, State of Quantum Computing: Building a Quantum Economy, World Economic Forum, 2022, https://www3.weforum.org/docs/WEF_State_of_Quantum_Computing_2022.pdf.

[4] David L. Chandler, "Quantum sensor can detect electromagnetic signals of any frequency," MIT News, June 21, 2022, https://news.mit.edu/2022/quantum-sensor-frequency-0621.

[5] Rajesh Uppal, "Quantum navigation is emerging technology for GPS-denied and deep space environments," International Defense, Security & Technology, October 20, 2020, https://idstch.com/technology/quantum/quantum-navigation-emerging-technology-for-gps-denied-and-deep-space-environments/.

[6] Strategic Research Project Report on Techno Sentient Warfare in 2035, United States Army War College, accessed on 4 Jun 2024.

[7] Ravindra Singh Panwar, "AI and the Rise of Autonomous Weapons" published in Future Warfare and Technology: Issues and Strategies, ORF and Global Policy Journal, 2022.

[8] Mauro Gilli, "Beware of Wrong Lessons from Unsophisticated Russia," Foreign Policy, January 5, 2023, https://foreignpolicy.com/2023/01/05/russia-ukraine-next-war-lessonschina-taiwan-strategy-technology-deterrence/.

[9] "Synthetic Biology Explained," Biotechnology Innovation Organization, n.d., https://archive.bio.org/articles/synthetic-biology-explained.

[10] Steven A. Benner and A. Michael Sismour, "Synthetic Biology," Nature Reviews Genetics 6 (2005): 533-543, https://www.nature.com/articles/nrg1637.

11 Park Si-soo, "US, India agree to cooperate on space situational awareness", *SpaceNews*, 12 April 2022, https:// spacenews.com/us-india-agree-to-cooperate-on-space-situational-awareness/.

12 "HCL Infosystems implements first-ever converged communication network between Indian Army, Navy and Air force," https://www.hclinfosystems.in/case-study-dcn/

13 "HAL takes a leap of technology, to develop unmanned pseudo satellite that can fly unmanned for upto 3 months," *Times Now Digital*, 04 February 2020, https://www.timesnownews.com/india/article/hal-takes-a-leap-of-technology-to-develop-unmanned-pseudo-satellite-that-can-fly-unmanned-for-upto-3-months/715932.

14 Air Commodore K. A. Muthana, "Fighting Future Wars: A Roadmap for Adoption of Disruptive Technologies In the Indian Context,'" *Council for Strategic and Defense Research*, Special Issue No. II; Policy Paper, December 2021, https://csdronline.org/upload/user/CSDR_KA_Muthana_An_Aerial_Prac_Perspective.pdf.

15 Ibid.

INDIA AND CHINA IN AN ERA OF ALGORITHMIC WARFARE

Maj Vishnu RJ

Abstract

The disruption in a multitude of computing technologies like algorithms is enabling the warfighting machines to interact, interplay and integrate to solve problems more efficiently and effectively. Algorithms are bringing a transformative shift in the way we perceive, plan, organise and fight wars. This critical capability enables field commanders to understand and assimilate minute circumstantial changes associated with each problem to find unique practical solutions. The lethal combination of Manned-Unmanned Teaming (MUMT) in algorithmic warfare is bringing an intimate intertwining of accuracy at tactical operations and creativity at operational and strategic planes to produce disproportionate dividends. China laid out its new modernisation goals in 2017 and new battle doctrines in 2020. Since then, China has been building the capability to conduct algorithmic warfare through significant organisational changes and capability enhancement using homegrown disruptive technologies. They are pursuing to develop the ultimate form of algorithmic warfare as 'Intelligentized Warfare' by 2050. The studies give the algorithmic warfare capabilities of the PLA to forecast its likely manifestation along the Line of Actual Control (LAC). The study also refers to the challenges posed by this new Chinese warfighting methodology to give broad guidelines to counter it. To mitigate this threat, a deliberate and deadline-driven modernisation of armed forces must be done by India on the backbone of homegrown disruptive technologies.

Introduction

Modern armies are pursuing the capability to undertake precision strikes on their adversaries in multiple domains including cyber, electromagnetic and space along with physical dimensions of warfighting. Though the military has always been a tool to show the political will of a nation, the cost of war is the primary factor affecting the decision to employ them. The recent disruptions in technology allow various stakeholders to integrate multiple domains of warfighting to fight as a cohesive unit by closing the gaps in the battlefield previously caused by huge space, time delays, difficulty in concentrating force and strained information sharing. Nations are embracing technology in all aspects of warfighting to reduce the cost of war and to increase the economy of effort for every action. PLA through a transformative shift has been embracing algorithmic warfare to make its armed forces leaner and meaner (Koh 2019).[1]

Algorithmic Warfare

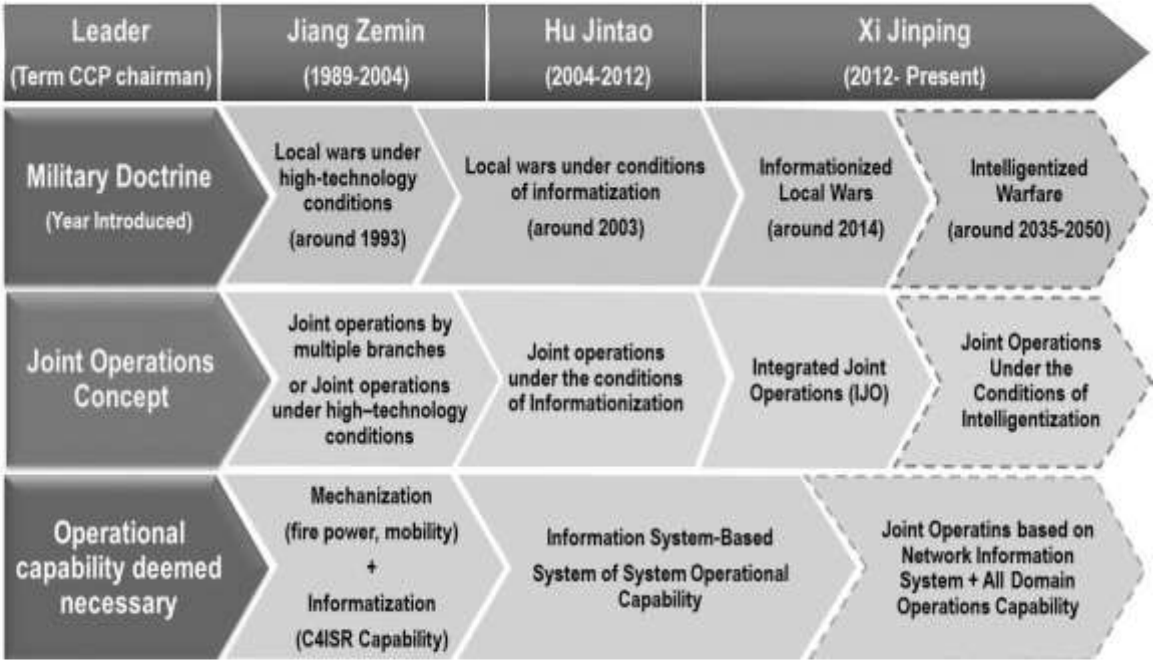
Algorithms are the sequence of instructions and rules that machines use to solve problems. They transform inputs to outputs and as such are the crucial conceptual and technical foundation stone of modern IT and the new intelligent machines (Layton 2018, 02).[2] Algorithmic warfare intends to reduce the number of warfighters in harm's way, increase decision speed in time-critical operations and operate when and where humans are unable to operate (Crosby 2020, 01).[3] The manually programmed machines require directions and instructions at each step to develop a solution for the problem at hand and the same instructions will have to be provided by the user every time he engages with the system. The intelligent machines on the other hand use the new guidelines and instructions created by the learning algorithm for a new task. Instead of being pre-programmed, they learn from their interactions with humans and the environment to continually update their internal model of the world (Layton 2018, 06).[4]

These intelligent machines create new rules and guidelines by fusing the latest information absorbed from the working environment with existing ones in their database. They can do intricate jobs that traditionally programmed machines would not be able to and the new self-learning algorithm can provide a different answer for the same scenario. Since this concept develops on the continuous interaction between the system and environment, the availability of data to train the algorithm will be critical in creating better rules and instructions. Thus, these machines must have substantial capabilities to collect large unprocessed data by interacting with the environment, analyse this big data and identify patterns or fresh insights to give intelligent answers to the queries of users.

Even though these machines are continuously trained on fresh data to give practical solutions, the logic behind arriving at them is usually absent in these solutions. This arises due to their incapability to recognise trivial situational alterations that are distinct in every instance and the absence of intuitive judgment of humans. This leads to difficulty in applying the knowledge gained from one scenario to another. Similarly, ethics and laws in this arena of technology are still nascent and responsibility is still with the person behind the machine. Thus, having a Man-Machine collaboration must allow us to understand the logic behind the decisions taken by the machines. The evolution of these warfighting doctrines and concepts will demand new force structures, new force components and training methodologies. The capacity of a nation to launch algorithmic warfare will depend on its capability in a multitude of computing technologies including Computer Processing Power, Big Data, AI, Cloud Technology, etc. Thus, algorithmic warfare is not a distinct capability but an integration of numerous technologies. Those who monopolize and embrace the nuances of this warfare will have a significant advantage over their enemies.

Algorithmic Warfare of PLA

Following General Secretary Xi Jinping’s modernisation speech at the 19th Party Conference in 2017, the Peoples Liberation Army (PLA) is pursuing significant organisational changes and made huge progress in building the capability to conduct algorithmic warfare through synchronized long-range precise strikes across multiple domains (Yasuyuki 2021, 24-31).[5] ‘Intelligentized Warfare’ is the term used by the PLA to describe their ultimate form of algorithmic warfare (Kania 2017, 12).[6] In 2020, the Central Military Commission issued a new battle doctrine for warfare and announced their plans to create the capability to be networked into a system of systems that will facilitate them to conduct 'Intelligentized Warfare' (Yasuyuki 2021, 01).[7] 'PLA Joint Operations Outline' clarifies the basis for conducting algorithm-based joint operations in the new era (Finkelstein 2021, 13).[8] Recent emphasis has been on conducting realistic training in this new warfighting doctrine.[9]



Leader (Term CCP chairman)	Jiang Zemin (1989-2004)	Hu Jintao (2004-2012)	Xi Jinping (2012- Present)	
Military Doctrine (Year Introduced)	Local wars under high-technology conditions (around 1993)	Local wars under conditions of informatization (around 2003)	Informationized Local Wars (around 2014)	Intelligentized Warfare (around 2035-2050)
Joint Operations Concept	Joint operations by multiple branches or Joint operations under high–technology conditions	Joint operations under the conditions of Informationization	Integrated Joint Operations (IJO)	Joint Operations Under the Conditions of Intelligentization
Operational capability deemed necessary	Mechanization (fire power, mobility) + Informatization (C4ISR Capability)	Information System-Based System of System Operational Capability	Joint Operatins based on Network Information System + All Domain Operations Capability	

Conceptual Diagram of Evolution of Intelligentized Warfare

Source: (Yasuyuki 2021, 29). Source: Yasuyuki, *"The PLA's Pursuit of Enhanced Joint Operations Capabilities"*, 29.

Technology the Catalyst for Intelligentized Warfare

China has included the Military Civil Fusion as part of its national policy to modernise the military to suit its national security needs (Yasuyuki 2021, 16).[10] They are taking bold measures to domesticate its defence manufacturing and expand its military sector. The key technologies being developed for Intelligentized Warfare are given below:-

- **AI & Advanced Robotics**. PLA will be using the processing power of AI for enhanced data exploration, decision support and C4ISR. The battlefield will be mapped using hundreds of AI-enabled sensors, cameras and similar surveillance systems operating in the ground air and space domains. These systems will enable them to sense, locate and identify objects on battlefields. Algorithms will quickly detect changes in the mapped battlefields to avoid set-piece mechanical response. A false and misleading picture of the battlefield will be orchestrated to create chaos for the enemy by jamming and deception systems. The enemy command and control setup will be both tempted and confused to act on the tricky battle front presented to him by these intelligent systems.

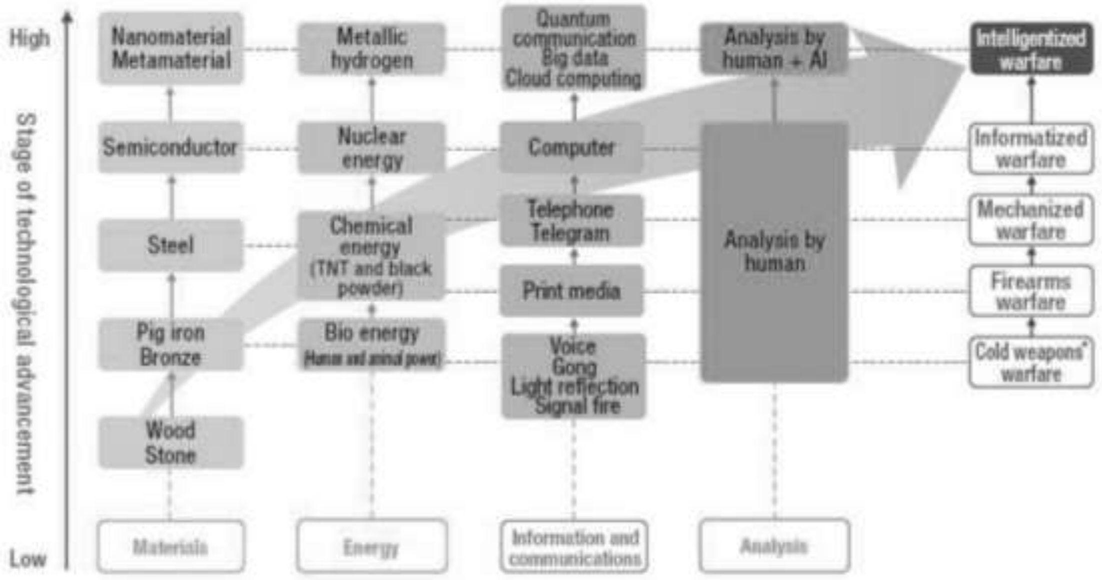
- **Big Data Analytics**. China's public security forces have been enthusiastic about adopting big data analytics; the capability would significantly enhance their ability to fulfill their missions (Derek Grossman 2020).[11] Mastering this will help them in the systematic processing and analysis of huge structured and unstructured data using various models such as predictive models, trend analysis, etc. The China Skynet, an intelligent surveillance network uses almost 600 million surveillance cameras equipped with facial recognition technology to monitor their population with 99.8% accuracy (McMillan 2024).[12] By analysing vast amounts of data from their local population, they are refining their algorithms to detect subtle changes in the volatile, uncertain, complex and ambiguous modern battlefield.

- **Quantum Technologies**. China has been investing heavily in quantum sensing, quantum communication and quantum computing technologies. These technologies ensure secure communications, enhanced computing capabilities and enhanced navigation capabilities. Quantum sensing can potentially improve lidar and radar for intelligence, surveillance, and reconnaissance and provide positioning and navigational capabilities in the absence of satellite-based systems. (Brian Hart 2024).[13]

- **Semi-conductor & Advanced Computing**. They play a crucial role in powering the sophisticated computing and advanced communication systems. To achieve self-reliance in this field, China has recently set up various semiconductor industries named Changsha Jingjia Microelectronics Co, Cambricon Technologies, etc, (Waldie

2022).[14] PLA has realised that replacing foreign chips in military equipment is critical in achieving military autonomy and guarding them against security risks.

- **Cloud Technology**. Cloud technology is a critical battle enabler in "Intelligentized Warfare" and has been an area of geopolitical manoeuvring between the US and China. Algorithmic warfare necessitates high-speed analysis of huge data for fast and precise decision-making. This is possible only through the intermingling of multiple technologies with the cloud technology. "Cloud technology has remained a relatively closed industry in China," said Thomas Zhang, Dezan Shira & Associates' IT Director (Dunseith 2018).[15] This isolation of cloud technology within China ensures faster and more secure services.



Conceptual Diagram of Evolution of Technology in Warfare Source: (Yasuyuki 2021, 17). Yasuyuki, "*The PLA's Pursuit of Enhanced Joint Operations Capabilities*", 17.

Critical Enablers of Intelligentized Warfare

Intelligentized Warfare will focus on subduing the enemy without actual human contact thereby reducing human casualty. The central tenet of this idea is the application of stealth, unmanned and precise operations supported by the information and space domain. The pace at which the battle will be unfolding, the critical battle-winning factor will still be the decisions taken by the commander who will be presented with multiple options by the algorithms. PLA will be able to manoeuvre their enemy to fight from an unfavourable position by precluding enemies' options and expanding their opportunities thereby defeating the enemy in the spatial dimensions of time. A few critical enablers are given below :-

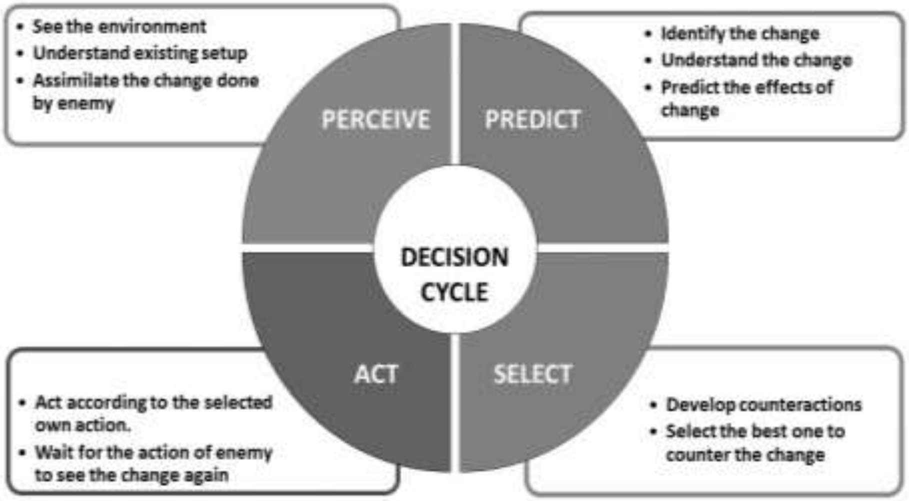
- **Human-Machine Collaboration**. Intelligent machines in the futuristic battlefield with the existing level of technology will have to leverage an optimal mix of the unique capabilities of both machines and humans. This lethal combination will overthrow the existing established beliefs and characteristics of warfighting. Even though the concept of MUMT will be used, initially machines will have a limited role in this team. The machine with inherent disadvantages of intuitive decision-making will mostly be used to collect large volumes of data and present processed data using their trained algorithms to the human team members till they mutate to become smart or intelligent systems.

- **Autonomous Systems**. PLA visualizes that autonomous systems will gradually replace human frontline combatants with the air domain having the highest potential due to the advent of drones and intelligent swarms. The initial steps will be the "mothership concept" in which the manned fighters will direct the unmanned drones and subsequently migrate to the "swarm warfare concept" in which intelligent drones will overwhelm the enemy with masses of intelligent drones. Even at tactical level operations, enhanced participation of intelligent systems can be visualised with swarm drones acting with much more autonomy.

- **Battlefield Targeting System.** The tactical knowledge achieved by the algorithms of the intelligent machines will support the intuitive thinking of the human being to work with greater operational and strategic depth. The algorithms will derive ideal target sets for the commanders from a pool of high-quality targeting data. These data will be communicated to autonomous weapon systems to engage with precision.

- **Cognitive Warfare**. The AI-enabled autonomous systems will be operated by the PLA to manipulate the minds of citizens to change not only what they but also how they think. It will aim to fragment otherwise cohesive society using synchronized chaos to create a crisis.

- **Battle Decision-Making Setup**. The intimate interlacing of precision at tactical operations and innovation at operational planes will mutate the Observe-Orient-Decide-Act (OODA) loop into the Perceive-Predict-Select-Act (PPSA) Decision Cycle which would be a predictive model based on data. Under this model, the intelligent machine supported by AI will recognise the battlefield changes to predict the various courses of action that can be envisaged from an enemy based on their capability, terrain, capability of their forces, etc. The multiple courses of action of the enemy will be analysed by algorithms to suggest suitable counteracts that PLA must take. The human interface in this MUMT will analyse both enemy and PLA actions suggested by the intelligent system to produce the most suitable one for PLA forces.

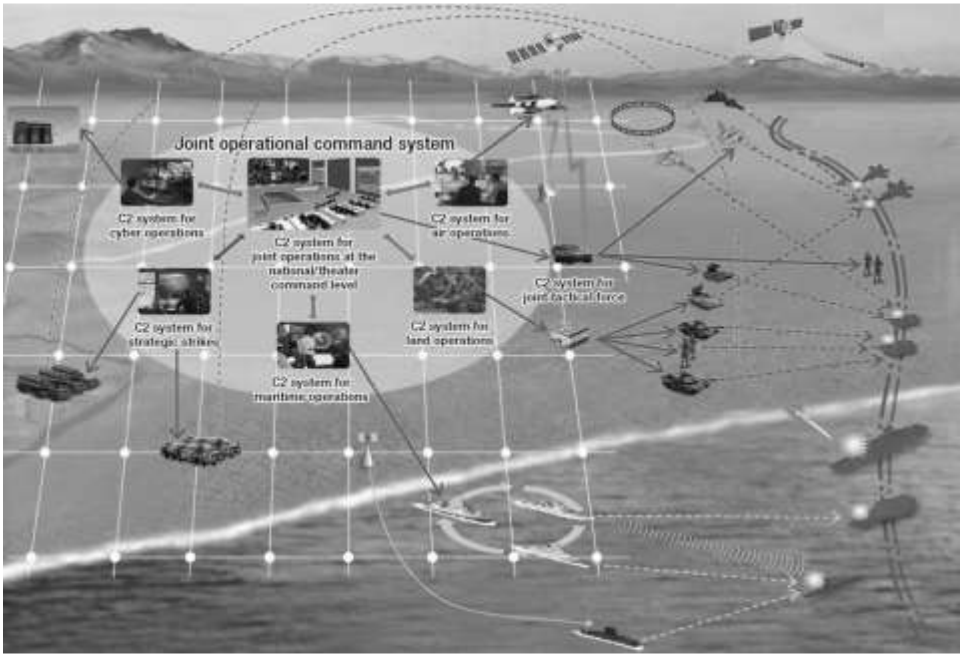


• See the environment
• Understand existing setup
• Assimilate the change done by enemy
• Identify the change
• Understand the change
• Predict the effects of change
PERCEIVE
PREDICT
DECISION CYCLE
ACT
SELECT
• Act according to the selected own action.
• Wait for the action of enemy to see the change again
• Develop counteractions
• Select the best one to counter the change

Conceptual Diagram of PPSA Decision Cycle (Source: Author.)

Likely Expansion of Intelligentized Warfare by PLA. PLA aims to complete force modernisation by 2035 and to be a world-class military by 2047 (Burke 2020, 01).[16] This entails them to evolve the 'Intelligentized Warfighting' capability over varying timeframes as given below: -

- **2030: Limited Area Limited Duration**. PLA in its pursuit to be a world-class military by 2047, is likely to achieve the capability to undertake 'Intelligentized Warfare' supported by algorithms and intelligent machines in a limited area and for a limited duration by 2030.
- **2040: Limited Area Longer Duration**. By 2040 manifestation of 'Intelligentized Warfare' would likely be for a longer duration due to the enhanced capability due to advancement in various disruptive technologies. This coupled with enhanced infrastructure development would assist them in fighting the algorithmic warfare for a longer duration in a limited area.


Joint operational command system
C2 system for cyber operations
C2 system for joint operations at the national/theater command level
C2 system for air operations
C2 system for joint tactical force
C2 system for strategic strikes
C2 system for land operations
C2 system for maritime operations

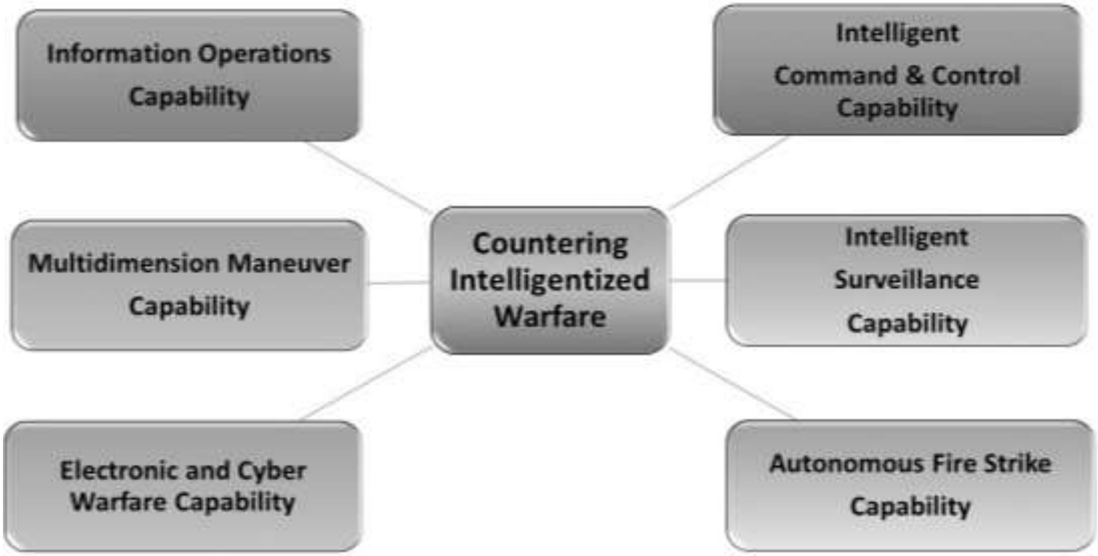
Conceptual Diagram of Intelligentized Warfare of PLA *Source: (Yasuyuki 2021, 27).Source:* **Yasuyuki, "*The PLA's Pursuit of Enhanced Joint Operations Capabilities*", 27.**

- **2050: Larger Area Longer Duration.** By 2050, PLA is likely to develop the capability to conduct Multi-Domain Integrated Operations supported by AI-enabled Autonomous Weapon Systems (AWS) for a longer duration across the northern borders of India. The disruption in chip manufacturing, AI, Big Data Analytics, Data Communication, space, cyber domains, etc enables these machines to interplay and solve problems more efficiently and effectively**.**

India Looking North

India and China have had a tantalizing relationship in the last few years, especially since 2017. India seems to have increased its faith in its military might which resulted in the rebalancing of its forces for a Northern Contingency. This perspective is necessary to understand the 'No War No Peace' like situation that now exists along the boundaries of the two countries. Since the conventional balance of power is measured on the size of armed forces that can be effectively brought about each other, the effects and capabilities of 'Intelligentized Warfare' are not being essentially considered. Therefore, we need to understand and visualise the integrated impact of Kinetic and Non-Kinetic Intelligentized Warfare in temporal and spatial frames to develop a counter capability.

Capability Development. National leadership has realized that technology will be a catalyst to transform the army to be future-ready and understands that being self-reliant will be the game changer. Army Design Bureau has been working with this purpose to integrate the entire defence ecosystem and is collaborating with premier academic institutes of the country. Major projects like Integrated Battlefield Management System, Netra and Daksh are taking confident steps in monitoring, collecting and analysing the battlefield with AI-powered systems in a network-centric real-time integrated setup (Sharma 2023).[17] Algorithms being the critical battle enabler, India must focus on developing algorithms that can understand the minute changes in the background and detect useful information from the clutters of big data. Self-sufficiency in intelligence and battlefield awareness supported by a robust disruption-free communication network will be key in fighting algorithmic warfare. Some of the required capabilities are given below:-


Information Operations Capability
Intelligent Command & Control Capability
Multidimension Maneuver Capability
Countering Intelligentized Warfare
Intelligent Surveillance Capability
Electronic and Cyber Warfare Capability
Autonomous Fire Strike Capability

Conceptual Diagram of Required Capabilities (Source: Compiled by the author.)

- **Intelligent Command Control Capability**. Intelligent joint command and control setups at strategic, operational and tactical planes equipped with multiple intelligent and autonomous systems can assist the commanders in following the 'PPSA Decision Cycle' to fight the fluid and volatile modern battles. This will facilitate an overarching dominance over the battlefield through information, cyber, electronic, cognitive and physical dominance of the battlefield.

- **Intelligent Surveillance Capability**. Units must be formed by dovetailing both surveillance and shooter drones to the same setup. It must have the flexibility to scale up as a system capable of functioning as an intelligent swarm of drones. The surveillance drones will map the battlefield and pick up the enemies through the algorithm to assist the shooters in striking them with precision. These units will critically dislocate enemies both physically and psychologically.

- **Autonomous Fire Strike Capability**. Tailor-made autonomous weapon systems can be integrated into existing setups to execute precision strikes to degrade and destroy enemy combat power. The 'CABisation' by the PLA emphasizes mobility and firepower to neutralize and destroy the enemy. The recent clashes in Eastern Ladakh highlighted the use of armoured vehicles in high-altitude areas. Even though the "CABisation" gives an edge through mobility and firepower, its application will be restricted by the limited availability of mobility corridors in the mountainous terrain. Tailor-made anti-tank units enriched with AI-enabled anti-tank weapons systems which are centrally controlled by an algorithmically enabled Joint Command Post can give disproportionate dividends. An autonomous integrated air defence setup must be organised at the national and command level with MUMT based on algorithms to adapt to fast-paced air operations with reasonable flexibility.

- **Electronic and Cyber Warfare Capability**. The new generation equipment like Software Designed Radio is electronically hardened to facilitate communication even in brutally jammed and electronically saturated modern battlefields. The electronic warfare units must exploit new generation disruptive technologies to provide information support to their forces and deny the same to the enemy. Modern armies are exploiting cyber as a dynamic weapon for non-contact non-kinetic warfare. The 'Cyber Militia' (Baughman 2022, 06)[18] of the PLA is turning regular corporate workers into part-time military workers. India should learn from its enemy and take active measures to launch large-scale cyber warfare on its enemies while protecting our systems. The key capabilities of the enemy can be neutralised or destroyed through cyber warfare to incapacitate them before contact warfare.

- **Information Operations Capability**. The modern era necessitates justice behind the war or 'Jus ad bellum' must be achieved before going to war. Thus, timely dissemination of credible information to support own cause of war and discrediting the enemy is an essential war-winning factor. Moreover, monitoring open-source intelligence like social media through algorithms will give credible intelligence for the military force to predict the enemy's plans. The "50 Cent Army" of the PLA employs civilians to collect data and spread disinformation (Allen 2021).[19] The aim will be to psychologically dislocate the enemy military, gain political and legal dominance through public opinion warfare, legal warfare and psychological warfare.

- **Multi-dimensional Manoeuvre Capability**. Joint fighting will necessitate a rapid switching of forces facilitated by rapid infrastructure development along the LAC and the capability for strategic communication supported by satellite communication. This capability must ensure the transportation of operational units and equipment to a designated area in a safe manner to ensure a smooth implementation of operational action.

Change in Doctrine and Organisation. The fast-paced fluid modern battles necessitate us to change the existing warfighting doctrines which are primarily based on contact battles and primitive battle planning tools like Intelligence Preparation of the Battlefield, Military Decision-Making Process, Joint Operations Planning Process, etc. Algorithmic warfare has changed the landscape and dynamics in which modern battles will be fought necessitating us to modulate the way we think and plan the battle. A futuristic and time-specific method must be evolved by the Indian Armed Forces to develop the capabilities not only to counter an 'Intelligentized Warfare' by PLA but also to launch algorithmic warfare using our force multipliers against them. India must take guidelines from ANC, SFC and HQ IDS to achieve jointness and integration (Kuanr 2019, 49).[20] There is an urgent requirement to have strategies and procedures to fully exploit the available technology by formalizing organisations at all levels of the military hierarchy. An organisation needs to be fashioned at the national level to collate and collaborate not only with the information needed for supporting joint algorithm-based operations but also for prompt dissemination of intelligence and orders.

Change in Selection, Training and Professional Military Education. There is an urgent need to evolve our joint training methodologies and practices with added emphasis on conducting joint exercises. This can be achieved through a focused effort in developing infrastructures and human resources conducive to jointness. The quality of the human capital must be enhanced and junior leadership must be trained to use these modern machines with proficiency. The staff officers must be trained to operate in a joint environment enabled with real-time information. Wargames must be fought more realistically to understand the capability of the machine and the new battle rhythms must be imbibed from the tactical to strategic level.

Marching Forward. We must 'Learn from the Enemy' and should take ambitious steps to fight as a joint organisation. The current superficially peaceful situation along the LAC will be debilitated by PLA through a well-planned and coordinated 'Intelligentized Warfare'. We should develop and construct capability for joint algorithm-based operations based on self-sustained technological development. The suggested roadmap is as given below: -

- **Between 2025-35: Force Strengthening Phase**. India must focus on increasing battle space awareness and training the technology including AI and algorithms to understand and assimilate the environment. The focus must be on developing the technology and human capital to fight algorithmic warfare. Organisational changes will be needed to facilitate our armed forces in fighting as an integrated unit under the umbrella of continuous networking. Dedicated effort must be taken in developing Defense R&D, Civil-Military Fusion and in training the human capital to use the technology-driven warfare. Joint training must be institutionalised by the formation of joint training institutes at each Command for training of troops especially officers of junior ranks and troops. India must form strong pillars for the development of algorithmic warfare capability between 2030-35 and strive to achieve the capability to counter the 'Intelligentized Warfare in a limited area'. The main pillars will be capability development based on technological advancement, doctrinal changes, reorganisation and restructuring of military forces to ease interoperability, infrastructure development and human capital development.

- **Between 2035-45: Strong Defensive and Limited Offensive Algorithmic Warfare Capability**. The organisations formed during the previous phase should be functioning to effectively counter the 'Intelligentized Warfare' of PLA. AWSs to counter PLA Rocket Force, artillery bombardments, cyber-attacks and unmanned aerial attacks are to be developed by integrating AI. Once effective autonomous counter capabilities are achieved, India must focus on developing a limited offensive in the framework of algorithmic warfare. The key to the success of this phase will be achieving self-reliance in disruptive technology dovetailed with the strengthening of rules, procedures and organisations formed during the previous phase. Strategic sustainability must be achieved through tangible steps from the conceptual to the practical stage in tailor-made logistics systems and strategic mobility is to be achieved by developing a capability to mobilise and maneuver forces at the area of interest with ease and speed.

- **Between 2045-55: Large Area Longer Duration Multidomain Joint Operations Capability**. India must achieve time-space-force-information dominance to conduct Effect-Based Operations using algorithms. The strong pillars of previous phases must enable India to fight Multi-Domain Algorithmic Warfare Capability for a large and longer duration along the LAC. During a conflict situation, India must pre-empt PLA by launching an offensive in a place and time of its choosing with the right force level and countermeasures against 'Intelligentized Warfare'. This type of conflict will heavily rely on technology to connect the actors in air, sea, network, electromagnetic spectrum, etc to achieve "cross-domain kill-capability".

Conclusion

Algorithms are being developed by various players as a decisive battle winning component capable of identifying critical vulnerabilities of the enemy. This enables any force to attack their enemy with improved speed, precision and intensity. The increased permeation of the algorithms will make it easier to influence the battle and force a system collapse. The evolution of algorithmic as a method of warfare will facilitate MUMT and an increased autonomy to the machines. The velocity of data creation, collection and collation will necessitate evolution of commander decision cycle from OODA to PPSA decision cycle. PLA is developing the capability to launch an algorithmic warfare and named its ultimate form as 'Intelligentized Warfare'.

The strengthening of the Mountain Strike Corps by side-stepping an existing Division Size Force towards the northern borders coupled with assigning dual tasks to several formations give a credible capacity for India to articulate its forces as per current threat perception (Negi 2021).[21] But, the complete evolution of 'Intelligentized Warfare' and further comprehensive application would have an overwhelming effect on this setup. By 2050, these capabilities would have been developed, allowing the PLA to engage in synchronous and simultaneous 'Intelligentized Warfare' in multiple domains. India and her Armed Forces must understand this criticality and should embrace jointness under the umbrella of disruptive technology. A 'whole of nation' approach must include infrastructure development, civil-military cooperation, development of homegrown disruptive military technology and creation of new doctrine that must enable us to fight technology-intense algorithmic warfare.

****

Maj Vishnu RJ is an alumnus of the Defence Services Staff College, Wellington, the Nation Defence Academy, Khadakwasla and the Sainik School, Kazhakootam. He is a serving officer in the Regiment of Artillery and is currently serving in the United Nations Organisations Stabilisation Mission in the DR Congo.

NOTES

[1] Collin Koh, "*Why a leaner, meaner PLA must be sensitive to worries about China's military rise*", South China Morning Post, 02 February 2019, Accessed 25 May 2024, URL: Opinion | Why a leaner, meaner PLA must be sensitive to worries about China's military rise | South China Morning Post (scmp.com)

[2] Peter Layton, "*Algorithmic Warfare Applying Artificial Intelligence to Warfighting"* (Canberra, Air Power Development Centre, 2018),02.

[3] Courtney Crosby, "Operationalizing Artificial Intelligence for Algorithmic Warfare", Military Review The Professional Journal of the U.S Army, (July-August 2020), Operationalizing Artificial Intelligence for Algorithmic Warfare (army.mil), 01.

[4] Layton, *Algorithmic Warfare Applying Artificial Intelligence to Warfighting*, 06.

[5] Sugiura Yasuyuki, "*The PLA's Pursuit of Enhanced Joint Operations Capabilities*" (China Security Report, National Institute of Defense Studies, Tokyo, 2021), 24-31.

[6] Else B. Kania, "*Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*" (Occasional Paper, Center for a New American Security, Washington, 2017),12.

[7] Yasuyuki, "*The PLA's Pursuit of Enhanced Joint Operations Capabilities*", 01.

[8] David M. Finkelstein, "*The PLA's New Joint Doctrine: The Capstone of the New Era Operations Regulations System*", (Occasional Paper, CNA, Virginia, 2021),13.

[9] Edmund J. Burke et al, "*People's Liberation Army Operational Concepts*" (RAND Corporation, 29 September 2020), 09. People's Liberation Army Operational Concepts | RAND

10 Yasuyuki, "*The PLA's Pursuit of Enhanced Joint Operations Capabilities*", 16.

11 Derek Grossman, et al, "*Chinese Views of Big Data Analytics*", RAND, 01 September 2020, Accessed 25 June 2024. URL : Chinese Views of Big Data Analytics | RAND.

12 Tim McMillan, "*600-Million-Camera 'Skynet' basis for new lunar spy system as China pursues surveillance state beyond earth*", The Debrief, 07 March 2024, Accessed 20 May 2024. URL: 600-Million-Camera 'Skynet' Basis for New Lunar Spy System as China Pursues Surveillance State Beyond Earth - The Debrief.

13 Brian Hart, et al, "*Is China a Leader in Quantum Technologies?",* China Power, 14 August 2023,Updated 31 January 2024, Accessed 25 June 2024. URL : Is China a Leader in Quantum Technologies? | ChinaPower Project (csis.org).

14 Bradford Waldie, "*How Military-Civil Fusion Steps Up China's Semiconductor Industry : A reliable customer, the military can keep firms afloat before they're ready to compete*", Standford University, 01 April 2022, Accessed 25 June 2024. URL : How Military-Civil Fusion Steps Up China's Semiconductor Industry (stanford.edu).

15 Bradley Dunseith, "*Cloud Technology in China: What Businesses Need to Know*", China Brief, 07 May 2018, Accessed 25 June 2024. URL : Cloud Technology in China: What Businesses Need to Know - China Briefing News (china-briefing.com).

16 Burke, "*People's Liberation Army Operational Concepts*", 01.

17 Akshit Sharma, "*Emerging Technologies and The Future of The Indian Army*", Defenc exp, 04 October 2023, Accessed 24 May 2024. URL : Emerging Technologies and The Future of The Indian Army » (defencexp.com).

18 Josh Baughman, "*Preparing the People's Liberation Army Militia for War*" (Research, China Aerospace Studies Institute, Alabama, 2022), 06.

19 Krassi Twigg and Kerry Allen, "*The disinformation tactics used by China*", www.BBC.com, 12 March 2021, Accessed 15 May 2024. URL: The disinformation tactics used by China (bbc.com).

20 Nihar Kuanr, "*An Appraisal of The PLA's Training for Integrated Joint Operations-India's Actions, Response and Counter-Strategy",* (New Delhi, United Services Institution of India,2019), 49.

21 Manjeet Negi, "*Army's Mountain Strike Corps gets 10,000 additional troops, firepower for ops along China border*", India Today,09 April 2021, Accessed 27 May 2024. URL: Army's Mountain Strike Corps gets 10,000 additional troops, firepower for ops along China border - India Today

STRATEGIC IMPLICATIONS OF 6G TECHNOLOGY DEVELOPMENT ON INDIAN DEFENCE ARENA

Gp Capt R K Dogra

Abstract

Future wars; both kinetic and cognitive, will be shaped by wireless communications. The wide scale use of communication networks and digital space in ongoing conflicts; Russian-Ukrainian and Israel-Hamas are testimony of the fact that not only the control of spectrum but also its intelligent and innovative use that will play a decisive role in times to come. The perceived military benefits of faster, widely available networks have accelerated the race for networks like 6G. Ubiquity is the unique features of 6G i.e availability on land, space and underwater. AI will be integral part of 6G technology and will revolutionise human-to-human, human-to-machine and machine-to-machine interactions. Amid all these fast emerging wireless technologies, militaries around the world need to adapt, innovate and re-design their strategies. With widening user base, increased data-centric applications, and Industry 4.0 requirements, 5G network is expected to saturate and eventually making way for 6G. To achieve the milestone of 6G rollout by 2030, a well funded research, government support and user participation is essential. Many countries have already made considerable investments in development of 6G infrastructure and components. 6G development should be top priority of India as the country not only has the potential to be a leader in 6G technology development but also can be a leading manufacturer of its components. Indian defence forces must capitalise on the benefits of 6G in war-fighting and should associate from the inception stage to develop defence specific applications of 6G. The article covers the limitations of 5G network, the AI entanglement in 6G, applications of 6G, joint military applications and the development story of 6G so far.

Introduction

Wireless mobile networks have seen significant revolutions in last three decades. Countries like China have taken leap steps in adding 'intelligence'[1] to the networks. Emerging niche technologies like Internet of everything (IoE), Edge computing, Quantum computing, Virtual reality, 3D media, AI and Machine Language (ML), which were originally designed for civil world, have found impacting applications in military world. By end of year 2025, 65% of the world's population is expected to have access to 5G network. While 5G is fully deployed, research has already begun on 6G networks also known B5G, 5G++ etc.[2] In wireless tech domain, it is believed that after every 10 years the next technology takes over. Going by this, by 2030, 6G technology should be fully implemented and standardised. Most of the niche technologies being developed need wireless networks and considering this fact, a strategic competition is being build up in the world to take lead in these wireless network technologies.

In the ongoing Russian - Ukrainian war, Russian forces used the tactics of blending cyber and physical attacks on Ukrainian C4ISR networks. On the other hand, Ukrainian forces extensively relied upon satellite public telecommunication and Cloud Computing as backup for its continued operations with the help of web based solution providers like Microsoft, Google and Amazon. Indian defence forces may face similar attacks from its adversaries and might have to resort to 'intelligent' strategies in future.

We have already witnessed extensive use of UAVs, UCAVs, Underwater drones in Russian-Ukrainian war. Warfare henceforth will definitely include use of 6G driven intelligence swarms, Cross domain mobile warfare, Cognitive control operations and AI based space confrontations. 6G has also revolutionised hypersonic missile communication technology. USA, UK, China and Finland are already patenting 6G technologies. India, has also taken some initiatives, albeit late, for nurturing 6G Technology. A 6G alliance (6GA) has been set up and research and development centres are being formed up in government and privately funded laboratories. Considering the implications of 6G on security, it's imperative for Indian defence forces to take a lead in steering faster development of 6G and associated niche technologies.

Evolution of 6G

Last three decades have witnessed revolutionary changes in mobile communication and exciting applications like Internet of Everything (IoE), Virtual Reality (VR), 3D media, Artificial Intelligence (AI), enhanced mobile broadband (eMBB)[3] have seen rapid growth. 5G network was expected to strengthen the Internet of everything. However, due to inherent limitations of 5G network, it is not able to create a fully automatic and intelligent network that enables high mobility service. 4G and 5G network also exhibit issues such as high mobility, Doppler Shift and lack of coverage in some zones. Table 1 gives a brief comparison of 4G 5G and 6G Technologies.[4]

KPIs	4G	5G	6G
Peak data rate /device	1 Gbps	10 Gbps	1 Tbps
latency	100 ms	1 ms	0.1 ms
Max. spectral efficiency	15 bps/Hz	30 bps/Hz	100 bps/Hz
Connection density	2000 devices/Km^2	1 million devices/Km^2	>10 million devices/Km^2
Coverage percent	< 70 %	80%	>99 %
Positioning precision	Meters precision (50 m)	Meters precision (20 m)	Centimeter precision
End-to-end reliability	99.90%	100.00%	100.00%
Receiver sensitivity	Around —100dBm	Around —120dBm	< —130dBm
Mobility support	350 km/h	500 km/h	≥1000 km/h
Satellite integration AI	No	Partial	Fully

KPIs	4G	5G	6G
Autonomous vehicle	No	Partial	Fully
Extended Reality	No	Partial	Fully
Haptic Communication	No	Partial	Fully
THz communication	No	Massive MIMO 90 GHz	Widely
Service level	Video	VR, AR	Tactile
Architecture	MIMO 6 GHz	Massive MIMO 90 GHz	Intelligent surface 10 THz
Max. frequency	Video	VR, AR	Tactile

Table 1: Comparison of 4G, 5G & 6G Technologies

6G architecture is being designed in a way to resolve these issues and provide high speed ubiquitous network. This network will be enabled through meshing of Satellite, Air and Terrestrial Communications. 6G Network will also cover underwater communication, giving vital coverage to under water vessels including submarines. 6G data coverage would be accomplished through hybrid networking of device to device, low Earth orbit satellites and satellite communication. 6G ultimately intends to amalgamate computation, navigation and sensing within the communication network. The expected technical features of 6G include a high data rate of 1 Tbps, operating frequency of at least1 Thz, end to end delay of not more than 1ms, reliability rate of 10-9, high mobility of at least 1000/h and a frequency range up to 300μm.[5]

Role of AI in Enhancing 6G Technology

AI would play an important role in enhancing the 6G network structure and will help ‘intelligentise’ 6G applications and functions for domains like architecture, computing storage etc. AI will enhance the speed of 6G networks.[6] AI may also be used for data analysis of the 6G network and identify the places where improvements are required. This will help reducing latency and improve overall network performance. AI will also help to optimise the network requirements while streaming videos or large files like real-time battlefield picture. One of the important aspects of use AI is the ability to detect and prevent suspicious activities on the network, identify them and block potential threats. This can help in improving security of 6G networks. AI will also help in detecting and preventing data breaches which will keep users safe and help protect their data. AI optimised 6G networks will ensure that user get the best possible digital experience.

General Application Domains of 6G

AI will change the way human life will behave after the year 2030. In fact, 6G will be the driver of broader AI applications. Some of the general applications of 6G in terms of emergence of niche technologies are[7]

- Bio-implants, wearable devices, skin patches, brain sensors with natural and intuitive interfaces.
- Typing will be replaced by gesturing and speaking.
- Cameras and Sensors will be deployed en masse due to rapid advances in AI, 6G and computer vision.
- Many of the human tasks will be replaced by Service robots.
- In-body devices and 24x7 parameter monitoring will forever change the healthcare fundamentals.
- Dynamic Digital twins will augment human intelligence and holographic telepresence (appearance of entity at multiple locations at same time) will be a reality with the help of 6G networks.
- Smart cities leveraging 6G technologies, AI enabled autonomous vehicles, sensors, cameras for traffic control, cashless transactions, environmental data and weather data for public assistance and much more will be a reality by 2030.
- The multi-sensory XR experience will be further enhanced using dynamic VA/VR.

Development of 6G and Associated Military Applications

Modern military forces by 2030 would be potentially based on industries standards 4IR or IR 4.0 (4th Industrial Revolution). These militaries will emerge as powerful 6G device forces and would be harnessing niche technologies like AI, ML, Big data, Cloud computing, AR, Quantum computing, Cognitive computing and IoT wave. 6G technology would make military operations highly digitized and intelligent and further would serve both as weapon of war and tool of deterrence. 6G would be the core technology of any net-centric strategy consisting of large number of assets that could operate from space, near space, fly in the air, on surface and deep into underwater to conduct large scale ISR missions and exploration. A wide network of sensors, vehicles and robots would operate with the help of 6G communication and using AI will highly influence the missions, which will be faster, deadlier and autonomous. At the tactical level, the 6G and AI interplay will further shrink the OODA loop and will help Tactical Commanders take faster decisions. The likely uses of 6G by military are as follows:

- Rapid data exchange between sensor and analytics will significantly improve ISR capabilities. More devices can be connected on different frequencies. For Indian defence forces 6G will be a big enabler for Theatre Commands and Theatre Commanders based on rapid real-time field picture and ISR can play a decisive role in guiding the forces and taking critical decisions like defence mobilization etc.
- 6G will enhance battlefield communication and make it more secure.
- UCAVs/UAVs/AVs/Drones will be the largest beneficiary of 6G communication. 6G will provide devices (surface space and underwater) with seamless connectivity, precise tracking and improving their speed and range.
- 6G communication is going to play major role in providing communication links for hypersonic weapons.
- Net-centric Warfare and Joint war fighting, wherein all three defence forces would be deploying their assets and execute effect based operations, would be enhanced using 6G.

- As discussed, precise, high rate of real-time data available would help in theatre monitoring easy.
- 6G will enhance training of soldiers, providing them with real-time experience using VR and AR and would help them formulate their own tactics and strategies using the vast data available.
- Undertaking remote medical procedures using 6G framework will help military doctors in treating battlefield injuries in field areas itself.
- Armed robots operating on autonomous 6G network using brain machine interface (BMI) of 6G will be an effective alternative to soldier on ground during critical operations.

6G Technology Challenges

Coverage in Mountains and Power Infra

So far, the focus of 6G development is on high data rates rather than connecting the remote areas; hilly terrains, the places where wars are likely to be fought. However, research has begun on challenges in connectivity; especially backhaul connection, the link between the internet and local access points. Coverage in hills can be demanding, in terms of range and power infra requirements. Recently, a research team from the University of Stuttgart[8] has succeeded in establishing a broadband connection in the mountains between the valley and the summit for the first time in Austrian Alps, at an altitude of 2334 meters over a length of 2 x 10.5 kilometers and transmitted data at a speed of 25 gigabits per second. In absence of fiber network, laying of which may not be viable in mountainous terrain, satellite constellations like Starlink by SpaceX and the systems by OneWeb and Telesat can be game-changers.[9] The forthcoming 6G networks are expected to leverage the power of flying platforms [e.g., unmanned aerial vehicles (UAVs) and high-altitude platform stations (HAPSs)] in different network segments including the backhaul part, especially in harsh terrains or if terrestrial deployments have collapsed or not been set up. To achieve this goal, non-terrestrial networks need to address a number of technical impediments related to their integration with terrestrial infrastructure, their placement in three-dimensional space, and their energy efficiency concerns, thus calling for further research.

Use of low-power Power Amplifiers is being explored to minimize the power requirements of 6G networks. Use of alternative power sources like Solar and Wind to power Base Stations is also been in works. There is also room for developing low-power beamforming hardware and software in 6G which will help to increase data rates or range and adjust radiation patterns based on need. On the other hand, intelligent reflecting surfaces (IRSs) are among the latest breakthrough technologies of the 6G ecosystem, used to passively reflect the signal without amplification. Since solar power is not always available, solar power can be supplemented by other off-grid energy sources, such as wind energy, hydrogen cells, and others. One way to reduce the number of towers and their heights is to utilize diffraction, wherein a signal propagates beyond LoS obstacles. The problem is how this phenomenon can be efficiently utilized. Network planning and propagation estimation tools are needed for simple and cost-effective planning.

Security and Cyber Challenges

6G applications also have specific vulnerabilities. The robotics and autonomous systems typically rely on the AI and the VLC (visible light technology) where malicious behavior, encryption and data transmission can be compromised.[10] The multi-sensory XR applications use the molecular communication technology, the THz technology and the quantum communication technology, which means they are susceptible to access control attacks, malicious behavior, and data transmission exposure. Wireless Human-Machine interface use the same techniques as the multi-sensory XR application, but have their own unique security and privacy issues. Essentially, 6G technology components are prone to five main types of security and privacy issues: authentication, access control, malicious behavior, encryption and data transmission.

The Cat and Mouse game of vulnerabilities and counter-measures will continue in 6G technology also. However, parallel tech is being developed to mitigate the possible security and cyber threats. For different phases of cyber security protection and defense in 6G, concept of distributed AI/ML can be used. The utility of AI/ML driven cyber security lies on the advantages in terms of autonomy, higher accuracy and predictive capabilities for security analytics.[11] There is hope of research in introducing ML based cyber-security and quantum encryption in communication links in 6G networks. Quantum ML algorithms may enhance security and privacy in 6G communication networks. There are promising 6G applications where there are potentials in applying quantum security mechanisms. PLS (Physical Layer Security) methods will be leveraged by 6G to provide an adaptive additional layer of protection in the context of new enabling technologies.

6G Development Scenario in Other Countries

6G developments at present are in a free competitive stage, focusing primarily on profitable avenues for 6G applications, the technology and associated requirements. The parent organisation for global wireless telecommunication standard setting activities, the 3GPP (the Third Generation Partnership Project) embodies the multinational nature of this technology. The group has partnering organisations from USA, Europe and Asia. Statistically 3GPP includes 439 companies from Europe, 171 from China, 145 from India, 95 from USA, 46 from Japan, 15 from Finland, 18 from Singapore, Nine from Taiwan and Two from Russia. These players are actively involved in designing 6G component technology, acquiring patents, anticipating standardisation and commercialisation in coming few years. Research is the current activity these organisations are at present involved in due to capital intensive and technical complexity of the technology. The major companies involved in 3GPP are Europe (Nokia, Ericsson, Orange), USA (Cisco, AT&T, Qulacomm, Verizon), China (Huawei, ZTE), South Korea (Samsung, LG), Japan (Fujitsu, NTT, Docomo).

Battlefield 6G: How USA And China are Shaping the Technology for Military Use

USA and China, both view 6G and associated disruptive technologies as key areas of competition for technological domination in the Civil and Defence sectors.[12] Beijing's efforts to combat intelligent warfare and system confrontation are progressing in sync with the 6G technological maturity. Chinese scientists recently developed a device that could effectively used 6G technology for hypersonic communication and target detection, overcoming previous problems of signal blocking that occurs at these speeds. Chinese defence in year 2020 had laid down the vision for how 6G could be used in future operations.[13] This include cross domain communication networks enabled by Satellite, Drone and Optical technologies. PLA may use 6G for enhancing ISR capabilities, especially of space. US Department of Defence, on the other hand is focusing on development of 6G in four major areas; contested logistics, joint fires across all domains and services, joint command and control of all domains (in both permissive and contested environments), and information advantage. DoD is putting emphasis on the downstream challenges post by improved data-centric warfare and future warfare concepts namely training and decision making requirements and security related strategies. As USA witnesses a great leap being made by China in 6G and AI, the DoD is pushing for increasing need for war fighters to better understand the strategy and get prepared and trained to be disruptive and becoming innovative soldiers who can make impact in contested and chaotic environments.

Bharat 6G - India's Road to 6G Network

Indian government is making all out efforts in driving 6G research and innovation with an aim to promote India as a global lead in 6G technology and becoming its mainstream manufacturing hub. The country has adopted a nationwide approach involving industry, start-ups, academia and research laboratories, standards bodies in not only achieving the self-reliance but also making useful contributions to the world.[14] In the year 2021, the Department of Telecommunications under Government of India (GoI) has formed a Technology Innovation Group (TIG) for 6G with members from various ministries/departments, research and development institutions, academia, standards bodies, telecommunication service providers and industry. The aim of the group was to develop vision, mission and goals for 6G and also develop a broad road map and draw plans for 6G development in the country. Based on the recommendations of this TIG, the GoI have prepared and issued a comprehensive Bharat 6G Vision Document.

The Bharat 6G Vision and Mission

"Design, develop and deploy 6G network technologies that provide ubiquitous, intelligent and secure connectivity for high quality living experience for the world"- this 6G Vision of

India[15] is based on principles of Affordability, Sustainability, and Ubiquity. The document envisions that India takes its legitimate place in the world order as a leading manufacturer, supplier of next-gen telecom technologies and possesses capabilities to offer solutions that are affordable and contribute to the overall global growth. As per the vision document, India plans to achieve 6G mission in two phases; Phase I from 2023-2025 (Ideation); Phase II from 2025-2030 (Conceptualization and delivery).

Bharat 6G Alliance - B6GA

The Bharat 6G Alliance is conceptualized to be an alliance of domestic industry, academia, national research institutes and standards organizations, sponsored by GoI. The B6GA is guided by broader guidelines of Bharat 6G Vision Document and have the authority to draw its further course of action. Strengthening its efforts on 6G, on 09 Sep 23, during the G20 Summit at New Delhi, Next G Alliance of North America networks and the Bharat 6G Alliance announced that they had signed a Memorandum of Understanding[16] (MoU) to further explore opportunities for joint collaboration on 6G wireless technologies.

Implications of 6G Developments for India and Joint Military Applications

Addressing the nation from New Delhi's Red Fort on India's 77th Independence Day, Prime Minister Narendra Modi said that the country is prepping to enter the 6G era soon. "We have formed a 6G task force," he said during his Independence speech at the Red Fort.

India today has more than 30 Crore smart phone users. As India approaches 'Swarnim Bharat' dream in 2047, the next two decades are a crucial period of growth. Technological advancements and manufacturing capacity and will determine the country's future. It is critical to take advantage of the opportunity presented by the 6G, even if the technology is in nascent stage. As the second largest telecommunications market in the world, India must evolve and project itself into a global provider and manufacturer of network technology. It should be the country's endeavor to actively participate in defining the contours of 6G and drive tech innovation to meet the urgent needs of not only India, but also of global world. India's early participation and lead in 6G technology development will help reduce differences in regional and social infrastructure. The impending integration of space and terrestrial networks into a seamless, unified India offers the opportunity to leverage its space technology capabilities to fill the gaps in the coverage of its vast rural hinterland and ensure that all Indians, regardless of their location have broadband connections.

Militarily, 6G and AI will help India modernize its forces, help optimize the forces and keep its deterrence high especially w.r.t China. The country is poised to grow at fast pace economically and is been seen as Global smart power. Space and underwater are two domains where Indian armed forces see huge potential to grow. Both these domains will be enormously benefited by 6G technology. India is also fast becoming a 'Drone hub' of the world. 6G technology will enable next generation of drones and robotics and can further establish India as a global supplier of these disruptive war fighting elements. In a nutshell, 6G and AI can propel the missing Indian quest for military exports besides strengthening its own boundaries.

Key Recommendations

Taking into consideration China's advances in AI and investments in 6G, the Indian security space needs to take definite steps to counter China's technological edge in 6G and AI. Limitations in the semiconductor industry, manufacturing and technology development must be prevailed over to position us at the starting line of this competition. Based on this paper, the recommendations for the military use of 6G in India are as follows:

- Keeping in mind the future wars, AI enabled equipment and changing tactics, there is a need for including military specific representatives in 6G Apex Body and Directorate. These representatives along with experts from academia, R&D labs and Private consortium will focus on developing 6G technology components for enhancing country's security infrastructure.
- R&D Labs, be envisioned as 'Military 6G & AI Clusters' and funded for 6G development based on competencies for orchestrating new generation equipments. The Labs should be agile and quickly adaptable to evolving military needs. *Formation of STEAG (Signals Technology Evaluation and Adaptation Group) by Indian Army and AI cell*

under UDAAN (Unit for Digitisation, Automation, Artificial Intelligence and App Networking) of IAF is a positive step in this regard.

- Dedicate funding for R&D in 6G and AI for developing military specific hardware and software. Use of 6G enabled ISR with AI technologies to assist the Local Commander at remote borders in war fighting must be the key priority of any 6G development project. Similarly, AI enabled Robotics, having high processing powers, propelled by 6G communication would be a revolutionary change for any military.
- Alliances with friendly nations to develop critical 6G technologies for defence and further commercialization of the same needs to be made.
- Government special funding for key 6G applications such as Drone communication, Human-Machine interfaces, Low Orbit Satellites (LEOs), Hypersonic Missile communication, Extended Reality, Digital Twins etc.
- While reviewing Spectrum requirements for 5G+/6G, the Military requirements must be taken into account.
- With an eye on Indo Pacific region and to secure our sea lines of communication, development of key 6G technologies for deep sea water and under water communication must be facilitated.

Conclusion

'Intelligent' warfare, driven by 6G and AI demands absolute integration of military and civil domains as we witness blurred lines between peacetime and wartime. The outcome of a war will be determined not by who destroys the other in a kinetic sense, but by who derives the greatest political benefit out of it, as is being seen in recent conflicts in Russia-Ukraine. Intelligent warfare integrates human and machine intelligence. Soldiers will eventually no longer be the first line of battle and wars will be fought under the overall gambit of intelligent systems, ultimately the war becoming a machine-on-man or machine-on-machine oriented. Strategically and tactically, human fighters, including the commanders will comprehensively enhance their inherent cognitive and physiological capabilities using 6G and AI. Cross-domain warfare and asymmetric combat in military operations will be new normal in future conflicts. Unmanned operations will reset the rules of engagement and redefine the support process. To protect our growing economy from these immediate future threats, India must keep accelerating efforts to develop 6G and its assisted niche technologies. The Bharat 6G vision document and the 6G Alliance, as well as recent collaborations with friendly nations, are steps in the right direction, but allocating more funds for research and development is the need of the hour. The overall objective for India as a nation remains to become global 6G technology provider for human good while maintaining strategic deterrence for its military.

****

Gp Capt R K Dogra is serving Aeronautical Engineering officer of IAF. He specialises in aircraft technology, especially the MRO functions. He has served as Chief Engineering Officer of an important base in EAC. He is currently working with LRDE, DRDO.

NOTES

[1] How to Win Intelligentized Warfare by Analyzing what are Changed and What are Unchanged),” 2019, Jiefangjun Bao (https://madsciblog.tradoc.army.mil/199-intelligentization-and-a-chinese-vision-of-future-war/)

[2] Mohammed Banafaa*, Ibraheem Shayea , Jafri Din , Marwan Hadri Azmi Abdulaziz Alashbi , Yousef Ibrahim Daradkeh , Abdulraqeb Alhammadi ; 2023, 6G Mobile Communication Technology: Requirements,Targets, Applications, Challenges, Advantages, and Opportunities

[3] ibid

[4] ibid

[5] Areq B. Ahammed, Ripon Patgiri, Sabuzima Nayak, A vision on the artificial intelligence for 6G communication, ICT Express, Volume 9, Issue 2, 2023, Pages 197-210, ISSN 2405-9595, https://doi.org/10.1016/j.icte.2022.05.005.

[6] Technology prospect of 6G mobile communications 2019 Zhang Ping , Niu Kai , Tian Hui , Nie Gaofeng, Qin Xiaoqi , Qi Qi2 , Zhang Jiao

[7] Harish Viswanathan, And Preben E. Mogensen 2020.Communications in the 6G Era.

[8] Jacqueline Gehrke, Ingmar Kallfass ; The EIVE-T project ,The University of Stuttgart; https://www.uni-stuttgart.de/en/university/news/all/6G-mobile-communications-tested-in-the-Alps-for-the-first-time/

[9] Harri Saarnisaari1, Abdelaali Chaoub, Marjo Heikkilä, Amit Singhal and Vimal Bhatia,Wireless Terrestrial Backhaul for 6G Remote Access: Challenges and Low Power Solutions, Nov 21, Frontiers in Communications and Networks.

[10] Shimaa A. Abdel Hakeem, Hanan H. Hussein, and HyungWon Kim1, March 2022, Security Requirements and Challenges of 6G Technologies and Applications

[11] Pawani Porambage_, G¨urkan G¨ury, Diana Pamela Moya Osorio, Madhusanka Liyanage_z, Mika Ylianttila, Jun 2021, 6G Security Challenges and Potential Solutions, Conference: 2021 Joint European Conference on Networks and Communications (EuCNC) & 6G Summit,Porto, Portugal

[12] John Lee, Meia Nouwens and Kai Lin Tay 2022 Strategic Settings for 6G: Pathways for China and the US

[13] CENJOWS Chinas-6G-to-Power-AI-Army-of-the-Future-dt-09-Sep-2020.pdf

[14] Website data of Department of Telecommunications, Ministry of Communications, Government of India, https://dot.gov.in/bharat-6g

[15] ibid

INDIA'S SEMICONDUCTOR ECOSYSTEM IN JOINT WARFIGHTING: EXPLORING STRATEGIC COLLABORATION IN THE INDO-PACIFIC

Dr Ulupi Borah

Abstract

To modernise the defence capabilities especially in terms of joint warfighting, the role of semiconductor and an efficient ecosystem is pivotal. Today, India is striving to create a comprehensive semiconductor ecosystem to reduce its reliance on the imported chips. The Indian semiconductor era appears to have begun in 2021 with the launch of the India Semiconductor Mission (ISM). It is anticipated that India is poised to become a dependable supply chain hub by capitalising on the geopolitical unrest amongst the major powers. However, challenges persist involving various factors. To overcome such challenges, India should make collaborative efforts with the major semiconductor hubs of the globe mostly in the Indo-Pacific region. The paper delves into the significance of semiconductors in joint warfighting and how India should strengthen its strategic collaboration with the QUAD countries along with the Southeast Asian nations, Taiwan, Vietnam, Singapore, and South Korea. The paper also discusses various initiatives need to be taken for India to become a global semiconductor hub followed by technological innovation.

Introduction

Modern military technology relies heavily on microelectronics. Semiconductors are an essential part of microelectronic devices, helping to improve functionality and performance. In military applications especially for joint warfighting, semiconductors are of utmost importance due to their ability to process and transmit vast amounts of data quickly and efficiently.[1] They enable the development of advanced radar systems, communication devices, navigation systems, and weaponry. Semiconductors also enable miniaturisation, making it possible to create smaller, lightweight military equipment without compromising functionality.[2] Overall, semiconductors are indispensable in modern military technology, providing the foundation for advanced and efficient systems that are essential for defence and national security.

Currently, India is aiming to establish a complete ecosystem, from design to manufacturing which would cater to the demands of the country's defence industry. A number of recent cabinet approvals have opened the door for significant industry advancements. For example, there is an approval for a greenfield initiative in which Tata Electronics Private Limited is collaborating with PowerChip Semiconductor Manufacturing Corporation (PSMC) in Taiwan.[3] TATA has also taken the initiative to set up the Outsourced Semiconductor Assembly and Test (OSAT) facility in Morigaon, Assam under the modified scheme for Semiconductor Assembly, Testing, Marking and Packaging (ATMP), with a total investment of about Rs 27,000 crore ($3.29 billion).[4]

The Odisha state government has encouraged the development of fabless chipmakers and provided them with state-of-the-art electronic design automation (EDA) tools. The Tamil Nadu state government's semiconductor policy also covers the cost of conducting additional research and development and creating a prototype. Within a decade it is expected that India could become the hub of the global semiconductor ecosystem.[5] However, there are several challenges India will have to face. The major semiconductor manufacturing countries are in the Indo-Pacific region. India being a member of the QUAD and a prominent country of the region, have ample of opportunities to collaborate with countries like the US, Japan, Taiwan, South Korea Vietnam, Singapore and Philippines.

The paper makes an effort to understand India's ecosystem and the challenges it faces due to various factors. It has also elaborated few recommendations as strategies keeping in mind India's interest to become a global hub in the next ten years.

Role of Semiconductors in Joint Warfighting

There are multiple areas of use of semiconductors. Some of them are covered as under:

- **Sensors and Actuators.**

Wireless sensors, a crucial semiconductor technology product, are one of the essential elements that are becoming more and more important in the military and aerospace industries. By using cutting-edge simulation techniques, sensors contribute to better aircraft control and lightweight design for enhanced weight performance. In addition, the smart sensor is a critical component of the internet of things (IoT) while providing unique identifier for almost anything especially in terms of transmission of data from or about those items over the internet or a comparable sensor network. Actuators are parts that make a system move, and their importance in the aerospace sector has been steadily growing. These actuators are immediately interfaced to flight control and autopilot systems via wireless sensor networks, which initiate the appropriate responses.[6] Thus, a country which is driving into the field of innovation and improvement especially in joint warfighting, will have an increased reliance on the transformative impact of such advanced technologies.

- **Microchips.**

It is amazing to see how a micro-chip has the ability to store huge amount of data with the manufacturing of the advanced memory devices. There is an increased interest of usage of non-volatile (NV) memory in autonomous military vehicles due to its data storage even after the cut down of the power supply.[7] Recently developed NV chipsets have high physical limits before degradation of the storage layer and can withstand extreme temperatures, similar to military conditions.[8]

- **Electro-Optical Systems.**

Semiconductor technology is becoming important in the development of electrooptical (EO) systems, particularly for military applications. EO/infrared systems have traditionally been used for imaging and situational awareness, particularly in low-light and night circumstances.[9] EO is tightly coupled to sensor technology and digital signal processing. Semiconductor is at the heart of signal processing.

- **Microcontrollers.**

In recent years, there has been a significant increase in the development of high reliability integrated circuits (also known as microcontrollers). HIREL microcontrollers are being utilised in mega-constellations, which are groups of artificial satellites used for large-scale broadcasting, as well as tiny and picosatellites by governments and private businesses.[10]

- **Logic Devices.**

A programmable logic device (Pld) is an electrical component used to create reconfigurable digital circuits, such as logic arrays. New logic devices, including field Programmable gate arrays (FPGA), are being developed to meet military requirements.[11]

In the global security scenario while discussing about joint warfighting today, the geopolitics of semiconductors are revolving around the microchips, logic devices, EO, microcontrollers etc. and their production, innovation and control. Thus, a country leading in these technologies will have the leverage to hold a crucial position at a global level.

Understanding the Ecosystem of the Leading Global Semiconductor Hubs and QUAD Partners

Among the leading global semiconductor hubs, the US is the unquestioned global leader in semiconductor design. Six of the top ten global fabless companies by revenue in 2019-20 were American. The following points show US's leading percentages in 2018, except in 'Outsourced ATP' and 'Contract Foundries' where Taiwan was leading:

- **Integrated Device Manufacturer (IDMs).** U.S.-based firms account for 51% of total global IDM revenues, followed by firms based in South Korea (28%), Japan (11%), Europe (7%), Taiwan (2%), and Singapore (1%). [12]
- **Fabless Firms.** U.S.-based firms account for 62% of total global fabless firm revenues, followed by Taiwan (18%), China (10%), Singapore (7%), Europe (2%), and Japan (1%).[13]
- **Contract Foundries.** Taiwan-based firms account for 73% of total global contract foundry revenues, followed by firms based in the United States (10%), China (7%), South Korea (6%), Japan (2%), and Singapore (2%).[14]
- **Outsourced ATP.** Firms based in Taiwan account for 54% of total outsourced ATP revenues, followed by firms based in the United States (17%), China (12%), Singapore (12%), and Japan (5%).[15]

The United States

American corporations dominate two important sub-stages before the design processes: EDA and licenced intellectual property. Chip design is done with EDA software, which has a highly concentrated market due to expensive R&D expenses. Cadence Design Systems, Synopsys, and Mentor Graphics are the three leading players in the space, all based in the United States.[16] The first two are American enterprises, while Mentor Graphics was acquired by the German multinational company Siemens in 2017 but continues to operate from the US. In addition to EDA tools, licenced intellectual property is a critical feature of semiconductor design, particularly for CPUs.[17]

In 2018, the US-based companies generated 62% of worldwide fabless firm revenues. It is also home to the world's leading integrated design manufacturers (IDMs), which are companies that build their own chips, such as Intel. In 2018, US-based enterprises accounted for 51% of global IDM revenues.[18]

Japan

While Japan maintained a 50.3% share of the world semiconductor industry in 1988, this percentage has slowly decreased since the 1990s, falling to 10 percent in 2019.[19] Ogino Yosuke, Director of the Device Industry and Semiconductor Strategy office at the Ministry of Economy, Trade and Industry stated:

'Maintaining and strengthening the domestic semiconductor industry is a crucial strategy for Japan's future and the safety of its citizens.'[20]

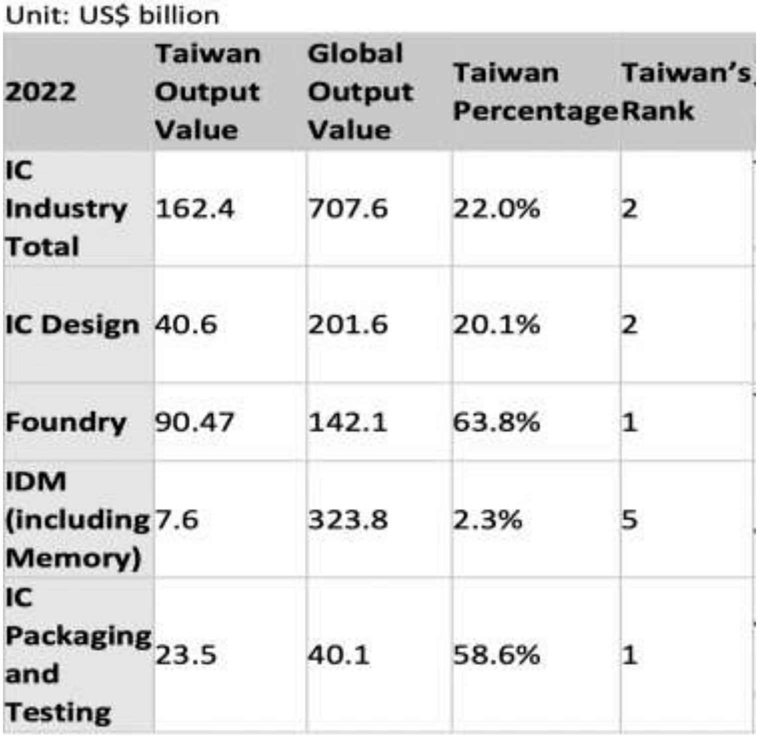
In 2021, the Ministry of Economy, Trade, and Industry developed a support strategy for the revival of the semiconductor industry including identifying semiconductor and digital sectors as national priorities. The strategy includes ambitious initiatives, such as the establishment of the Post-5G Fund of JPY200 billion (approximately $1.3 billion) for technological innovation in post-5G and the Green Innovation Fund of JPY2 trillion (approximately $13 billion), which focuses on the development and implementation of semiconductors.[21]

In addition, the domestic semiconductor-related sales are expected to exceed JPY15 trillion (about $99.4 billion) by 2030, more than tripling the amount in 2020.[22]

Taiwan

Taiwan produced 63.8 percent of the world's semiconductors in 2022, with sub-7 nanometer (nm) high-end integrated circuits accounting for more than 70 percent of the global market.[23] Taiwan's integrated circuit (IC) packaging and testing output value is likewise the highest in the worldwide semiconductor market, accounting for 58.6 percent. In addition, Taiwan's IC design production value accounted for 20.1 percent of the global market, ranking second only to the US. There is no doubt that Taiwan is essential to global economic growth and technological innovation.[24]

More than 90 percent of the primary production sites, as well as cutting-edge technologies, advanced processes, and forward-thinking research and development, remain in Taiwan. Major foreign corporations, including ASML, LAM Research, and Entegris, are expanding their investments in Taiwan, creating production facilities and investing directly in semiconductor companies. Applied Materials and Tokyo Electron have also established training centres for modern process equipment in Taiwan. Leading worldwide ICT and IC businesses, including Apple, Broadcom, and Qualcomm, have chosen Taiwanese companies to provide contract wafer production, IC packaging, and testing services.[25]



Unit: US$ billion

2022	Taiwan Output Value	Global Output Value	Taiwan Percentage	Taiwan's Rank
IC Industry Total	162.4	707.6	22.0%	2
IC Design	40.6	201.6	20.1%	2
Foundry	90.47	142.1	63.8%	1
IDM (including Memory)	7.6	323.8	2.3%	5
IC Packaging and Testing	23.5	40.1	58.6%	1

Table 1, Output Value of Taiwan's IC Industry as a Percentage of the Global Industry Output Value in 2022. Source: Taiwan and the Global Semiconductor Supply Chain, ed. Chen-Yuan Tung. URL: https://www.roc-taiwan.org/uploads/sites/86/2024/02/240202-February-Issue.pdf

Table 1 shows the position of Taiwan in various segments of global value chain of semiconductors. Out of the five segments, Taiwan leads in foundry and IC packaging and Testing. Taiwan holds the second position in terms of IC Industry and IC Design. Taiwan Semiconductor Manufacturing Company Limited (TSMC), the leading Taiwanese semiconductor company, has been invited to establish operations in the US, Japan, and

Europe. However, the new plants are not expected to impact Taiwan's global position in the semiconductor industry.

South Korea

The semiconductor ecosystem is rapidly evolving in South Korea reinforced by investments from both the private and government sectors. Being quite robust in nature, the semiconductor industry in South Korea is able to assert its global competitive edge.

In 2024, the government of South Korea announced a funding package worth 19 billion dollars (26 trillion won) for the chip manufacturing industries. These packages are meant to support research and development, infrastructure including the financial needs. This is also focused to support the medium sized and small enterprises.[26] According to the comments reported by Al Jazeera, President Yoon Suk-yeol stated:

"As you all know, semiconductors are a field of national all-out war."[27]

The country being home to companies like Samsung and SK Hynix, the top chip manufacturers of the globe, vowed to commence the largest chip centre. This would mostly require investing at least $456 billion.[28] Ensuring supplies of advanced semiconductors has become a critical issue on a global scale, especially with the US and China competing for market dominance. Kim Dae-jong, a professor of business administration at Sejong University in Seoul, told the AFP news agency, "South Korea is supplying 80 percent of the world's memory semiconductors and has said it is investing 300 trillion won ($220bn) in the Yongin cluster, but there has been a water supply issue with it." He also added:

"On top of tackling such issues, today's announcement seems to be an effort to support innovative small and medium-sized enterprises to further strengthen their competitiveness against [rivals] like Taiwan."[29]

As the 'China Plus One' is gaining traction, it has been anticipated that South Korea will gain medium-term business in the semiconductor sector. Dina Ting, Head of Global Index Portfolio Management at Franklin Templeton affirmed that the US Inflation Reduction Act

2022, which encourages supplies from the free-trade partner might help South Korea in enhancing its business in this sector.[30]

However, Seoul's semiconductor sector is mostly concentrated in South Korea and China. This definitely enhances the chances of over-reliance on a particular location. To avoid that, diversification of manufacturing is necessary. At this point, South Korea can think of India as an alternative which has shown great enthusiasm in this sector in the last couple of years. India survived the COVID-19 shock demonstrating great resilience along with a stronger political will to expand the semiconductor sector.

International cooperation in this sector is a significant aspect for South Korea today. Developing synergies with other semiconductor hubs of the globe and ensuring supply chain resilience remain critical to its goals. Thus, expanding it to India, it can reduce its dependence just on China and enhance its global presence.

People's Republic of China (PRC)

PRC has released several directive policy statements that outline a broader framework for science and technology development, which includes China's semiconductor sector policy. China realised the need to reduce its foreign import since 2009 and remained focused with is initiatives such as the 02 Special Project. According to a 2017 report, at least 16 types of frontend wafer fabrication equipment have been commercialised.[31] Out of the 16, one of the products (7nm process nodes) was approved by the TSMC, the global foundry leader. China started its semiconductor policy to reach the current phase was when it issued the 'National Integrated Circuit Industry Development Outline' in 2014 (2014 Outline). The 2014 Outline included development goals for manufacturing tools and materials, as well as for chip design, fabrication, packaging, and testing. The Made in China 2025 (MiC 2025) industry upgrade plan, released by the State Council in 2015, set widely publicised goals of achieving 40 percent and 70 percent self-sufficiency in China's total IC consumption by 2020 and 2025, respectively.[32]

According to Mercator reports, in 2020, China's self-sufficiency was just 16 percent in terms of producing ICs. By 2021, the imports increased by 30 percent. This encouraged

Beijing to develop an entire ecosystem for IC while commencing in areas where it was lacking.[33] This included R&D capacity, enhancing skilled labourers and extending its collaboration with the global semiconductor hubs.

In the first quarter of 2024, China's overall output of ICs increased by 40 percent to 98.1 billion units despite the US restrictions on chip making equipment.[34] Trend Force, a Taiwan based IC research company stated:

"The mainland's global share of mature-process capacity is expected to reach 39 per cent by 2027, up from 31 per cent in 2023."[35]

By 2025, Beijing expects that its tech sector reaches an annual output worth US $13. 9 billion.[36]

Understanding India's Semiconductor Ecosystem

In many ways, India's current focus on Aatmanirbhar Bharat is reminiscent of its early post-independence technology initiatives. Prime Minister (PM) Jawaharlal Nehru's initial meetings with American industrialists seemed to be similar as that to India's current industrial plans. During the 1960s, a few Indian companies started manufacturing germanium semiconductors. Fairchild Semiconductors, a leader in integrated circuit (IC) technology, was considering establishing its first Asia facility in India. During this time, Bharat Electronics Ltd. (BEL) and Hindustan Aeronautics Ltd. (HAL), public sector enterprise PSU under the Ministry of Defence were significant players in the Indian semiconductor market. India's semiconductor sector gained momentum in the 1980s because of the several initiatives undertaken by the then PM Rajiv Gandhi.[37]

A major initiative was taken in 1984 when the Indian government established Semiconductor Complex Limited (SCL) as a public sector enterprise. Licencing arrangements with Hitachi, AMI, and Rockwell enabled this endeavour. However, within a decade India lost its manufacturing advantage caused by a severe fire that occurred in 1989 at the SCL complex in Chandigarh. The Indian government originally announced the creation of the country's first semiconductor policy in 2007 although it wasn't very successful until 2015. However, in 2021-2022, to promote semiconductor factories, ATMPS, and the design ecosystem in India, the Indian government released the 'Modified Semiconductor Policy', allocating US $ 10 billion for this purpose.[38] In 2023, the US based chipmaker Micron declared that its USD 2.75 billion ATMP would be established in Gujarat, India.[39] The Government of India initiated the "India Semiconductor Mission (ISM)" to develop a sustainable semiconductor and display ecosystem as a part of "Program for Development of Semiconductors and Display Manufacturing Ecosystem" in December 2021. The document states that it will be guided by world-class semiconductor and display industry professionals. It will serve as the nodal agency for the efficient and smooth implementation of initiatives for the establishment of semiconductor and display fabs.[40] The size of the Indian semiconductor market was estimated at USD 34.3 billion in 2023 and is projected to grow at a CAGR of 20.1 percent to reach USD 100.2 billion by 2032.[41] Comparatively, the global projection of semiconductor market was USD 664.54 Billion in 2023 and is projected to reach USD 1.9 trillion by 2032, expanding at a CAGR of 12.5 percent during 2024–2032.[42] This illustrates that India's goals in this sector is aligning with the data projected at a global level. The three factors involving, an expanding market, technological capabilities and the political will definitely put New Delhi in a position to enhance its semiconductor sector.

This data illustrates that India is experiencing significant growth in this sector, aligning well with global trends. The country's expanding market, coupled with strong political will and technological capabilities, positions it favourably for advancing its semiconductor industry.[43]

The 3i^2 Formula

The 3i^2 formula discusses the challenges and solutions/recommendations faced by the semiconductor sector of India. Figure 1 shows the 3i's investment, infrastructure, and intellect as the major challenges. To deal with these three challenges there are additional 3i's incentives (government policies), integration (state collaboration), improvement (skill development).

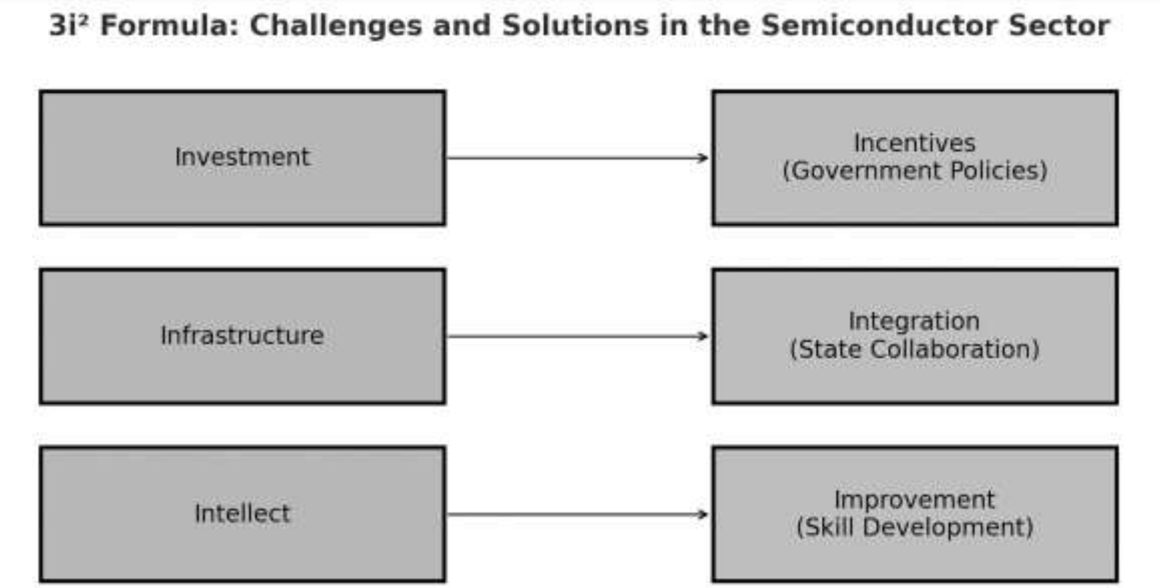

3i² Formula: Challenges and Solutions in the Semiconductor Sector
Investment
Incentives (Government Policies)
Infrastructure
Integration (State Collaboration)
Intellect
Improvement (Skill Development)

Figure 1, the 3i^2 Formula, Source: Author

Based on this formula, the challenges and recommendations have been discussed in the following paragraphs.

Challenges for India

Investment

- Setting up a semiconductor manufacturing facility takes a large investment, and India seems quite behind. The technologies used in joint warfare are militaries that use smaller volumes of high-end logic and memory chips and specialised sensors, high efficiency, low power storage devices, quantum computing, AI requiring high-end microprocessors, and GPUs. However, India's semiconductor ecosystem faces challenges in terms of manufacturing semiconductors required for the high-tech defence technologies. In comparison, India imports a significant amount of semiconductor components. Although the Modi administration has placed a great deal of attention on domestic defence manufacture, there is still a significant reliance on foreign semiconductors. The Defence Public Sector Undertaking (DPSUs) are dependent on the imported semiconductors to a great extent.

- India relies on other nations to meet its needs for semiconductors. From Rs 67,497 crore ($8.23 billion) in 2020–21 to Rs129,703 crore ($ 15.83 billion) in 2022–2023 in chips, imports increased dramatically.[44] Meanwhile, China has been attempting to create its own domestic supply chain since 2014, investing tens of billions of dollars annually, but it is still a long way from being able to do so. At least 25 percent of chips are produced domestically by China while importing the remaining ones.[45]

  Comparatively India still faces challenges in creating a significant indigenous semiconductor ecosystem, as does China.

- PM Narendra Modi has repeatedly stated that India must be 'Atmanirbhar' (self-reliant) for it to prosper. However, in terms of the semiconductor sector, this self-reliance would not be that easy because New Delhi does not have much to offer in the semiconductor manufacturing as yet although attempts have been made in the past, nothing much has materialised.[46]

Infrastructure

- While India has excelled in chip design and electronics manufacture, establishing Semiconductor Wafer Fabrication (FAB) units has proven difficult for several years. Setting up a semiconductor manufacturing facility takes a large investment. It has thus become challenging for India to compete with nearby countries such as China and Vietnam, which have long been preferred locations for global chip manufacturers because to their lower costs. For these reasons, 'Intel stated' in 2014 hardly showed any interest in establishing production in India.[47]

- Another significant challenge is ensuring an uninterrupted power supply. The core issue is that India currently lacks the fundamental infrastructure required to undertake ventures in the chip manufacturing industry. Other global companies, particularly China, are always putting pressure on prices. China is also developing a homegrown chip program with the goal of incorporating local chips into 70 percent of its goods by 2025.[48]

Intellect

- For decades, India remained a mere observer to the competition in the chip manufacturing industry. Although, the country has a pool of skilled human resources but has not been able to take a lead in fabrication or chip packaging. There is a scarcity of semiconductor engineers who are knowledgeable in device physics and process technologies.
- New Delhi has already started its journey of chip manufacturing with a focus on creating 28 nm node as one of the best alternatives. It is expected that such chips could offer a strategic sweet spot for India's rapidly developing semiconductor industry.[49] Anurag Awasthi, Vice President of the India Electronics and Semiconductor Association (IESA), stated:

  "Of this, most applications will be in the aerospace and defence, automotive, industrial, wearables, consumer electronics, and handset segments. We have to cater to our own markets and focus on their growth with the prospective economies of scale and the corresponding job creation".[50]

  Meanwhile, China's Semiconductor Manufacturing International Corporation (SMIC), wants to create increasingly tiny 5-nanometer chips by utilising the technology it now has, which is produced in the US and the Netherlands. The HiSilicon unit of Huawei will design the Kirin chips that will be produced on this line.[51]

  Although India has initiated its efforts in terms of design and software but is still at a nascent stage when compared with countries like China, US, Taiwan or South Korea.

Other Challenges for India

- Currently, New Delhi doesn't have a dedicated policy for this sector to cater to the defence needs of the country. There is a requirement of a 'comprehensive defence semiconductor policy'. This could be a structural impediment hindering the growth of the indigenous defence manufacturing. In addition, this may also reduce the potential for cooperation between the various branches of the government and the military forces.

- In 2021, at the QUAD summit, the four leaders mentioned about 'working groups on critical and emerging technologies (C&ET)'. This would mean the four countries would collaborate with each other in strengthening the semiconductor capabilities. However, the question arises as to how far these countries can collaborate being on different trajectories. For example, the US is an equipment, patents, and design leader, in terms of manufacturing Japan is excelling and Australia has a rich reservoir of basic material. Considering, their strengths in the different domains, India has to navigate intelligently to use their potential.
- The semiconductor global value chain is highly integrated and very complex. If merely setting up a semiconductor ecosystem in India will afford India independence from China's dominance in this sector, it is incorrect. The US-China chip war is an example where both countries are interdependent yet imposing sanctions and trade barriers. Therefore, China's influence on the Indian semiconductor industry will persist, though India may exercise autonomy in this industry as it develops newer capabilities.
- In light of India's relationship with Taiwan in this sector, it is crucial to understand the dynamics of the US-Taiwan and Sino-Taiwan relationship too. Taiwan's collaboration with the US is driven by the former's leadership in advanced chip manufacturing including initiatives such as CHIPS and Science Act. Furthermore, China remains an important factor, as both Taiwan and the US feel that through technology transfer and investments, they may challenge China's growth in this field. Comparatively, Taiwan's relationship with China is strained considering Taiwan's advancement in this field which poses strategic concern for China. In this context, understanding India's collaboration with Taiwan is crucial. New Delhi is cautious and doesn't want to antagonise Beijing. However, aspires to seek benefit from Taipei while attempting to balance its foreign policy.

On the other hand, Taiwan saw sense in bolstering its engagement with India given the country's rising prominence in the Indo-Pacific. In addition, its status as a crucial participant in the QUAD, and the US priority placed on US-India relations couldn't be ignored. Taiwan has become one of India's most important economic partners as it develops its semiconductor industry.[52] S. Jaishankar, India's Minister of External Affairs, in November 2023 at the Indian High Commission in London stated:

"We have substantial technology and economic and commercial relations with Taiwan and certainly Taiwan has a reputation when it comes to electronics and of course, more recently with semiconductors. So, there has been an upswing in the levels of cooperation."[53]

However, New Delhi's strong interests in attracting investments from the TSMC, have not been fully successful. Such investments were seen as game changer in this sector especially in terms of manufacturing capabilities. Despite such interests from New Delhi, TSMC has not made any plans to invest in greenfield fabrication in India. Instead, the company has concentrated exclusively on the US market. In India, although this is sometimes interpreted as a sign of Taiwan's lack of dedication and desire, but India needs to develop a favourable business condition, infrastructure and significant demand for the semiconductor market.[54]

In addition, India has been quite cautious regarding a possible free trade agreement (FTA) with Taiwan. Although Taiwan has been keen to initiate a FTA with India, it did not show much enthusiasm for pursuing such an arrangement. India appears to consider it more as a political agreement than an economic one, and its hesitation may partly be attributed to worries over the trade balance.[55]

This could be a prudent initiative by New Delhi considering the geopolitical landscape. This might enable India to avoid diplomatic fallout with China and maintain economic ties with Taiwan at the same time.

Recommendations

Incentives.

- In 2021, India launched its about $10 billion Production-Linked Incentive (PLI) to promote semiconductor and display manufacturing in the nation. A Design-Linked Initiative (DLI) was also announced to encourage global and domestic investment in design software, intellectual property rights, and other areas.[56] However, the application and the approval process for such initiatives should be smoother and quicker devoid of much bureaucratic hurdles.
- Such incentives should be available to more stages of the semiconductor value chain. This could be involving R&D, testing, packaging etc.
- India could emphasis on creating its 'comprehensive defence semiconductor policy'. The Department of Defence Production in collaboration with the Ministry of External Affairs (MEA) and National Security Council Secretariat (NSCS) could take an initiative in creating a semiconductor strategy. Notably, around 98 percent of semiconductors is used in civilian applications. In order to satisfy the demands of the defence industry, which is looking for high-end, low-volume semiconductors, a sizable subsidy must be provided to the semiconductor sector.

Integration and Collaboration

- With about 800 distinct steps needed, the fabrication of semiconductors is regarded as one of the most complex industrial processes. Three separate processes make up the entire production process: design, fabrication, assembly, and testing. Following fabrication, the chip is put through testing, assembly, and packaging to keep it safe. Some claim that no nation possesses all of the products within its borders.[57] Therefore, the four QUAD countries despite being on different trajectories the main objective should be to create enough redundancy in the supply chain to prevent China from dominating or endangering it. The QUAD members must invest in creating a strong collaborative semiconductor ecosystem rather than focusing only on achieving national self-sufficiency in semiconductor production. They can emphasis on the following significant aspects:

- A QUAD consortium needs to be created with the goal of developing a diverse basis for semiconductor manufacturing in these four nations. This would involve pooling resources to advance fabrication capabilities. This strategy will not only save costs, but geographic diversification will strengthen the resilience of the supply chain. From a strategic perspective, fabs built by this cooperation might grant fabless companies in the QUAD grouping priority access.[58]

- The stated goal of the QUAD semiconductor collaboration should not be to build an exclusive industrial bloc, but rather to serve as a springboard for the formation of broader "bubbles of trust." The collective strength of QUAD is insufficient to attain total control over the semiconductor industry, nor should it attempt to do so. Rather, the semiconductor QUAD should serve as a foundation for the eventual inclusion of additional siliconpolitik heavyweights like the European Union (EU), Taiwan, Vietnam, South Korea, Israel, and Singapore.[59]

- Governments are not the best arbiters of efficiency, but the semiconductor companies are. These companies calculated their competitive advantages to optimise costs in their pursuit of efficiency. Global consumers benefited as a result. Governments have recently used export limits and subsidies for domestic semiconductor manufacturing which is going against the trend. Instead of such measures, the QUAD governments should commence more R&D cooperation between countries in terms of knowledge sharing, cross-licensing, cooperative development and licencing agreements.

- One of the reasons India’s world-class semiconductor services industries cannot move into producing its own products is the high cost of EDA tool licences. The QUAD members can offer preferred access to EDA tools at reduced rates by establishing a common finance mechanism, which will diversify fabless design outside of the US.[60]

- ASEAN countries, namely Taiwan, Vietnam, Singapore, Philippines including South Korea have integrated into the global value chain of semiconductors. Major semiconductor companies have their facilities in these nations. It is a strategic move to collaborate with the ASEAN nations that has potential.[61] Collaboration with Taiwan and South Korea is already in progress. India will benefit from Taiwan and South Korea, the semiconductor market leaders. As Taiwan is a leader in the foundry model of the semiconductor manufacture, India can offer skilled technical manpower, stable governance and a large market. In addition, proximity to consumer, proximity to resources play a crucial role. Being closer to resources and the significant markets, India could offer logistical advantage to Taiwan.

  Today, India is home to roughly 250 Taiwanese businesses. This is sufficient to give India a strong basis for a number of upcoming collaborations. It is noteworthy that the majority of recently established semiconductor manufacturing and assembly/test facilities in India are dispersed over various locations.[62]

  A semiconductor expert stated that the manufacturing chain of semiconductors is diverse, spreading over countries, if not continents. Raw materials, design houses, fabrication units, foundries, assembly and testing and packaging are already located in different countries. By design, no single country can claim total strategic dominance over the entire semiconductor ecosystem. For example, China's strength lies in small chip manufacturing, logic design and fabs, and Taiwan's strength in foundries, South Korea's IDM model, numerous fab plants of Japan, design and fabs of the US, manufacturing machines of Netherlands are intricately dependent on each other for sustenance and profitability. The ecosystem is symbiotic in nature and a collaboration among the semiconductor 'nations' is essential.

  Against this backdrop, the US, Japan, and Australia have a strong case to collaborate with India with their country-specific strengths to ensure a free, open, prosperous Indo-Pacific region. Most importantly, collaboration in the field of semiconductors by the QUAD nations is imperative to tackle the hegemony of China in the Indo-Pacific region.[63]

- Creation of multiple supply chains should be commenced through multilateralism while picking members from different groupings/alliances. This should enable in keeping the national interest paramount. Such a supply chain will de-risk dependence on a single source and ensure stable and strategic position in the global value chain.

  A notable example is the China Plus One and China Plus Two strategy, and the offset strategy of the US.The third offset strategy which emphasises on leveraging cutting-edge technologies including, artificial intelligence (AI), quantum computing, cyber capabilities etc. In the case of China Plus One and China Plus Two strategies, alternate routes/channels were established outside China to reduce dependence. Apple, FOXCONN and Tesla moving out of China to India is an example of China Plus One. This should be encouraged by New Delhi and be efficient especially in terms of infrastructure, skilled human resource, effective implementation of the government initiatives and building confidence amongst the investors through maintaining consistency in the policies.

Improvement in Skill Development

- Skill upgrade must be a national mission. Use Digital Public Infrastructure to penetrate the skill and knowledge to every district of the nation.

- Encourage academia to establish campuses in the vicinity of the fabs. Universities with R&D facilities must be part of the semiconductor ecosystem. Industry must also invest equally in academic institutions and seek solutions to every problem faced by the industry. For a limited period, the visa may be granted to citizens of the nation's possessing the required skills as building the skills capability requires a longer time horizon than three to four years.

- In India, ATMP plants have the potential to establish the foundation for the growth of a comprehensive semiconductor ecosystem and could be the focus in the upcoming years. An official in the Ministry of IT stated, "In terms of the semiconductor ecosystem, China holds a 38 percent share of the global market for packaging and India

> will follow the ATMP path to achieve fab success. The proper method to go is to use this stage as the beginning point because it is a crucial one."[64]
>
> Experts in the semiconductor sector think that ATMP facilities not only solve current supply chain issues but also promote an innovative environment. Poornima Shenoy, former president of IESA and presently CEO of Hummingbird Advisors opined, "Setting up an ATMP or OSAT could be the right step. The global market for ATMPs is estimated at $32 billion. It is expected to grow to be worth $180 billion by 2028. There are global ATMP firms registering nearly $12 billion in revenue per year already!"[65]

Conclusion

India's semiconductor sector has already been able to draw global interest with investments from various renowned companies. However, New Delhi's ability to completely capitalise this potential requires emphasis on few aspects including robust design talent especially in terms of manufacturing capacity.

Strengthening collaboration with the QUAD and few Southeast Asian countries is a good initiative, however, India should encourage its cooperation with European countries especially Netherlands which leads the world in the semiconductor industry. The Dutch company ASML is the global leader in the Lithography segment. The government should also play an active role in pushing incentives to attract semiconductor manufacturing in India. The academia especially IIT's should be encouraged in this sector to bring innovation.

Overall, India has already started its journey and is expected to become acknowledged as one of the world's leading semiconductor manufacturing nations in due course.

****

Dr Ulupi Borah is a Senior Fellow at the Centre for Joint Warfare Studies (CENJOWS). Previously, Dr Borah served as an Assistant Professor at the Rashtriya Raksha University, Gandhinagar. Her expertise lies in the Indo-Pacific region, particularly Japan's security polices and availed the prestigious JASSO scholarship offered by the Japanese government in 2019. Dr Borah is also

researching on Europe and the new security issues, post completion of a course at the Geneva Centre for Security Policy, Switzerland.

NOTES

[1] Mark Stone, "An Overview of Military Semiconductor Applications", City Labs, [Online: web], Accessed 12 June 2024, URL: https://citylabs.net/military-semiconductor-applications/

[2] Ibid

[3] Sitakanta Mishra and Nisarg Jani, (2024), "The Dawn of India's Semiconductor Era", The Diplomat, URL: https://thediplomat.com/2024/03/the-dawn-of-indias-semiconductor-era/

[4] Press Information Bureau, (2024), "PM to participate in 'India's Techade: Chips for Viksit Bharat' and lay the foundation stone of three semiconductor facilities worth about Rs 1.25 lakh crore on 13th March", Prime Minister's Office, [Online: web], Accessed 10 July 2024, URL: https://pib.gov.in/PressReleasePage.aspx?PRID=2013750#:~:text=The%20Outsourced%20Semiconductor%20Assembly%20and%20Test%20(OSAT)%20facility%20in%20Morigaon,of%20about%20Rs%2027%2C000%20crore.

[5] Sitakanta Mishra and Nisarg Jani, (2024), "The Dawn of India's Semiconductor Era", The Diplomat, URL: https://thediplomat.com/2024/03/the-dawn-of-indias-semiconductor-era/

[6] Arjun Gargeyas, (2022), "The Role of Semiconductors in Militray Defence Technology", Defence and Diplomacy Journal, 11 (22): 45

[7] Arjun Gargeyas, (2022), "The Role of Semiconductors in Militray Defence Technology", Defence and Diplomacy Journal, 11 (22): 46

[8] Ibid

[9] Ibid

[10] Arjun Gargeyas, (2022), "The Role of Semiconductors in Militray Defence Technology", Defence and Diplomacy Journal, 11 (22): 48

[11] Arjun Gargeyas, (2022), "The Role of Semiconductors in Militray Defence Technology", Defence and Diplomacy Journal, 11 (22): 49

[12] Congressional Research Service, (2020), "Semiconductors: U.S. Industry, Global Competition, and Federal Policy", CRS Report, URL: https://fas.org/sgp/crs/misc/R46581.pdf

[13] Ibid

[14] Ibid

[15] Ibid

16 Pranay Kotasthane, (2021), "Siliconpolitik: The Case for a QUAD Semiconductor Partnership", Institute of South Asian Studies, National University of Singapore, [Online: web], Accessed 7 July 2024, URL: https://www.isas.nus.edu.sg/papers/siliconpolitik-the-case-for-a-quad-semiconductor-partnership/

17 Ibid

18 Ibid

19 Naoko Kutty, (2023), "**How Japan's semiconductor industry is leaping into the future**", World Economic Forum, [Online: web], Accessed 9 July 2024, URL: https://www.weforum.org/agenda/2023/11/how-japan-s-semiconductor-industry-is-leaping-into-the-future/#:~:text=In%20Japan%2C%20semiconductors%20are%20recognized,domestic%20production%20system%20of%20semiconductors.

20 Ibid

21 Ibid

22 Ibid

23 Chen-Yuan Tung, (2024), "Taiwan and Global Semiconductor Supply Chain", ROC, Taiwan site, Taiwan Representative Office in Singapore, URL: https://www.roc-taiwan.org/uploads/sites/86/2024/02/240202-February-Issue.pdf

24 Ibid

25 Ibid

26 Charlotte Trueman, (2024),: "South Korea's President calls semiconductors a field of 'all-out war'; announces $19bn support package for industry", Data Centre Dynamics, [Online: web], Accessed 6 July 2024, URL https://www.datacenterdynamics.com/en/news/south-koreas-president-calls-semiconductors-a-field-of-all-out-war-announces-19bn-support-package-for-industry/

27 Ibid

28 Al Jazeera, (2024), "South Korea unveils record $19bn package to support chip industry", [Online: web], Accessed 6 July 2024, URLhttps://www.aljazeera.com/economy/2024/5/23/south-korea-unveils-record-19bn-package-to-support-chip-industry

29 Ibid

30 Sayan Ghosh, (2023), "South Korea's semiconductor ecosystem gets 'mega cluster'", Asia Fund Manager, [Online: web], Accessed 10 July 2024, URL: https://asiafundmanagers.com/in/south-korea-semiconductor-ecosystem-gets-mega-cluster/

31 John Lee and Jan-Peter Kleinhans, (2021), "Mapping China's Semiconductor Ecosystem in Global Context", Mercator Institute for China Studies, URL: https://merics.org/en/report/mapping-chinas-semiconductor-ecosystem-global-context-strategic-dimensions-and-conclusions

32 Ibid

33 Ibid

34 Coco Feng, (2024), "China's semiconductor output jumps 40% in first quarter amid growing dominance in legacy chips", South China Morning Post, [Online: web], Accessed 12 July 2024, URL:https://www.scmp.com/tech/tech-war/article/3259221/chinas-semiconductor-output-jumps-40-first-quarter-amid-growing-dominance-legacy-chips

35 Ibid

36 Ibid

37 Trisha Ray, (2023), "Lessons from India's past for its semiconductor future", Observer Research Foundation, [Online: web], Accessed 12 June 2024, URL: https://www.orfonline.org/expert-speak/lessons-from-indias-past-for-its-semiconductor-future

38 Ministry of Electronics and Information Technology (2022), "Modified Programme for Semiconductors and Display Fab Ecosystem", Government of India, URL: https://www.meity.gov.in/esdm/Semiconductors-and-Display-Fab-Ecosystem

39 Hindustan Times (2023), "Micron begins construction of $2.75 billion semiconductor plant in Gujarat", [Online: web], Accessed 12 June 2024, UR: https://www.hindustantimes.com/business/micron-begins-construction-of-2-75-billion-semiconductor-plant-in-gujarat-101695478422567.html

40 Ministry of Electronics and Information Technology (2022), "Modified Programme for Semiconductors and Display Fab Ecosystem", Government of India, URL: https://www.meity.gov.in/esdm/Semiconductors-and-Display-Fab-Ecosystem

41 Katelin Kharrati, (2024), "Indian Semiconductor Market Size to Likely to grow by 20.1 CAGR by 2033", Custom Market Insights, [Online: web], Accessed 26 June 2024, URL: https://www.custommarketinsights.com/press-releases/indian-semiconductor-market/

42 Growth Market Reports, (2024), "Semiconductor Market Size, Share, Trends | 2032", [Online: web], Accessed 31 July 2024, URL: https://growthmarketreports.com/report/semiconductor-market-global-industry-analysis

43 Neeraj Bansal, (2024), "India's semiconductor ambitions: How to move up the value chain?", KPMG, [Online: web], Accessed 26 June 2024, URL: https://kpmg.com/in/en/blogs/home/posts/2024/06/indias-semiconductor-ambitions-how-to-move-up-the-value-chain.html#:~:text=The%20India%20advantage,building%20an%20indigenous%20semiconductor%20ecosystem.

[44] Naandika Tripathi, (2024), "Keeping focus on Make in India and sunrise manufacturing sectors like semiconductors crucial for new coalition government", Forbes, [Online: web], Accessed 2 July 2024, URL: https://www.forbesindia.com/article/take-one-big-story-of-the-day/keeping-focus-on-make-in-india-and-sunrise-manufacturing-sectors-like-semiconductors-crucial-for-new-coalition-government/93302/1

[45] Ibid

[46] Mukul Yudhveer Singh (2022), "ATMPs: The Founding Stone Of India's Semiconductor Era", Electronics B2B, [Online: web], Accessed 2 July 2024, URL:https://www.electronicsb2b.com/industry-buzz/invest/atmps-founding-stone-indias-semiconductor-era/

[47] Vishal Chawla, (2024), "Why Has India Lagged Behind in Semicondcutor Chip Manufacturing?" AIM, URL: https://analyticsindiamag.com/ai-origins-evolution/india-semiconductor-chip-manufacturing/

[48] Ibid

[49] Nidhi Singal, "Can 28 nm catapult India to semiconductor manufacturing leadership?", Business Today, Online: web], Accessed 2 July 2024, URL: https://www.businesstoday.in/tech-today/news/story/can-28-nm-catapult-india-to-semiconductor-manufacturing-leadership-433902-2024-06-19

[50] Ibid

[51] Quiner Liu, "China close to shipping 5 nm chips, despite Western curbs", ARS Technica, [Online: web], Accessed 2 July 2024, URL: https://arstechnica.com/gadgets/2024/02/china-close-to-shipping-5nm-chips-despite-western-curbs/

[52] Sana Hashmi, "China's Influence on India-Taiwan Economic Dynamics",Global Taiwan Institute, [Online: web], Accessed 6 July 2024, URL: https://globaltaiwan.org/2024/05/chinas-influence-on-india-taiwan-economic-dynamics/

[53] Ibid

[54] Ibid

[55] Ibid

[56] Drsihti IAS (2022), "Modified Incentive Scheme for Semiconductor Chip-Making", URL: https://www.drishtiias.com/daily-updates/daily-news-analysis/modified-incentive-scheme-for-semiconductor-chip-making

[57] K P Prabheesh and C T Vidya, "Interconnected Horizons: ASEAN's Journey in the Global Semiconductor Trade Network Amidst the COVID-19 Pandemic", Economic Research institute for ASEAN and East Asia Discussion Paper Series ERIA-DP-2023-32 No. 504, [Online: web], Accessed 2 July 2024, URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.eria.org/uploads/Interconnected-Horizons-ASEAN%E2%80%99s-Journey-in-the-Global-Semiconductor-Trade-Network.pdf

58 Pranay Kotasthane, (2021), "Siliconpolitik: The Case for a QUAD Semiconductor Partnership", Institute of South Asian Studies, National University of Singapore, [Online: web], Accessed 7 July 2024, URL: https://www.isas.nus.edu.sg/papers/siliconpolitik-the-case-for-a-quad-semiconductor-partnership/

59 Ibid

60 Ibid

61 Earnst and Young, (2022), "When the chips are down ASEAN could be the answer to the semiconductor crunch", URL: file:///Users/ulupiborah/Downloads/ey-asean-semiconductor-publication%20(3).pdf

62 Anurag Awasthi, (2024), "China, Chips, Taiwan: Trade, trunk infra, talent and tech expertise in India's favour", Economic Times, [Online: web], Accessed 1 July 2024, URL: https://government-economictimes-indiatimes-com.cdn.ampproject.org/c/s/government.economictimes.indiatimes.com/amp/news/technology/china-chips-taiwan-trade-trunk-infra-talent-and-tech-expertise-in-indias-favour/109209996

63 Online interview, (2024), Air Commodore Ramamohan Mantha, 4 July 2024, New Delhi

64 Bhaswati Guha Majumdar, (2023), "Mission Semicon | How ATMP Route Will Help India Achieve Fab Success in Chip Manufacturing Ecosystem", News 18, [Online: web], Accessed 1 July 2024, URL: https://www.news18.com/tech/mission-semicon-how-atmp-route-will-help-india-achieve-fab-success-in-chip-manufacturing-ecosystem-8539519.html

65 Mukul Yudhveer Singh (2022), "ATMPs: The Founding Stone Of India's Semiconductor Era", Electronics B2B, [Online: web], Accessed 2 July 2024, URL:https://www.electronicsb2b.com/industry-buzz/invest/atmps-founding-stone-indias-semiconductor-era/

IMPACT OF ADDITIVE MANUFACTURING - A DISRUPTIVE TECHNOLOGY FOR JOINT WAR FIGHTING

Gp Capt Ashok K Singh (Retd)

"Investing in tomorrow's technology today is more critical than ever…" —*Bill Gates*

Abstract

Security and sovereignty of a nation is paramount. It is maintained through its military. The war fighting has been ever evolving, and technology has played a determinant role in the outcomes of all the major wars or military operations. Hitherto the technology has been ever evolving and the rate of evolution too has been almost exponential. The ongoing Russia-Ukraine and Israel-Hamas wars have shown to the world that technology will play a dominant role in the maintenance of the aim of the war and determining the outcome. The wars have become very dynamic and, threats keep evolving right through the war to the extent that the cardinal principle of 'surprise' of war has remained sacrosanct.

Additive Manufacturing (AM) or 3D Printing is a niche disruptive technology. It is termed as Digital Manufacturing (DM) as well. This technology has greatly impacted the war zone where the workshops have come right beside the fighting men and machinery. The AM technology has opened up humongous possibilities to keep the machines operational, and tilt the outcome of the operations and the war. The military with an edge of applying AM will have an edge in the outcome too. The Indian military has to examine this technology and apply it in a manner that the entire military is AM enabled! The paper aims at apprising the military practitioners at home to embrace AM at the right earnest.

Introduction

The present belongs to JW; having its own challenges, i.e., operational, logistical, tactical etc. One major bone of contention is command and control. The thrust today is towards a structured JW, through integrated commands. It is aimed at instilling synergy between the elements of the fighting instruments of the military. Jointness in JW is not limited to the military, but civil as well. The JW, akin to any other fighting doctrine, aims to achieve the objectives, be it operational, tactical or strategic, by integrating the forces for war at land, sea, air, space and cyberspace. It encapsulates that the desired results, be achieved in the shortest time, and with a minimal to optimal use of the limited resources. The ongoing Ukraine-Russia and the Israel-Hamas wars are being studied closely by the strategic military practitioners. JW is going to evolve further drawing lessons from these two wars. A great deal of jointness exists in the Indian military, and more is on the anvil. The second edition of the Joint Doctrine of the Indian Armed Forces 2017 is a comprehensive document on the Indian Military JW.[1] It is a reference document on the Indian Military Jointness.

Discipline & Disruption in the Indian Armed Forces: A Necessity

Discipline is one of the most important attributes of the militaries across the world. Yet, in order for there to be growth, along with discipline; disruption is needed. There is an importance of disruption which should be understood by the military policy making echelons. The discipline is instilled into the soldiers as a part of the evolving training and working culture. Indian military policy makers need to factor instilling disruption along with discipline. The disruption can be in terms of thinking, training, operations, technologies, use of resources, alternative thinking, etc. An example of disruptive thinking is in the story of David and Goliath, quoted from the Bible. When none had the gumption to take on Goliath, a young boy David took the gauntlet. He defeated Goliath by merely slinging a stone which hit Goliath on his forehead. The invincible giant fell flat on his face and was then killed by David.[2] It is a stellar example where a daunting giant, feared by all, was humbled by an opponent who used his mere presence of mind, using his humble resource, his wit and courage intact, attained victory. This is an epitome of disruption.

Ever Evolving Technology and War Fighting

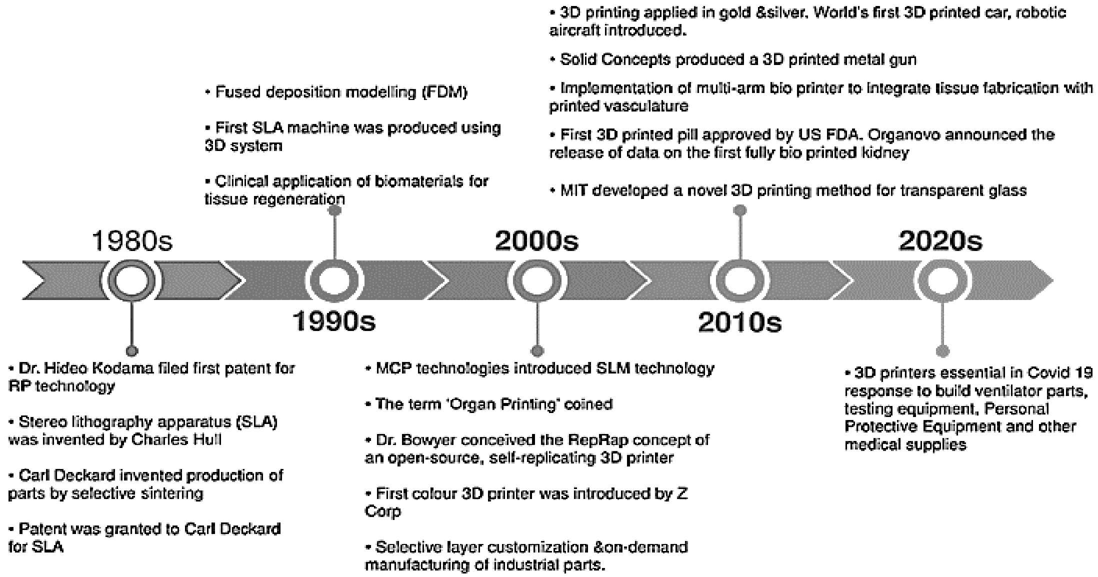
Disruption in technologies impacts the war and its outcomes. Dropping atomic bombs on Japan by the USA, in World War II, was the use of disruption.[3] It swiftly brought to an end the hostilities and the war. Technology is the backbone of the military, for it to train with and win the operations or wars it undertakes, or is compelled to take. The use of a cheap and an innocuous drone destroying a tank costing millions of dollars, is disruption. The technology has been evolving at a very fast speed.

In order that our ancestors could control and use fire, the time taken was 2.4 million years.[4] An insight into the technological transformation rate over the centuries, one may refer to endnote no.5. Technology changes the way war is fought, and thus the emphasis on JW. Disruptive technologies like CyberSpace, AI, ML, Blockchain, Drones, Generative AI, VR/AR, Space Technology, Additive Manufacturing, Biotechnology, Humanoid Robotic Soldiers etc, are changing the warfighting ways. Several niche technologies were mentioned in the preceding paras. One such disruptive technology is 'Additive Manufacturing' (AM), also known as '3D Printing (3DP)' or 'Digital Manufacturing (DM)'. This has made a significant impact on the JW. When AM is envisaged with COVID-like situation in the background, its significance gains larger proportions.

This paper attempts to highlight the importance of AM/3DP/DM in JW operations. How the military will exploit to apply the technology in peace and war. It is certain that the future wars will be joint. The details of different types of AM processes, input materials for AM, and all kinds of technical information have a passing reference in the paper. This has been done intentionally. There is an amazing amount of information in the open source on these matters. In spite of the mammoth amount of relevant information on AM in the open source, and case studies on its use by the militaries globally, the AM has not found favour with the Indian military practitioners. This paper's focus is to get the Indian military practitioners and the policy makers, to appreciate AM technology. Scepticism about the functionality of AM is common. The attempt to set aside the scepticism, if not completely, even partially will vindicate its purpose.

History of Additive Manufacturing/3D Printing

Fig-1[5] Below, depicts the historical timeline of AM which had its advent in the 1980s. Initially it faced a great deal of criticism and scepticism. It was labelled as a means of merely prototyping of products or parts.



1980s
- Dr. Hideo Kodama filed first patent for RP technology
- Stereo lithography apparatus (SLA) was invented by Charles Hull
- Carl Deckard invented production of parts by selective sintering
- Patent was granted to Carl Deckard for SLA

1990s
- Fused deposition modelling (FDM)
- First SLA machine was produced using 3D system
- Clinical application of biomaterials for tissue regeneration

2000s
- MCP technologies introduced SLM technology
- The term 'Organ Printing' coined
- Dr. Bowyer conceived the RepRap concept of an open-source, self-replicating 3D printer
- First colour 3D printer was introduced by Z Corp
- Selective layer customization &on-demand manufacturing of industrial parts.

2010s
- 3D printing applied in gold &silver. World's first 3D printed car, robotic aircraft introduced.
- Solid Concepts produced a 3D printed metal gun
- Implementation of multi-arm bio printer to integrate tissue fabrication with printed vasculature
- First 3D printed pill approved by US FDA. Organovo announced the release of data on the first fully bio printed kidney
- MIT developed a novel 3D printing method for transparent glass

2020s
- 3D printers essential in Covid 19 response to build ventilator parts, testing equipment, Personal Protective Equipment and other medical supplies

Fig – 1, Historical Timeline of AM, Source: Ministry of Electronics and Information Technology, Government of India, "National Strategy on Additive Manufacturing", https://www.meity.gov.in/writereaddata/files/Additive%20Manufacturing%20Booklet%2014.02.2022.pdf

The AM technology has been in existence for almost five decades now. It has matured along the way. The end-use parts are being 3D printed directly. There is not one industry, or a R&D/training/MRO organisation, not using 3DP. 3DP reached the NASA space station way back in 2014. It is being used for parts manufacturing and has its special applications in spare parts needed for maintenance of the space station.[6]

Fig – 2, The 3D printer at the space station.

On 30 May 2024, an Indian startup company Agnikul Cosmos successfully test-fired its launch vehicle (rocket) with a fully 3D-printed rocket engine, the first of its kind, globally.[7]

An insight to the basics of conventional manufacturing and AM will be useful for anyone who is uninitiated in the nuances of AM. In order to get a finished product, one took a blank and removed material to obtain the end part. On the other hand, AM or 3DP, builds a part, by adding the input material layer by layer. In the case of the AM, the wastage is far reduced when compared to the subtractive manufacturing, refer to Fig - 3.[8] There are several types of 3DP Technologies where input material can be either metal or non-metal (polymer).

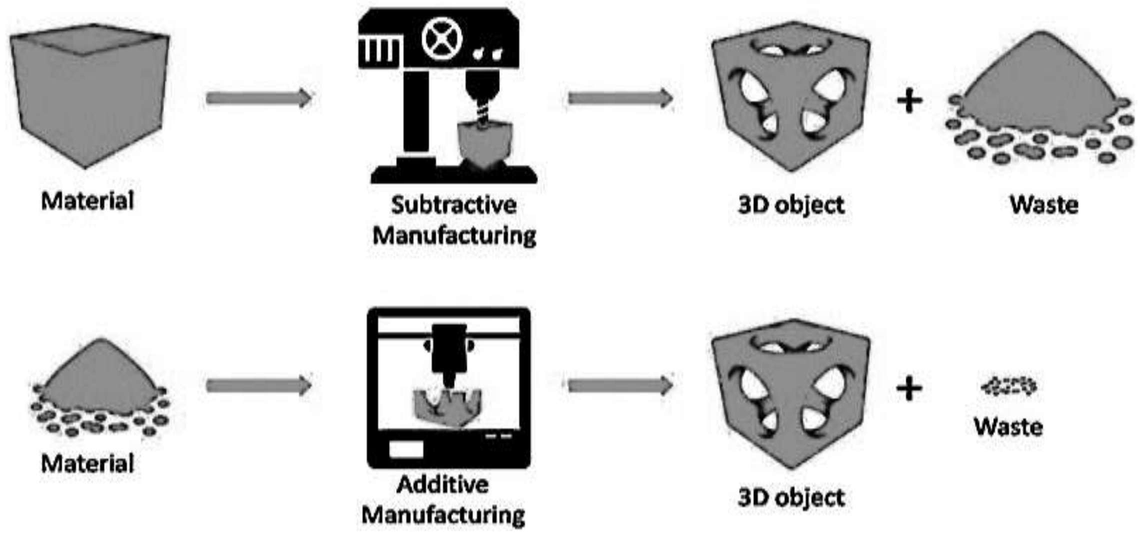


Fig – 3, Difference between additive manufacturing and conventional manufacturing, Source: Stanford Advanced Materials, "Additive Manufacturing vs Traditional Manufacturing 27 Dec 2023 https://www.samaterials.com/additive-manufacturing-vs-traditional-manufacturing.html accessed on 12 Jun 2024.

The types of 3DP for polymers are Stereolithography (SLA), Selective Laser Sintering (SLS), Fused Deposition Modelling (FDM), Digital Light Process (DLP), Multi Jet Fusion (MJF) and Poly-Jet Fusion. At the same time, types of metal 3D printing are Direct Metal Laser Sintering (DMLS), Electron Beam Melting (EBM) and Direct Energy Deposition (DED).[9] Several videos on YouTube, and on the websites of 3DP companies on the differences between conventional manufacturing and AM will be helpful to anyone trying to understand the basic differences. Atmanirbhar Sena (military) is a dire need for the nation's security and sovereignty. The government, having grasped the importance of AM, brought out a national policy on AM.

Indian Government's Initiative in Additive Manufacturing Domain

National Institution of Transforming India (NITI Aayog), in its vision document dated 28 July 2016, has listed out fifteen disruptive technologies in its roadmap for technology advancement and assimilation by the nation; one is 3DP. The Ministry of Electronics and Information Technology (MeitY) published, 'National Strategy for Additive Manufacturing', on 24 Feb 2022.[10] The document is comprehensive and well-written. NITI Aayog has established more than 10000[11] Atal Tinkering Labs (ATL) in schools pan India. Each lab is equipped with a 3D Printer, and impart theoretical and practical training on 3DP. The government rightfully has placed due importance on the 3DP.

A thrust to develop and populate such technologies has been from the National Skill Development Council[12] and National Skill Training Institutes, under the Directorate General of Training, which functions under the Ministry of Skill Development and Entrepreneurship.[13]

The proactive government is setting the right template for the nation to adopt 3DP. 3DP is not replacing conventional manufacturing. It will be complimenting and/or, supplementing it.

AM has been used for military applications by almost all militaries globally, directly or indirectly. It will be worth examining how foreign militaries use the 3DP.

Advantages of Additive Manufacturing or 3D Printing in Military Applications

The advantages are several and significant. Therefore it is pertinent that the military practitioners understand 3DP in order to gainfully apply it.

3DP's great advantage is a fast-paced production of parts involving complex designs. The precision achieved is high and would meet the desired specifications, barring exceptions. On-Demand Production is a key feature. This obviates the long timelines of a typical existing supply chain. AM or 3DP has already proven its battle-worthiness in the ongoing wars. A military can use 3DP to its great advantage in the Tactical Battle Area (TBA), by on-demand production of the needed part(s), bringing about redundancy in the existing supply chain, and increasing operational efficiency.

In peacetime, 3DP is valuable in speedy customisation of military equipment towards improved performance, functionality and reliability. Reverse engineering and prototyping of any military product is expeditious. It does not the entail tooling needed in conventional methods. The weapon parts can be quickly manufactured to mitigate the evolving threats in operations. 3DP has impacted military logistics in a very big way. It is a precursor to a digital inventory, a part of Industry 4.0, leading to reduced warehousing needs.

It is imperative for the military to harness 3DP's versatility and strength to maintain an edge in any tactical battle scenario.

ADDITIVE MANUFACTURING IN THE FOREIGN MILITARY DOMAINS:

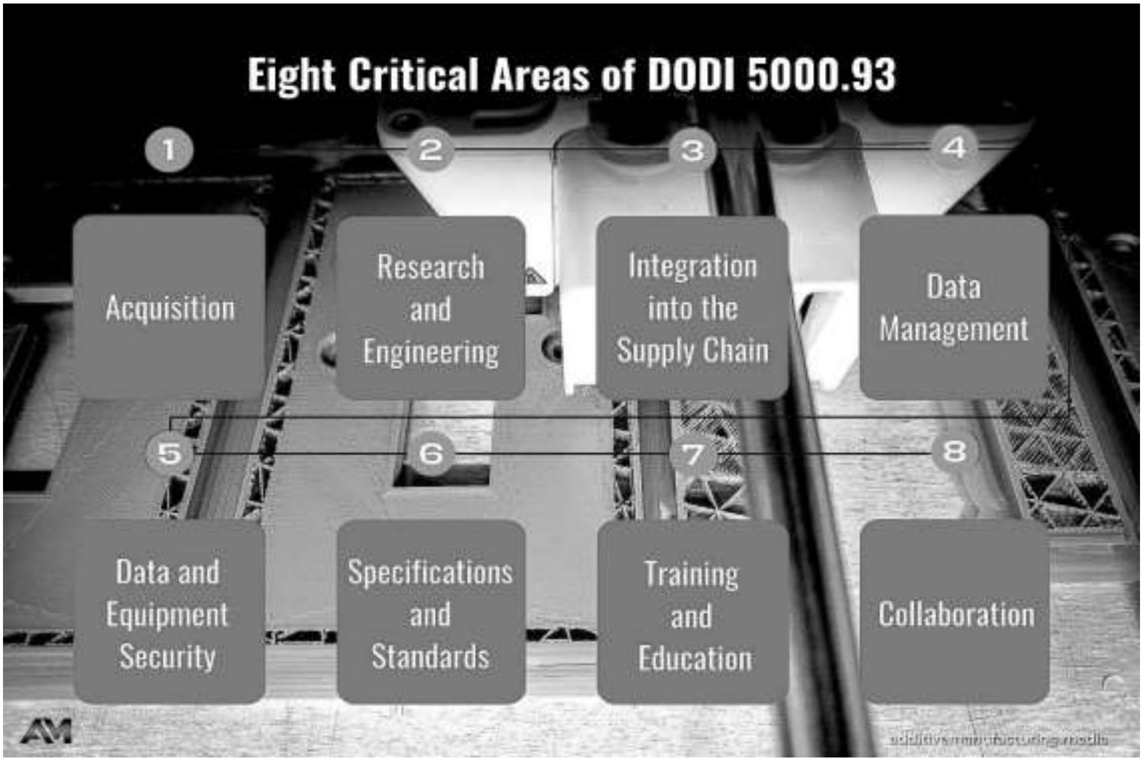
A Look at the US Military Tryst with 3DP

US DoD has constituted a Joint AM Working Group (JAMWG). The JAMWG is a cross-cutting DoD community focused on communication and coordination among the Services and Defence Agencies to maximise AM application in support of the warfighter and sustainers. Formalised in July 2017 and led by the OSD ManTech Program, the team consists of leaders from Military Services, Defence Agencies, other Federal agencies, industry and academia, to reduce barriers to the adoption of innovative AM technologies that benefit DoD and the warfighter.[14]

The US National Strategy for Additive Manufacturing was published in 2022 to address climate change, strengthen supply chains, ensure national security, and improve healthcare.[15]

The US DoD AM Strategy was published in 2021. The US Army, Navy and the Air Force came up with the AM Strategy for their respective services. It was tailored to suit the unique requirements of the respective services for which the US DoD AM Strategy was the guiding document.

Several initiatives of the US DoD and the respective services have been in place. The critical areas being addressed are depicted in the figure below, Fig - 4.



Eight Critical Areas of DODI 5000.93

1 Acquisition

2 Research and Engineering

3 Integration into the Supply Chain

4 Data Management

5 Data and Equipment Security

6 Specifications and Standards

7 Training and Education

8 Collaboration

Fig – 4, Areas addressed by additive manufacturing. Source: Brett P Conner, "DOD Drives Transformation of New Additive Manufacturing Policy", Additive Manufacturing, 09 Feb 2022, https://www.additivemanufacturing.media/articles/dod-drives-transformation-with-new-am-policy

The above figure can be adapted by any military and further customised. The US Navy has taken up at-sea production of AM parts and parts of submarines, to enhance the efficiency of the Logistics and Supply Chain. The US Army is using AM for rapid logistics, field level on demand manufacturing, and R&D. US Air Force thrust areas in the field of AM are to manufacture qualified parts for flight critical applications, 3D printed electronics, drones design and manufacture, and its applications for space.[16] The Indian military can take a cue from the above.

UK Military's Foray into Additive Manufacturing or 3D Printing

Project Brokkr is the British Army's enterprise of taking metal manufacturing out of the sheds or shops onto the field. In the Scandinavian mythology, Brokkr & Eitri were legendary dwarf brothers famous for their skills in metal manufacturing of magical objects, leading to the project, named Brokkr.[17]

In 2019, Royal Engineers of the British Army resorted to 3DP for their role in the UN mission in South Sudan to obtain parts at site. It envisaged the production of parts which otherwise could take long to procure. They have now deployable 3DP, called 'Field Army Additive Manufacturing Concentration'.[18] It enhances efficiency and speed of repair, saves on transportation cost, and carbon emission. Fig - 5 depicts the standard ISO container which houses the deployable 3D metal printer and its mobility is also of an ISO container.

Fig – 5, Field Deployable 3D Printing Source: UK MOD Army, "British Army Deploys 3D Printing in the Field", 10 May 2024 https://www.army.mod.uk/news-and-events/news/2024/05/brokkr-pioneering-the-british-army-s-deployable-additive-manufacturing-capability/.

Additive Manufacturing Applications in Russia-Ukraine & Israel-Hamas Wars

The two wars being fought in the present times are unique and unprecedented. The four nations are facing challenges, and sustenance is the key.

Supply Chain Maintenance has been the major concern of all the warring nations. Economic sanctions, diplomatic isolation, rebuilding of critical infrastructure, maintenance of transportation, communication and civil infrastructure while conflict is on, is a great challenge. Healthcare of wounded in the operational zone, and the patients both civil and military in peace locations too, suffer from the scarcity due to choked supply chains resulting from war.

AM obviates supply chain bottlenecks for requirements of end-use spare parts for the war fighting machinery; medical supplies, first aid kits, critical life-saving kits for the wounded etc.

Additive Manufacturing's Stellar Role in Ukraine Military Operations

Project DIAMOND[19] has been a success story of distributed manufacturing, as printers installed across the US and elsewhere in the world, are networked. These can be centrally tasked to produce an item, in the required volumes. More than 300 desktop 3D Printers simultaneously produced tourniquet components needed for Ukrainian wounded soldiers, an excellent example of the agility of the DM process.

Seven massive Speed3D printers have been supplied by the US DoD to Ukraine, to be deployed in the field to help the Ukrainian army rapidly fabricate critical parts for more than forty different armoured platforms. It will serve to overcome the challenges of legacy military platforms' spare parts availability at the war zone.[20]

Ukraine started 3D printing bombs to augment its depleting assets of ammunition. These candy bomb manufactures involved amateur groups who were experienced in AM. One group made 30000 casings in four months for the candy bombs; and the other group working on 800 gas anti-personnel bombs was manufacturing 1000 casings per month. They had demands which were ever increasing. The military did the filling of charge. It is hitherto an unknown combination of civil military war time cooperation. A possibility unfolded here only due to AM.[21] Several 3D printing companies and service providers volunteered to help the military. 3DP based sustenance here is noteworthy.

Additive Manufacturing's Role in Russian Military Operations

Russia had been using 3D Printers of foreign origins. The indigenous 3D printers don't have the same class. The sanctions impaired the operations. Yet Russia has resorted to the use of home grown Industrial 3D printers, for mass manufacture of drones and UAV components. It's a significant feat in light of the ongoing war.[22]

Additive Manufacturing's Applications of 3DP by the IDF (Israeli Defence Forces) in the ongoing war

AM has proven to be a saviour for the IDF. Israel was caught totally unaware on 07 Oct 2023 when it was attacked by Hamas. Since then the war has been ongoing.

Applications of 3D Printing at the War Zone

Fig – 6

Fig - 7

Fig - 8

Ariel Harush, a material engineering student of Ben Gurion University, started by helping one friend, fighting at the Gaza border, by 3D printing a connector, a small radio part (Fig - 6). Seeing growing demands, he formed a group which has printed more than 43000 parts. Fig - 7 is a 3D printed knee cap, while Fig - 8 shows the kits for the Israeli troops.[23]

Shilo Segev, a 21 year-old soldier was shot in his knee which got shattered. His knee got reconstructed with the aid of 3DP.

Additive Manufacturing in the Indian Armed Forces

The Indian Military has been warming up towards embracing 3D Printing technology. All the three services have used the 3DP for prototyping or for end use parts. AM has been used for reverse engineered spare parts. The details on the AM applications by the three services are scarce in the open domain. The Indian Navy has partnered with a 3D printing service provider company think3D for manufacturing of parts to salvage obsolescence.[24] Military Engineering Services (MES) of the Indian Army used 3DP to construct residential houses.[25] MES 3D printed a runway controller hut at Air Force Station Pune.

The Indian Air Force has set up a metal 3D Printing facility at one of its bases. Any AM facility with the Indian Army & Navy is not publicly known. Ordnance Factory Dehu Road Pune, has set up a 3D Printing facility, recently; the first in any of the ordnance factories.

Hindustan Aeronautics Ltd (HAL) and Wipro3D have collaborated to 3D print aero engine metal parts. They successfully 3D printed a nozzle guide vane with high temperature resistant steel A286 which was certified by CEMILAC (Centre for Military Airworthiness and Certification).[26] A great beginning.

BEML and Wipro Infrastructure Engineering signed a MoU for working together in the domain of AM, AI and the Hydraulic System Engineering.[27] Further there is no information on the association.

The MoD, the Indian Armed Forces, Indian Coast Guard, DPSUs and the DRDO Labs have used AM and also have established AM centres. R&D Engineers Pune has been tasked to develop metal 3D printable bridges and prototypes. Plastic and composite parts of missiles are being developed by Defence Research and Development Lab Hyderabad, and 3D printed metal components are being developed by Defence Metallurgical Research Lab Hyderabad.[28] AM is an Industry 4.0 disruptive technology, and needs to be adapted by all echelons of the MoD.

In the preceding paras, AM technology and its use in ongoing wars, was covered. Briefly, the AM technology and its evolution in the US DoD, Army, Navy and the Air Force has been visualised. The purpose is to intrigue and ignite the military minds. Indian MoD and the Services Headquarters may consider the use of the information in developing indigenous plans to roll out the AM technology in right earnest at all echelons of the India Armed Forces, and organisations under it. The following will illustrate the impact of AM or 3DP on Joint Warfare.

Impact of Additive Manufacturing on Joint Warfighting

- Impact on Logistics and Supply Chain Management (SCM): Logistics and SCM improves by 'On Demand Manufacturing'. The parts can be manufactured and supplied at the war zone, on board the naval vessels or submarines, and at the air forces operational bases.

- Expeditious and Improved Repair & Maintenance: A weapon platform can be restored to its operational readiness by manufacturing replacement parts on demand on site. This positively impacts the operations and optimal exploitation of the weapons. Spare parts for legacy weapons poses a formidable challenge. AM technology can reverse engineer and 3D print the legacy parts.

- Enhanced Jointness: Land, sea and air forces; operate several platforms which are common. These can be jointly developed using 3DP and maintained digitally. It leads to better interoperability resulting in a more efficient JW. It will foster a collaborative ecosystem where joint forces work together to maintain, innovate and standardise.

- Tactical Advantage : AM can prove vital in manufacturing critical parts whose requirements come from the battle fronts. The 3D printed bombs mentioned in preceding paras for IDF by amateurs is an example. The cycle encompassing design, development, prototyping, testing and obtaining 3D printed end use parts, can be short or swift. The beauty is that a collaborative effort of experts working in displaced and different locations, is possible. The pooled 3D printers in different locations can be used for the simultaneous manufacturing of a common product, known as distributed manufacturing. The Indian military can establish 3DP set-ups in a strategic manner, in different parts of India. These could serve to cater for on demand parts production depending on the proximity of TBA, or for distributed manufacturing. The 3DP set up can be field deployable or established at the borders, on and off shore, or at any part of the mainland.

- Strategic cum Tactical Advantage: Digital inventory obviates large stores leading to a better economy and efficiency. AM technology is apt for mitigating effects of sanctions and diplomatic isolations. Russia's war waging potential is impaired in the ongoing war.

- Enhanced Agility and Resilience: Situation in a TBA is ever evolving. Mitigating risks on the go is enabled by AM. AM innovations have resulted in lighter end parts. Metal parts have suitably been replaced by carbon-fibre parts with comparable or better mechanical properties but lighter weight. A soldier's mobility gets better if the weight to be carried is lighter.

- Additive Manufacturing Technology Enabled Efficient and Effective Training: AM is being used in more than 10000 schools under ATL, a NITI Aayog's initiative. It simply proves its value in terms of training and development, and can be adapted by the Indian Military.

- Medical & Health Care: In the preceding paragraphs it was seen that AM has come to be a life saving proposition. Doctors and paramedics are able to tend to wounded and injured, close to the TBA aided by AM technology. The real-time examples of IDF, Hamas and Ukrainian military in harnessing AM for life saving propositions and printing of healthcare parts, is phenomenal. This will be of equal value for the Indian Military

- Tapering Down of Costs: AM helps in maintaining the costs, or bringing them down. 3D printed parts produced on demand on site will not carry several other costs of inventory holding, transportation and damages in transit. The wastage is very minimal. These are tangible costs. There could be intangible cost benefits. A life saved due to an on time provisioning of a needed contraption is priceless. An operation won, or weapon platforms saved due to AM of parts on time on site, will empower the operation. A life or a limb saved will boost the morale of both who are fighting and those for whom they are fighting. AM can be mobile and field deployable, a workshop on the move.

Challenges in the Additive Manufacturing Adoption

AM/3DP is a technology which is evolving and has been able to overcome several shortcomings of conventional manufacturing. Not every manufacturing work will be suitable for the 3DP. Ideally low volume high design complexity manufacturing jobs will be suitable. 3DP will be a good fit for prototyping! It can be applied to replace metal with carbon fibre. The testing and validation procedure for the 3D printed parts for military applications is in the evolving phase, and will take time to mature organically. There are limited materials, and related costs of 3DP could be more than when conventionally manufactured.

The safeguarding of IP, designs and data is paramount, which warrants a robust cybersecurity. The availability of trained resources is a challenge.

A Model Indian MoD Vision for Populating AM in the Three Services, R&D Organisations and Defence Public Sector Undertakings (DPSUs)

Presently AM technology assimilation and its application in the Indian defence construct is sub minimal. Our military environment is discipline heavy and disruption light. Change is resisted vehemently. The Indian military may learn from entities like automotive, IT, infrastructure, agriculture, communication, space etc.; who embraced changes with agility.

Recommendations

National Strategy on Additive Manufacturing, a policy document has been placed by the MeitY in 2022. This can be the guiding document for the MoD.

- At the MoD, a Joint Additive Manufacturing Working Group (JAMWG) will be constituted under IDS HQs. It comprises personnel from the MoD, Department of Defence Production, DRDO, CEMILAC, DGQA, DGAQA, Naval Quality Circle, DPSUs, Indian Army, Indian Navy, IAF, Academia, Ex-Service Men and Industries.

JAMWG in six months time may bring out the National Defence Strategy on Additive Manufacturing (NDSAM).

- JAMWG may join hands with CENJOWS or any other body to create the NDSAM. Simultaneously the quality group will look into formulation of terms of accreditation of quality conformances and approvals.
- At the IDS HQs, an Integrated AM Working Group (IAMWG) will be formed comprising the three services, academia and industry. The group should be a balanced mix of representations from all echelons of the military. This group will create an Integrated AM Force (IAMF), which can take up any AM job from any of the services. Literally a true JW Force.
- AM be the part of curricula of every training institution. 3DP can be used and adapted by anyone irrespective of his education or qualification.
- Creation of five National Defence Additive Manufacturing Growth Centres (NDAMGC): These centres (NDAMGC) could be integrated and be used by all the three services. These centres will be the ones who will develop and groom the IAMF. They will undertake the rapid prototyping, obsolescence management through reverse engineering, R&D and 3D printing.
- Deputing engineers for training on 3DP, as a part of post graduate courses which the services subscribe to. Engineers should be trained at the AM facilities of the overseas defence OEMs like Boeing, Lockheed Martin, Israel Aerospace etc. as part of the discharging offsets, or as a part of the deliverables of the weapon systems contracts.
- Scaling of 3D Printing Labs for the workshops of the Army, dockyards of the Navy and Base Repair Depots of the Indian Air Force would be a prudent step. The assets with the NDAMGC should be of complimentary nature. The assets of 3D printing can be networked and exploited as per need. These will enable distributed digital manufacturing in peace and war.

- j) 3D printing should be placed on every Indian naval vessel for it to serve the emergent spare parts needs.
- k) Weapon platforms green field design mandate to adopt the 3DP and digital inventory from the AON stage itself.

A Fascinating Comparison between Additive Manufacturing & Cellular Phone Technologies

The mobile phones incorporate integrated cutting edge communication and information technologies which are extremely complex. Yet the mobile phones can be used even by an illiterate. AM or 3DP is comparable to mobile phones. They use cutting edge technologies but are simple to use. Any soldier, sailor or an air warrior can use AM technology with ease. This is a potential which could bring about exponential gains in terms of training, operations, MRO and innovation for the services to become Atmanirbhar!

Additive Manufacturing in Military : A Futuristic Perspective

3DP cost will come down. It will enhance the canvas of military rapid prototyping and manufacturing of parts. Printing of complex designs and customised parts will grow. 3DP integrated with Artificial Intelligence (AI) and robotics is the future. The capabilities to handle even far more complex designs will evolve. It will have integrated cybersecurity measures for securing the IP, obviating unauthorised reproduction, maintaining safety and security of critical assets during manufacturing and deployment.

There will be a spur in the innovation in weapon systems design, prototyping, development and manufacturing. 3DP with AI will directly impact the TBA.

It will mark the advent of the digital inventory era in the military.

SCM will get reliable, lead times reduced, bring in tactical gains through distributed manufacturing, and traceability will get robust.

Hybrid 3DP is where a 3D printer and a CNC machine works as an integrated unit. The gain is in enhanced speed, accuracy and economy. The maximum size of the 3D printed part dimensions are not limited to the bed size and travel, but is the volume the CNC machine can handle. The size limitation of 3D printed parts will cease.

Bio-3DP applications in artificial limbs, regenerative surgeries, 3DP of human organs and tissues etc is shaping up and will prove beneficial in nursing of the wounded soldiers and their healthcare.

The indigenous 3DP/AM hardware is lagging behind the global levels in terms of automation, precision, speed and input materials. The military and the industry-academia combine can work to attain, and surpass global standards. Russia has suffered in the ongoing war by using foreign origin 3D printers from nations imposing sanctions. Indian military drawing lessons from this should act towards indigenous 3D printers and materials.

The following two applications will help in appreciation of 3DP in military applications.

Innovative 3D printed runways, using 3D printed mats for expeditionary military runway laying Fig-8[29] a war fighting enabler. 3D printed propeller for a naval ship by the Naval

Group France, the largest so far, for the French military mine hunter, is a classic example of printing a critical part! Fig - 9.[30] There are thousands of case studies which can be alluded to by our military in the open domain.

Typical 3D Printing Military Applications

Fig - 8

Fig - 9

Conclusion

The 3DP/AM in the military is transformational. It offers immense possibilities in the military manufacturing and MRO. It has found its utility in operations right at the TBA, using deployable 3DP. 3DP has developed technologies where the plastic waste, and 3D printed plastic parts which are discarded, are gathered to be reused as input filaments for 3DP. It is termed as **reclamation** leading towards a safe environment. A military who exploits better 3DP or AM, will always have an edge over its adversary. It is albeit not the weapon, but it is a soldier-weapon duo enabler at war and peace.

AM/3DP will enable, empower and energise the Indian military with tangible and intangible gains in peace and war. A AM/3DP trained military will be a force to reckon with. 3D printing is a medium of infinite possibilities, where the only limit is our own imagination

****

Gp Capt Ashok K Singh, (Retd) is a post graduate mechanical engineer, and currently is the founder director of StratMRO Pvt Ltd. He has experience of working in several geographies, and at home endeavoured to be a technology evangelist.

NOTES

[1] Integrated Defence Services, "Joint Doctrine Indian Armed Forces 18 April 2017 https://ids.nic.in/WriteReadData/Document/2/13/1718bbb2-cb9c-4ef5-9843-cb670e58afb7.pdf

[2] Bible Study Tools, "David and Goliath - Bible Story", updated 24 May 2024 https://www.biblestudytools.com/bible-stories/david-and-goliath.html

[3] Wikipedia s.v. "Atomic Bombings of Hiroshima and Nagasaki", accession 09 June 24 https://en.wikipedia.org/wiki/Atomic_bombings_of_Hiroshima_and_Nagasaki accessed on

[4] World Economic Forum, "This timeline charts the fast pace of tech transformation across the centuries, 27 Feb 2023 https://www.weforum.org/agenda/2023/02/this-timeline-charts-the-fast-pace-of-tech-transformation-across-centuries/ accessed on 10 Jun 2024.

5 Ministry of Electronics and Information Technology, Government of India, "National Strategy on Additive Manufacturing", https://www.meity.gov.in/writereaddata/files/Additive%20Manufacturing%20Booklet%2014.02.2022.pdf

6 NASA, https://www.nasa.gov/missions/station/solving-the-challenges-of-long-duration-space-flight-with-3d-printing/ accessed on 11 jun 2024.

7 Sharmila Kuthunur, "India Launches Nation's First 3D Printed Rocket", https://www.space.com/india-agnikul-3d-printed-rocket-engine

8 Pratiparn Ninpetch, https://www.researchgate.net/figure/The-comparison-of-a-subtractive-manufacturing-process-and-b-additive-manufacturing_fig1_346418607 accessed on 11 Jun 2024

9 Stanford Advanced Materials, "Additive Manufacturing vs Traditional Manufacturing 27 Dec 2023 https://www.samaterials.com/additive-manufacturing-vs-traditional-manufacturing.html accessed on 12 Jun 2024.

10 Ibid n.6

11 Niti Aayog, "List of Atal Tinkering Labs", https://aim.gov.in/pdf/_OperationalATLsInIndia.pdf accessed on 11 Jun 2024.

12 National Skill Development Council, "Installer & Operator Additive Manufacturing (3D Printing) https://nsdcindia.org/job-role-list/installer-and-operator-additive-manufacturing3d-printing accessed on 11 Jun 2024.

13 National Skill Training Institute Trivandrum, "Additive Manufacturing Technician 3D Printing", https://nstiwtrivandrum.dgt.gov.in/node/337 accessed on 12 Jun 2024.

14 USA Department of Defense manufacturing Technology, "Joint Additive Manufacturing Working Group" https://www.dodmantech.mil/Manufacturing-Collaborations/Joint-Additive-Manufacturing-Working-Group/ accessed on 12 Jun 2024.

15 USA Whitehouse, "National Strategy for Advanced Manufacturing", October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Strategy-for-Advanced-Manufacturing-10072022.pdf accessed on 12 Jun 2024.

16 News Research & Markets, "United States Additive Manufacturing for Military and defense market, research report", 05 Jan 2024, https://www.prnewswire.com/news-releases/united-states-additive-manufacturing-for-military-and-defense-market-research-report-2023-from-concept-to-deployment---the-future-of-critical-asset-development-302027088.html.

17 UK MOD Army, "British Army Deploys 3D Printing in the Field", 10 May 2024 https://www.army.mod.uk/news-and-events/news/2024/05/brokkr-pioneering-the-british-army-s-deployable-additive-manufacturing-capability/.

18 Ibid.

19 Additive Manufacturing, "Additive Manufacturing And The War in Ukraine", 06 August 2022, https://www.additivemanufacturing.media/articles/additive-manufacturing-and-the-war-in-ukraine accessed on 14 Jun 2024.

20 Carolyn Schwaar, "Metal 3D Printers at Ukraine Frontlines Make Critical Spare Parts", 20 Sep 2023 https://www.forbes.com/sites/carolynschwaar/2023/09/20/metal-3d-printers-at-ukraines-frontlines-make-critical-spare-parts/ accessed on 14 Jun 2024.

21 Sinead baker, "Ukraine is 3D printing bombs to keep up with its battle field demands" *Business Insider India,)2 Aug 2023* https://www.businessinsider.in/international/news/ukraine-is-3d-printing-bombs-to-keep-up-with-its-battlefield-demands-says-report-with-some-costing-as-little-as-3-85/articleshow/102355182.cms accessed on 14 Jun 2024.

22 TASS Russian News Agency "Russia Creates 3D Printers for Industrial Production of Drones", 01 Aug 2023 https://tass.com/defense/1655075 accessed on 14 Jun 2024.

23 Sara Miller, "Volunteer Engineer is 3D Printing Kit For Israeli Troops at war", *Nocamels Israeli Foundation New, 03 Mar 2024* shttps://nocamels.com/2024/03/volunteer-engineer-is-3d-printing-kit-for-israeli-troops-at-war/accessed on 14 Jun 2024.

24 Indian Navy partners with think3D to 3D print spare parts on demand for vessels, 08 Apr 2020 https://3dprintingindustry.com/news/indian-navy-parnters-with-think3d-to-3d-print-spare-parts-on-demand-for-vessels-170632/ accessed on 14 Jun 2024.

25 Abhijit Abhaskar, "India's armed forces turn to 3D printing for military construction work", *Techcircle, 15 mar 2022* https://www.techcircle.in/2022/03/15/india-s-armed-forces-turn-to-3d-printing-for-military-construction-work accessed on 14 Jun 2024.

26 HAL, Wipro3D collaborate to manufacture metal 3D printed aircraft engine component, *Economic Times of India,* 09 Feb 2021 https://economictimes.indiatimes.com/news/defence/hal-wipro3d-collaborate-to-manufacture-metal-3d-printed-aircraft-engine-component/articleshow/80764369.cms?from=mdr accessed on 14 Jun 2024.

27 BEML and Wipro to work together in Aerospace, AI and 3D Printing, *Economic Times of India, 16* Sep 2019 https://economictimes.indiatimes.com/news/defence/beml-wipro-to-work-together-in-aerospace-ai-and-3d-printing/articleshow/71153551.cms?from=mdr accessed on 14 Jun 2024

28 https://www.drdo.gov.in/drdo/labs-establishment/contact-us/defence-research-development-laboratory-drdl accessed on 14 Jun 2024.

29 ITAMCO wins contract with US Air Force to develop 3D Printed runway mat, 02 Jul 2019 https://itamco.com/news/itamco-wins-contract-with-us-air-force-to-develop-3d-printed-runway-mat/

30 Largest Metal 3D-Printed Propeller Certified by Bureau Veritas, *The Maritime Executive,* 05 feb 2021 https://maritime-executive.com/article/largest-metal-3d-printed-propeller-certified-by-bureau-veritas

ADDITIVE MANUFACTURING IN A JOINT WARFARE SCENARIO : A CASE FOR INDIA

Air Cmde M S Rama Mohan, VSM & Brig (Dr) Anand Tewari (Retd)

Abstract

Additive manufacturing has changed the character of warfare. On-demand manufacturing of parts for end-use, shortening the supply chain, and improving the battlefield readiness of equipment are some use cases of additive manufacturing in recent conflicts. The use cases are restricted to non-critical areas. The barriers to extending additive manufacturing to the aerospace and defence sector require a regulatory framework for qualification and certification, testing and validation infrastructure and a trained workforce. India has promulgated a national strategy for applying additive manufacturing in the defence sector. Substantial use of additive manufacturing in joint warfare scenarios must be evolved by aligning with the national strategy. The paper assesses the barriers to the widespread use of additive manufacturing. It reviews India's status of additive manufacturing before giving a few policy recommendations for accelerating the use of additive manufacturing in the armed forces.

Introduction

Technology is changing the character of warfare. New methods, weapons, and technology have evolved to wage war and gain an advantage over the adversary. Conventional to non-conventional weapons intersecting the conflict zone to no-war-no peace zone have been practised. Recent armed conflicts have demonstrated the ingenious application of technology to defeat conventional weapons. Technology has disrupted the traditional approaches to warfare in all domains – land, sea, and air. Additive manufacturing is one of the emerging technologies that has disrupted conventional warfare. Some quarters have assigned additive manufacturing as a strategic enabler in next-generation warfare. The emerging technology of additive manufacturing may be an enabler that could change the face of warfare. Still, it must cover a long maturation cycle and demonstrate its ability in different armed conflict scenarios. The paper analyses the operational challenges and barriers to implementing additive manufacturing in a full-blown armed conflict and examines the opportunities for military strategists and technologists. The paper covers the status of additive manufacturing in the Indian armed forces. It concludes with a few policy recommendations so that the potential of additive manufacturing can be harnessed in joint warfare scenarios.

Literature Review

Many quality technical papers, book chapters, and news media articles on additive manufacturing were reviewed. The literature ranged from fundamental research to diverse applications of additive manufacturing. Each paper covered the basics, advantages and disadvantages of additive manufacturing. Daniel M "Emerging Technology and Risk Analysis Additive Manufacturing" has brought out the science, technology, and use cases to ensure that additive manufacturing is acceptable and that technology will be affordable.[1] This is an optimistic forecast for additive manufacturing technology, considering only the proliferation of technology. Micheal Kidd has argued that additive manufacturing, when deployed, will be a force multiplier in the "Additive Manufacturing Shaping the Sustainment Battlespace".[2] However, Henry A Colorado concluded in "Additive Manufacturing in Armour and Military Applications Research, Materials, Processing Technologies, Perspectives and Challenges" that additive manufacturing must overcome the challenges of the poor regulatory framework and lack of testing and validation infrastructure.[3] The conclusion provides a user's perspective, underscoring the widespread use of additive manufacturing. Frank Alifui-Segbaya in "Opportunities and Limitations of Additive Manufacturing that end-use applications of additive manufacturing can solve the scale-scope dilemma".[4] Having seen a diverse discourse on technology and use cases of additive manufacturing technology, Ajay Lele, in "Disruptive Technologies for the Militaries and Security", stated that additive manufacturing reduces the logistical challenges and improves the tooth-tail ratio of militaries.[5] Paneerselvam has made intuitive recommendations for additive manufacturing to benefit the Indigenous aerospace and defence sector.[6] He further stated that the government must develop mechanisms to capture the changing nature of manufacturing in India. The literature does not cover the application of additive manufacturing in a military operational scenario. Considering the sensitivity of the knowledge, the scholarship may be silent. However, several news articles and corporate communication in the open domain claim that additive manufacturing has supported recent armed conflicts, which partially validates the application of additive manufacturing in armed conflicts. Therefore, there is a gap in understanding the operational barriers, which, if addressed, pave the way for additive manufacturing use in operational scenarios. The paper aims to identify the barriers to adopting additive manufacturing in warfare and recommends an approach for the focused and result-oriented application of additive manufacturing in joint warfare scenarios.

Additive Manufacturing

Additive Manufacturing (AM) is a process of joining materials to make parts from three-dimensional model data, usually layer upon layer, as opposed to subtractive manufacturing and formative manufacturing methodologies.[7] The Conventional Manufacturing (CM) process involves the removal of material or the forming of a shape using the material. Additive manufacturing, or three-dimensional printing (3DP) or Direct Digital Manufacturing (DDM), is an advanced manufacturing technique. Essential features of additive manufacturing in the context of aerospace and defence applications are

- Parts with complex geometries and shapes, such as aero-engine fuel system components, can be manufactured using additive manufacturing techniques. Polymers, metals, and ceramics are used as materials for the AM.
- Every part is printed using the three-dimensional geometric model as a computer code based on the computer-aided design drawing. Intended geometric and physical

characteristics, namely dimensional tolerances, surface finish and the part's material strength, are part of the computer code.

- The AM parts are lighter as no excess material is added to produce a form, while in conventional manufacturing, material is removed to produce a form. The excess material, if not removed in conventional manufacturing, adds to the weight of the part.[8]
- The manufacturing process involves the preparation, production, and post-production phases. No specific tools are required to be manufactured in the preparatory phase. Parts are produced in small batches per the computer program during the production phase. During the post-production phase, the surface finish is restored, or support material is removed.
- AM has moved the Technology Readiness Level from laboratory prototype to commercialised technology.[9] Several challenges remain to be addressed.
- AM is a disruptive and path-breaking technology waiting to be adopted and exploited to its full potential, notwithstanding the challenges and barriers.[10]

Operational Advantages of AM

AM is considered to accelerate the development process from a prototype to a production standard. The tooling requirements are negligible. Selection of the material and the type of production is part of the design process, which in any case is aided by a computer. The production batch is small, and the lead time is less. Translate these features of the AM to operational scenarios, the following advantages will accrue: -

- The iterative cycle of the design-produce-validate-refine is short, implying that the response time between the prototype and the final product is short. Compression of time and cost encourages innovation in equipment in case of protracted armed conflicts when all the supply lines are disrupted, and one's forces are under stress to achieve a breakthrough. Innovation of equipment using AM at the end-use location shortens the iterative cycle by directly considering the end-user's experience. A product thus manufactured for the field on the field. A case in point is the addition of fins to grenades to stabilise its flight before hitting the target. The Ukrainian army improvised the grenade by attaching the fins printed by AM in the field location. The improvised grenades were installed on drones to mount attacks using the drones on the Russian armoured vehicles and tanks.

- Based on the computer program files, a part is manufactured for direct end-use in a remote location, away from the mass production sites. The end-use product using AM shortens the supply chain and reduces inventory costs. AM thus permits distributed manufacturing where the production facility is near the end-use location.[11] The production facility may be on the front line, forward bases, or the logistics supply and support ships. Therefore, the response time for an on-demand production of a part is shorter than that of conventional manufacturing. Own forces could disrupt Colonel John Boyd's Observe-Orient-Decide-Act (OODA) loop of the adversary by adopting the AM's short rapid prototyping to rapid product delivery loop and the short decision loop.[12] The advantage thus gained over the adversary by employing AM is significant.
- The strength of the AM lies in its computer programme and zero-tooling requirements, which can be customised to the part production requirements. The lower cost of production in AM overcomes the scale economies, and flexibility and customisation address the scope of economies. Thus, AM beats the scope-scale dilemma, which otherwise impacts conventional manufacturing.[13]
- The AM also permits varying the mechanical and physical characteristics of the part across its cross-section through topology optimisation techniques, which is difficult to achieve in conventional manufacturing.[14] Such a feature saves wastage and reduces weight without compromising strength, which is essential for aerospace and defence parts.

Limitations of AM

Limited choices of materials for AM will have operational implications.[15] The limited material choices may affect the operating envelope of the part as its mechanical and physical properties may be optimised. Adhering to stringent geometric tolerances is difficult in the AM as variations between the production batches are common. Rework to restore the tolerances is a challenge, unlike in conventional manufacturing. Repeatability and traceability of the quality levels of the AM parts are difficult owing to the variations in the microstructure of the AM material.

The global standards for manufacturing, qualification, and certification of parts manufactured through AM are evolving.[16] Conventional qualification and certification methods do not apply to AM-produced parts in terms of material properties and manufacturing processes. In such a scenario, evolving the route to the certification plan for a part manufactured under AM is difficult. Global standardisation organisations, such as ISO and ASTM, have taken steps to develop standards.[17] However, the AM is still in a nascent absorption stage, particularly in the aerospace and defence sectors. Mass production of various parts in different sectors using AM is yet to happen. The AM is being applied at the low end of the value chain. "Parts of consequence" or critical and complex components have yet to be manufactured using AM techniques. Few parts of the aero-engine fuel system have been attempted using the AM, with little success.

The proliferation of digital designs, materials, and ease of manufacturing are concerns of security apparatus in the military. The ease of hacking a digital design computer programme file and modifying it is a severe limitation to deploying AM in field conditions. The order of effect is unpredictable when the part manufactured by the hacked digital design is used by the adversary against its own forces.

Barriers to AM

With AM's operational advantages and limitations, what are the barriers to AM becoming as widespread as conventional manufacturing? The barriers must be addressed when employing the AM in joint warfare scenarios.

- Global best practices and standards are essential for the aerospace and defence parts manufactured under AM. Separate material, mechanical, and environmental qualification and certification standards for AM parts are evolving. The prolonged lead times of certification and qualification, inadequate standards, rules and regulations and the high cost of certification are some of the decision points restricting the widespread use of AM parts in aerospace and defence.[18] The testing and validation infrastructure for certification and qualification must be established based on the standards.[19]

- The AM parts are being used in non-critical aerospace and defence applications. The AM parts have yet to prove their worth in battle scenarios, though Ukraine has used them in its ongoing conflict with Russia at the low end of the value chain. Innovations in the form of medical devices like stethoscopes, prosthetics, personal protection equipment, body armour, fins for stabilising the flight of lofted grenades and drones were used by Ukraine in its conflict with Russia.

- Non-metal material for the AM parts has acquired certain acceptability, but AM technology for metal parts has yet to mature. The efficiency of the manufacturing, cost of manufacture, and availability of suitable materials for metal AM will result in increased absorption of metal AM parts.[20]

- The repeatability and reproducibility features of the AM must be improved. The accuracy of the manufacturing process must be improved, covering the material forming and printing stages. Since AM prints layer by layer, a variation in material property between two layers will result in poor process repeatability. Real-time monitoring, prediction, and control of the vital parameters of the manufacturing process, such as temperature, stress, microstructures, and mechanical properties of the printed parts, are essential for repeatability in AM.[21] The feature of reproducibility must be harnessed for manufacturing legacy parts. Using the 3D scanning process and digitalisation of the legacy part, a new lease of life can be given to old and legacy systems by creating the spare parts. Sikorsky Utility helicopter UH-60L has been stripped open, and nearly 20,000 parts were scanned to identify replacement parts using AM.[22]

- AM uses a very high level of digitalisation from the design to the production stage. The computer-aided design files of the parts, printing machines, control and monitoring of the manufacturing process, digital inventory of the part files, and printing of the parts from a remote location are some steps involving digital technology in the AM. The level of digitalisation of AM is a barrier for smaller manufacturers to enter the AM domain, but it affords advantages over conventional manufacturing. Digitalisation also brings to the fore the intellectual property rights and license production aspects, which must be addressed legally.[23]

AM Use Cases

The AM was developed in 1984 to accelerate the prototype design and development process. In 1993, Soligen manufactured the first commercial 3D printer. By 2005, a high-resolution printer was introduced. AM has been used for prototype development in aerospace and defence applications since 1988. The breakthrough for applying the AM to aerospace and defence equipment came with "Liberator", a 0.308 calibre automatic firearm, printed from a CAD file in 2013.[24] The firearm or gun did not print the firing pin and ammunition for apparent reasons. The time from design to full-scale development was progressively reduced from a few months to a few days. Rapid prototype development, therefore, was the central theme for the development of the AM. The initial stages of the AM polymers were used as feedstock for AM.[25] Ceramics and metals were also introduced for the AM. The cost of AM's "printing" equipment and the material to manufacture the parts have also been reduced significantly. Prompted by its affordability and advantages, AM was applied to aerospace and defence applications.

In the ongoing Ukraine-Russia conflict, additive manufacturing printers were installed to overcome the shortage of spare parts and critical components across the Ukrainian force's diverse fleet of war equipment. Australia has donated three WarpSPEE3D metal 3D printers to Ukraine in Sep 2023.[26] The 3D printers manufactured the "parts of consequences" or critical parts, a shortage of which may halt an operation or disrupt a mission. The hinge of the door of a troop carrier and specialist tool for the M113 gun were some of the critical parts produced using the cold spray AM technique. Printing the critical components near the end-use location in a contested environment will positively impact the tempo of operations. The argument must be substantiated with the tangible benefits from the battlefield spread over a period, and any conclusion at this stage will be pre-mature. The Israel-Hamas conflict has also seen the use of application of the AM techniques in the conduct of the operations. In Oct 2023, patient-specific instruments were manufactured using 3DP by an Israeli company, Synergy3DMed, to treat wounded civilians and IDF soldiers.[27] In Aug 2023, IDF seized a few pistols, rifles and weapon parts besides eight 3D printers. These developments in the Isael-Hamas conflict show the improvisation in battlefield tactics using emerging technologies such as AM. In the Nagorno-Karabakh conflict of 2020, a swarm of drones manufactured using the 3DP was used to attack the military command posts of the air defence systems, thereby immobilising the air defence systems.

Australia has used AM to repair the rudder anti-rotation bracket on the F/A-18 fighter aircraft and the landing gear shell bracket of a C-130 J transport aircraft.[28] Concepts of lighter and stiffer designs with topology optimisation (alignment of the microstructure of the part's metal) were employed in the AM of the parts. The parts have been qualified and certified for airworthiness, a milestone development. Notwithstanding, the airworthiness certification is a long-drawn process. In Nov 2022, the US Navy conducted trials to manufacture damaged or repaired parts by installing a 3D printer onboard USS Essex.[29] Later, in Nov 2023, another printer was installed on the USS Bataan, an amphibious assault ship. The US Navy has ensured a supply of legacy parts on demand, shortening the supply chain. US Airforce uses 3D printing to manufacture obsolete parts for several legacy fighter jets, including fleets of B-52 bombers, the B-2 Stealth Bomber and C-5 Super Galaxy transport aircraft.[30] In a significant development, the US Army has five large-scale machines capable of printing concrete. US Army has built two 512-square-foot buildings. Another project that the US Army has started is the jointless hull project for the underside of the vehicles. The Brazilian Air Force has used 3D printers for aerothermodynamics and experiments in hypersonic regimes. The 3D printers manufactured aircraft models and hypersonic engine prototypes for feasibility tests.

A critical use case of AM is parts replacement and reverse engineering. Various countries are progressively realising the potential of this feature of the AM. Digital twin technology, a digital representation of hardware, part, or component, is used in the AM technique for reverse engineering. The digital twin technology recommends processes to generate the hardware's physical, metallurgical and mechanical data for reverse engineering. The digital twin application to AM involves the Internet of Things, AI / ML, and cloud computing concepts to ensure that the AM digitally re-constructs legacy hardware with acceptable accuracy and precision.[31] As the idea amalgamates several cutting-edge technologies, the digital twinning application is in the research stage.[32]

Status of AM in India

India has responded to the changing manufacturing dynamic and its implications on national security. The strategic nature of the AM and its application in the Indian armed forces has been recognised by the Indian industry and strategic community. National Strategy for Additive Manufacturing issued by the Government of India in February 2022 is a policy-level response to the AM.[33] The strategy aims to integrate seamlessly into the global AM architecture while ensuring India attains a global AM hub status. The strategy covers the defence and public sector for AM implementation and identifies aims to address critical challenges for AM in India. The strategy is aligned with the objectives of the Atma Nirbhar Bharat Abhiyan and Make-In-India initiatives of the Government to make India self-reliant. The challenges for AM technology absorption in India are recognised in the strategy, which has opened the avenue for opportunities.

The industrial, research, and development ecosystem of AM in India has taken significant measures. The DRDO has constituted a specialist panel on material and manufacturing, emphasising digital manufacturing and the development of advanced materials.[34] It has assigned the AM development to three of its, namely DMRL, DRDL and R & DE. Fuel nozzles in a small turbofan engine used in the weapon systems were manufactured.[35] In another case, a radio frequency transmitter-receiver antenna was manufactured by AM. The design, manufacture and post-processing process was completed in less than a week.[36] DRDO uses AM to manufacture critical components for missiles, aircraft, handheld weapons, and drones. In another area, CEMILAC, the airworthiness agency under DRDO, has indigenised several polymers, composites and metal alloys that can be used for AM.[37] A chapter has been introduced in the Indian Military Technical Airworthiness Regulations for the development of materials for the AM. A non-critical AM part has been certified and has already been deployed. CEMILAC is adopting a similar approach to certify a critical part. In Dec 2022, CEMILAC entered an MoU with ASTM to establish a qualification test framework for certifying AM parts, machine and material qualification processes, post-processing, and part qualification.[38] This is a significant development in the field of AM in India.

Agnikul Cosmos, an indigenous start-up in the space domain, has developed a semi-cryogenic, fully 3D-printed rocket engine.[39] The three services have also seized the opportunity to exploit the AM. A two-storey AM Dwelling Unit for soldiers at Ahmedabad Cantt was commissioned.[40] This 3D-printed house is a disaster-resilient structure that complies with Zone-3 earthquake specifications and green building norms. IAF signed an MoU with IIT Palakkad on 18 July 2022 for cooperation in aviation components with the specific aim of undertaking research in 3D Metal Additive Manufacturing.[41] This cooperation between IAF and academia will enhance the AM usage in the Base Repair Depots of IAF for maintenance and repair functions. On Nov 22, the Indian Navy installed a 3D printer on its medium-sized frigate.[42] The 3D printer is an industrial-grade metal printer.

Way ahead for India

The AM in India is in its nascent stage. Measures taken by the government encourage research and development in additive manufacturing. Fostering the growth of the additive manufacturing industry requires a whole-of-the-government approach as India aspires to contribute 25% of its GDP to the manufacturing sector. A focused approach for applying AM in the joint warfare scenario is required. The aim of the approach must be to move up the value chain of AM, progressively shortening the OODA loop of an adversary by rapid replenishment, rapid prototyping and rapid recovery of capability suffered due to battle damage in a time-bound and result-oriented manner. Considering the maturity of the AM and its implications, the approach may have short-term objectives with a perspective of three to five years and long-term objectives with a standpoint of eight to ten years. The following points are suggested for the approach.

- Along the lines of the National Strategy for Additive Manufacturing, the Joint Strategy for Additive Manufacturing must be evolved for all three services. The strategy may nominate a lead service and assign each service a core domain within additive manufacturing. Academic institutions, defence R & D organisations and the indigenous private sector must be part of the joint strategy. A consortium route for applying AM in joint warfare scenarios should be adopted.

- DIAT should be nominated as the nodal agency for applied research of AM in the operational scenarios. MoUs with leading academic institutions such as IIT Madras and research institutions such as Central Mechanical Engineering Research Institute and private industry may be executed. The research must cover materials, manufacturing processes, sensors for real-time monitoring and control, and quality assurance and certification. Three services should present problem statements for focused and result-oriented research outcomes from short- and long-term perspectives.

- Centres of excellence in additive manufacturing may be created in each service. Three services must actively include additive manufacturing in maintenance, repair and operational logistics activities. The repair organisations of all three services, including army base workshops, dockyards, aircraft yards, and base repair depots, must adopt additive manufacturing aggressively. A proof-of-concept project may be taken up in a short-term perspective.

- The services must develop a roadmap for progressively absorbing additive manufacturing in the operational scenarios. The roadmap must include a plan to utilise AM parts in battle damage repair instances, joint exercises, or joint warfare scenarios. Battle damages may be simulated to exercise the potential of the AM in terms of the time to recover, cost incurred, assurance of quality and functionality.

- Qualification and certification regulatory framework must be evolved to remove the barrier to deploying the AM parts in the conflict zone. Conventional QA and certification agencies should develop a lean, cost-effective, pragmatic framework from a long-term perspective. The framework must be producer- and user-friendly and conform to local conditions.

Conclusion

The potential of the AM will only be fully harnessed, and the AM will be accepted by services only when the AM parts survive the challenges of the battlefield. Towards this, the three services, academia, and industry, must strive to exploit the potential of the AM. A focused approach by these agencies will ensure that the application of the AM achieves the desired end state of gaining technological and strategic advantage over the adversary till the advent of a new emerging technology. Till then, AM will remain a technology demonstrator only.

****

Air Commodore M S Rama Mohan, VSM is pursuing PhD in Relevance of Multilateral Export Control Regimes and Policy Implications for India. He is a Flight Test Engineer and has participated in several flight test trials. He is presently posted to Air Headquarters.

Brig Anand Kumar Tewari (Retd) has 33 years of vast experience in Educational Administration. He completed his PhD from the University of Pune in Chinese Geopolitics and recently published a very contemporary Book – 'Chinese Geopolitics in the 21st Century-A Post-Pandemic Perspective'. He has also been a Chinese language interpreter and is a recipient of the Chief of Army Staff Commendation Card. He now leads the AIDSS at Amity University, Noida as a Professor & Director.

NOTES

1. Daniel M. Gerstein, Erin N. Leidy, "Emerging Technology and Risk Analysis", Homeland Security Operational Analysis Center, RAND Corporation, Research Report, 2024, Available at https://www.rand.org/pubs/research_reports/RRA2380-1.html, Accessed on 07 Jun 2024.
2. Micheal Kidd, Angela Quinn, and Andres Munera, " Additive Manufacturing Shaping the Sustainment Battlespace", Joint Force Quarterly, 4th Quarter, 2018, National Defence University Press, November 05, 2018, Available at https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1681686/additive-manufacturing-shaping-the-sustainment-battlespace/, Accessed on 07 Jun , 2024.

3. Colorado, Henry & Cardenas, Carlos & Gutierrez-Velazquez, Elkin & Escobedo, Juan & Monteiro, Sergio, "Additive Manufacturing in Armor and Military Applications: Research, Materials, Processing Technologies, Perspectives, and Challenges", Journal of Material Research and Technology, 27(2023), Elsevier, https://doi.org/10.1016/j.jmrt.2023.11.030, Available at https://www.researchgate.net/publication/375926162_Additive_manufacturing_in_armor_and_military_applications_research_materials_processing_technologies_perspectives_and_challenges, Accessed on 07 Jun 2024.

4. Frank Alifui-Segbaya, Inigo Flores Ituarte, Seymur Hasanov, Ankit Gupta, and Ismail Fidan, "Opportunities and Limitations in Additive Manufacturing, " in Pei, E., et al. Springer Handbook of Additive Manufacturing, Springer Handbooks, Springer, Cham. https://doi.org/10.1007/978-3-031-20752-5_9, Accessed on 07 Jun 2024.

5. A. Lele, "Disruptive Technologies for the Militaries and Security", Smart Innovation, Systems and Technologies, 132, Springer, https://doi.org/10.1007/978-981-13-3384-2_5, Accessed on 07 Jun 2024.

6. Prakash Panneerselvam, "Additive Manufacturing in Aerospace and Defence Sector Strategy of India", Journal of Defence Studies, Vol. 12, No. 1, January–March 2018, pp. 39–60, Available at https://www.idsa.in/system/files/jds/jds-12-1-2018-additive-manufacturing.pdf, Accessed on 07 Jun 2024.

7. ISO/ASTM 52900:2021(EN), Additive manufacturing — General principles — Fundamentals and vocabulary, 2021, International Organisation for Standardisation, Geneva Available from: https://www.iso.org/obp/ui/#!iso:std:74514:en , Accessed on 03 Jun 2024.

8. Ibid, Note 5, pp 101-108.

9. Pedro Espadinha-Cruz, Angela Neves, Florinda Matos, Radu Godina, "Development of a maturity model for additive manufacturing: A conceptual model proposal", Heliyon, Vol 9, Issue 5.E16099, May 2023, DOI:https://doi.org/10.1016/j.heliyon.2023.e16099, Available at https://www.sciencedirect.com/science/article/pii/S2405844023033066, Accessed on 07 Jun 2024.

10. European Patent Office, " Innovation trends in additive manufacturing Patents in 3D printing technologies", Sep 2023, pp 15 Available at https://www.epo.org/en/service-support/publications?size=n_10_n&filters%5B0%5D%5Bfield%5D=node_id&filters%5B0%5D%5Bvalues%5D%5B0%5D%5B0%5D=885235&filters%5B0%5D%5Btype%5D=any&sort-field=publication_date_content&sort-direction=desc

11. Ibid.

12. Brett Cooner, "Paradigm Shift Additive Manufacturing and the New Way of War", Defence AT & L, November-December 2016, DAU, Vol 45, Number 6, pp 35-37, Available at https://apps.dtic.mil/sti/pdfs/AD1027005.pdf, Accessed on 07 Jun 2024.

13. Ibid. Note 4, pp 131, and Petrick, I.J., Simpson, T.W.: 3D printing disrupts manufacturing: how economies of one create new rules of competition. Res. Technol. Manag. 56(6), 12–16 (2013)

14. Jihong ZHU, Han ZHOU, Chuang WANG, Lu ZHOU, Shangqin YUAN, Weihong ZHANG, "A review of topology optimisation for additive manufacturing: Status and challenges", Chinese Journal of Aeronautics, Volume 34, Issue 1, 2021, Pages 91-110, ISSN 1000-9361, https://doi.org/10.1016/j.cja.2020.09.020, Available at https://www.sciencedirect.com/science/article/pii/S1000936120304520, Accessed on 07 Jun 2024.

15. In 2016, the AM facility saved an estimated €150,000 on jigs and fixtures - a figure that is expected to increase to €250,000 in 2017. Ben Redwood, Filemon Schöffer & Brian Garre, "The 3D Printing Handbook", 3D Hubs B.V. Amsterdam, 2017, pp 287.

16. Ibid. Note 3, pp 3309.

17. Ze Chen, Changjun Han, Ming Gao, Sastry Yagnanna Kandukuri & Kun Zhou (2022) A review on qualification and certification for metal additive manufacturing, Virtual and Physical Prototyping, 17:2, 382-405, DOI: 10.1080/17452759.2021.2018938, Available at https://doi.org/10.1080/17452759.2021.2018938, Accessed on 07 Jun 2024.

18. Ibid. pp 393.

19. Ibid. Note 3. Pp 3309.

20. Rodney Brennen, "State of the PM Industry in North America—2023", Metal Powder Industries Federation, New Jersy, 2023, pp 4, Available at https://www.mpif.org, Accessed on 07 Jun 2024.

21. Zhang, L., Zhou, W., Chen, X., "Digital Twins and Additive Manufacturing", In: Lv, Z., Fersman, E. (eds) Digital Twins: Basics and Applications, Springer, Cham,2022, pp 27-35, https://doi.org/10.1007/978-3-031-11401-4_4, Accessed on 07 Jun 2024.

22. Sydney J. Freedberg Jr, "Army Dissects Black Hawk Helo, Scans Parts For 3D Printing", Breaking Defense, Oct 15, 2020, Available at://breakingdefense.com/ 2020/10/army- Amr dissects-black-hawk-helo-scans-parts-for-3d-printing/, Accessed on 07 Jun 2024.

23. "3D opportunity in the Department of Defense: Additive manufacturing fires up", A Deloitte series on additive manufacturing, Deloitte University Press, 2014, Available at https://www2.deloitte.com/content/dam/insights/us/articles/additive-manufacturing-defense-3d-printing/DUP_1064-3D-Opportunity-DoD_MASTER1.pdf, Accessed on 07 Jun 2024.

24. Ibid. Note 4. pp 106.

25. Ibid. Note 5. Pp 104.

26. Carolyn Schwaar, “Metal 3D Printers At Ukraine’s Frontlines Make Critical Spare Parts”, Forbes, 23 Sep 2023, Available at https://www.forbes.com/sites/carolynschwaar/2023/09/20/metal-3d-printers-at-ukraines-frontlines-make-critical-spare-parts/, Accessed on 07 Jun 2023.

27. “Revolutionary Israeli 3D Printing Technology Produces Custom Parts for Patients, Applied to Wounded IDF Soldiers”, Aurora, 16 May 2024, Available at https://aurora-israel.co.il/en/A-revolutionary-Israeli-3D-printing-technology-produces-personalized-parts-for-patients-and-is-applied-to-wounded-IDF-soldiers/, Accessed on 07 Jun 2024.

28. Fact Sheet Department of Defence, Science and Technology, Australian Government, “ Additive Manufacturing”, DSC 2064, Aug 2018, Available at https://www.dst.defence.gov.au/publication/additive-manufacturing, Accessed on 07 Jun 2024.

29. Jaren K. Price, Miranda C. La Bash, and Bart Land, “ 3D Printing for Joint Agile Operations”, Joint Force Quarterly, 4th Quarter, 2019, National Defence University Press, October 05, 2019, Available at https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-95/jfq-95_92-99_Price-LaBash-Land.pdf/, Accessed on 07 Jun 2024.

30. “How are Different Branches of the US Military using Additive?”, Markforged, Available at https://markforged.com/resources/blog/how-are-different-branches-of-the-us-military-using- additive, Accessed on 07 Jun 2024.

31. Shen, T., Li, B., “Digital twins in additive manufacturing: a state-of-the-art review”, *Int J Adv Manuf Technol* **131**, 63–92 (2024). https://doi.org/10.1007/s00170-024-13092-y, Accessed on 07 Jun 2024.

32. Ibid. Note 21, pp 30.

33. “National Strategy for Additive Manufacturing”, GoI, Ministry of Electronics and IT, Available at https://www.meity.gov.in/content/national-strategy-additive-manufacturing, Accessed on 07 Jun 2024.

34. Materials & Manufacturing Panel, DRDO Available at https://www.drdo.gov.in/drdo/aeronautics-research-development/materials-manufacturing-panel, Accessed on 07 Jun 2024.

35. Case Studies- Wipro 3D, “STFE Starting Nozzle”, Wipro 3D, Available at https://wipro-3d.com/industry-application/metal-3d-printing-in-defense, Accessed on 07 Jun 2024.

36. Ibid. “Receiver & Transmitter Antennae”.

37. Ada Shaiknag, “AMSI Bangalore 2023: Airworthiness and certification of AM parts for defense and aerospace applications”, 3D Printing Industry, 23 Sep 2023, Available at https://3dprintingindustry.com/news/am-2023-airworthiness-and-certification-of-am-parts-for-defense-and-aerospace-applications-224799/

38. Ibid.

39. Agnilet, AM developed a cryogenic rocket engine of 3kN. Several parts of have been captured in one single piece of the 3D printed hardware. Source https://agnikul.in/#/tech

40. Aditya Chandavarkar,"The Growing Indian Additive Manufacturing Ecosystem: A Promising Frontier", AM Chronicle, 21 November 2023, Available at https://amchronicle.com/insights/the-growing-indian-additive-manufacturing-ecosystem-a-promising-frontier/, Accessed on 07 Jun 2024.

41. "IIT-PKD signs MoU with IAF for 3D Metal Additive Manufacturing", IIT-PKD, 25 Jul 2022, Available at https://iitpkd.ac.in/news/iit-pkd-signs-mou-iaf-3d-metal-additive-manufacturing, Accessed on 07 Jun 2024.

42. Jaiharshvardhan Rathore, "Rapid Manufacturing in Naval Defense Engineering",Medium, 04 Nov 2023, Available at https://medium.com/@jaiharshvardhan.rathore20/rapid-manufacturing- in-naval-defense-engineering-c5e06441102a, Accessed on 07 Jun 2024.

IOT & DIGITAL : TWIN-BASED SITUATION AWARE SMART ASSETS AIDING DECISION SUPPORT FOR COMPREHENSIVE NAVAL MAINTENANCE AND WARFARE

Capt (Dr) MSN Murthy, Lt Cdr Apurva Mayank, Indian Navy

Abstract

In Indian Navy, multiple organisations interact with each other for a common goal: combat ready ships. Each organisation works independently for its defined charter of duties and interacts administratively with each other. It is pertinent to observe that although each organisation works independently, their mutual interaction with each other is a highly complex phenomenon akin to multiple heavy machinery interacting with each other in a complex engineering system. In some of the organisations like naval dockyards and shipbuilding yards, where ships are refitted/ built, Indian Navy has migrated to Enterprise Resource Planning (ERP) where the interaction of individual departments of dockyard is co-ordinated using software-based tools to optimise efficiency. However, most of these ERP systems used in Navy are intra-organisational. Sub departments within the organisation interact through these ERP systems simplifying the complexity and interdependency of the multi-faceted nature of the organisation. A similar characteristic is relevant for the jointmanship of the three services. This paper goes a step beyond and proposes an inter organisational ERP based model. This proposed IT tool would serve to achieve administrative co-ordination between multiple organisations of Indian Navy and other sister services, as well as, will aid in decision making of each organisation based on various kinds of maintenance data of their assets that would be analysed in a Reliability Centric Maintenance generated ecosystem. Therefore, a three pronged, comprehensive RCM-based inter-organisational ERP model for optimised efficiency and performance of tri-services is proposed herewith. The first step is a digital data and machine learning-based reliability monitoring system onboard naval platforms, as well as for similar assets of the army and airforce. The second step is transferring all the digital data to a central data processing centre ashore. The third step is integrating data from repair yards and logistic services to deliver a comprehensive process optimisation solution. This data-based ERP model would work independently at the lowest component level through equipment level, system level, ship/unit level, fleet/ formation level, command/ brigade level to the highest level of command and control.[1]

Introduction

In the modern era, the performance of war machinery plays a bigger role than leadership and strategy, towards the success of any conflict. Currently, the Indian Navy relies on condition monitoring tools for Condition Based Predictive Maintenance, as the maintenance philosophy which drives the operational cycle of the ships. This operational cycle defines the work for repair yards and logisticians to plan their charter of duties and inventory schedule respectively. There are two basic challenges in this workflow. The first is in the CBPM based maintenance philosophy and the second challenge is lack of data-based decision support system for mutual interaction amongst these organisations towards optimal availability of assets, which in turn determine the combat capability of the naval force. Similar, situation is perhaps relevant for assets of other sister services.

Bottlenecks in CBPM and ERP

There are many state-of-the-art CBPM tools presently in use in Indian Navy. These CBPM tools {like Narrowband analysis, trend analysis, lub oil particle analysis or Unified Maintenance Management System based reliability monitoring tool, like NETRA} depend on the manually logged data. Manual logging has inherent problems like erroneous entry, undefined sampling rate, loss of data etc. The manual data is also not situation-aware. Before dwelling any further to discuss the merits and demerits of manually logged data, it is important to define the term "Situation Awareness". The concept of 'Situation-Aware' is being increasingly used in data analytics and human factor circles. The concept of situation awareness is explained further.[2]

Situation Awareness

A Challenger II tank, engaged in defending a bridge over the Shatt al Basra canal on the western outskirts of Basra, fired upon what its Commander believed were enemy personnel moving in and out of an ammunition bunker. Unknown to the Commander, the engaged target was actually two friendly Challenger II tanks from another squadron, sited in an overwatch position adjacent to a dam only 1,500 metres to the southeast of his own position. The first High Explosive Squash Head (HESH) round fired landed short but the effects of the blast were sufficient to throw the crew members from the tanks' turrets. The second round was a direct hit, detonating in the Commander's hatch of one of the Challenger tanks, killing its two occupants instantly. The incident described is an extreme example of what can happen in a complex sociotechnical system when the operators working within the system are not fully cognisant of everything that they need to know. In the aftermath, the official government inquiry (Ministry of Defence, 2004) identified various causal factors, including a lack of what is called Situation Awareness (SA) on behalf of those involved. SA is the term that is used within Human Factors (HF) and ergonomics circles to describe the level of awareness that people have of the situation that they are engaged in. It focuses on how people develop and maintain a sufficient understanding of 'what is going on' and what is likely to go on in order to achieve success in task performance.

Safe and efficient task performance within complex sociotechnical systems depends on organisations acquiring and maintaining appropriate levels of SA. Systems, devices and procedures therefore need to be designed so that they facilitate, rather than inhibit, SA acquisition and maintenance. Designing systems in this manner depends on the accurate description of how SA operates in the system in question, on exactly what information SA comprises during task performance and on how this information is integrated and used by different enterprises working within the system. Further, reliable and valid approaches for modelling SA are required in order to determine how a new system, device, training programme and procedural design affect SA during operations.

Having understood what is SA in our context of enterprise resource planning, let us return to the original discussion about the data that we use for monitoring our equipment and systems being not situation-aware and how this affects our decision making and efficiency. The inescapable conclusions from this understanding of SA are that currently there is a lack of an appropriate model of 'Situational Awareness' (SA) for complex collaborative environments and also that existing SA assessment methods are inadequate when considering the measurement of SA during real-world collaborative activities.

These observations of monitoring or being situation-aware is not at an individual organisational level but at a complex system of systems level where each individual organisation is interacting with each other and therefore giving us an emergent behaviour which is an output of complex interactions. This complex interaction of individual enterprises confirm the assumption that our understanding of SA in such environments remain limited and subsequently serve to set the agenda for the rest of the paper; that is, it is our aim to further investigate the description and measurement of SA in collaborative environments. Our lack of knowledge regarding enterprise-level SA acquisition and maintenance and the accompanying lack of approaches for measuring team SA is the issue that is being addressed by this paper.

Considering the bottlenecks in our present processes and systems, the current proposal is a solution aided by the digital data-based RCM philosophy and how this digital RCM will aid in enterprise-level decision making.

Proposed Solution.

A Distributed Situational Awareness (DSA) model, accounts for SA in collaborative environments. Following this, the propositional networks methodology – an RCM based modelling approach that can be used to describe and assess DSA during real world collaborative tasks – is described. A simple command and control paradigm example is then used to demonstrate both approaches.

Distributed Situational Awareness

- **Data on the Network**. The present-day Indian Naval Ships are being commissioned with Integrated Platform Management Systems (IPMS). All the equipment, machinery, systems, system of systems are connected to a common network called IPMS. All the assets of a ship are sharing their running parameters on this IPMS network. The running parameters of each equipment are being logged in both digital (Unlabelled data) and CSV format . This data can profusely aid in developing fleet level, system level and equipment level situational awareness. This data in the IPMS can be collected in three ways.[4]
    - **E- Logging**. On those ships where the data is being logged in CSV format, the data can be directly taken through any suitable hard disk format or through NUD. The challenge with this kind of data extraction is that the data cannot be taken when the ship is sailing. The intermittent logging of data will not support the machine learning-based condition monitoring models or the RCM models.
    - **Digital Data**. The second option is to directly transfer the sensor-based digital data through the Navy's own satellite bandwidth. The digital data from the IPMS would be encrypted and compressed and then transferred to a shore-based data processing centre. At the data processing centre, this data will be decrypted and decompressed for further processing and labelling of data. The labelled data can be further fed into the machine learning-based reliability assessment models.
    - **Digital Data without Access to Network Protocol**. A major bottleneck in the data extraction would emerge if the OEMs of the IPMS do not share the network

protocol. If the network protocol is not provided to the end user under proprietary laws, then we can harness the data by developing a software patch to extract the data. Using this patch, we can break into the network protocol of any IPMS-based platform and utilise the data.

- **Data Transfer to a Reliability Assessment Centre**. The data that is collected from the IPMS platforms would have to be compressed and encrypted before it could be transferred to a data processing centre or reliability assessment centre. For compression of the data, a collaborative effort is underway with M/s CDAC which holds a patent for a supercomputer that can compress the data by upto 10X. The compression of data by 10X will have two benefits. The first benefit would be in utilising only a limited bandwidth of the satellite communication system for transferring the data. The second benefit would be improved sampling frequency. Improved sampling frequency would give a better result out of the reliability assessment models. After the data is transferred to a reliability assessment centre, the data would be decompressed and decrypted. The data labelling and data processing would be done on the original data after decompression and decryption. The processed data would now be integrated with data from Material Organisation, which provides information on inventory consumption and from dockyard/ repair yard which provides maintenance data, for feeding into the machine learning-based reliability assessment model.

- **Data Integration**. Data integration is a crucial component for enhancing material and inventory management through situational awareness and reliability-centred maintenance. It involves the aggregation and harmonization of data from various sources to provide a unified, comprehensive view of inventory status, maintenance requirements, and operational conditions. Effective data integration supports informed decision-making, optimizes resource allocation, and enhances overall operational efficiency. The data taken from IPMS-based ships will generate only ship-level situation awareness. To derive any meaningful value addition in the enterprise-level situation awareness, data from the individual organisations like

Material Organisation, Naval Dockyard, MTU, INSMA etc has to be integrated with the IPMS-based data from ships.[3]

- **Key Elements of Data from Dockyard and Material Organisation**[4]
    - **Supply Chain Databases**. Capturing data on procurement of equipment parts, time taken in effective shipment from the vendor and bureaucratic delays in receiving the item from the time demand is raised and inventory levels from material organisation etc. This data can be captured from ERP software tools like ILMS and transferred to the data processing centre.
    - **Maintenance Logs**. Gathering historical and real-time data from maintenance records, including details on repairs, part replacements, and equipment performance has to be extracted from the Naval Dockyards for integration with MO and Ship data.
    - **Operational Reports**. Data from daily maintenance operations like repair requests, operational defects, mission logs, and utilization reports help in understanding equipment usage and wear patterns from ships. Maintenance logs and operational reports may be taken from the software tools used in repair yards and shipyards or through the various returns provided by yards on ship refit and repair.
- **Machine Learning Based Reliability Assessment Model**. In recent years, the utilization of Bayesian Belief Networks has emerged as a powerful approach for risk analysis in complex systems such as gas turbines. Bayesian networks, a subset of probabilistic graphical models, leverage principles of conditional probability to represent and analyse the interdependencies amongst different variables influencing system performance and reliability. The authors, in collaboration with IIT Bombay, have taken a comprehensive study on the application of Bayesian Belief Networks for risk analysis of complex equipment like marine gas turbines. Through the integration of concepts from decision-making, predictive maintenance, and machine learning, the authors aim to develop a sophisticated

model that can identify key failure modes, assess their likelihood, and quantify their impact on downtime and performance on equipment, system and even enterprise level process flow.

- **Model for Risk and Failure Analysis of a Gas Turbine**. The following example illustrates how a component and a subcomponent of the Gas turbine can be modelled for failure and risk analysis. This work has been done by IIT Bombay as part of project NETRA. The same model can be extrapolated to develop a system or enterprise-level risk, failure and reliability analysis tool for better enterprise-level decision making. The gas turbine equipment was divided into different sub-assemblies and components for understanding the mutual interaction between subcomponents and their emergent behaviour on the gas turbines. Then each subcomponent was checked in FMD and OREDA software for failure modes. In the software initially, a node (component/sub-assembly/equipment) was defined and then its states were defined as shown in Fig.1.

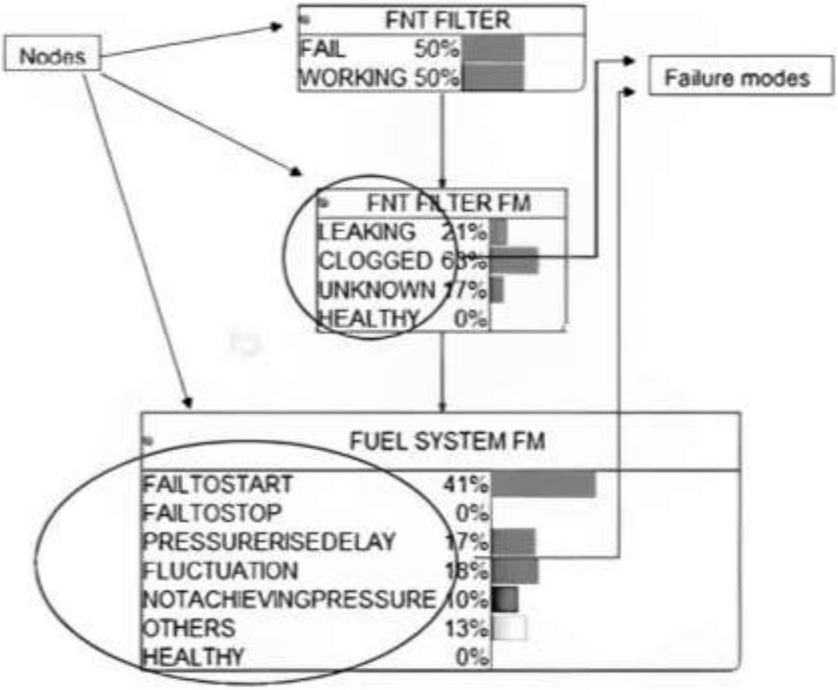


Fig. 1 Sub-Component and Component Level Failure Nodes

- Failure mode of an individual system, say the fuel system as above was mapped with the failure mode of the parent equipment i.e. Gas Turbine. The whole layout contains component failure modes and system failure modes. In this example, the model which is created on the failure modes of individual systems, will provide us with a probability of a particular failure mode occurring in a gas turbine. Similarly, this model when extrapolated at the enterprise level, will map the failure modes of individual sub-systems to give the probability of failure of the overall system. It is reiterated here that the model is based on Bayesian theory which gives conditional probability of an event when other events have already occurred. This entire process will happen in real-time, continuously updating itself as new events keep occurring.

- To develop a Bayesian network, Netica software was considered but due to the limitations in the academic version of this software Bayes Fusion software is utilised. As a test case, Failure analysis Networks have been developed for the mentioned systems as follows:-

    - **Fuel System**. The complete fuel system was divided into its individual components and these components were displayed as nodes in the network and failure modes of these components were displayed as the states of a particular node. These failure modes of the components were taken from FMD 91 and OREDA. The same procedure was followed for all the systems.

    - **Integrating all Systems for GT Failure Analysis.** Similarly, all the individual sub-systems of GTs like starting system, Gear Box systems, shafting, fuel systems etc., were mapped into the software. After simulating the depicted networks it was pertinent to combine all these to get a common troubleshooting diagram that can be used to diagnose the GT-level Failure Modes.

Utility of ERP System Backed with RCM Data.

Employing machine learning algorithms to predict reliability based on digital data, current trends, and mission requirements will aid in data-driven decision-making and improve the collective efficiency of the Indian Navy and other services. The maintenance log data from the Naval dockyard will be the integrated with Material Organisation data like time lag in the supply chain, idle time of spare parts in inventory etc., to optimise the demand-supply gap of the engineering spares to achieve overall optimisation in resource planning and utility. The following points will further illustrate how the defence forces will benefit by RCM data-backed ERP system through an example of a naval ship refit management:-

- **Decision Support Systems**. In the present-day scenario, the timelines of a ship's refit are planned during the Annual Refit Conference (ARC). Similarly, planning is presumed to exist for the maintenance of war machinery of the Indian Army and Indian Air Force. Based on these planned maintenance routines, scope of work is planned by repair yards and Fore Cast List of spares (FCL) is planned and demanded by material organisation. However, the flow cycle of refits and the operational cycle is not linear. Operational requirements, unavailability of dry docks in repair yards and other administrative bottlenecks add non-linear dimensions to the refit planning. The situation awareness of non-linearity of life cycle management through the machine learning and condition monitoring software tools will aid in optimised decision-making. For example, in present circumstances, if the attenuation of shock mounts of a diesel alternator is showing increasing trend and may merit replacement in the upcoming refit, the Engineer Officer of the ship will intend to place demands of as many shock mounts as are fitted on the alternator. This intent of over demand comes from the lack of predictive failure data of the shock mounts to the Engineer Officer. The same trend extrapolates with the Yard and Material Organisation. Each organisation will intend to overestimate the number of shock mounts required. The underlying issue in this kind of overestimation of demand is in view of the lack of data-driven decision support system. It is therefore imperative to appreciate that decision-making at all levels be supported by RCM data.

- **Correct Causative Analysis of Defect.** The present-day condition monitoring tools being utilised for causative analysis of defects are based on manually logged data, as explained during the introductory part of this paper. This kind of data may not always result in the correct assessment of machinery health. For example, let's say, the ship is undertaking a hard turn towards port or starboard. While taking a hard turn, the loading on the engine will increase at the same engine rpm but the same reason may not be evident in the diagnostic study of higher lubrication oil temperature. The precise reason of the increase may only be found by regression analysis of lub oil data with all other engine parameters. Therefore, only a comprehensive data-driven machine learning model, as demonstrated above, would be able to predict the comprehensive machinery health.

- **Maintenance Cards**. Based on the inputs given by this proposed model, Yard can generate automatic maintenance cards for its repair teams thus aiding them with a comprehensive analysis of the failure and the corrective measures to be taken. Similar kinds of maintenance cards may be given to each ship under the refitting authority for optimised maintenance work.

- **Resource Allocation**. Based on the inputs given by this proposed model, yard can optimise its resource allocation for both workforce and spares as follows:-

  - **Workforce Management**. The workload and skill level required would be predicted by the model so workforce management may be done by using advanced scheduling tools based on the RCM-backed data to assign maintenance tasks to personnel based on availability, skill levels, and workload.[1]

  - **Parts and Supplies Coordination**. Ensuring that maintenance schedules are aligned with the availability of spare parts and necessary supplies, leveraging the RCM-ERP system help to manage inventory levels effectively.

- **HR Assessment**. Apart from planning its requirement of the required manpower for a particular refit project, the Yard can also assess the quality of the work undertaken by the yard workers. This assessment would be foolproof because the quality of work done by the yard team will reflect in the machinery reliability number predicted by the model.

- **Adaptive Maintenance Scheduling**
  - **Dynamic Scheduling**. Utilizing adaptive scheduling systems that can adjust maintenance plans in real-time, based on changing operational conditions and equipment status.
  - **Risk-Based Prioritization**. Prioritizing maintenance tasks based on risk assessments, focusing on equipment that is critical to operations and more prone to failure.
- **Feedback and Continuous Improvement**
  - **Performance Monitoring**. Continuously monitoring the effectiveness of maintenance schedules and making adjustments based on performance data and feedback.
  - **Lessons Learned**. Documenting lessons learned from maintenance activities to refine predictive models and scheduling algorithms, ensuring continuous improvement.
- **Workflow Automation and Process Standardization.**
  - **Automated Workflows**. The ERP system will automate workflows, reducing manual intervention and minimizing the risk of errors.
  - **Standard Operating Procedures**. SOPs may be implemented based on continuous trends within the ERP to ensure that all processes are standardised, enhancing consistency and quality.[4]
- **Collaboration and Communication**
  - **Stakeholder Collaboration.** An ERP system provides a platform for seamless communication and collaboration among various stakeholders, including shipyard personnel, engineers, and suppliers.

- **Document Management.** Centralized storage and management of documents related to the refit process, such as blueprints, technical manuals, and compliance reports.

Recommendations

Considering the rapid pace of digitisation of assets as well as processes and the advantages offered by the same as discussed above, through IoTs and digital twins, the following are recommended for the armed forces towards an integrated warfare setup:-

- **Reliability-Centred Approach.** While HR and leadership at different levels or 'man behind the machine' is always relevant, the significance of the role and performance of equipment and machinery or the assets used for warfare is irrefutable. These war-fighting assets are expected to meet their respective desired purpose with a defined performance for a defined period of time without failure. 'Reliability', which is defined as 'the degree to which the result of a measurement, calculation, or specification can be depended on, to be accurate', of an asset plays a vital role at the delivery end of a combat force. Reliability is a direct function of both the design and the maintenance philosophy adopted and is a critical aspect for a fighting force. Thus, a reliability-centred approach for managing the optimal availability and performance of assets is a mandatory requirement of the defence forces. Reliability Centred Maintenance is a maintenance philosophy that assures the desired end state of the assets involved in warfare. However, an RCM philosophy is dependent on accurate data of the assets, both performance and operational related. Therefore, it is pertinent that defence forces acknowledge the importance of RCM for effective life cycle management and high reliability of their assets. [4]

- **Data Acquisition.** Currently, the data related to the performance of the war and related machinery/ equipment is recorded manually in most cases across the defence forces. The maintenance and repair-related data though available is only used locally and ineffectively without any integration and situational awareness. In the haste of task completion and not acknowledging the significance of this data, defence forces face an opportunity loss. Extending the utility of the data over a longer time domain in a structured manner provides institutional retention of knowledge and experience, and aids in accountability of machinery performance. This further equips the user with information that is useful in technological upgradation. Indian Navy, in all new acquisition ships, has upgraded to the state of the art 'Integrated Platform Management Systems' with features of integrated data acquisition, which aids in situationally aware combat management within the ship. Extension of the same to the proposed RCM-based integrated DSA philosophy is thus implementable as the next step. The same is, however required to be upgraded on the platforms of older vintage. In the Indian Air Force, the aviation assets including support equipment are sophisticated in nature and are built with data acquisition systems. Integration of the database of these assets in an ERP system is essential to embark on the philosophy of DSA. In the Indian Army, the wide distribution of assets geographically poses a challenge as well as reiterates the necessity of the performance and operational data acquisition, to achieve the desired integration in real-time basis. Thus, all defence services are recommended to adopt to a data acquisition system to capture the operational and maintenance data for effective assets management.

- **Assets with Situational Awareness.** With a real-time data acquisition from all the assets, the stage is set for ERP-based integrated setup for situationally aware of assets management at multiple levels. Each of the defence forces is required to embark on such a data management system embracing digitisation and interoperability within various organisations of respective service using Big Data Analytics running on an ERP framework towards an enhanced decision support and management system. This would involve creation of an ecosystem that facilitates data acquisition from each asset at sufficient sampling rate, including supply chain data followed by assimilation of this data and converting it to maintenance decisions based on RCM to ensure high reliability of the assets. And this data is shared with other stakeholders at all levels of authority in a secure manner equips operational commanders to arrive at decisions without gaps ensuring optimal utility of the assets in consonance with other assets in the same or connected roles.

- **Distributed Situational Awareness.** Linking of organisational data, within the respective defence forces and amongst themselves aids in decluttering and streamlining of information overcoming the fog of war. Sound communication networks are essential to achieve this framework of integrated warfare. Indigenous space technology which provided us world-class satellite communication is a strong facilitator in this context. In an integrated framework, the data sharing amongst the sister services is imperative for smooth and dynamic flow of real-time information for effective DSA. The learning curve in the implementation of DSA will commence with the setting up of the required ecosystem followed by progressive implementation from the local assets management to a centralised system of each service and further a data sharing system amongst all the combat forces involved in the integrated warfare towards an effective DSA.

- **User Role in Collaborative R&D.** All defence forces are required to recognise and acknowledge the significance of reliable war machinery, in light of the rapid technological advancements through collaborative R&D with all stakeholders. OEMs are considered to have a complete know-how of equipment or machine, being the designers. However, the domain expertise of a user in exploiting the equipment is equally valuable in optimising the designs, though not being utilised effectively. Retention of institutional knowledge is a challenge in the organisational set up of a defence force, which involves turnaround of personnel within limited duration of one to three years in a given role. ERP-based data management not only aids in the retention of institutional knowledge but aids in the effective life cycle management of assets. Implementation of advancements in technology in defence forces provides the required edge over adversity, which is directly dependent on the economic prowess of a country. However, effective utilisation of the assets and drawing continuous lessons from the experience can aid in pole vaulting the required technological growth. While the defence production depends on the integrated efforts and collaboration of academia, (like IITs & IISc), designers and the industry, it is the user who has the potential as well as the responsibility to bridge gaps between these agencies. Our country has embarked on a mission to achieve self-reliance in the defence sector as a top priority and our country as such is set to become a developed nation by 2047. Driving the defence technologies is also a prerogative of this ambition because of the inherent potential in the implementation of new technologies in the civil domain. Thus, defence forces are expected to involve in collaborative R&D proactively and assume a leadership role in the development of the nation.

- **Resource Sharing.** The backbone of an integrated management system is sharing of resources like institutional knowledge in common technological domains, repair yards, advanced field-level testing equipment, satellite communications etc., The resource sharing should cater for overall redundancy within and amongst the defence forces. Optimal peacetime usage by resource sharing with civil applications too in a secure manner will reduce the strain on the government for a developing nation like ours. Common framework and system architectures within and amongst the defence forces will aid in a smooth interface to implement an integrated warfare management system. Multilevel engagement across the services is essential to define and create this common framework.

Conclusion

Situational awareness, reliability-centred maintenance using machine learning, and ERP integration are powerful tool that can significantly enhance material and inventory management in the armed forces. By providing real-time data, predictive analytics, and comprehensive visibility, these approaches enable more accurate inventory management, efficient supply chain operations and improved operational readiness. The Indian Navy, likewise the Indian Army and Indian Airforce, continue to modernise and expand their capabilities, integrating situational awareness, RCM, and ERP systems in its logistical processes will be crucial for maintaining the strategic edge for services in an integrated manner.

****

Capt (Dr) MSN Murthy is an alumnus of, Naval College of Engineering , INS Shivaji and Naval War College. He is an MTech in Thermal and Fluid Engineering and a Doctorate from IIT Bombay with the research topic of 'Combustion Characteristics in Gas Turbine Engines'. He holds a patent on an innovative heat engine concept called 'Part Electric Gas Turbine' through IIT Bombay and has applied for another three patents (under review) on 'Simple and efficient fuel consumption measuring system for Heat engines', 'Recuperator for open architecture GT', 'Semi-Closed PEGT for AIP' through Indian Navy. He is currently heading Centre of Excellence (Marine Engineering), INS Shivaji as Officer-in-Charge.

Lt Cdr Apurva Mayank is an alumnus of Manipal Institute of Technology, Manipal. He is an MTech in Mechanical System Design from IIT Kharagpur and an MBA from Narsee Monjee Institute of Management Studies – Global Access School of Continuing Education. He also holds a Graduate Certificate in Public Policy with specialisation in Defence & Foreign Affairs from Takshashila Institution, Bangaluru. He is currently appointed at Centre of Excellence (Marine Engineering), INS Shivaji and is heading the research verticals related to RCM, BDA, Control Systems and auxiliaries. He is currently pursuing his PhD from IIT Bombay.

NOTES

[1] Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors, 37, 32-64.

[2] Thakkar, J., & Deshmukh, S. G. (2006). Supply Chain Management in Indian Manufacturing: A Case Study. Production Planning & Control, 17, 512-523.

[3] Rao, R. (2017). IoT-Based Smart Inventory Management System. International Journal of Advanced Research in Computer Science, 8, 45-50.

[4] Indian Navy. . Annual Report. [online: web] URL: www.indiannavy.nic.in [Accessed 10 June 2024]

IOT INTEGRATION IN WARFARE: REVOLUTIONIZING MODERN BATTLEFIELD OPERATIONS

Lt Col Rachit Ahluwalia

"Any sufficiently advanced technology is indistinguishable from magic" —Arthur C. Clarke

Abstract

The meteoric rise of IoT has the potential to impact several spheres of humanity, warfighting being one of them. This paper highlights the perspective of IoT implementation in modern battlefield scenarios, analysing its role in augmenting situational awareness, delivering information superiority and supplementing decision support system through comprehensive analysis. While acknowledging the benefits of the technology, the paper also addresses security and ethical concerns associated with IoT in military applications.

Introduction

The present era has been ushered by advancements in Information, communication and technology (ICT). This advancement has impacted the transformation of almost all aspects of society, warfighting being one of them. Contemporary armies across the globe are experimenting to deploy niche technologies into battlefield as force multipliers to gain tactical edge. Out of various new technologies viz AI, robotics, quantum computing, virtual and augmented reality; IoT has been generating immense interest among defence researchers and industry. IoT records an exponential proliferation rate in the domain of emerging computing technologies, with an estimate market revenue of $212 billion worldwide and more than 25 billion devices connected with each other by the year 2027[1]. IoT is an intersection of real-life things/ objects, communication networks and data. It is empowered by plethora of sensors, actuators, identifiers, pervasive information systems, embedded computing, software intelligence and network connectivity. It should not be perceived as any other app on the World Wide Web but as a radical Information Technology enhancement.[2]

IoT harnesses the power of Wireless Sensor Networks (WSNs), RFID, Machine to Machine Communication (M2M) and Control Systems to collect, process and transfer vital info from heterogeneous nodes across time and space. To convert the extracted information into intelligence either localised hardware resources can be employed or geographically dispersed virtual machines over cloud computing.[3] The power of IoT processors is in making informed choices and executing tasks based on what its sensors observe. The range of processing tasks may vary from measuring simple physical parameters viz temperature, humidity, altitude etc to as complex as recognising patterns and extracting weather forecasts using predictive AI algorithms. IoT actuators execute planned actions, post consuming information from sensors that tangibly change the setting. Actuators may perform a trivial task, even as remotely turning on a security light or can accomplish an intricate mission of target identification, tracking and destruction.[4] They can operate on a both sides of the spectrum scale which is significantly smaller and larger than human limits. People may form part of the IoT action loop but it is designed to function autonomously as well.[5]

The meteoric progression of IoT has propelled the deployment of intelligent sensors and actuators in the battlefield, lending it the name Internet of Battlefield Things (IoBT).[6] IoBT is an inventive technology that incorporates WSNs, actuators, portable & ruggedised IoT devices, routers and gateways to create a modern integrated warfighting force with refined operational efficiency.[7] Although it can be argued that IoT technology is not new and has its roots dating back to the work done by Mark Weiser at Xerox PARC in the 1990s, recognising the power of IoT took years of evolution in five key technology domains i.e.

wireless sensors, communication & networking, cloud computing, smart algorithms and digitally controlled actuators.[8]

IoT's Transition to IoBT

The defence sector has been a fountainhead for numerous emerging technologies for ages. Gaining a battlefield edge has always been a driving factor to explore and experiment with radical ideas. Post the first Gulf War one such idea started taking shape when Admiral William Owens, the then Chief of US Naval Operations, introduced the idea of a 'System of Systems' in a research article published under the aegis of the Institute for National Security Studies, United States. He articulated the way data and networks would transform warfighting.[9] This appreciation translated into the concept of 'Network Centric Warfare', which is a convolution of three domains namely physical; where manoeuvres are conducted, producing data from sensors, the info domain; where data is transferred and archived and the cognitive domain, where data is processed and analysed.[10] After more than two decades since this concept was floated, military leaders and defence experts across the world are now sanguine about it's implementation primarily because of IoT technology maturation. Javelin anti-tank missiles and Switchblade loitering missiles which are being extensively used by Ukrainian ground forces to challenge the mighty Russian armour exemplify the successful implementation of IoT technology in the combat zone.[11]

IoBT should not be looked at with the same lens as that of "just another singular niche technology", rather it engulfs and encompasses a range of many such technologies. Hence comprehending IoBT as an idea is more appropriate and rational.[12] It is the result of the convergence of several intelligent, networked and dynamically constructed devices and technologies that can deliver effects in both physical and virtual space. The goal of IoBT is to administer complex, intelligent systems-of-systems, ubiquitously housing smart sensors and actuators, powered by adaptive learning processes to achieve the Military's strategic and tactical objectives.[13] IoBT grid functions with a varied assortment of sensor nodes wired or wireless, all meshed together. Operations can be coordinated across the network consisting of early warning ground and UAV-based sensors, autonomous weapons, smart soldiers and state-of-the-art command posts. It can perform a dual role of collecting intelligence as well as delivering a kinetic strike. Removing soldiers from the execution loop and placing them in a supervisory position at the highest level, it can enable weapons to assign and engage targets with a high degree of autonomy.[14] It also has the ability to exacerbate the tempo of operations and remove the fog of war.

Advantages Accrued

Future wars will be fought in a highly contested and coercive environment, densely populated by an ensemble of both smart and legacy equipment. This will require accomplishing sprawling responsibilities of collating, corroborating, disseminating and collaborating actionable information with both men and machines.[15] IoBT system can function as an integration platform for these devices and men, helping commanders to shorten the OODA loop and make informed decisions. Some of the advantages that can be accrued by introducing IoT on the battlefield are listed below:-

- **Autonomous Systems**. IoT will act as a catalyst to automate the process of warfighting; from ISR to weapon platforms to Decision Support System all facets of ops can cohesively function without human intervention.

- **Tempo of War**. Increased autonomy in weapon platforms shifts human control from execution to a supervisory role. The process of making a decision to execute the command can be accomplished in split seconds, accelerating the tempo of war.

- **Reduced Attrition**. With the application of remote supervisory oversight better situational awareness and lesser foot on the ground can be achieved, resulting in a lower casualty rate of own troops.

- **Precision Strikes**. Weapons can be guided more precisely to their intended target via an IoT network using both onboard and offboard sensors. Automated control loops outperform soldier-controlled, sight-and-aim weaponry in terms of speed and accuracy. By integrating disparate weapon types IoT increases the enemy's attack surface.

- **Effective ISR**. Wide-ranging unmanned and dispersed sensors can be meshed together over IoT networks. Additionally, IoT gathers data by monitoring software programs, sniffing networks and accessing databases. Such networks provide a more comprehensive, multi-view and continuous observation of a space, event or activity.

- **Dispels the Fog of War**. During operations when sensors and early warning elements are destroyed or data and sitreps become unreliable, a commander's vision of the events unfolding in front becomes obscured. This fog of war that engulfs decision-making can be dispelled by IoT technology, which constructs dynamic self-healing, adaptive and resilient information sources over secured communication channels. Even amid the melee of battle, better situational awareness can be ensured using these capabilities.

- **Intelligent Processing**. IoT enables sophisticated processing to increase the capacity for human observation. It can spontaneously plan and autonomously execute actions. To ensure that commanders on the battlefield are not overwhelmed by the flow of information, smart processing offers the necessary component for ingesting, filtering, prioritizing, and abstracting it. IoT transforms Data into Info, Info into Awareness, Awareness into Plans and Plans into Action.

- **Agile Logistics**. IoT can supercharge operational logistics by achieving just-in-time and just-in-case supply chains. By convoluting sensors, actuators and monitoring algorithms IoT can keep track of what, where, when, and how much is needed in real-time. Conditioned-based maintenance is another paradigm that can be explored by harnessing IoT technology which can enhance productivity, reduce expenses and improve op reliability.

- **Interfacing Legacy Systems**. IoT networks can join legacy stovepipe systems by using inexpensive sensors, control systems and automatically compiled software. Gateways can be created as an interface between contemporary and legacy platforms to optimally utilise resources at the disposal of theatre commanders.

- **Technology Adaptation**. IoT facilitates quick and inexpensive adaptation of technology because of its ability to introduce new and improved components in existing networks. This facilitates incremental upgrades, distributing the associated costs and enabling continual development to keep abreast with the changing technology paradigm.

Use Cases

With the immense potential that IoT offers for its military usage, its application in tactical battle areas appears to outshine and promises to deliver rich dividends. In network-centric operations scenario, the employability of IoBT can seamlessly and effectively integrate all the available resources at the disposition of the battlefield commander, which can aid in making informed decisions. Some possible application areas are briefly described below.

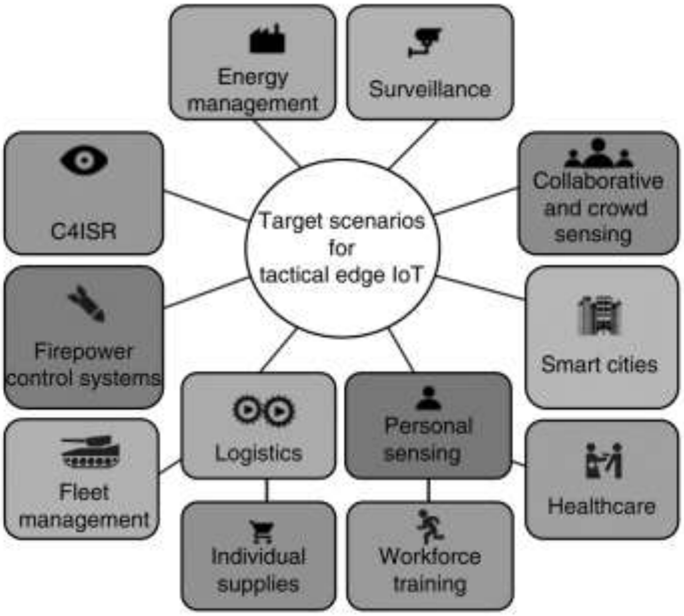


Figure 1: Target Scenarios for Tactical Edge IoT in Defence

Source: https://www.researchgate.net/ profile/Paula-Fraga-Lamas/publication/309404867/figure/fig2/ AS:614078204612624@1523419061829/Promising-target-scenarios-for-defense-and-public-safety.png

- **C4ISR**. An integrated network of IoT sensors deployed across a variety of platforms can provide improved situational awareness in a contested and coercive environment.[16] The amalgamation of ground and aerial sensors, surveillance satellites and also soldiers having a foot on the ground is bound to collect a variety of data. Such information can be filtered, processed, collated, corroborated and conserved in a platform, which regulates critical data transmission up and down the chain of command, allowing better battlefield coordination, command and control.

- **Weapon Control Systems**. The possibility of having an autonomous weapon system and fire control is being explored using sensor networks, machine learning and advanced AI analytics. Such a sensor shooter grid can provision precisely targeted firepower delivery and completely automated responses to attacks in real-time.

- **Op Logistics**. Effective fleet management and efficient shipment tracking can be easily achieved by harnessing smart sensors, RFID tags and M2M communication. Edge IoT devices can augment real-time tracking and provisioning of ordnance, critical supplies, ration and clothing. As consumption patterns are being monitored push model of provisioning supplies based on the inherent priority and necessity can be implemented, greatly improving op efficiency.

- **Man Management**. Wearable IoT sensors can be embedded within combatants' personal equipment like small arms, helmets, clothing, back-pack etc. enabling ubiquitous physical activity tracking and operational data gathering. Using context-aware data to infer and track soldier's health parameters and psychological state during operations in real-time may provide crucial insight and help in taking preventative measures for force conservation.

- **Training**. IoT can also find utility in providing enhanced training and war gaming experience. The IoBT concept can be integrated into military training to create more realistic, adaptive and effective preparation for future operations. Wearable sensors can be exploited to track the physiological and cognitive states of soldiers undergoing training which allows the conveyance of tailored feedback and personal optimisation.

- **Power Management**. Managing power requirements in the theatre of operation remains an underrated area but with the increased introduction of electronic devices in the battlefield, power and energy management will pose some serious challenges in planning and executing future operations. Employing predictive algorithms and real-time IoT data can significantly save military energy effort and help understand usage patterns.

- **Smart Surveillance**. Advanced Audio Visual and seismic sensors along with visual AI and pattern recognition techniques can facilitate the establishment of a smart surveillance and monitoring grid which can span not only over the ground but also the maritime environment. IoT solutions make it possible to sense and forecast ecological conditions thus keeping tabs marine operations over wide areas.

- **Collaborative & Crowd Sensing**. Mobility and manoeuvrability of tactical resources present a unique set of communication challenges in the modern battlefield. Collaborative sensing refers to the process of disseminating sensor data among mobile devices, often using dependable short-range communication.[17] IoT nodes can utilise idle sensors to augment their own sensing needs. Any ad-hoc ISR missions can be facilitated by matching sensors with task assignments. The available sensing and communication resources at the disposition of operational commanders can therefore be optimally utilised.

Implementation Challenges

Along with the benefits of employing IoT in the battlefield comes unique challenges. Designing and implementing IoT network in a war-like scenario is a challenging task that necessitates a thorough comprehension of both standard cybersecurity issues and complex ethical issues related to military applications.[18] IoT devices are mandated to operate in harsh hostile conditions muddled with misinformation and deception. Because these networks are deployed in dynamic and hostile battlefield conditions, they are extremely vulnerable to cyber assaults. It is crucial to understand that IoBT networks bring a surfeit of security issues that go beyond traditional IT settings.[19] These networks are made to connect a wide range of equipment from sensors and unmanned vehicles to soldier-worn gadgets.

One of the principal security concerns in IoBT networks is the vulnerability of connected devices. The growth of IoT devices in the military space increases the attack surface and provides enemies with multiple points of entry, as each device has its own set of sensors and communication protocols.[20] IoT enhances defence efforts, but if an IoT system is compromised, it can also intensify harm done by the enemy. IoT components are networked by design, in the event of a single node getting compromised, it could have a cascading effect, jeopardising the others. Safeguarding the integrity of specific IoT nodes does not assure the integrity of the network due to system interdependence and emergent behaviours.[21] Securing these devices requires implementing robust authentication methods, encryption protocols, and regular security upgrades to obviate the threat of unauthorised access and exploitation. Moreover, the issue of data transmission security arises from IoBT network's dependence on wireless communication. Communication routes may be attempted to be intercepted, manipulated, or disrupted by adversaries, endangering the integrity and confidentiality of critical data.[22]

To combat these attacks and guarantee that mission-critical data is secured, it is imperative to implement secure communication protocols and modern encryption standards. Another security threat that defence forces and security agencies should be vary of is identifying and guarding against embedded threats. The hardware components are exported from different countries, and the equipment suppliers maybe located in a specific country but may be utilising manufacturing facilities of another country, therefore, it is quite challenging to govern foreign manufactured components and also determine what constitutes an overseas source.[23]

Given the possible repercussions of security breaches in military operations, ethical considerations in IoBT networks are critical. Privacy and ethical information management become more important because of the colossal volumes of data getting collected and used via sensors and devices. A delicate ethical dilemma is finding a balance between the collection of actionable intelligence and the protection of people's right to privacy, particularly during CI/CT operations and zones where civilians and military coexist.[24] In addition, the introduction of autonomous systems into IoBT networks presents decision-making-related ethical conundrums. For example, split-second choices with big ramifications would be needed for autonomous weapons, smart munitions and drones. To avoid unintentional harm and collateral damage, it is important to make sure that these systems follow moral precepts like discrimination and proportionality.[25] The effect that IoBT sensor networks may have on the civil population is a further ethical consideration. Inadvertently putting civilians in danger might occur when military IoT devices are placed during contested or urban warfare. Minimising damage to civilians, guaranteeing the prudent application of monitoring technologies and integrating moral principles into military policies require detailed study, analysis and planning before making any IoBT deployment.

Way Ahead

To have a future-ready fighting force it is important for nation states to explore and invest in emerging technologies; however, the gestation period for developing and inducting any new combat-ready equipment or system is fairly long. The sluggish pace of progression and related research and development cost are significantly higher as compared to Commercial off-the-shelf (COTS) available devices. IoT devices based on commercially available open-source and proprietary technologies are developing rapidly. It is possible to acquire and deploy technology in a quicker timeframe by using COTS IoT devices. The promise of system dependability, reliability, security, redundancy, portability and consistency in the theatre of battle can be achieved by tweaking these devices to military-grade specifications and standards.[26] Presently commercial IoT technology is substantially ahead of the defence IoT. Focussed efforts from government and industry optimising commercial investment to meet specific needs of defence forces is the need of the hour. Stakeholders involved in national security should engage with both industry and academia to stay updated with the rapidly evolving technological landscape, given the widespread availability of commercial IoT solutions.

Handling the colossal volume of data that IoBT sensor network can churn during active operations will require data filtering, refining and processing within the network. Such processing methodology also extends elastic multi-vantage multi-modal authentication of the IoT device's health and threats. Another idea that's garnering a lot of attention is CPDDS or the Design for Cyber-Physical Data-Driven Systems. Broadly stating, it is an embedded system in which computing units use feedback loops to connect with sensors and actuators in the real-world environment as well as each other. Applications for CPDDS can be found in vital infrastructure, including the distribution of fuel, water, electricity grid and transportation. In IoBT unmanned autonomous systems can be designed using this principle.[27] CPDDS can ensure information assurance encompassing verifiable safety, dependability and credibility. Assurance is also necessary for the system as a whole to guarantee the accuracy and security of decisions that follow, as well as for the interconnection of the networks, which frequently need to transfer data over poor communication channels.

Traditional cyber security measures involve implementing access control mechanisms and network security protocols at physical and network layers. However, transposing a similar template for IoBT devices will require hardware modifications and firmware updates making it inefficient with respect to both time and cost. SDN i.e. Software Defined Networking is a novel technique to overcome these issues. It provides an agile framework to efficiently and effectively manage large networks. SDN tends to separate control and data planes thus injecting flexibility into the network.[28] This augment in creating network layer security systems which are flexible and dynamic. The method of least privilege should be adopted while designing access control system for IoBT devices, as it negates the asymmetric nature of access control violations. The scale of the network and severe resource constraints pose unique challenges that IoBT devices must function under; therefore it is necessary to evaluate the conservative approach of host vs network-based defences. Due to their very nature IoT devices are unable to support end-point security protection. Hence deployment of an Intrusion detection system yields better dividends than employing legacy anti-viruses and firewalls on an IoBT network.

Ethical issues pertaining to use and misuse of IoBT necessitate the adoption of accommodative doctrine and policies, ensuring that the country exploits technological benefits while preventing the prospective for damage to the civil populace. In a democracy this will require consent of the people who consume or are subjected to the technology.[29] Transparency, accountability and security are some of the tenants that consent is built upon and cannot exist without. It is also necessary to preserve the integrity and security of the supporting data of an IoT system. This includes the history of its own processing activities and perceived results of those activities in addition to the extracted data. Records of disclosure statements, reviews, audits, and patches/ updates are a few examples of collateral information. Preserving the authenticity of the data demands not just keeping it safe but also ensuring it is properly recorded, saved and archived.

Conclusion

IoT is an innovative technology that should be harnessed to increase military operational efficacy and efficiency. IoBT is a network of sensors, actuators, wearables and portable IoT equipment that uses state-of-the-art computing to link soldiers with smart technology and build an integrated, coherent, and cohesive fighting force. Since it is a loosely coupled integration of numerous key technological components, harnessing the potential of IoBT in the modern battlefield requires a through understanding of the opportunities and challenges being presented by it. From the commander's perspective, IoBT can be alluded to as a smart and adaptive common operating platform that can accomplish Network Centricity and augment as a force multiplier on the battlefield.

IoT systems and devices will need to function independently in the modern battlefield to reduce the cognitive strain on warfighting soldiers and prevent human error brought on by coercive environments. On the other hand, little study has been done on how to allow IoBT systems and devices to function independently while yet being aware of their surroundings and able to make wise choices. The focus area for modernizing the IoBT should be on decision process multipliers, underlying technology interactions and scientific cross-technology experimentation.

The review has highlighted the potential benefits of implementing contemporary IoT concepts in military settings, while also acknowledging the unique challenges posed by tactical battlefield environments and adversarial conditions. These issues and challenges merit attention and require smart innovative solutions to ensure successful implementation of IoT technology in military operations.

****

Lt Col Rachit Ahluwalia was commissioned in Corps of Signals in March 2003. He holds an Mtech Degree in Computer Science and is pursuing PhD in IoT. The officer is currently posted at MILIT, Pune as Instructer Class 'A'.

NOTES

[1] Satyajit Sinha, "State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally," *IoT Analytics*, January 26, 2024, https://iot-analytics.com/number-connected-iot-devices/.

[2] Somayya Madakam, R. Ramaswamy, and Siddharth Tripathi, "Internet of Things (IoT): A Literature Review," *Journal of Computer and Communications* 03, no. 05 (January 1, 2015): 164–73.

[3] Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future Generation Computer Systems* 29, no. 7 (September 1, 2013): 1645–60.

[4] Abdelzaher, Tarek, Nora Ayanian, Tamer Basar, Suhas Diggavi, Jana Diesner, Deepak Ganesan, Ramesh Govindan, et al. "Toward an Internet of Battlefield Things: A Resilience Perspective." *Computer* 51, no. 11 (November 1, 2018): 24–36.

[5] Zhu, Lin, Suryadipta Majumdar, and Chinwe Ekenna. "An invisible warfare with the internet of battlefield things: A literature review." *Human Behaviour and Emerging Technologies* 3, no. 2 (November 29, 2020): 255–60.

[6] Poltronieri, Filippo, Laurel Sadler, Giacomo Benincasa, Timothy Gregory, John M. Harrell, Somiya Metu, and Christine Moulton. "Enabling Efficient and Interoperable Control of IoBT Devices in a Multi-Force Environment," October 1, 2018.

[7] Feng, Yuan, Menglin Li, Chengyi Zeng, and Hongfu Liu. "Robustness of Internet of Battlefield Things (IoBT): A Directed Network Perspective." *Entropy* 22, no. 10 (October 16, 2020).

[8] Alexander Kott, Ananthram Swami, and Bruce J. West, “The Internet of Battle Things,” *Computer* 49, no. 12 (December 1, 2016): 70–75.

[9] Owens, William A. “The Emerging U.S. System-of-Systems.” *Strategic Forum*, February1, 1996. https://www.questia.com/library/journal/1G1-130124286/the-emerging-u-s-system-of-systems.

[10] Zheng, Denise E., and William A Carter. *Leveraging the Internet of Things for a More Efficient and Effective Military*. Rowman & Littlefield, 2015.

[11] Leigh Kaplan, “Loitering Munitions in Ukraine and Beyond - War on the Rocks,” War on the Rocks, April 21, 2022, https://warontherocks.com/2022/04/loitering-munitions-in-ukraine-and-beyond/.

[12] Stephen Russell, Tarek Abdelzaher, and Niranjan Suri, “Multi-Domain Effects and the Internet of Battlefield Things,” November 1, 2019.

[13] Reza Tadayoni, Anders Henten, and Morten Falch, “Internet of Things — The battle of standards,” November 1, 2017.

[14] Alberts, David S., John J. Garstka, and Frederick P. Stein. “Network Centric Warfare: Developing and Leveraging Information Superiority.,” February 1, 2000.

[15] Neag, Mihai-Marcel, and George Mogoş. “Challenges and Opportunities of the Network-Centric Warfare on the National Defense System of Romania.” *Land Forces Academy Review* 25, no. 1 (March 1, 2020): 15–21.

[16] Ming-Jing, Lu. “Conceive on Modeling Platform in Training Simulation System of C4SIR.” Jisuanji Fangzhen, January 1, 2013.

[17] Sejun Song et al., “Effective Opportunistic Crowd Sensing IoT System for Restoring Missing Objects,” June 1, 2015.

[18] Alexander Kott, David S. Alberts, and Cliff Wang, “Will Cybersecurity Dictate the Outcome of Future Wars?,” Computer 48, no. 12 (December 1, 2015): 98–101

[19] Lin Zhu, Suryadipta Majumdar, and Chinwe Ekenna, “An invisible warfare with the internet of battlefield things: A literature review,” *Human Behavior and Emerging Technologies* 3, no. 2 (November 29, 2020): 255–60.

[20] Pedro Miguel Sánchez Sánchez et al., “SpecForce: A Framework to Secure IoT Spectrum Sensors in the Internet of Battlefield Things,” *IEEE Communications Magazine* 61, no. 5 (May 1, 2023): 174–80.

[21] U. Rahamathullah and E. Karthikeyan, “A lightweight trust-based system to ensure security on the Internet of Battlefield Things (IoBT) environment,” *International Journal of System Assurance Engineering and Management*, September 3, 2021.

[22] Federico Mancini and Frank T. Johnsen, “A Novel IoBT Security Assessment Framework: LoRaWAN Case Study,” January 1, 2020, https://ffipublikasjoner.archive.knowledgearc.net/handle/20.500.12242/2909.

[23] Sharjeel Riaz et al., "Malware Detection in Internet of Things (IoT) Devices Using Deep Learning," *Sensors* 22, no. 23 (November 29, 2022): 9305.

[24] Rita Francese, Maria Frasca, and Michele Risi, "Are IoBT services accessible to everyone?," *Pattern Recognition Letters* 147 (July 1, 2021): 71–77.

[25] Fiona Carroll, Ana Calderon, and Mohamed Mostafa, "Ethics and the Internet of Everything: A Glimpse into People's Perceptions of IoT Privacy and Security," in *Springer eBooks*, 2012, 3–29.

[26] Pradhan, Manas, Fahrettin Gokgoz, Nico Bau, and Daniel Ota. "Approach towards application of commercial off-the-shelf Internet of Things devices in the military domain," December 1, 2016.

[27] Niggemann, Oliver, Gautam Biswas, John S. Kinnebrew, Hamed Khorasgani, Sören Volgmann, and Andreas Bunte. "Data-Driven Monitoring of Cyber-Physical Systems Leveraging on Big Data and the Internet-of-Things for Diagnosis and Control.," January 1, 2015, 185–92.

[28] Kim, Hyojoon, and Nick Feamster. "Improving network management with software defined networking." *IEEE Communications Magazine* 51, no. 2 (February 1, 2013): 114–19.

[29] Draetta, Laura, and Caroline Rizza. "The 'silence of the chips' concept: towards an ethics(-by-design) for IoT." *International Journal of Information Ethics* 22 (December 1, 2014): 23–31.

PREPARING FOR QUANTUM WARFARE

Maj Gen AK Srivastava, VSM (Retd)

Abstract

In the ever-evolving realm of present day warfare, the emerging and disruptive technologies play a vital role in shaping of military strategies. In this context, it is imperative that military commanders at all levels must be conversant with new developments in technological domain to maintain a right balance of weapons, equipment and the warfighters. One such emerging and potent technology is Quantum Technology which has seen tremendous focus in the recent past. Quantum technologies are proving to be very potent for military domain, promising to provide technological capabilities far beyond the present landscape. The technology is already on the path towards revolutionising the fields of Quantum Computing, Quantum Sensing, Quantum Communications, Quantum Imaging and Quantum Navigation. Quantum technologies for specific military applications, introduce new capabilities, increasing effectiveness and improving precision and have led to the emergence of 'quantum warfare'.

In the article, we take a glimpse of the quantum technologies, understand their importance for our armed forces and explore major defence applications. A brief review of the initiatives taken for indigenous development of the technology has been carried out with recommendations to address the global challenge of Quantum Warfare.

Introduction

Quantum technology is an upcoming field of applied physics and engineering, which harnesses the properties of quantum mechanics and unique phenomena like quantum superposition, quantum entanglement and quantum tunneling.

A quantum is described as the smallest measurable quantity of matter or energy. Thus, in case of electricity, a quantum is an electron and in case of light, a quantum is a photon. Classical physics and Newton's laws of motion can accurately explain the behaviour of objects that are larger than atoms and molecules. However, classical physics goes wrong in explaining the behaviour of sub atomic particles. The advent of Quantum physics has not only resolved the imbroglio but has also led to the development of all powerful Quantum Technologies.[1]

Dual Behaviour of Matter and Radiation

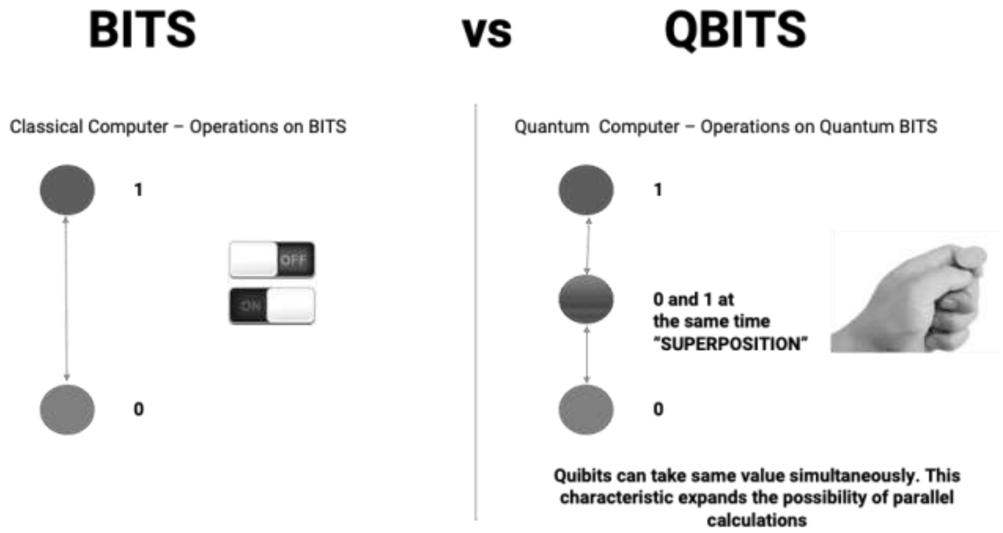
Sub-atomic particles like electrons, being matter, exhibit particle like behaviour. However, simultaneously they also exhibit wave nature. Particles larger than atoms also have associated wave nature but the wave component is negligible due to large mass. The sub-atomic particles have very small mass and hence both particle and wave like behaviour are dominant in them. This is known as dual behaviour of particles and defined by De-Broglie relationship, a mathematical explanation of the phenomena. Dual nature is not only applicable to sub atomic particles but also applicable to electromagnetic radiation. EM waves demonstrate the properties of wave as well as of particle. According to electromagnetic wave theory, the energy is emitted or absorbed continuously whereas, according to Plank's theory, energy is emitted or absorbed discontinuously i.e. in packets called Quantas.[2]

Some unique phenomena of Qauntum Technology which are harnessed for the applications are briefly explained in the succeeding paragraphs.

Quantum bit or Qbit

In conventional computing, coding of data is carried out using a binary bit, which takes the values of "0" or "1" at a time. In Quantum technology, the basic unit of information is a quantum bit or Qubit. A qubit is a two-level system, which can attain two values of any physical property. There can be many systems which can qualify as a Qubit. A quibit can be an electron in which its spin in two opposite directions can be considered as two values. Similarly, in case of a photon, its polarization degree can have two values, say, horizontal and vertical.[3]

A qubit uses the quantum property of superposition to be simultaneously in two states. A qubit can signify '0' and '1' at the same time and a system having two qubits can represent four states at the same time (00, 01, 10, 11). Consequently, quantum computing of a two qubit system will be four times faster than a two bit classical computing. Accordingly, In case of 'n' bits, the speed will increase to 2^n times. If n =56, then 2^56 is of the order of 'Trillions'. It is expected that quantum computers, in future, may be million times faster than a super computer.


BITS
vs
QBITS
Classical Computer – Operations on BITS
1
OFF
ON
0
Quantum Computer – Operations on Quantum BITS
1
0 and 1 at
the same time
"SUPERPOSITION"
0
Quibits can take same value simultaneously. This characteristic expands the possibility of parallel calculations

Source: Properties of Quantum Computing, Drishti IAS,
URL: https://www.drishtiias.com/mains-marathon-daily-answer-writing-

practice/papers/2022/quantum-computing-different-conventional-computing-discuss-applicability-challenges%C2%A0paper-3-science-and-technology/print

Superposition

In quantum technology, a phenomena that permits quantum objects to simultaneously exist in more than one state is known as Superposition. This implies that an object can be in two states at the same time while remaining a single object. Superposition permits the qubits of the quantum technology to carry out multiple simultaneous operations, making them exponentially faster than classical computers. Superposition enables quantum algorithms to perform operations in a much shorter time as compared to the conventional supercomputers to solve certain problems.[4]

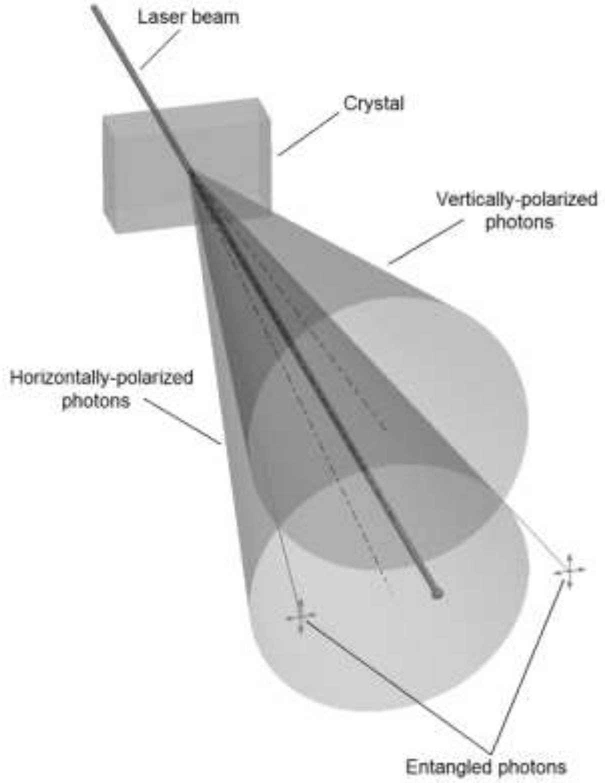
Quantum Entanglement

Quantum entanglement is an occurrence in which two or more subatomic particles interact with each other in such a way that that their quantum states get dependent on each other. The particles continue to remain entangled even when they move away and are large distance apart.[5]

Entanglement can take place between quantum particles like electrons or photons. When this happens, the state of one particle gets dependent on the other. Any change in the state of one particle has instant effect on the other whatever may be the distance between them. This phenomena is a very important aspect in quantum information technologies.

There are many methods which have been invented for achieving quantum entanglement. For example one popular method of achieving quantum entanglement of two photons is 'Spontaneous Parametric Down Conversion' which is explained in the diagram below.[6]

Spontaneous Parametric Down-Conversion



Source: Logan P. Kaelbling , Production of Entangled Photons via Spontaneous Parametric Down-Conversion, URL:https://digitalcommons.bard.edu/cgi/viewcontent.cgi?article=1359&context=senproj_s2020#:~:text=Spontaneous%20parametric%20down%2Dconversion%20is,converted%20photons%20in%20its%20place/

This spontaneous parametric down-conversion diagram illustrates a Laser beam passing through a crystal's optical axis which leads to photons' diffractions and polarizations leading to quantum entanglement. Measurements carried out on entangled photons proved beyond doubt that the properties were perfectly interrelated.

Nobel Prize for Physics for the year 2022 was awarded to three scientists John Clauser, Alain Aspect and Anton Zeilinger for their work in quantum entanglement, who experimentally proved and validated the phenomena. This phenomena has proved to be very useful in reducing the time for processing information transfer between qubits. Long back in 1935, this phenomena was demonstrated to Einstein, who called it "a spooky action at a distant" as it was against the laws of classical physics.[7]

Quantum Computing

Quantum computers utilise the unique principles of quantum science to achieve very high computational power and ability to store huge volumes of data. They are proving to be exceptionally advantageous and faster than conventional supercomputers for certain type of tasks.

Present day computers encode data using binary bits which can be either "0" of "1" at a time. As we have seen, the basic unit of memory in a quantum computer is a quantum bit or qubit. Quantum bits can acqure many arrangements simultaneously. Qubits can also get into quantum entanglement and can represent different information at the same time.

For example, a conventional computer requires eight bits for representing any number between 0 and 255. However, eight qubits can represent every number between 0 and 255 at the same time. A 100-qubit quantum computer can carry out more than 1,000 billion billion billion simultaneous calculations. Where there are large number of possible combinations, quantum computers can process them simultaneously. On the other hand, there are certain other types of computing where classical computers will continue to perform better in the immediate future.[8]

As of now, quantum computers are very noisy and sensitive to the environment. The present day quantum computing technologies are being called Noisy Intermediate-Scale Quantum Computing (NISQ). Sensitivity to electromagnetic fields, heat, and collisions with air molecules can cause a qubit to lose its properties and collapse. This phenomena is called quantum decoherence and may cause a system to crash. The problem is more severe as the number of qubits increase. Quantum computer components are being designed to protect the qubits from interferences by shielding and keeping them at very low temperatures.

Just as in conventional computers, quantum computers consist of hardware and software. There are three main constituents of quantum hardware. The data plane is the core of the quantum computer and houses qubits. The control plane performs the task of transferring signals to qubits. The control processor plane runs programs. The host processor interacts with the quantum software and sends signals to the control and measurement plane.

Quantum software runs quantum algorithms using quantum circuits. Developers use software development tools and libraries to code quantum algorithms.

Types of Quantum Technology

Rapid advancements are taking place in the development of quantum technologies. Efforts are on to take the quantum computers from the present day NISQ level to fault tolerant computers. Brief example for some of the qubit technologies are given in the succeeding paragraphs.[9]

Gate Based Ion Trap Processors use charged atoms (ions) based qubits which are housed on micro fabricated trap controlled by electric field and managed by laser beam. They work more efficiently at cryogenic temperatures. Gate Based Superconducting Processors use qubits built on superconducting circuits which also work on cryogenic temperatures. Other technologies being used are Photonic Processors using light pulses, Neutral Atom Processors which work at room temperature, Rydberg Atom Processors and Quantum Annealers which allow larger number of qubits in the system compared to other methods.

Military Applications of Quantum Computers

Applications where quantum computers are making considerable impact and their upcoming military usage are discussed in succeeding paragraphs.[10]

- **Quantum Computing.** Military applications of Quantum Technology are under research and development. Quantum computing is one of the areas which is considered capable of exponentially increasing the speed and computing power. The storage and computing of large volumes of data is likely to be much more efficient as compared to conventional computers. This can have a very positive influence on military operations, due to the ability of quantum computers to process colossal amounts of data with speed and precision. It is also likely to enhance the capabilities of Big Data Analysis which is again very important for the defence forces.

- **Quantum simulation.** Quantum computers are highly efficient for modeling as they employ quantum technologies in their computation. They are more capable of dealing with complex and ambiguous problems compared to conventional computers. Thus, they can be very gainfully employed to augment our capabilities in war gaming and constructive simulation.

- **Cryptography.** Complex algorithms used in cryptography can be implemented with greater efficiently using quantum computers. This will also provide more capabilities in breaking of crypto algorithms providing opportunities as well as challenges.

- **Optimization.** It is the method of arriving at the most optimum solution to a problem with given inputs and desired outputs. The method is used for critical decision making. For example, the factors can be manpower, cost, quality, and time. The factors can be optimized for an optimum output. Using quantum based algorithms, solutions have been found which were earlier not feasible. There is tremendous scope for using quantum optimization in sensor deployment, target detection, transportation, logistics and defence production.

- **Quantum machine learning and AI.** Quantum technology provides the potential of enhanced machine learning and more efficient AI.

- **Search.** Quantum algorithms are tremendously speeding up searches of unstructured data, carrying it out in lesser steps compared to traditional algorithms.

Quantum Communications

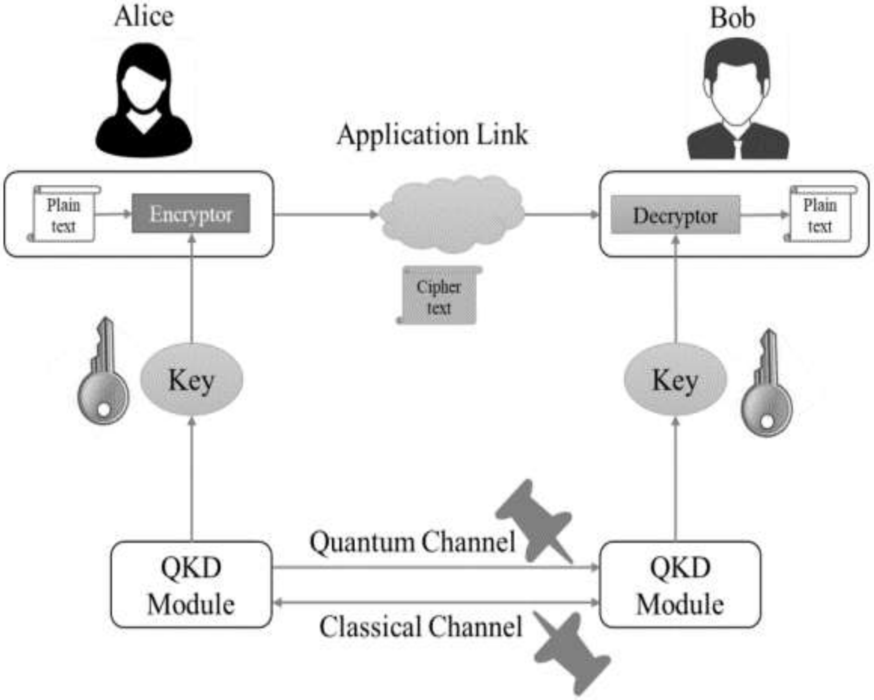
Quantum communication is a promising and rapidly growing field of quantum technology which takes advantage of quantum principles to provide high level of data security. Quantum information exchange is achieved by using a photon as qubit as the carrier of data and transmission of quantum states. Commonly used channels for information exchange are low loss optical fibre cable or free space channels.

The high level of security is provided by using the property of fragile nature of entangled photons or qubits. In case these entangled qubits are interfered with, they immediately collapse to zero state and carry not information further. Thus the receiver detects the interference and the qubit is rejected. In effect, if a hacker tries to tamper with a qubit, the network will get alerted.[11]

We will discuss some underlying technologies which make quantum communications highly secure and resilient.

Quantum Key Distribution

The conventional encryption systems with asymmetric encryption keys are vulnerable to hacking. QKD provides solution to the problem as it is considered to be super secure. In QKD system, only the encryption keys are sent in quantum state using qubits. Once the keys are perfectly shared, the encrypted data is transmitted using classical bits over insecure networks.



Source: Quantum Key Distribution Source: Martin Giles, “What is Quantum Communication?”, MIT Technology Review, 14 Feb 2019. https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/

There are many protocols which have been developed for QKD. BB84 is one such QKD which is already in use. Understanding its working will clear the concept of QKD. Suppose, there are two persons Alice and Bob. Alice wants to transmit information securely to Bob. For this, she generates an encryption key as sequence of qubits which are sent to Bob through a quantum channel and measurement data through classical channel. With this information, he is able to decode the key. In case there is any attempt to intercept the signal, some of the qubits collapse and the receiver gets alerted. In that case they reject the key and generate a new key and accept only when there is no indication of attempt to intercept. Alice can now encrypt the data with her keys and send it in classical bits to Bob, who, in turn decodes the data with his keys.[12]

There are a number of QKD networks being establish world over. China has established the longest link extending over 2,032 km from Beijing and Shanghai. In the US, a company named Quantum Xchange has been tasked to establish a 500 miles link of OFC along the East Coast to create a QKD network. The project will link Manhattan with New Jersey.

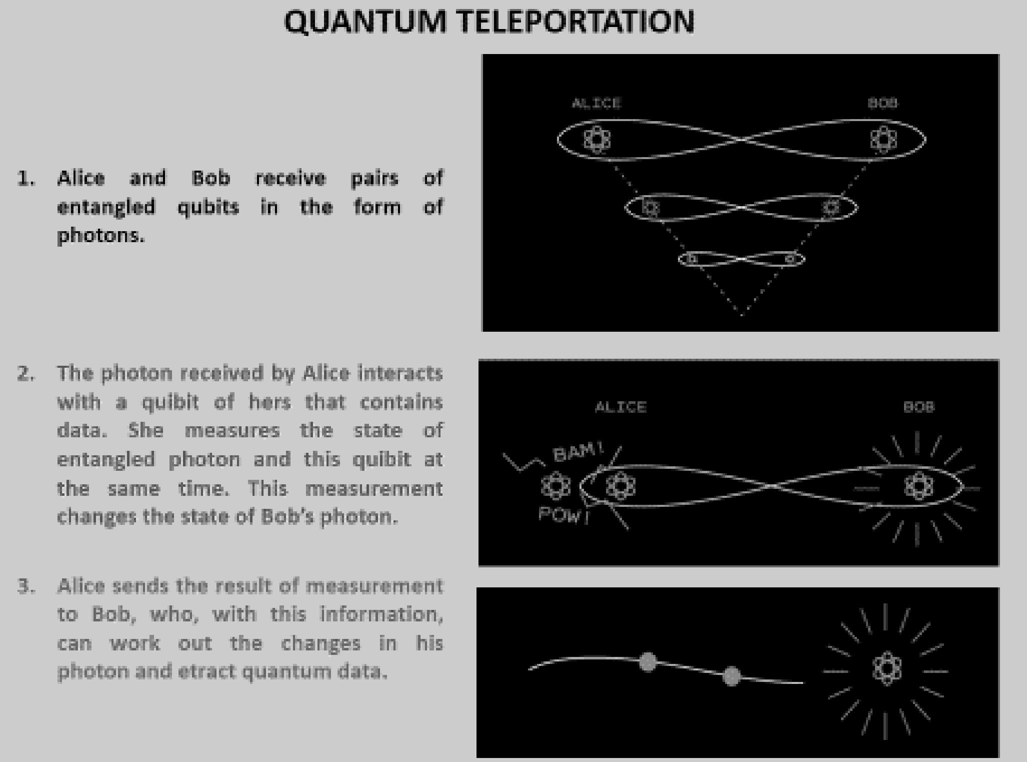
Quantum Repeater

Due to absorption of photons in OFC, the range of communications gets restricted. Hence repeaters are required along the cable to amplify the signal. QKD networks also need to establish "trusted nodes" at various points. The Beijing-to-Shanghai network has 32 such nodes. At these nodes, quantum keys are decrypted and then re-encrypted in a new quantum state for transmission to the next node and here lies the vulnerability. A hacker can copy the decrypted keys without leaving a trace.[13]

The above vulnerability can be overcome if we use quantum repeaters where quantum processors enable the keys to remain in quantum form while they are amplified and retransmitted. Such repeaters have been created in the labs, but no working model has so far been deployed. To take care of the QKD vulnerabilities, there is another very advanced solution called quantum teleportation.

Quantum Teleportation

Quantum teleportation is a very innovative technology for transmitting data in pure quantum form. This technology is based on the principle of quantum entanglement. Here, entangled photons pairs are created. One photon of this pair is transmitted to Alice who is sender of data and the second photon is transmitted to Bob, the receiver. Alice, on receiving her entangled photon, allows it to interact with a "memory qubit" that houses the data to be transmitted to Bob. This exchange alters the state of her photon, and since Bob has the entangled photon, its state also changes simultaneously. Thus, the data in Alice's memory qubit from her photon is "teleported" to Bob's photon from where it is extracted. The graphic below lays out the process:[14]



QUANTUM TELEPORTATION

1. Alice and Bob receive pairs of entangled qubits in the form of photons.
2. The photon received by Alice interacts with a quibit of hers that contains data. She measures the state of entangled photon and this quibit at the same time. This measurement changes the state of Bob's photon.
3. Alice sends the result of measurement to Bob, who, with this information, can work out the changes in his photon and etract quantum data.

Source: Martin Giles, "What is Quantum Communication?", MIT Technology Review, 14 Feb 2019. https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/

The technology is complex and poses many challenges. However, tremendous efforts are being made as it promises great benefits in quantum communications.

Quantum Internet

Quantum internet will be similar to conventional internet with the difference that it will be supported by quantum communication network. Quantum internet is not likely to replace the entire present day internet. Conventional internet will continue to be used for not very sensitive information and quantum internet will be used for data requiring high grade of security.

China is making very fast progress in quantum technologies and quantum network. It launched Micius, a quantum communication satellite and through this satellite, they demonstrated world's first video conference secured by QKD between Beijing and Vienna as long back as 2017. They have linked one ground station connecting the satellite with Beijing to Shanghai terrestrial network[15]

Free Space Quantum Communications

The free-space quantum channel is more challenging compared to optical fibre. The ranges of optical photons are limited in free space due to strong atmospheric attenuation. Hence, the commonly established quantum networks make use of quantum satellites as the losses in satellite–ground link is lesser compared to the loss between two ground stations at a distances. Optical photon communication in free space for short distances is possible with the use of drones. Information is transmitted using the method of Quantum Teleportation.

Quantum Sensing

Quantum Sensing is advanced sensor technology that uses the principles of quantum physics. It harnesses the unique quantum phenomena like superposition and entanglement. It greatly improves the accuracy of measurement as data is collected and analysed atomic levels. The sensing is carried out by detecting changes in electric, magnetic fields, and motion.

Collecting data at the atomic level involves extracting information from individual atoms. This enables quantum sensors to be exceptionally accurate, highly detailed and extremely efficient. They are also much more reliable than conventional sensors being less susceptible to jamming and other electromagnetic interference.

Quantum Sensing Fundamentals

There are many quantum technologies which support and enable quantum sensing. These are being discussed below.[16]

- **Superconducting circuits. S**uperconducting Quantum Interference Devices (SQUIDs) are sensing devices which have already been developed and are basis for basis of most sensitive magnetometers. However, they require cryogenic cooling.
- **Atoms and ions.** Atoms contained in an atomic vapor cell or magneto-optical trap (MOT) and ions in a RF trap are used for sensing. These are being used in compact atomic clocks and optically pumped magnetometers (OPMs) Wideband RF sensors use Rydberg states of atoms. MOT is also being used for gravity sensing.
- **Quantum time-keeping and clocks** technologies are vital for communication and navigation.
- **NV diamonds generated qubits** offer the potential for sensing operation at room temperature.
- **Quantum photonics** using single photon are providing increased sensitivity.

Quantum Sensing Applications in Defence

Situational awareness is an extremely important factor on the battlefield which provides the ability to visualize the environment, develop a Common Operating Picture, assess enemy threats, and take informed decisions. Presently, the conventional surveillance devices like radars, satellite imagery, optical and thermal imagers are networked together on the battlefield to achieve data fusion. However, these systems are vulnerable to jamming and interference.

The development of quantum sensing technologies have potential to exponentially enhance the situational awareness capabilities. Quantum sensors will help overcome the complexities and vulnerabilities of present day systems and will provide better accuracy, higher sensitivity, and enhanced ranges. The new capabilities will be more robust and resilient. For example, in the PNT (Positioning, Navigation & Timing) technology, the use of cold atom- based systems provide capability to accurately navigate in GPS denied environment.

There are abundant possibilities of using quantum sensing techniques in defence domain. The potential is diverse and unlimited, though presently there are challenges which need to be overcome. Quantum sensors have the potential of detection, identification and tracking of targets like stealth submarines, providing early warning of ballistic missile launches, providing ultra-accurate navigation etc. Quantum gyroscopes and accelerometers carry out highly precise measurements, thus providing accurate guidance in GPS-denied environment.

Quantum Inertial Navigation is an important quantum sensing application in the defense domain. Our adversary China is known to have developed counter space capabilities including GPS jamming. Our defence forces are heavily dependent on GPS for navigation. In a GPS denied environment, the navigational capabilities will be seriously impacted. Also GPS navigation is not available in underground and underwater areas. To cater for this, Inertial Navigation Systems are provided for military aircrafts, missiles, naval vessels and ground vehicles. INS works by continuously calculating acceleration and rotation to determine location. However, these measurements have certain errors which accumulate over a period of time. Hence they require frequent calibration. INS drifts by about 1,8 km per day for ships and 1.5 km per hour for aircrafts. Quantum sensors promise to overcome the drawbacks of the INS with exceptionally high measurement accuracy. Quantum accelerometers are found to be 50 times more accurate than conventional accelerometers.[17]

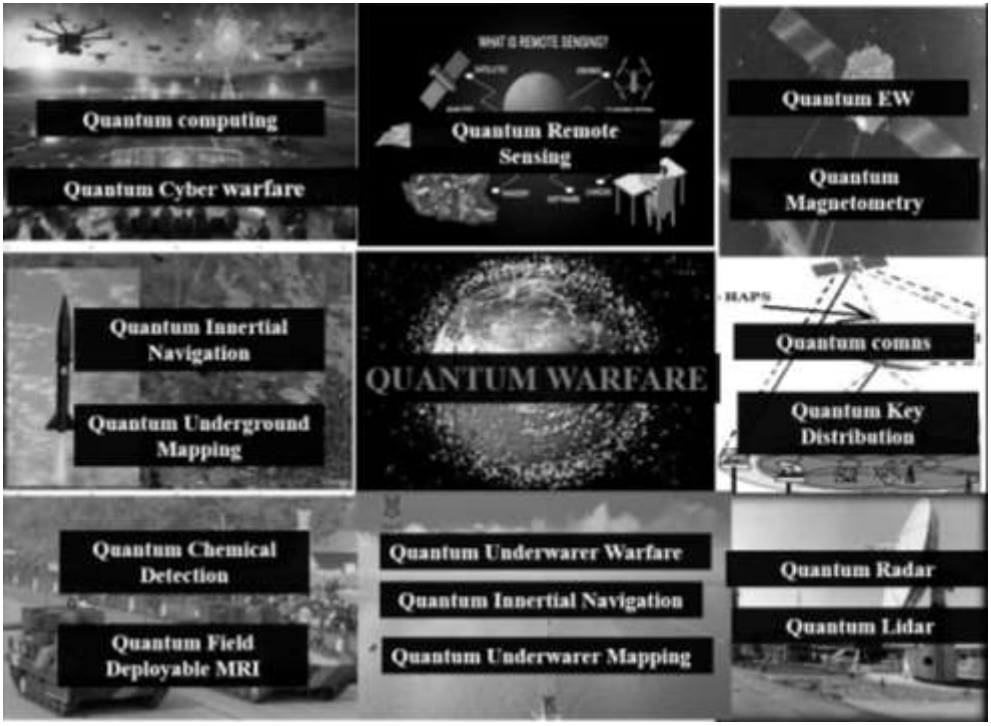
Portable MRI Systems based on Quantum technology use Optically Pumped Magnetometers (OPM) working at cryogenic temperatures. Field deployable version of this equipment is very well suited for treatment of solders in remote operational areas.

Small Sized Ultra Wideband RF Sensors use the quantum technology of Rydberg atoms. US companies, BAE and Infleqtion are developing a 1 cm3 RF sensor capable of detecting signals from 10MHz to 40Ghz.

Gravity Sensing detects changes in gravity gradient, thereby any voids get detected. It uses cold-atom technology. Its ability to detect air pockets underwater and underground is leading to detection of submarines and also IEDs and underground tunnels.

Quantum Warfare

Quantum technologies have the potential to revolutionize the military technological capabilities by bringing in enhanced precision, increased effectiveness and redefining the future warfare. Realizing its importance for the military domain, there has been an increased emphasis on development of these technologies. There appears to be a race amongst the major powers for developing quantum technology as it is leading us into a new technological revolution. Quantum technologies are finding scope for application in entire military domain and spectrum of conflict. The growing competition in this field is emerging as Quantum Race for science & technology and Quantum Warfare for the military. A paradigm of Quantum Warfare is shown in the figure below:



Source: Author

United States passed the National Quantum Initiative Act in 2018 to give boost to quantum R&D. Realising its importance, other counties like Russia, Germany, the UK, France and Canada have also started investing in quantum technologies. China has taken a lead in development and have achieved important milestones. Under the program Quantum Experiments at Space Scale (QUESS) they launched a satellite solely for quantum communication in the year 2016. They have reported success in quantum teleportation, world's first quantum router and setting up quantum-encrypted government network. They have plans to establish a satellite-based quantum communication network.[18]

To remain in the race, India has also made a beginning in development of this technology. Government of India announced National Quantum Mission in April 2023 and allocated an amount of Rs. 7000/- crores for this purpose. NQM has laid down timelines for development of various quantum technologies.

Other initiatives to provide impetus to Quantum Technologies include:-

- Quantum Computing Applications Lab (QCAL) was established by Ministry of Electronics and Information Technology (MeitY) to work in the areas of quantum computing.

- The National Mission on Quantum Technologies and Applications (NM-QTA) was started in 2020 by Department of Science and Technology for developing quantum technology eco system.

- Prime Minister's Science and Technology Innovation Advisory Council (PM-STIAC) has been set up for Quantum Technologies & Applications.

- Quantum Measurement and Control Laboratory (QuMaC) is working for the development of superconducting and nanofabricated electrical circuits to produce quantized "artificial atoms"..

- In Indian Army, a Centre of Excellence has been set up at MCTE, Mhow.

- ISRO's Space Applications Centre (SAC), Ahmedabad, in Sep 2023, successfully established free-space QKD at 300 mtrs, which is a major breakthrough.

- Recently, a joint team OF DRDO and IIT Delhi demonstrated QKD link over OFC.

Though India has made a beginning, it has to go a long way for keeping pace with our adversary China. Focused and sustained efforts are required to speed up the progress. Also, cooperation amongst all agencies are required to achieve synergy at national level to be “Quantum Ready”.

Way Ahead

Quantum technologies are ushering in a technological revolution which can change the nature of warfare. This offers us tremendous opportunities and also pose many challenges. For example, unless we upgrade, quantum computers will be able to break the classical cryptography with ease posing serious threat to national security. [19]

Some recommendations in this regard are given below.

- Maximum emphasis needs to be given to indigenous development with public – private partnership including SMEs, startups and academia.
- Being dual use technologies, there is need to synergise the efforts, within the armed forces, amongst government R&D organisations, PSUs and Industry.
- A focused approach is required for development and manufacture of Quantum hardware as this is a weak area for our country. Cooperation for sharing of knowledge with friendly foreign countries is a must.
- Joint missions and projects with countries for development of systems and projects will be of great help.
- Development of common facilities within the country like infrastructure for simulation and testing is needed.
- Capability building and training should include workforce development, training programs and international cooperation.
- Centres of Excellence for Quantum Technologies must be identified and adequately supported.

- Realistic timelines and monitoring of development must be instituted.
- Enhanced Government funding is the requirement which should be duly prioritized, judiciously granted and monitored.

Conclusion

Quantum technologies have huge potential to exponentially enhance the capabilities of computing, cyber warfare, sensing, navigation, autonomous weapon systems, cryptography, radars, EW and provide highly secure communications. It is evident that this technology is a great enabler of military power. Hence, there is now a race amongst the leading nations of the world to develop these technologies and their military applications. It is therefore a must that India also gets into this race and all out efforts are made to develop these technologies to remain militarily powerful.

****

Major General AK Srivastava, VSM (Retd), has commanded a Signal Regiment in the sensitive Akhnur 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 & Strategic Studies, M. Phil Defence & Management Studies, M. Phil Social Sciences and Advanced Communications Course in Signals Academy Leningrad, USSR, (Now St. Petersburg, Russia).

NOTES

[1] Adam Mann & Robert Coolman, "Quantum mechanics: Definitions, axioms, and key concepts of quantum physics+, Livescience, 30 Apr 2024. https://www.livescience.com/33816-quantum-mechanics-explanation.html/

[2] Paul A Tipler & Ralph A Llewellyb, "Modern Physics", (New York: WH Freeman & Company, 2008) 185-187. https://web.pdx.edu/~pmoeck/books/Tipler_Llewellyn.pdf/

3 Stephen Gosset & Brennan Whitfield, "What is quantum computing", BuiltIn, 19 Mar 2024. https://builtin.com/hardware/quantum-computing/

4 Martin Giles, "Explainer: What is Quantum Computer", MIT Technology Review, 29 Jan 2019. https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/

5 ibid

6 Logan P. Kaelbling, "Production of Entangled Photons via Spontaneous Parametric Down-Conversion", Bard College, Spring 2020. https://digitalcommons.bard.edu/cgi/viewcontent.cgi?article=1359&context=senproj_s2020#:~:text=Spontaneous%20parametric%20down%2Dconversion%20is,converted%20photons%20in%20its%20place/

7 Michelle Frank, "The Little-Known Origin Story behind the 2022 Nobel Prize in Physics", Scientific American, 01 Apr 2023. https://www.scientificamerican.com/article/the-little-known-origin-story-behind-the-2022-nobel-prize-in-physics/#:~:text=In%202022%20the%20Nobel%20Prize,on%20their%20predecessor's%20experimental%20design/

8 Donna Lu, "What is Quantum Computer?", New Scientist, 15 Mar 2024. https://www.newscientist.com/question/what-is-a-quantum-computer/

9 James Dargan, "What Types of Quantum Computers Exist in 2024?", The Quantum Insider, 06 Jun 2024. https://thequantuminsider.com/2023/06/06/types-of-quantum-computers/

10 Azure Quantum Resources, "What is Quantum Computing – Quantum Computer Uses and Application Areas", Microsoft Azure. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-quantum-computing#Real-world-uses

11 Martin Giles, "What is Quantum Communication?", MIT Technology Review, 14 Feb 2019. https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/

12 ibid

13 Michal Hajdusek, "Quantum Repeater Goes the Distance", 22 May 2023, Keio University, Fujisawa, Japan. https://physics.aps.org/articles/v16/84

14 Martin Giles, "What is Quantum Communication?"

15 ibid

16 Michiel van Amerongen, "Quantum Technologies in Defence and Security", Nato Review, 03 Jun 2021. https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html

17 Technical Article, "The Future of Inertial Navigation Is Classical-Quantum Sensor Fusion", Advanced Navigation, 07 Jun 2024. https://www.advancednavigation.com/tech-articles/the-future-of-inertial-navigation-is-classical-quantum-sensor-fusion

18 James Der Derian and Stuart Rollo, “Quantum Warfare”, Rutledge Handbook of Future Warfare, Taylor and Francis Group, 1st Edition, 2023. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003299011-34/quantum-warfare-james-der-derian-stuart-rollo

19 Lt Gen DS Hooda (Retd) & Jay Oberoi, “Quantum warfare poses threat to national security”, The Tribune, 15 Jun 2023. https://www.tribuneindia.com/news/comment/quantum-warfare-poses-threat-to-national-security-517162

MANNED-UNMANNED TEAMING: ENHANCING LETHALITY

Gp Capt (Dr.) DK Pandey (Retd)

Abstract

Manned-Unmanned Teaming (MUM-T) is a revolutionary strategy in the military domain that synchronizes the manned and unmanned platforms to support the operations. MUM-T gives the amalgamated features of both platforms, with enhanced awareness of battle scenes, enhanced lethality, and better chances of survival. MUM-T slightly makes employment of soldiers, manned and unmanned air and ground vehicles, robotics and sensors synchronised to provide a multi-domain, ever changing battleground action plan. MUM-T leverages AI to enhance the collaboration between manned and unmanned systems, significantly improving mission effectiveness and safety. The study focuses on how the MUM-T concept facilitates the immediate exchange of data, enhancement of force, and reduction of risk. They can conduct dangerous reconnaissance and surveillance operations and pass information to manned systems. As technology is evolving at a rapid pace, the functions of the MUM-T are going to increase in the future in various dimensions, and enhance modern warfare even more, making it even more unconventional.

When manned and unmanned systems jointly operate to perform a mission, this process is called as “manned-unmanned teaming" (MUMT). People can do the tasking for MUMT, and various unmanned systems (robots) will do the work for them. When manned and unmanned platforms join together to use

their own skills, they might be able to do many things better and faster. For example, military activities in hazardous areas, search and rescue tasks, and efforts to protect the environment are just a few examples.

MUMT involves a human pilot and an unmanned robotic platform working together on land, sea, and air. The goal of this cooperation is to do the tasks and chores that have been given to them in military operations. On land, sea, and air tests, MUMT systems show that they can be used in a variety of situations. Nevertheless, the air domain has exhibited the highest enthusiasm in advocating for the MUMT concept.

Introduction

The extensive utilisation and accomplishments of unmanned aerial vehicles (UAVs) have prompted concerns over the future relevance of human aviation systems. An idea was conceived to join both elements to achieve what was tedious or not easily feasible.

Existing technology is insufficient to allow unmanned aircraft to make complex judgements in an unknown environment independently. However, in practical terms, they must be linked to human perception. Data connections are susceptible to being obstructed or altered. The current threat of cyberattacks is more formidable than any before. Commanded guidance delays can result in severe, potentially lethal outcomes. Human analysts are tasked with assessing and interpreting the data collected by UAVs.

Although, utilising manned aircraft for data collection offers ISR capabilities in typical scenarios, unmanned platforms with latest software are able to accomplish intended military objectives in most of cases. The Russia-Ukraine conflict has illustrated that to operate in contested environment is too challenging. However, the characteristics of the mission will dictate the appropriate kind of aircraft platform to be employed.

MUMT in the Russia-Ukraine Conflict

The cooperation with unmanned equipment, known as Manned-Unmanned Teaming (MUM-T), has become the subject of a provocative gambit between Russia and Ukraine that sheds light on the capabilities in the current conflict. Both Russia and Ukraine, have undertaken MUMT operations. The details are:

(a) MUMT by The Russian forces:

By using UAVs like Eleron-3SV and Orlan-10, Russian forces determined the coordinates of the Ukrainian artillery, which Russians further shelled.

The Forpost-R, that is, the armoured personnel carrier, designed on the basis of the Israeli Searcher Mk II, was specifically intended for reconnaissance operations and operations against the Ukrainian forces.

UAV have been employed integrated with manned aircraft such as the Su-34 to improve engagement efficiency, primarily in regards to the overall awareness and target acquisition.

(b) MUMT by Ukrainian Forces:

The UAV, from Turkey, known as Bayraktar TB2, supported the Ukrainian side in targeting and eliminating Russian gun batteries, logistics, convoys and command positions.

The Ukrainian forces engaged unmanned aerial vehicles or drones, known as PD-1 and PD-2, that are manufactured in Ukraine for reconnaissance and attacking Russian forces.

Further augmented by incorporating the MUM-T capabilities with the help of UAVs with manned aircraft such as the Su-24 as well as MiG-29s in order to amplify the effectiveness of these strikes.

With respect to the conduct of wars, the MUM-T operations are considered effective retaliatory tool. These have been attributed to factors such as better situational awareness of targets, real-time targeting etc.

The current conflict between Russia and Ukraine underscores need for MUM-T in the current warfare and the ability to transform military forces and alter the nature of the operations.

Advantages of Manned Platforms

Manned platforms do have numerous advantages which give them edge over UAS. The major advantageous features of manned platforms are:

Human decision-making: In this case, pilots are capable of making decisions on the same planes within the shortest time possible, regardless of the circumstance.

Real-time situational awareness: Perception and response processing depend on many factors that cause pilots to notice or respond differently to continually changing circumstances.

Capability to Adapt: Pilots aim to alter their plans depending on the progression of activities. Pilots are allowed to combine data gathered by a few types of sensors.

For instance, incidents permit aviators to act regarding failed systems in an emergency.

Aircraft relevance to both extensive and limited Operations: As for the size of the aircraft that, is to be used for data collection, depends on the dimensions and financing options of a certain project. It is imperative to mention that specific corridor mapping operations might be more advantageous when utilising vehicles with comparatively lower costs of operation. Some of the projects are meant to last for several days, while others may involve the ability to transport other complex equipment like LIDAR sensors, and metric digital cameras, which may, in turn, require larger aeroplanes. Carriage of heavier pods by HALEs, in most of the cases, may not be feasible, Using it in contested environment may be vulnerable also.

Piloted planes show flexibility in geographical mapping because they are fitted with comparatively modern mapping sensors. These advanced sensors are often considered a hassle for unmanned devices to import into their ecosystems due to the platform's payload limitations despite the necessity for accurate and wide-ranging mapping outputs they help to produce. This is a major strength of manned aircraft in so far as flexibility in data acquisition is concerned.

Airspace-Compatible Operations: Large manned aircraft capable of flying over most missions can freely operate, subject to air traffic congestion. The other factor that makes manned aircraft preferable when it comes to flying over populated areas is that their operations are significantly limited by fewer restrictions compared to operations of Unmanned Aerial Systems (UAS).

The pilot on board may take evasive actions in case the situation (in an emergency) demands, while UAS may be on obstruction in the air for other manned or unmanned operators. Therefore, Safety-wise, human-crewed operations seem to have an edge over UAS operations. Thus, the measures that the regulations have laid down regarding operating UASs near or over populated areas are more stringent. Given that multiple fatal accidents with piloted aircraft still occur fairly rarely, such planes could be easily viewed as one of the most enticing options that can be considered when talking about ISR operations.

Limitations of Manned Aircraft

The various limitations of manned platforms are enumerated below:

This exposes pilots to a situation in which they are literally placed in a position where the risk of their lives is at stake.

This implies that pilots, like any other human being, undergo fatigue and stress and are restricted in specific ways due to the human anatomy.

Higher operating expenses: Manned aircraft consumes a lot of people and fuel and requires more frequent maintenance than most other aircraft.

Limited endurance: Manned aircraft have relatively short mission endurance due to fatigue.

The manned aircraft operations are generally expensive to conduct. Many aircraft, including the large ones, are costly to own and fully maintain. These costs are then either added to the price of the geospatial data acquisition directly or, more commonly, reflected as a part of this cost. Furthermore, the deployment of piloted aircraft to a project location might incur significant expenses as a result of the exorbitant price of aviation fuel. Typically, the collection of data from manned aircraft necessitates the presence of a sensor operator in addition to the pilot, hence increasing the overall cost of the operation.[1]

Unsuitable for Small Projects: UAS is a cost-effective choice for projects for smaller area, for instance - an area of 2 square miles or less. The significant operational expenses associated with manned aircraft, especially when smaller aircraft are employed, typically render their employment impractical for projects covering an area of 10-20 square miles.[2]

Lower-resolution photography is more productive for imagery acquisition, often done with a resolution ranging from 7.5cm to 15cm. High-resolution imagery is feasible with manned aircraft, but it is not as efficient. Due to their affordable acquisition and operational expenses, tiny unmanned aerial systems are most preferred for projects that are insufficient in scale to warrant the use of human aircraft.

Advantages of Unmanned Aircraft

The advantages of MUM-T operations have dividends on war-waging capabilities. better situational awareness, more accurate hits, targeting in real-time and Battle damages assessment, and mitigating danger for manned aircraft and on-board air crew. The various reasons that make unmanned aircraft a popular choice for military and civilians are appended below:

- This reduces the risk of endangering human life since no pilot is precariously positioned.
- Extended endurance: UAS can hover and be airborne for a couple of hours or even days.

- Lower operational costs: UAS take less crew, fuel, and maintenance than conventional aircraft types.
- Improved precision: Unmanned Aerial Systems maintain their flying patterns; hence, generic models of these flying objects hold an improved flying pattern.
- The UAS can handle several operations and will not tire the pilot, even if there are many operations.

The Other Factors:

- Cost-effective Operations: UAS are the most economical means of obtaining aerial photography for small-scale project areas. Transporting UAS to the project site is cost-effective as they may be easily delivered as cargo or checked in as luggage on a trip. Unlike manned aircraft, UAS does not need the presence of a sensor operator (copilot) beside a pilot. UAS is highly appealing for gathering airborne data.
- High-resolution imagery is often gathered by UAS due to the limitation on flight altitude, namely below 400 feet above ground level (AGL). Attaining a high resolution of 2cm or less is challenging and costly when using manned aircraft.
- Optimal for Small ISR Projects: UAS is the preferred choice for projects that span a smaller area. Though UAS is capable of covering larger areas over an extended duration of operation, if the operation involves taking numerous photos during that time, the effort required to manage those photos from multiple software applications becomes a problem and slows down the completion of the project.

Limitations of Unmanned Aircraft

- UAS only has poor situational awareness because it operates depending on the sensors and data linkages.
- Delays in communication: UAS may take time or even fail to respond or communicate in a prescribed or expected time due to the above reasons.

- Openness to cyber-attacks: UAS are propelled by software as well as data communication.
- Reliance on GPS: UAS rely on GPS, so its safety is paramount for the proper functioning of the unmanned aircraft. This means that the UAS is occasioned by challenges as subsequent regulations.
- A common observation regarding UAVs is "lack of situational awareness and on-the-spot decision-making". However, MUMT operations have addressed it to a certain extent. Unmanned components may be controlled in relation to developing air situations.
- Operational Limitations: The limitations due to size, the technology architecture used, and design issues do restrict the operational exploitation of the Unmanned platforms.

Other Functional limitations are appended below:[3]

- Unsuitable for Large Projects: UAS's poor speed and endurance make it impractical for imaging projects exceeding 2 square miles or corridors longer than a few linear miles.
- Payload Incapabilities: UASs are unable to carry advanced mapping sensors that are bulky and of high quality, such as metric cameras and full-size lidar sensors, because of their restricted capacity for transporting payloads. UASs are only capable of carrying miniaturised cameras and lidar sensors. However, it is important to note that these miniaturised sensors produce products with reduced quality and accuracy when compared to their full-size counterparts.
- Operational Regulations: The degree of freedom of operations of UAS, in military operations, is unrestricted subject to the position of other friendly military aircraft. Although the degree of freedom of operations is unrestricted for combat, the drone regulations impose limitations on the use of UAS in populated areas, hence constraining its application in many non-military usages. For example, the highest-flying altitude is restricted to below 400 feet AGL under Indian Drone Regulations[4] and the regulatory rules, which hampers its efficiency in gathering aerial data.

The comparison table is given below to highlight the differences between Manned and Unmanned Aerial Platforms:

Comparison between Manned v/s Unmanned Aircraft

Capabilities	***Manned ac***	***Unmanned ac***
Operational Risk (Vulnerability)	Yes	No
Lag time for Operations	More	Less
Effect of weather	More	Less
Expandability	More	Less
Autonomous Ops	Yes	Limited
Payload Limitations	Low	High
Attrition Resilience	Low	High
Easy Mobilisation	No	Yes
Capability to undertake Large Projects	Yes	No
Capability to undertake Small Projects	No	Yes
Imagery Quality	Yes	Comparatively Low

Growth of MUMT

In the early years of the 2020s, technology attained a notable degree of complexity, enabling algorithms to execute an expanding array of ordinary and repetitive tasks typically carried out by individuals. The progression of relevant technology has facilitated significant advancements in unmanned technology. These developments have occurred since the end of the Second World War, yet their noteworthy momentum has been observed primarily since the onset of the 21st century.

The utilisation of unmanned aerial vehicles (UAVs) significantly facilitated the advancement of unmanned technology by the United States and its allies to provide military assistance in Afghanistan and Iraq starting in 2001 and 2003, respectively. UAVs have been utilised by the US and Israeli militaries, among others, since the 1960s. However, during operations Enduring Freedom and Iraqi Freedom, unmanned aircraft undertook more missions than previously carried out by manned platforms.

The scope of these operations included intelligence, surveillance, and reconnaissance (ISR) missions, such as aerial surveillance. Over time, they changed their focus to using UAVs like the General Atomics Predator series for kinetic air-to-ground attacks. These robotic aerial vehicles (UAVs) had air-to-surface weapons and guided bombs on board to ensure they could attack quickly. Unmanned Combat Aerial Vehicles, or UCAVs, are useful for two main reasons.

- First, they hit strategic targets in secret and with accuracy, usually in places where manned planes would face high air defence risks.
- Secondly, they are utilised in situations where the implementation of these platforms might potentially have negative political repercussions.

Although the ethical and practical implications of completely replacing people with robots on the battlefield are a worry, recent technological progress has made it possible to create unmanned vehicles. These vehicles are now able to accompany individuals and take on specific parts of their tasks that were previously done by humans, therefore providing support to them. In addition, this strategy is to reduce the number of troops in conflict zones, hence decreasing losses and easing the logistical challenges caused by human presence. Nevertheless, it is crucial to acknowledge that autonomous vehicles will still require fuel, spare parts, and maintenance.

The extent to which the MUMT can be exploited will depend on the intrinsic capabilities of the system. Therefore, it is imperative that the design of the MUMT possesses the capacity to accommodate all foreseeable military objectives effectively. The development of manned-unmanned joint capabilities has been influenced by various factors, such as

- The development of sensor technologies
- The progress in artificial intelligence

- Progress in communications protocols and network topologies
- User-centered design methods

The evolution of manned-unmanned teaming has been driven by technology improvement, improved communication skills, and prioritisation of user-centered design concepts. By using both human and artificial intelligence, it is quite possible to optimise work and improve the level of results of addressing various issues in several sectors and industries.

Advantages of MUMT

It might be mentioned here that the MUMT technology can be regarded as a force multiplier, offering the needed toolkit to address the increasing challenges that larger-scale, more extensive threat operations pose to provincial forces and industry. This approach also safeguards both the operator and its assets against potential challenges as hedges related thereto.

- Enhanced Situational awareness: It is as follows: It is evident that the frequent use of MUMT may enhance the assurance of situation awareness of both manned and unmanned systems. For instance, to reduce the risk factors associated with traffic or any activities that involve human interaction with the environment, autonomous systems integrated with up-to-date data on the environment could assist human systems in making better decisions when controls have been enhanced by augmented situational awareness. Machines and individuals if they would use MUMT, there is a possibility that they would also become more perceptive with regards to their environment.

- Enhancing Intelligence, Surveillance, and Reconnaissance (ISR) Capabilities: Above all, the present study found that MUMT is a more effective communication strategy for escalating ISR, more so in stressing operations. In naval endeavours, the bobbing may be more of observation, spying, and intelligence collecting (ISR) that is often done by helicopters manned from one ship hence enabling exploration.[5]

- Increased Probability of Survival: Since these shooter platforms are drones then they are easier and more efficient to operate and cheaper to replace than manned platforms, which in turn minimises technical failure risks and the loss of personnel.
- Adaptability: MUMT can be beneficial when it comes to the ability to change and scale up the flow of military functions. Often, it can be done where manned operation is not safe or feasible or where manned vehicles are unavailable, for example, performing scouting in front of a convoy or close air support. Such a configuration enables manned systems to conduct activities that are directly related to mission aims, while unmanned systems can effectively handle risky or intricate tasks.

With respect to efficiency, the following have been observed:

  - Better and shorter time cycle for completion of projects
  - High productivity in project development in relation to time

- Cost-Effectivity: It has been pinpointed that employing MUMT may substantially help to reduce the cost burden on a country's budget associated with managing military activities. Thus, when it is compared to human systems, unmanned systems are relatively less costly and are capable of working in risky environments. Modern and technologically advanced manned fighter aircraft have a heuristic value of cost in the range of one hundred million US dollars. On the other hand, the approximate cost of each unmanned wingman as predicted is believed to be less than five million US dollars. MUMT strategy has the potential of leading to the realisation of some expenses while at the same time decreasing the chances of conception of casualties.

However, MUMT is still in its infancy, though once well-developed it can radically alter, in the near future, the very conduct of war. The progress made in the technology would facilitate the integration to boost its role as a weapon system.

The realisation of these possible advantages infers the replacement of traditional human methods with MUMT systems. In order to prevent the improper usage of MUMT systems from becoming the norm, it is important to identify and prevent security risks within them.

Limitations of MUMT Operations

Unmanned Military Systems have advantages. MUMT systems have the same risks as human operators; they can be targeted by enemy fire and IEDs. The enemy may not know much about unmanned systems but they can strike fast. Unmanned systems can also increase the risk of collateral damage as there is a higher chance of hitting unintended targets.

MUMT has many challenges. Communication and synchronisation are key for MUMT systems, but achieving that environment can be tough, especially in complex and dynamic situations.

The probable weaknesses in MUMT systems are appended below:

- **Communication and Coordination failures.** The problem of exchanging info and coordinating between human and unmanned systems is due to different communication protocols and data formats used by both.
- **Vulnerability to Cyber Attacks.** Unmanned systems are connected to the internet, so they are vulnerable to hackers.
- **Exposure to enemy fire and IEDs.** MUMT does have potential risks to hard-kill.
- **Task overload.** Too much workload can be a big challenge for pilots who are operating manned platforms and unmanned aircraft (UA) during MUMT. According to the United States Army Aeromedical Research Laboratory (USAARL) study, pilots will face several challenges of heightened workload in MUMT operations.[6]

Countering the Vulnerabilities of MUMT

MUMT systems must operate autonomously and talk to each other. A contingency plan is needed in case of system failure or loss. However, maintaining the autonomy of communication and control systems while keeping them efficient can be tough.

- Resilient communication and control systems with standardised communication protocols and data formats will enable seamless info exchange and task synchronisation between manned and unmanned devices.
- Cybersecurity can harden unmanned systems against cyber-attacks. Implementing strict security protocols and using techniques that are less hackable will enable operations to continue.
- There are ways to prevent brutal killings. To reduce the risk of collateral damage, we must use advanced precision weapons and improve target identification and avoidance mechanisms.

Recognising and addressing MUMT vulnerabilities is key to improving military effectiveness, safety and resilience.

MUMT in India

India is looking at MUMT for its Air Force and focusing on its Tejas light combat aircraft. India wants to integrate UAVs with its manned aircraft and ground stations to enhance its ISR capabilities.[7]

The Indian MUMT project is the 'Hindustan Aeronautics Limited (HAL) Combat Air Teaming System (CATS'. It is an ongoing project to develop a manned and unmanned aircraft system that can work together in various operational scenarios. HAL is the main agency involved, along with agencies like Newspace Research and Technologies, DRDO, and NAL.[8]

The CATS Warrior project was launched in 2018. Showcased at the Aero India 2021 expo. Currently, the CATS Warrior is undergoing wind tunnel tests, with the rollout planned for 2024 2025. Flight testing of the CATS Warrior is expected to take place in 2024.[9]

The CATS system integrates an LCA-based mothership with the Tejas Mk1 Trainer serving as the MAX (Mothership, for Air Teaming eXploitation). The development of the Tejas twin-seat trainer aims to enhance its capabilities for manned teaming as a Multirole Aircraft for Tactical Support within the CATS framework. The weapon system operator of the Tejas MAX aircraft will oversee the UAS or SWARM (Smart War Fighting Array of Reconfigured Modules)[10], which is a drone associated with each Light Combat Aircraft (LCA). The goal of the CATS system is to establish a network of drones integrated with fighter aircraft.

The plan, which requires an investment of Rs 400 crore, includes an aircraft called the Tejas Mk1 Light Combat Aircraft (LCA) and various unmanned platforms such as the CATS Warrior, CATS Hunter and CATS Air Launched Flexible Asset (ALFA). These unmanned units can be activated individually or simultaneously. They are designed to be controlled from a fighter aircraft (LCA) known as the 'mothership' which releases them from a safe distance, under the supervision of its pilot. This innovative concept will effectively optimise firepower against enemy targets while effectively safeguarding the pilot and fighter aircraft from enemy fire.[11]

The prototypes of various integrated unmanned vehicles and their corresponding capabilities were unveiled in mid-2018 as part of the ongoing development process.[12] The vital elements of CATS are:

CATS Warrior: The CATS Warrior UAV can be coupled with the CATS MAX and is simply a small wingman that can be operated remotely from the ground. Its armament would consist of the Chamundi missile system, which forms the basis of the CATS Warrior's weaponry. The HAL PTAE-7 would be upgraded twin turbojet engines used in the DRDO Lakshya. This kind of element can still be applied in conditions where there is rivalry. This is done by allowing the CATS Warrior to work concurrently with or preceding the LCA or even independently. The Warrior vehicle has a lot of other technologies, and some of them include the following: Electro-Optic/Infrared (EO/IR) Payload, Active Electronically Scanned Array (AESA) Radar, Inertial Navigational Unit and a Jammer. These enhanced technologies enhance the Warrior's capabilities with regard to ISR operations and engagement in combat. The aircraft has the capability to carry 2 advanced and sophisticated air-to-air missiles neatly externally – these maybe short-range or beyond visual range. Besides, it is incorporating internal accommodation to accommodate the Smart Anti-Airfield Weapon (SAAW).[13]

CATS Hunter: As part of the HAL CATS project, the HAL is in the developmental stage of an air-launched cruise missile that is named the CATS Hunter and has low observability while remaining at stand-off range. Thus, the CATS Hunter can be launched from fighter aircraft such as LCA Tejas, Jaguar, Sukhoi-30 MKI etc., for deep penetration strikes. HAL boasts of asserting that it is capable of flying 700 miles, locating a target and releasing hellfire missiles or 350 km, deploying its Brimstone attack drones before it has to go back to base.[14]

CATS ALFA-S: Consequently, Swarm's efficiency has improved due to the application of AI technologies. The recent advancements in air-launched swarm technology have given impetus to the development of the CATS ALFA-S project. HAL is collaborating with New Space Research & Technologies, a startup located in Bengaluru, to develop a UAV known as "Air Launched Flexible Asset-Swarm" (ALFA-S). The Alpha-S, which the Warrior can carry and release, is a swarm of up to 24 drones that can individually carry roughly 5-8kg of explosives and concurrently target numerous enemy positions.[15]

In the 2019 unveiling of the 'Jaguar Max' update package, the ALFA-S swarm drone system was introduced, showcasing its ability to target multiple entities effectively. The reliable companion can be equipped with both aerial and terrestrial missiles. The ALFA-S drones are contained within the CATS ALFA carrier. The LCA can transport a maximum of five CATS ALFA variant glide pods. The initial prototypes of the ALFA-S drones will be anticipated to be deployed utilising the Hawk Advanced Jet Trainers.[16]

CATS Infinity (CI): The MUMT package needs to be well connected through communication links. This connectivity is accomplished by the help of CI. The 'CI' is an aerial control vehicle developed as a High-altitude platform satellite (HAPS). It is designed to operate at elevated altitudes (65000 ft), predominantly within the stratosphere, and serves as a communication relay system. It can maintain a prolonged orbital presence, typically three to six months. The CI system is classified as a solar-powered pseudo-satellite. The wings of the CI can unfold, thereby exposing solar panels. This technology is an interface for transmitting visual data from the battlefield to satellites, thereby enhancing communication between UAVs. The initial prototype is expected to be finished by 2025.

Recommendations

The successful execution of the MUMT concept will rely on the inherent capabilities and functionalities of the system in consideration. The mission has been allocated specific objectives in accordance with the specified criteria. Hence, the progress of MUMT necessitates the incorporation of comprehensive strategies to address all anticipated military objectives.

To address the operational and maintenance issues, the following processes should be executed.

- **Analysing the Performance.** It is crucial to evaluate MUMT operations to address any operational gaps. Formulating strategies to accomplish the required mission objectives should be allocated to an 'expert' agency.
- **Challenges in Coordinating Airspace.** Collaboration among aviation authorities, air traffic management organisations, and industry stakeholders is necessary to ensure the secure and efficient integration of MUMT operations inside the airspace.
- **Maintenance and Logistical Assistance.** To keep operations going, various steps may be taken to ensure that both – human and unmanned resources for maintaining, repairing, and providing logistical support are timely met.
- **Training and Skill Development.** Allocate essential resources to provide relevant training and education for team members engaged in the operations and integration of manned and unmanned systems, enabling them to do so with expertise.
- **Research and Development (R&D).** Depending on the strategic goals and objectives of MUMT, there is requisite importance in maintaining the FGCP, followed by consistent prioritisation and investment in R&D to improve the efficacy and efficiency of the operations.

Freeware improvements, increased autonomy capabilities, and advancements in interoperability will continue to bring higher integration between MUMT and manned vehicles in the future.

Conclusion

The idea behind MUM-T surpasses modern thought regarding a mission's capacity to reach elevated levels of autonomy and delivers a considerable improvement in situation awareness and decision-making, boosting the probabilities of success in military operations.

The MUMT is defined as the ability to combine manpower, manned, and unmanned systems to achieve particular objectives. It is rapidly becoming the most significant technological revolution with an alarming impact on the future of aerial combat.

Low waypoint platforms will be incorporated into a constellation of intelligent ground nodes to improve crewed vehicle performance. These devices will work as 'force multipliers', will make the team stronger, and establish order and authority to safeguard the driver.

Addressing the issues with MUMT systems may offer solutions that would enhance the efficiency and safety of military processes and make these activities more robust. HAL has been developing CATS to be integrated into existing aircraft with an anticipation that will revolutionise aerial combat. In addition, the growth of the IAF's Operational Capability, with induced firepower, shall improve the Indian defence and Aerospace sector globally. It clearly depicts that the innovative and productive participation of private sector enterprises is capable of contributing to developing a competitive aerospace environment in the country. It must be looked after.

****

Gp Capt (Dr) DK Pandey (Retd) had served in the IAF for more than three decades. He has experience of more than 2500 Air combats. He was the Director Air Staff Inspections and retired as Director, Joint Control and Analysis Centre. He has written research papers for journals and websites. Presently he is a 'Senior Fellow' at 'the Centre for Air Power Studies' (CAPS).

NOTES

[1] Qassim Abdullah, "Manned vs. Unmanned Aircraft: Which is Best for Aerial Data Acquisition?", Woolpert, 2024, https://woolpert.com/news/blogs/manned-vs-unmanned-aircraft-which-is-best-for-aerial-data-acquisition/. Accessed on June 21, 2024.

[2] Ibid (Woolpert).

[3] Ibid (Abudiullah).

[4] MoCA, "Ministry of Civil Aviation releases India's airspace map for drone operations", PIB Delhi, September 24, 2021, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1757850. Accessed on June 21, 2024.

[5] KarthikVeeraman, "An Insight: Mannned Unmanned Teaming (MUM-T)", CENJOWS:Issue Brief, December 1, 2022, https://cenjows.in/pdf-view/?url=2022/12/Issue_Brief_Lt_Col_Karthik_V.pdf&pID=18842. Accessed on July 30, 2023.

[6] Livio Rossetti, "Manned-Unmanned Teaming: A Great Opportunity or Mission Overload?", The Journal of the Joint Air Power Competence Centre, Ed: 29, January 2020, https://www.japcc.org/articles/ manned-unmanned-teaming/. Accessed on July 30, 2023.

[7] PTI, "DRDO decides to produce ten unmanned aircraft like Rustom-II", The Indian Express, November 20, 2016, https://indianexpress.com/article/india/india-news-india/drdo-decides-to-produce-10-unmanned-aircraft-like-rustom-ii-4386000/. Accessed on July 26, 2023.

[8] David Hambling, "War of The Wingmen: New Robot Fighters Promise to Transform Aerial Combat", Forbes, March 3, 2021, https://www.forbes.com/sites/davidhambling/2021/03/03/war-of-the-wingmen-new-robot-fighters-weigh-in/?sh=33639cd26c86. Accessed on July 29, 2023.

[9] AkhilKadidal, "HAL loyal wingman project to go airborne by 2024", Janes, March 23, 2022, https://www.janes .com/defence-news/air-platforms/latest/hal-loyal-wingman-project-to-go-airborne-by-2024.

[10] ParvinMohmad, "What is Drone Swarm Technology?", Analytic Insight, May 30, 2023, https://www.analyticsinsight.net/what-is-drone-swarm-technology/. Accessed on July 29, 2023.

[11] AksharaParakala, "Aero India 2021: HAL's loyal wingmen break cover", Janes, February 5, 2021, https://www.janes.com/defence-news/news-detail/aero-india-2021-hals-loyal-wingmen-break-cover. Accessed on July 29, 2023.

[12] AksharaParakala, "Aero India 2021: HAL's loyal wingmen break cover", Janes, February 5, 2021, https://www.janes.com/defence-news/news-detail/aero-india-2021-hals-loyal-wingmen-break-cover. Accessed on July 29, 2023.

[13] Ibid Janes.

[14] Ibid New IE.

[15] Ibid New IE.

[16] "HAL Combat Air Training System", May 18, 2021, http://fullafterburner.weebly.com/next-gen-weapons/hal-combat-air-teaming-system. Accessed on May 29. 2023.

DIGITAL TRANSFORMATION IN JOINT WAR FIGHTING – A 'DIGITAL TWIN' USE CASE

Wg Cdr Anand R Navaratna

Abstract

Integration and joint war fighting in today's landscape are aided by niche technology to maintain strategic edge and operational effectiveness. Digital Twin technology in recent times has emerged as a transformative paradigm in military applications. This paper comprehensively reviews the ongoing studies around the world in digital twin, presents various case studies and result of the studies. The paper touches upon definitions of digital twins, clears few myths surrounding the concept, presents strategic and tactical implications and also lists the challenges in adaptation of this technology in military application. The paper concludes by outlining future perspectives on the continued development and integration of digital twin technology in joint war fighting, emphasizing the need for adaptive strategies to harness its full potential while addressing associated challenges.

Introduction

We live in the 'digital age'. Defence technology is inherently complex. The 'digital age' is making things across the world, including defence technology, more challenging to deal with and cope with. The digital age means "the present time, in which many things are done by computer and large amounts of information are available because of computer technology".[1] While extended concepts like Industry 4.0, the Internet of Things, big data and Artificial Intelligence are already tilting the dynamics of most processes, the academic study surrounding the management, adaptation and regulation of these niche technologies are gaining prominence under the umbrella of Digital Transformation. The primary aim of digital transformation is to solve challenges thereby increase efficiency and effectiveness. Few works state that companies have to develop and implement digital transformation strategies else will have perish.[2] The improvements in computational power, better compiler languages and evolving underlining technology are significant attributes of this revolution. Adapting technology to better the efficacy of offensive and defensive warfighting needs to reap the benefits of this evolution. The 'digital twin' is one such use case for all-round capability enhancement.

Understanding Digital Twin (DT) is essential as it is not only emerging and evolving but is also surrounded by many myths. The origin of the Digital Twin is attributed to Michael Grieves and John Vickers of NASA; Grieves presented the concept in a lecture on product life-cycle management in 2003.[3] The National Aeronautical Space Administration (NASA) released a paper in 2012 titled "The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles'' setting a key milestone for defining Digital Twins.

Defining Digital Twin

As new the field of digital twins is, so is its definition. Various studies have suggested various definitions of digital twins. NASA stated in 2013 that ''A Digital Twin is an integrated multiphysics, multiscale, probabilistic simulation of an as-built vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its corresponding flying twin."[4] Also, Madani, in 2019, stated, "Digital Twin is a virtual instance of a physical system (twin) that is continually updated with the latter's performance, maintenance, and health status data throughout the physical system's life cycle". Though various definitions have evolved surrounding digital twin, a significant leap to fame in digital twin technology was by Gartner, one of the world's leading research organisations, published the 'Hype Cycle for Emerging Technology' studies and termed digital twin technology the 'innovation trigger technology' that triggers other technologies. Gartner also proposed that this technology would change other technology within 5-10 years, as shown in Fig. 1.

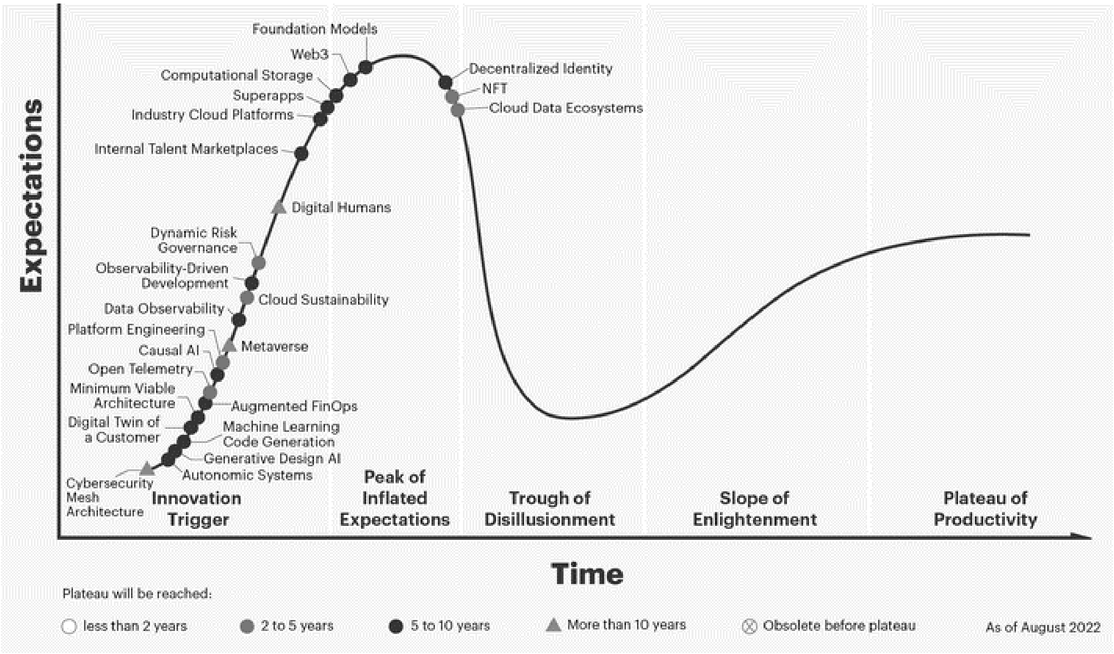


Figure 1: Garther Hype Cycle for Emerging Technology

(Source: www.gartner.com, 2022)

Digital twins bridge the gap between the physical and digital worlds by providing an interface that links past data and present processes. They also can make predictions for the future through the culmination of induced intelligence and actionable data. Twin is created by collecting live data from sensors embedded in physical systems. Specific test points whose output cannot be predicted on physical systems can be performed on digital twins repeatedly until satisfactory results are achieved. Based on these results, the behaviour of physical entities can be predicted without actually validating that on the physical systems. This approach enables costly, complex and challenging estimation of physical systems easy and foolproof. By making fine tweaks on the digital twins, the effect on the physical system can be analysed to test and run complex military scenarios, be it operations or maintenance domain. This also provides a validation mechanism for modifying, optimising, and implementing changes to existing systems.

With the increased complexity of technology, data-driven systems, better sensors, artificial intelligence and fast computing power, the 'digital twin' can prove to be a force multiplier for military warfighting ability. Its acceptance in services, development life cycle and field adaptation, is not farfetched but a reality. The digital twin creation process is reflected in Fig. 2.

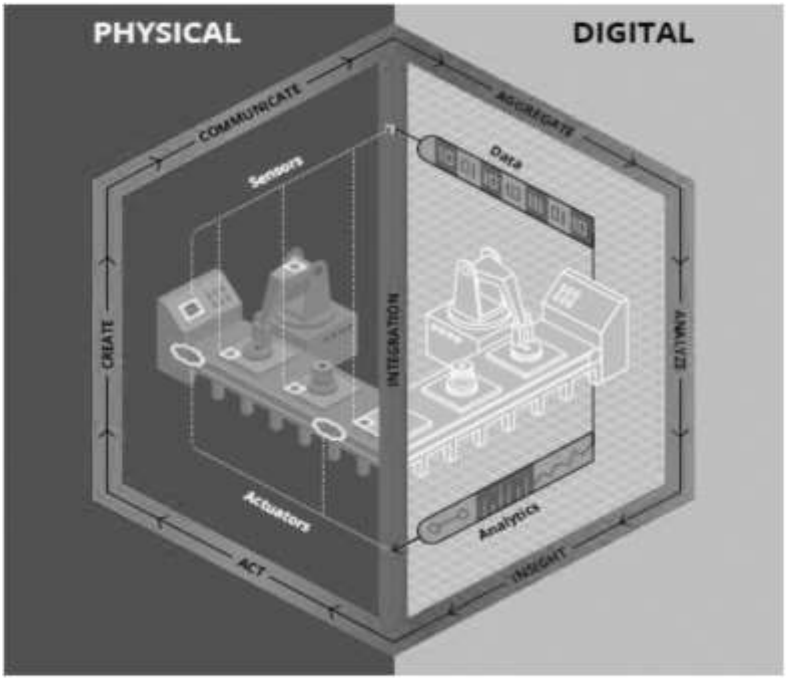
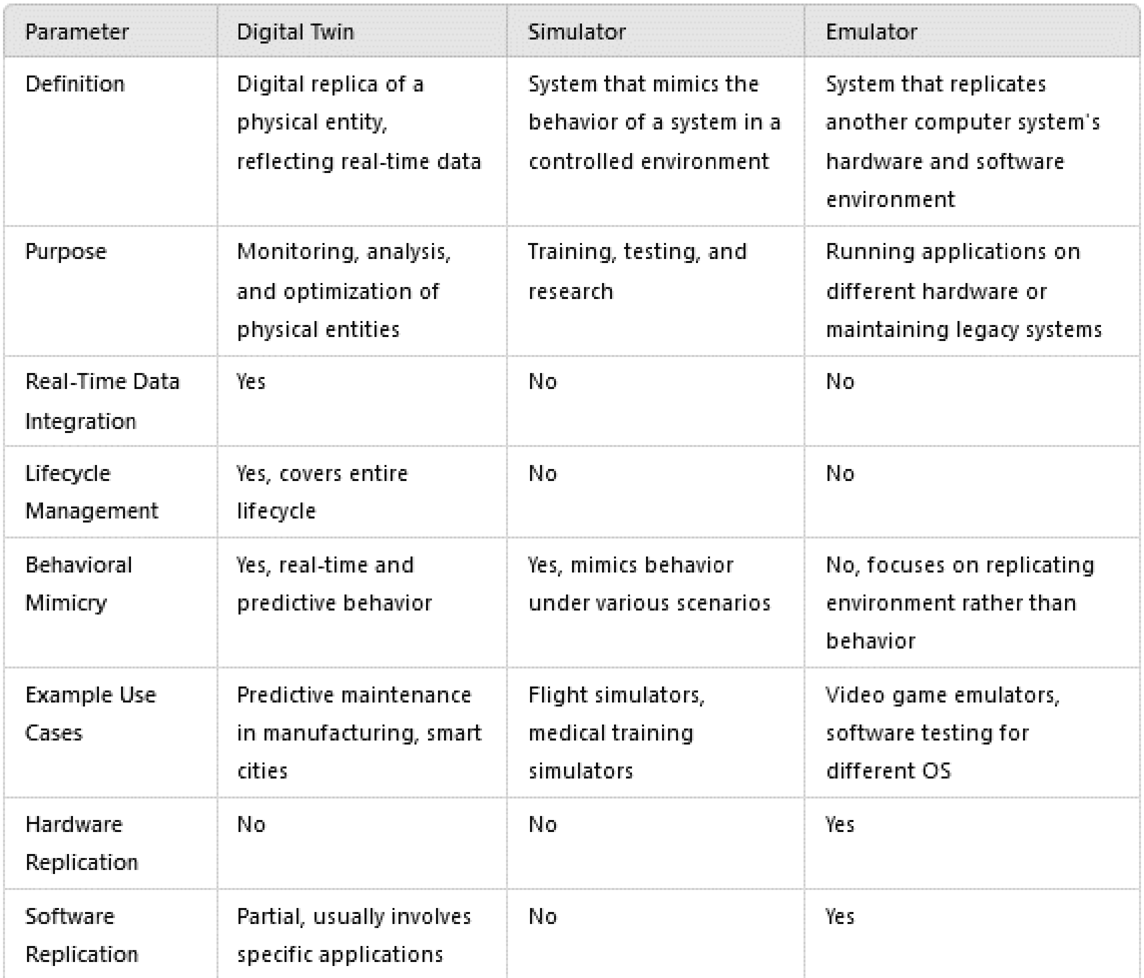


Figure 2: Digital Twin creation process[5]

(Source: Parrott, Aaron, and Lane Warshaw. 2017)

Breaking Myths of Digital Twins

Before dwelling on the applications of digital twins in joint warfighting and their adaptation into service, it is appropriate to break some myths surrounding digital twins and draw fine differentiations between a few already existing terminologies. Most readers by now could have dwelled into the questions as to how 'digital twin' is different from 'simulators' or 'emulators'. These systems already exist in military applications, especially in the training domain. Refer to the Table 1, below that summarises the key difference between them. Apart from DT being real-time, the critical differentiator is speed, use, and ability to integrate sensors/ IoT devices and big data. Also, researchers argue that DT is more suitable for operational training than others as it can provide a vast gambit of possibilities that can otherwise not be tested or seen on physical systems.



Parameter	Digital Twin	Simulator	Emulator
Definition	Digital replica of a physical entity, reflecting real-time data	System that mimics the behavior of a system in a controlled environment	System that replicates another computer system's hardware and software environment
Purpose	Monitoring, analysis, and optimization of physical entities	Training, testing, and research	Running applications on different hardware or maintaining legacy systems
Real-Time Data Integration	Yes	No	No
Lifecycle Management	Yes, covers entire lifecycle	No	No
Behavioral Mimicry	Yes, real-time and predictive behavior	Yes, mimics behavior under various scenarios	No, focuses on replicating environment rather than behavior
Example Use Cases	Predictive maintenance in manufacturing, smart cities	Flight simulators, medical training simulators	Video game emulators, software testing for different OS
Hardware Replication	No	No	Yes
Software Replication	Partial, usually involves specific applications	No	Yes

Table 1 Comparison between DT, Simulator and Emulator ***(Authors Compilation)***

A few terms exist Within the digital domain, such as digital shadow and digital model. The critical difference between them is the ability to interact with physical and digital objects and their modus-operandi. It is important to note that any change in the physical entity must be incorporated into a digital object. However, in terms of digital twins, this happens in an automated and real-time manner. *T*hese systems are represented in Fig. 3[6]

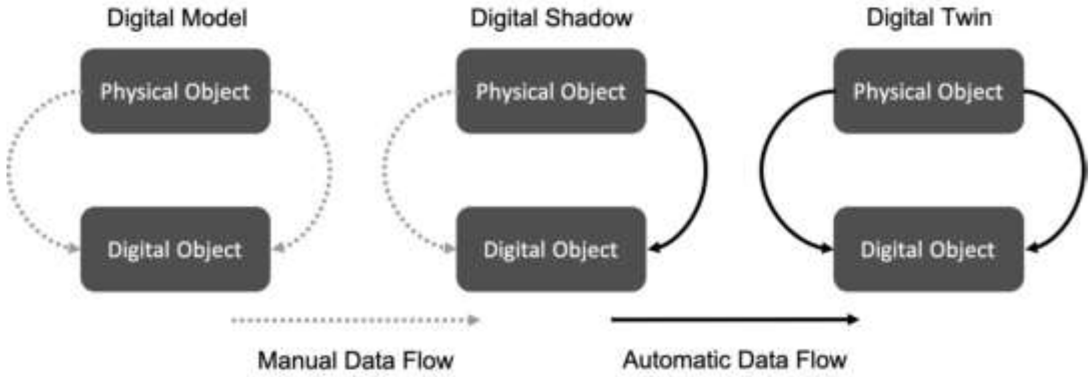
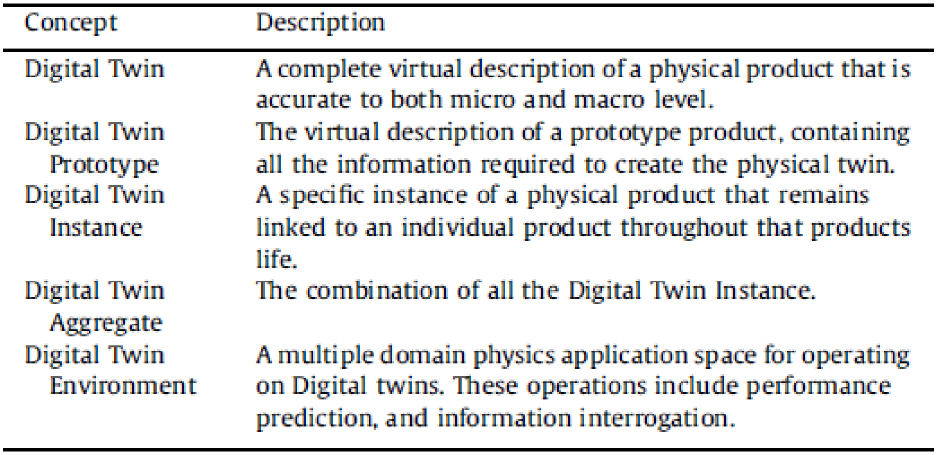


Figure 3: Fuller Model of DT

(Source: Fuller, Aidan, Zhong Fan, Charles Day, and Chris Barlow. 2020)

Further, Grieves, in 2017, proposed a few more concepts in the context of the digital twin's product life cycle, which are listed in **Table 2**[7]



Concept	Description
Digital Twin	A complete virtual description of a physical product that is accurate to both micro and macro level.
Digital Twin Prototype	The virtual description of a prototype product, containing all the information required to create the physical twin.
Digital Twin Instance	A specific instance of a physical product that remains linked to an individual product throughout that products life.
Digital Twin Aggregate	The combination of all the Digital Twin Instance.
Digital Twin Environment	A multiple domain physics application space for operating on Digital twins. These operations include performance prediction, and information interrogation.

Table 2 DT Concept and its definition ***(Source: Grieves, M., Vickers, J., 2017)***

DT in Military Applications

The applications of digital twins are not limited to product life cycle in general or R&D in particular. In defence application parallels, its applications are not limited to maintenance or sustenance only. Characteristics like adaptability, implementation efficiency, interoperability, fidelity and accuracy of results make this technology niche and most suitable for joint warfighting mechanisms, which are plural and complex. The individuality of each service equipment, training, and bias can be overcome using a robust digital twin. The subsequent paragraphs highlight the known and established applications of DT in the context of military applications.

Operations and Mission Planning

One of the significant fields in which DT is contributing immensely is aviation. Aviation, by nature, is expensive and multi-dimensional. Further, aircraft training, testing and maintenance are very costly and dynamic. Air operations are limited by safety, weather and enemy tactics, adapted through training. The OEM manuals and procedures usually guide the aspects like limitations of operations and maintenance. Thus, the variables can be many, but academic or design constraints loosely bind them. The resources available to stretch and test these operational parameters are limited or cannot be simulated. In these scenarios, DT comes in handy. DT, aided by sensors onboard, provides real-time dynamic solutions to pilots on aspects like fuel consumption, route predictions, airframe stress, and profile or missile launch validations. Further, based on historical data, future actions can be predicted by aircraft behaviour in battle or routine flight. Aspects like probable component failure, fatigue, and an alerting system can add value and increase situational awareness within the aircraft.

Adaptive Vehicle Manufacturing (AVM) is a US Defense Advanced Research Project Agency (DARPA) that started in 2010 and aims to shorten the R&D cycle and cost of weapon systems. DT is expected to aid these systems in all warfighting domains, including cyberspace, simulation, experiment, processing, testing and production.[8] The announcement of the US F-35 fighter jet clone to predict component failure, future performance, life expectancy and failure rates. US Army is conceptualizing the use of DT in collaboration with Wichita State

University to increase efficiency and training on the Black Hawk helicopter fleet. General Electric has started a Technology Acceleration Centre to bring operators, engineers, and manufacturers together to step up the adaptation of DT. With the ability to monitor data from sensors onboard and validate the parameters on its digital twin, it can define how complex wars are fought. In a model-based system engineering study, DT was used on a UAV to validate the route selection process through mission objective achievement. The results of the study were auspicious and path-breaking. In the Fig. 4 (a and b), the UAV is on a last-mile delivery mission to supply a friendly target, as indicated in blue. Based on its history, the system has acquired knowledge of adversary presence through its onboard sensors (EW data, Geo-location data, range of adversary weapon system, etc.). These data are now tried on the digital twin of the UAV. Based upon mission objectives of time on target, payload, speed, range and endurance, route optimization is to be undertaken by the digital twin well within time. The DT in this study suggested three routes, A, B and C and suggested taking Route B to keep UAVs safe from adversaries. As per the simulation setting and risk assessment, this is the least vulnerable route[9].

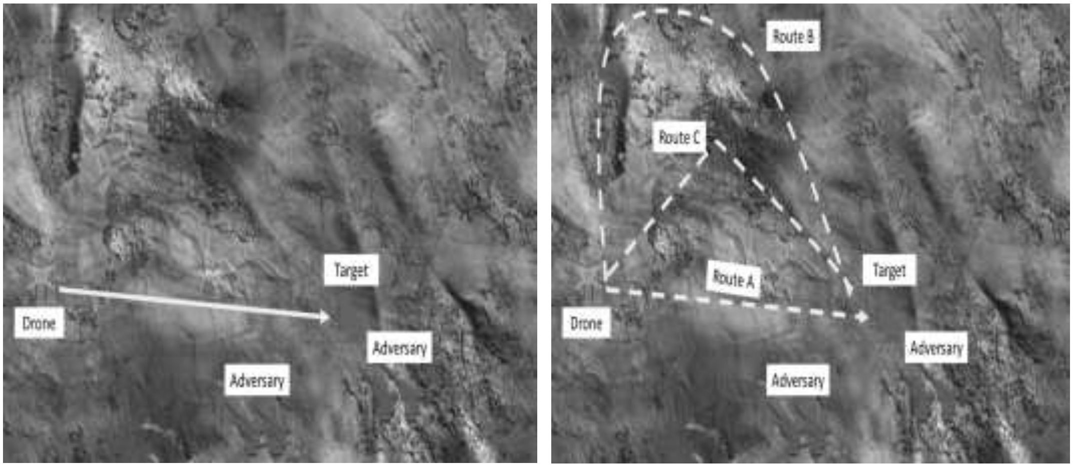


Figure 4 (a) Mission Plan[10] (b) System suggested route[11]

(Source: Lee, Eugene Boon Kien, Douglas L. Van Bossuyt, and Jason F. Bickford, 2021)

Joint warfighting is not just about terminal weapons. Command and control centre plays a critical role in field commanders' decision-making. DT has also paved the way in this complex

C4ISR domain to run and validate complex decision-making matrix and provide better and more robust strike solutions. In the 1991 Golf War, the US Army provided a battlefield environment simulation system[12] for its M1A1 tanks, catering to terrain, roads, buildings, rivers and vegetation to carry out effective strike planning. Simulating the same using DT for accurate battle simulation or training has created a scientific, high-precision and credible environment. Massive data must be captured in real-time scenarios to make such complex systems work. One suggested and workable solution is using data-acquiring sensors and IoT devices during routine training and actual scenarios. Based on the data gathered, DT can simulate a mature decision-making environment. A representation is indicated in Fig. 5.[13] This calls for greater joint training for data generation and integration of systems and logistics to improve accuracy and timelines. At strategic level, the DT can significantly enhance command and control capability through better situational awareness, strategic planning, fusion of various data source like satellites', ground assets and drones. In USA it is reported that a joint all domain command and control (JADC2) is aimed at being constituted for joint planning cross domains of land, sea, air, space and cyber.

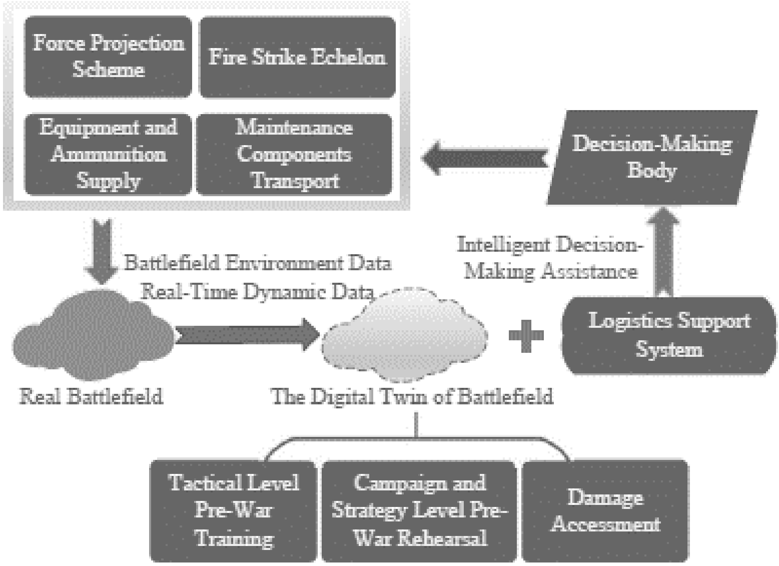

Force Projection Scheme
Fire Strike Echelon
Equipment and Ammunition Supply
Maintenance Components Transport
Decision-Making Body
Battlefield Environment Data
Real-Time Dynamic Data
Intelligent Decision-Making Assistance
Real Battlefield
The Digital Twin of Battlefield
Logistics Support System
Tactical Level Pre-War Training
Campaign and Strategy Level Pre-War Rehearsal
Damage Accessment

Figure 5: DT representation of battle Mission System[13]

(Source: Li, Suliang, Qiliang Yang, Jianchun Xing, and Shenggui Yuan, 2020)

Military Engineering and Equipment

USAF and NASA have proposed the Airframe Digital Twin (ADT) framework, which aims to replace traditional deterministic individual aircraft tracking systems with more sound, probabilistic, risk-based and accurate systems. This system has also been validated by the National Research Council of Canada (NRC). NRC defines ADT as "a digital representation of as-built/as-maintained airframe system, i.e. an integrated multiphysics, multiscale, probabilistic simulation of an as-built airframe system that uses the best available models, sensor information, and input data, to mirror and predict activities/performance over the life of the corresponding individual airframe system." The NRC's vision of ADT is represented in Fig. 6.[14] It consists of five building blocks. They are represented by numbers 1 to 5, where 1 is the Common fleet database, 2 is individual digital twin, 3 is quantitative risk assessment, 4 is individual physical aircraft, and fifth is Bayesian Inference[14].

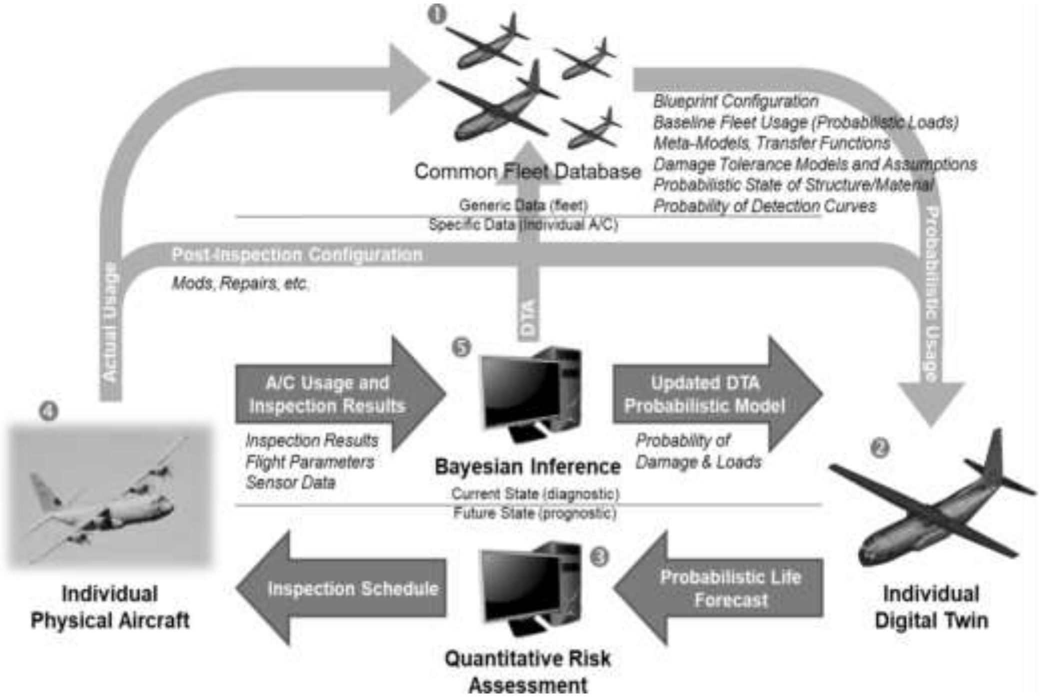

1
Common Fleet Database
Blueprint Configuration
Baseline Fleet Usage (Probabilistic Loads)
Meta-Models, Transfer Functions
Damage Tolerance Models and Assumptions
Probabilistic State of Structure/Material
Probability of Detection Curves
Generic Data (fleet)
Specific Data (Individual A/C)
Post-Inspection Configuration
Mods, Repairs, etc.
Actual Usage
Probabilistic Usage
DTA
5
A/C Usage and Inspection Results
Inspection Results
Flight Parameters
Sensor Data
Bayesian Inference
Updated DTA Probabilistic Model
Probability of Damage & Loads
Current State (diagnostic)
Future State (prognostic)
4
Individual Physical Aircraft
2
Individual Digital Twin
Inspection Schedule
3
Probabilistic Life Forecast
Quantitative Risk Assessment

Figure 6: NRC vision of ADT

(Source: Liao, Min, Guillaume Renaud, and Yan Bombardier, 2020)

The study by NRC concluded that the Royal Canadian Air Force (RCAF) could adopt the ADT framework for better component life monitoring, extension, durability/ damage, and risk assessment management programs. The study also suggests utilizing high-fidelity DT for the life cycle management of individual and common fleets.

Four significant aspects of military equipment, are design, test, production and maintenance, as indicated in Fig. 7.[15] These four aspects contribute towards the total life cycle of the equipment.

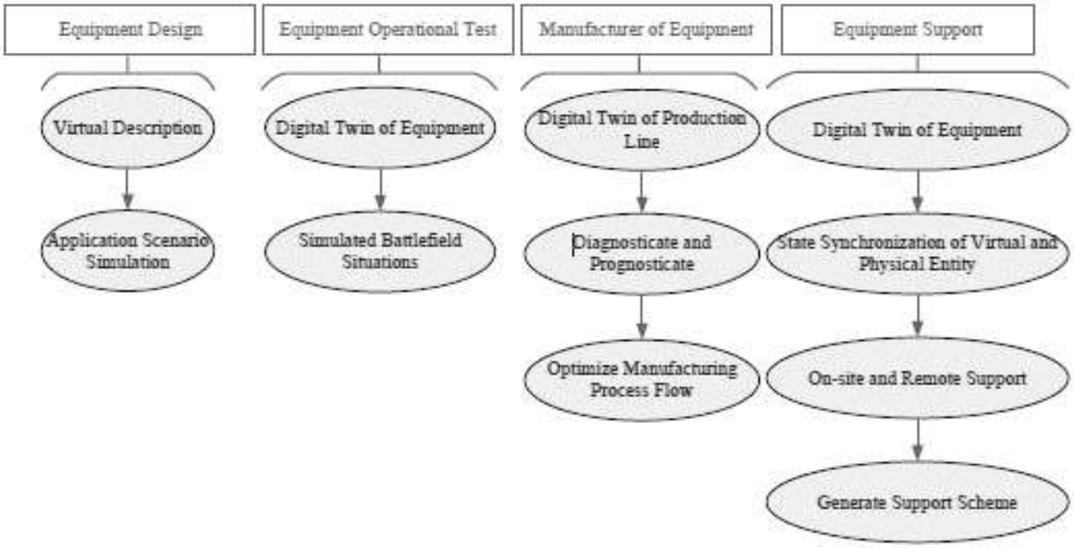

Equipment Design
Equipment Operational Test
Manufacturer of Equipment
Equipment Support
Virtual Description
Application Scenario Simulation
Digital Twin of Equipment
Simulated Battlefield Situations
Digital Twin of Production Line
Diagnosticate and Prognosticate
Optimize Manufacturing Process Flow
Digital Twin of Equipment
State Synchronization of Virtual and Physical Entity
On-site and Remote Support
Generate Support Scheme

Figure 7: DT in four significant aspects of military equipment

(Source: Liao, Min, Guillaume Renaud, and Yan Bombardier. 2020)

Maintenance costs are attributed to about 30-40% of the profits incurred by the companies. During the said period of rectification or MRO, the operations are affected. DT poses a unique opportunity to use its clone with a large amount of sensor data for easy repair assessment, reducing downtime significantly. The data and DT validation outcome can bring aspects and clauses that can form part of service-level agreements and contracts. This will lead to data-driven maintenance planning.

DT in Space Operations

Space and satellite-based warfare is professed and is a time-tested operational philosophy. The application of DT in space, especially in satellite management, anti-satellite attacks, EW mapping and GPS positioning. Any downtime or mismanagement of satellites can lead to prolonged unavailability of vital data. A DT-based fault diagnostics and health monitoring (FD-HM) has dramatically increased interoperability and expressiveness[16]. Data-driven algorithms are employed to implement fault prediction, diagnostics and maintenance. This will ensure constant cover of satellites over battle areas and provide safety to satellites.

DT Applications in the EW Environment

The electromagnetic clout and density have increased with the increase in digital footprint in war zones. With modern concepts of active decoys, low probability of intercept and better material engineering, all three organs of the EW tree face challenges. With the application of DT in this domain, the ever-challenging aspects of threat determination, library updating, offensive action, and evasive solutions can be tactically validated. Most EW systems used in military applications have large amounts of data. These data can be effectively used to digitally recreate the electromagnetic scenario of the natural world. Further, the ranges of adversary emitters can be parametrically tweaked and probabilistically located. With onboard sensors and ground-based clones, the EW cycle can further be tightened and provide immense training value to operators. In a joint warfare scenario, the determination of friend and foe becomes more complex. DT can discern and provide actionable solutions with robust algorithms and computational power.

Other Applications

Military operations are complex and include a wide range of assets, from offensive to defensive to support services. Technology can be a strong catalyst for onboarding individual systems in a joint warfare scenario. Various publications and scholarly works are carried out in various fields, which can play a critical role in joint military applications. Some of the applications are listed in Table 3 :-

Domain	Application	Description	Reference
Manufacturing	Predictive Maintenance	Monitor, predict and schedule maintenance based upon health of system	Tao, F., et al. (2019). "Digital Twin in Industry: State-of-the-Art." *IEEE Transactions on Industrial Informatics*, 15(4), 2405-2415
Healthcare	Digital Solider Clone	Monitor soilder vitals and health when in battle field through sensors	Lloyd et al. 2023. "Maintaining Soldier Musculoskeletal Health Using Personalised Digital Humans, Wearables And/or Computer Vision." *Journal of Science and Medicine in Sport* 26 (June): S30–39.
Battle Area Vehicle/ tank movement optimization	Vehicle performance and route optimization	Simulates and analyzes vehicle performance parameters and path	Boschert, S., & Rosen, R. (2016). "Digital Twin—The Simulation Aspect." *Mechatronic Futures*.
Logistics Management	Supply chain optimization	Monitor stock, network and demand scenarios and cater to needs dynamically	Barricelli, B. R., et al. (2019). "Human Digital Twin for Fitness Management." *IEEE Access*, 7, 134374-134388
Communication	Network and optical communication management	Simulate and monitor latency, network and performance for better communication	Macchi, M., et al. (2020). "A Digital Twin Framework for Telecommunications Network Management." *Procedia CIRP*, 93, 1072-1077

Table 3: Indication of military application of DT *(Authors Compilation)*

Tactical and Strategic Advantages

Few case studies already emerging in military applications suggest that DT is here to stay and may have profound implications on joint warfare operations. The future scope can be tactical, capability building and strategic. As twins can validate data and situations that humanly cannot be possible, this will prove to be a significant testing, tactics development and 'proof of concept' validation platform. This overarching ability will help us continually adapt and innovate tactics against adversaries. The ability to accurately replicate physical entities will fundamentally change our capability. Tactical aspects of routine operations, mission planning and maintenance-logistic optimization will significantly enhance controlled parameters under field commanders.

With the evolution of computational power, better and stronger algorithms, speed, and capabilities requiring high precision and accuracy can be achieved in real-time. Certain aspects, like training on more realistic data acquired by onboard sensors, immersive training, and the ability to stretch beyond limits within a controlled environment, can be among the most prominent capabilities that DT can provide.

Strategically, most of the systems in service used for war fighting today are digital. The extensive data available to us about our systems can further be used to enhance strategic interests. Many applications developed in civilian parallels can also aid military applications. Fields like terrain mapping, communications, 3D modelling, city planning, vehicle mobility, and pharmacy have already been rolled out and are in use. Once the model matures, there will be a meteoritic rise in DT adaptation in complex battle planning, tactics and joint war fighting domains.

Challenges of DT Adaptation

The significant challenges surrounding the adaptation of digital twins in joint military operations are more infrastructural. To begin, the success of DT depends on the availability of a large dataset for scenario creation. If the system intended for DT is not digital or has provision to capture data through the installation of sensors, then implementation of DT becomes more complex. Thus, the availability of compatible and sustainable sensors is a big challenge for an extensive military application. Further, to make the system real-time and fast, the need for a reliable, secure and fast network is a challenge. The data flow is duplex. Ensuring fast throughputs remains a grey and independent area for deliberation. While the communication medium ensures speed, providing data safety is another challenge. The army-navy-air force-space force will require larger synergy and more comprehensive cover in a joint warfighting effort. Thus, ensuring security through encryption or other techniques remains a grey area. Highly computational machines and robust algorithms usually undertake processing within DT. Hence, developing robust algorithms becomes a key focus area to ensure the desired replication of physical system performance.

Further, though a steadfast approach is adopted in the conceptual and framework development of DT, it remains expensive as a concept for large-scale implementation. Finally, the ecosystem required for building a complex and overarching technology requires expertise and skill. Military application development is challenging as it requires high standards and accuracy. Currently, dedicated R&D institutions mostly owned by Governments and large corporate bodies are working on this technology. For large-scale adaptation and sustainability, larger ecosystems are to be built. Lastly, the ethical considerations on using digital twins for offensive military applications need more extensive debate and framework. In addition, the data privacy of physical entities must be protected.

Conclusion

Integrating digital twin technology into joint war fighting can revolutionize military operations at all levels—strategic, operational, and tactical. It has enormous applications in operations, maintenance and administration. Digital twins enhance situational awareness, optimize resource allocation, improve coordination, and augment human capabilities. However, adopting digital twins in military contexts also presents significant challenges, including data integration and standardization, cybersecurity, and ethical and legal considerations.

The continued development and integration of digital twin technology will shape the future of joint war fighting. As digital twins become increasingly advanced, they will drive the evolution of warfare tactics, the development of new capabilities, and the attainment of strategic advantages. Military forces must adapt and innovate to leverage the full potential of digital twin technology while addressing the associated challenges to ensure the ethical and secure use of these transformative technologies.

****

Wing Commander Anand R Navaratna is serving as Aeronautical Engineer in IAF. He has done his M Tech in Artificial Intelligence and is perusing his PhD in Digital Transformation from IIT Jodhpur.

NOTES

[1] Cambridge Dictionary. 2024. "DIGITAL AGE | Meaning in the Cambridge English Dictionary." Dictionary.cambridge.org. 2024. https://dictionary.cambridge.org/dictionary/english/digital-age.

[2] Hess, Thomas, Christian Matt, Alexander Benlian, and Florian Wiesböck. 2016. "Options for Formulating a Digital Transformation Strategy." *MIS Quarterly Executive* 15: 123–39.

[3] Grieves, Michael. 2014. "Digital Twin: Manufacturing Excellence through Virtual Factory Replication." *NASA White Paper*, 1–7.

[4] Glaessgen, E., and D. Stargel. 2012. "The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles." Semantic Scholar. 2012. https://doi.org/10.2514/6.2012-1818.

[5] Parrott, Aaron, and Lane Warshaw. 2017. "Industry 4.0 and the Digital Twin." Deloitte Insights. May 12, 2017. https://www2.deloitte.com/us/en/insights/focus/industry-4-0/digital-twin-technology-smart-factory.html.

[6] Fuller, Aidan, Zhong Fan, Charles Day, and Chris Barlow. 2020. "Digital Twin: Enabling Technologies, Challenges and Open Research." *IEEE Access* 8 (May): 108952–71. https://doi.org/10.1109/access.2020.2998358.

[7] Grieves, M., Vickers, J., 2017, "Digital twin: mitigating unpredictable, undesirable emergent behaviour in complex systems" *Transdisciplinary perspectives on complex systems*, 85–113.

[8] Cheng, X, F Song, Z Lv, X Ping, and X Zhang. 2019. "Deconstruction and Restructuring: The New Era of Intelligent Economy." *Ali Research*.

[9] Lee, Eugene Boon Kien, Douglas L. Van Bossuyt, and Jason F. Bickford. 'Digital Twin-Enabled Decision Support in Mission Engineering and Route Planning'. *Systems* 9, no. 4 (14 November 2021): 82. https://doi.org/10.3390/systems9040082.

[10] Ibid

[11] Ibid

[12] Li, Suliang, Qiliang Yang, Jianchun Xing, and Shenggui Yuan. 'Preliminary Study on the Application of Digital Twin in Military Engineering and Equipment'. In *2020 Chinese Automation Congress (CAC)*, 7249–55. Shanghai, China: IEEE, 2020. https://doi.org/10.1109/CAC51589.2020.9326911.

13 Ibid

14 Liao, Min, Guillaume Renaud, and Yan Bombardier. 2020. “Airframe Digital Twin Technology Adaptability Assessment and Technology Demonstration.” *Engineering Fracture Mechanics* 225 (February): 106793. https://doi.org/10.1016/j.engfracmech.2019.106793.

15 Ibid

16 Mendi, Arif Furkan, Tolga Erol, and Dilara Dogan. ‘Digital Twin in the Military Field’. *IEEE Internet Computing* 26, no. 5 (1 September 2022): 33–40. https://doi.org/10.1109/MIC.2021.3055153.

HYPERSONIC WEAPONS IN JOINT WAR FIGHTING

Lt Gen P R Shankar, PVSM, AVSM, VSM (Retd)

Abstract

Hypersonic weapons which have speeds in excess of 5 Mach have caught every one’s imagination. The popular thinking is that hypersonic weapons are gamechangers in battle and that they give a nation a winning edge. Whilst that may be so, it might not be true fully. Hypersonic weapons do have tremendous advantages but have problems also. Being high-tech they are very costly. Further, many in the strategic community discuss hypersonic weapons very glibly without understanding what they are. In this context there is a need to understand ‘Hypersonic Weapons’ better in order to make an informed judgement and assessment on their utility and employment in various circumstances. This article attempts to do so.

Introduction

On 1 October 2019, the DF 17 missile was paraded during China’s National Day.[1] The DF17 had been under development since 2014. It was the first and only hypersonic missile, on a mobile platform to enter active service in the world. Even USA and Russia did not have it at that time. The DF 17, equipped with a with hypersonic glide vehicle (HGV), was designed with a speed above Mach 5. Two years later, around Jul-Aug 2021, China tested two hypersonic weapons where, ‘a payload was sent into low-Earth orbit, which travelled partially around the globe and released a HGV that travelled through the atmosphere to a target site in Chinese territory’.[2] These two events made everyone sit up. They marked the onset of the hypersonic age. Ever since then, hypersonic weapons have caught every one's imagination. Current day popular thinking is that hypersonic weapons give a nation a winning edge and that they are gamechangers in battle. In this context there is a need to understand 'Hypersonic Weapons' better in order to make a judgement one way or the other on them. The understanding will enable the defence planners to look at these emerging options in context with Joint Warfighting.

China's Hypersonic Future, Missile Threat
Source : https://missilethreat.csis.org/chinas-hypersonic-future/

Hypersonic Missile - Basics

Technically, "Hypersonic" implies speeds above Mach 5 but also 'within the Earth's atmosphere.'[3] The trajectory of a hypersonic missile is therefore mostly inside the earth's atmosphere. A hypersonic missile uses aerodynamic forces to execute its manoeuvre. Hence the missile has aerodynamic control surfaces such as wings or tail fins to manoeuvre while gliding. It is very similar to an aircraft in flight. Air resistance and density are necessary for its control surfaces to generate lift. Overall, a hypersonic missile manoeuvres within the earth's atmosphere. This is unlike ballistic missiles which spend a considerable part of their flight in space. Ballistic missiles use a combination of aerodynamics and astrodynamics for manoeuvre unlike hypersonic weapon which rely on aerodynamics alone.

A hypersonic missile could be a cruise missile, a boost glide missile, or a boost glide missile based on a fractional orbit bombardment system. A hypersonic cruise missile is based on a SCRAMJET (supersonic combustion ramjet) which accelerates it to the desired Mach speed number. The missile is powered throughout its flight and flies at about 30-40 kms above the earth well within the atmosphere. It manoeuvres to its target like any other cruise missile. The maximum altitude for a hypersonic flight could be up to100 kms. Beyond that earth's atmosphere ceases to exist and one enters into space. A hypersonic missile combines high speed, low altitude trajectory and manoeuvrability to overwhelm air defences[4].

In a boost-glide system, the missile contains a glide vehicle with a warhead. It is initially propelled by a rocket motor to a high speed. It commences on a ballistic trajectory but is either not allowed to escape the atmosphere or is made to turn back into the atmosphere early. Hypersonic missiles mostly fly at suborbital altitudes and are generally not allowed to go out of the earth's atmosphere. The HGV is detached at some point and made to coast and manoeuvre at high speeds within the atmosphere to hit the target. The HGV uses its kinetic and potential energy, as well as lift generated by its movement through the air to coast at high speeds to the target.

In a hypersonic boost glide missile, based on a fractional orbit bombardment system, the missile is fired into a low-Earth orbit and made to travel around or partially around the globe. At a designated time and point, it releases a hypersonic glide vehicle that re-enters the atmosphere and travels through it to a target like a normal boost glide system as described above. In the terminal phase, the glider can release another missile on to the target as attempted by China.

The question which often comes to mind is that how does a hypersonic system differ from a ballistic missile. In essence, a ballistic missile consists of a warhead mounted on a propulsion system with a control and guidance arrangement. Depending upon the range to be achieved, the propulsion system of a ballistic missile could be single or multistage system. Normally, a long range ballistic missile is propelled into space at high speeds. Once the missile reaches space, the motor is shut off and jettisoned. The unpowered warhead then follows a ballistic path to the target with the help of some thrusters to keep it on the trajectory. Control and guidance are minimal once the main rocket motor is ejected out. Manoeuvre is minimal except in the case of manoeuvrable re-entry vehicles. However, their speeds remain high being in space. Once they re-enter the atmosphere, they gather speed due to gravity. On the other hand, hypersonic missiles possess the high speeds associated with ballistic missiles along with the manoeuvrability and lower-altitude flight of cruise missiles. These characteristics stress early warning and defence mechanisms of adversaries.

When hypersonic weapons are compared with ballistic missiles, or subsonic cruise missiles certain issues emerge. Generally, hypersonic weapons which fly in the atmosphere are likely to have better chance at overcoming long-range missile defences rather than ballistic missiles which operate in space for a considerable part of time of their trajectory. Their detection and interception will be difficult due to their hyper velocities and below the horizon flight trajectories. Their low trajectories make detection late and thus gives very little reaction time to an adversary to intercept them. Their speed and manoeuvre capability makes them unpredictable. It can confuse the adversary of the intended target as compared to a ballistic missile which is quite predictable. They are likely to have better midcourse survivability against ballistic missile defence systems. However, hypersonic missiles lose speed as they glide towards their targets. They are likely to be traveling with lesser terminal speeds as compared to re-entry vehicles which can maintain their speeds closer to the target. Therefore, their vulnerability against terminal defences increases. However, both missiles can carry out manoeuvres near their targets to make interception difficult. A major point of consideration is that hypersonic technology is still maturing as compared with all other missile technologies. Further, hypersonic boost-glide missiles are costlier by about 1/3rd as compared to equivalent range ballistic or cruise missiles. A fractional orbital bombardment system with a glide vehicle is costlier and more complicated. From available literature, it is not accurate enough to be considered as a fully deployable weapon and is still in the process of evaluation. A holistic comparison between ballistic missiles, subsonic cruise missiles and hypersonic boost glide vehicles is very well illustrated in the Fig 1.[5]

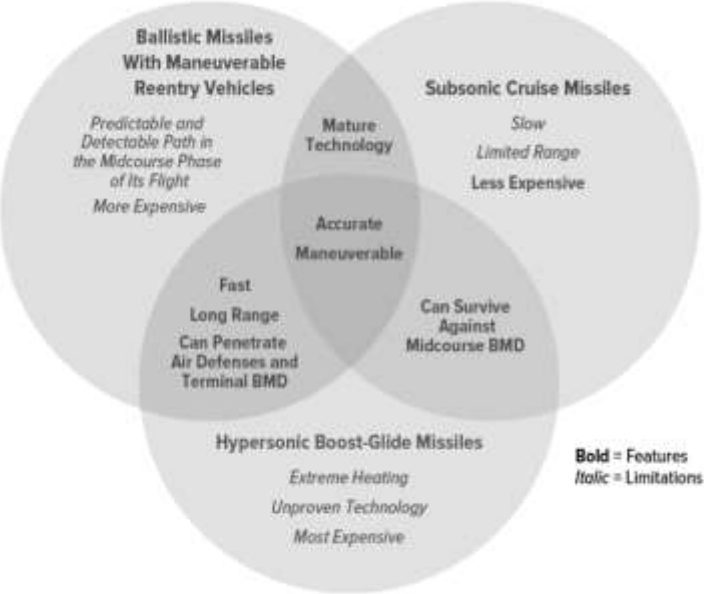

Ballistic Missiles With Maneuverable Reentry Vehicles
Predictable and Detectable Path in the Midcourse Phase of Its Flight
More Expensive
Mature Technology
Subsonic Cruise Missiles
Slow
Limited Range
Less Expensive
Accurate
Maneuverable
Fast
Long Range
Can Penetrate Air Defenses and Terminal BMD
Can Survive Against Midcourse BMD
Hypersonic Boost-Glide Missiles
Extreme Heating
Unproven Technology
Most Expensive
Bold = Features
Italic = Limitations

Fig.1: A holistic comparison between ballistic missiles, subsonic cruise missiles and hypersonic boost glide (Source :- U.S. Congressional Budget Office (https://www.cbo.gov/publication/58924)

The operational implication of all missile systems described hitherto fore is best understood from the Fig 2. When a ballistic missile is fired at a target, its trajectory stands exposed for the best part of its flight as can be seen in the graphic above. It can be detected and dealt with at almost any stage of its flight. On the other hand, a hypersonic cruise missile (HCM) or a HGV can be kept under the radar horizon and evade detection for the best part of their flights. A Manoeuvrable Re-entry Vehicle is a via media compromise between the almost complete exposure of a ballistic missile and the complete undetectability of hypersonic systems. The fractional orbit bombardment system with a HGV is different in the sense that it drops down on an unsuspecting target at greater speed with a near vertical approach. It achieves surprise and leaves a target with very little reaction capability. Hypersonic weapons are visualised to be employed against distant, time-sensitive, or well defended targets.[6] Their high speeds compress engagement times drastically compared to ballistic missiles. Their low trajectories enable them to evade missile defences.

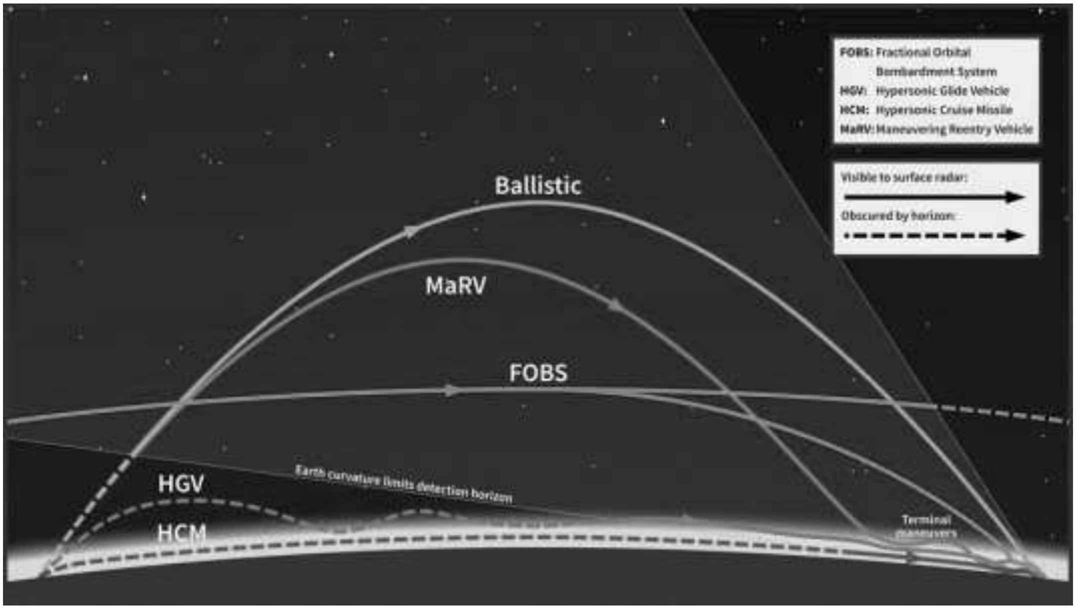

FOBS: Fractional Orbital Bombardment System
HGV: Hypersonic Glide Vehicle
HCM: Hypersonic Cruise Missile
MaRV: Maneuvering Reentry Vehicle
Visible to surface radar:
Obscured by horizon:
Ballistic
MaRV
FOBS
HGV
HCM
Earth curvature limits detection horizon
Terminal maneuvers

Fig 2: **Operational Implication Of All Missile Systems**
Source : **https://missilethreat.csis.org/wp-content/uploads/2022/02/220207_Karako_Complex_AirDefense.pdf**

Hypersonic Technology

Technology which differentiates a normal missile and a hypersonic missile revolves around two issues. Firstly, the propulsion system must be able to propel the missile to Mach 5 and above. Secondly, the Glide vehicle must be able to withstand the effects of high speeds and reach the target intact and in working condition to perform its task.

Propulsion systems of normal rockets/missiles use liquid, solid, or even gaseous propellants which contain an oxidiser.[7] These are ignited in the rocket motor to produce thrust. On the other hand, Hypersonic missiles are based on air-breathing engines which carry only fuel rich propellants in their tank. These engines 'breathe in' pressurised oxygen required for combustion from the air during flight through well designed air intakes. The oxygen gets forcefully pressurised into the rocket motor due to the relative motion of the high speed of the missile and air. When air intake is at subsonic speeds it is called a Ramjet. When the air intake is at supersonic speeds, it is called a Scramjet. Airflow in a scramjet engine is kept supersonic throughout the entire engine. This ensures that the Scramjet can theoretically operate efficiently even at speeds between Mach 12 and Mach 24[8]. In practice, a Scramjet engine enables a missile to achieve speeds beyond Mach 5. Hypersonic missiles are therefore based completely on Scramjet engines. This technology is currently available with a few countries only. Scramjet engine is shown in Fig 3 for reference. A major point to be noted is that a Scramjet engine has to be taken up to a speed of Mach 1.5 or more through a booster engine before it can function. Hence a Hypersonic missile is invariable always a two stage propulsion system.

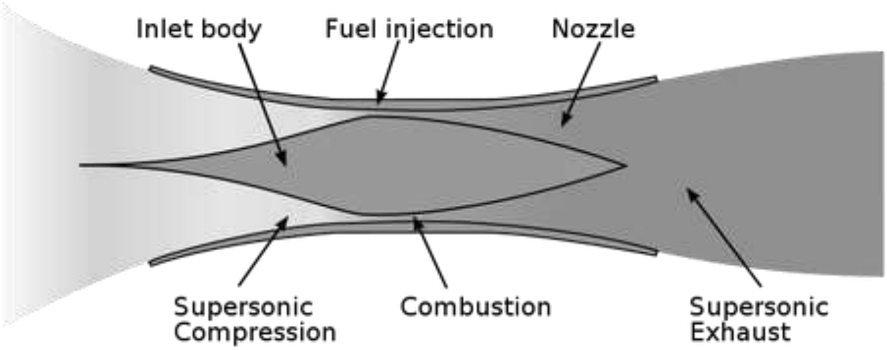


Fig 3: Scramjet Engine

A glide vehicle is essentially a remotely/autonomously piloted air craft which is flying at very high speeds in a very challenging environment. The design of the glide vehicle is therefore cutting edge technology. When a missile transits from supersonic conditions into the hypersonic environment, the external aerodynamic flows and forces on the surface of the glider are dominated by severe aerothermal heating. The high speeds at which a hypersonic missile flies creates a superheated atmosphere due to sheer air friction. This results in extreme thermal gradients and high pressures which stresses any material to fatigue point at accelerated rates as operational Mach numbers increase. This will invariably lead to material failures. Hence the material used is of utmost importance. The material is usually a combination of refractory metals, composites and ceramics. The design of the hypersonic vehicle is equally critical. It involves design of the aeroshell/primary structure, leading edges, control surfaces, thermal protection of exposed surfaces, propulsion, and guidance systems to perform satisfactorily under such extreme conditions. Existing materials are not resilient in such extreme environments. Design of such materials and structure involves cutting-edge research.[9]

Employment in Battle

Hypersonic weapons were employed for the first time in battle by Russia against Ukraine in their ongoing conflict.[10] Russia targeted an underground ammunition dump and a fuel depot in March 2022. Russia used the air launched Kh-47M2 Kinzhal hypersonic missile to strike targets in Ukraine on multiple occasions.[11] Russia has also demonstrated a ship launched hypersonic cruise missile named Zircon. In April 2024, President Putin stated that the Zircon was used in battle[12] and that it would be impossible to defend against it since the missile has a speed of Mach 8. These two episodes give us a basis on which one can visualise the likely employment of Hypersonic weapons in battle.

Hypersonic systems would be used against high value time specific targets at long ranges (from a hundred to a thousands of km). They would be employed where there is a requirement of high accuracy while attacking a pinpoint target. For instance, the Chinese have made much of the DF 17 being a 'carrier killer' [13]; implying that their hypersonic weapons have the capability of pinpoint accuracy against a fast moving and well protected target like an aircraft carrier. This also implies that hypersonic missiles will be used to overwhelm and penetrate the air defences of the adversary through their sheer speed. The manoeuvrability of hypersonic missiles gives them the advantage of creating uncertainty about their final target. This also enables to spread and stretch the adversary's air defence system. Hypersonic missiles could also be equipped with nuclear or conventional warheads. This creates ambiguity in the opponent's mind.

It must also be realised that hypersonic weapons are 'niche' by nature and are far costlier than ballistic missiles.[14] Nations will only have a limited number in their kitty. Hence, they need to be employed with care. More importantly they cannot be employed everywhere. Further, a missile can hit only one target with a given warhead. To that extent they can be game changers only when used with care. Hence ISR of a very high order as also a thorough target analysis will be necessary. Reconnaissance strike integration will have to be through a dedicated command and control system. In such an environment, there will also be a necessity of space-based inputs through a global positioning system combined with wide spread ground stations to provide control inputs to the missile once launched. On the whole executing a hypersonic strike in a dense AD environment against a target moving at about 30-40 miles per hour will be a complicated, challenging task which needs detailed planning and coordination.

From all available sources it is pretty apparent that the Russian use of hypersonic missiles have really not been a game a changer in battle. In fact, if Russia had not announced that it had employed its hypersonic weapons, it would not have been even known. Russia has used its hypersonic systems for conveying a strategic message as part of its deterrence plan to keep NATO out of battle. From all available analysis, it has achieved its aim of keeping NATO out of the contest not only by use of a hypersonic missile but by employing an implicit nuclear threat. Overall whether a hypersonic weapon is actually used against a high value target or used demonstratively against any other target, its employment has geostrategic ramifications. This is a factor one must be cognisant of.

Defending Against Hypersonic Weapons

The rationale of a hypersonic weapon is that its high speed and low trajectory makes defence against it very difficult. It is supposed to be impervious to even advanced air defence systems. However, it is to be noted that "Ukraine has announced that the Ukrainian Air Force shot down a Kinzhal hypersonic missile using the Patriot PAC-3 air defence missile system on May 4, 2023."[15] Hence hypersonic missiles can be detected and intercepted.

Defending against a Hypersonic attack hinges on disrupting its 'kill chain'. A kill chain consists of surveillance systems to locate targets, communications networks to relay targeting information to weapons launchers followed by actual launch of a missile. Once launched, the missile needs to home on to its target. Each step in the 'kill chain' is vulnerable to interdiction or disruption. Very often the effort is to discern and home on to the weakest links in the chain. It is axiomatic that defending against a hypersonic threat will involve a detailed analysis of the threat and how it can manifest. This would lead to a plan to defeat the threat.

One of the basic methods is to put in a passive missile defence. Passive methods include dispersion, deception and hardening. Dispersion of asset bases and personnel across the battle field in sync with the terrain and environmental conditions is a time tested method. It ensures that the detractive impact of a missile attack is limited and strike effectiveness is reduced while retaining own combat potential. Missiles can also be deceived by presenting them with false targets either physically or electronically. One can resort to an elaborate system of decoys or flood the enemy information system with false targets. The alternative is of course to camouflage the likely targets either physically or electronically. Likely missile targets can be hardened and made resilient so that they can withstand a missile attack and bounce back. This could be through a system of having adequate reserves or through good repair and recovery methodology.

There would also have to be a surveillance system in place to effectively monitor hides and launch sites of the weapon so as to actively disrupt its deployment in the first place. Alternately, the weapon/missile can be tracked throughout its flight, either through over the horizon or space based capability. Invariably it would have to be a combination of the two. The weapon can be disrupted either electronically or physically on launch, in mid-flight or in its terminal phase. Hence a layered surveillance and air defence capability must be put in place. The current thought process is to shoot incoming missiles down through down kinetic interception. It could be done by direct collision or blast-fragmentation interceptors that explode at close distance, spraying shrapnel into the hypersonic vehicle. In future use of lasers, high-powered microwaves, rail guns, or particle clouds designed to disrupt hypersonic weapons in flight will invariably be devised. These could be space or land based.

However, this is easier said than done since 'Hypersonic weapons are extremely difficult to detect and counter given the weapons' speed and manoeuvrability, low flight paths and unpredictable trajectories.[16] The entire concept of a countering and defending against a hypersonic system is a work in progress. As days go by better and more holistic counter hypersonic systems will evolve.

China's Thought Process on Hypersonic Weapons

It is well known that China possesses 'the most significant ground-based missile force on Earth.'[17]. It is also the largest and most diverse missile arsenal in the world.[18] An important component of China's rocket force is its hypersonic weapon capability. The Chinese opine that hypersonic weapons give it the capability to 'fight and win wars against a strong enemy (United States), counter an intervention by a third party, and project power globally'. China places faith in its rocket force to threaten U S Forces with a barrage of long range precision guided missiles. They believe that such a tactic will force the US military to keep a safe distance away from its shores/area of operations. As explained by one Pentagon official when the Chinese can deploy [a] tactical or regional hypersonic system, they hold at risk our carrier battle groups. They hold our entire surface fleet at risk. They hold at risk our forward-deployed forces and land-based forces. The Chinese also aim to paralyze or incapacitate US military capability in the initial phases of any future battle. In Chinese thinking, hypersonic weapons will help immensely in disintegration of US force capability. They also feel that China can also pose a new threat to mainland USA if their hypersonic weapons are deployed as part of naval task forces operating from forward bases in the Pacific.

China, at this point of time sees itself as being far ahead of its peer competitors in Hypersonic technologies and weapons. Hypersonic missiles with conventional warheads could provide China with better escalation controls and capability to deter USA from intervening in a regional conflict specially in a Taiwan scenario. Against this backdrop, in 2019, China deployed its first operational hypersonic system, the DF-17 hypersonic glide vehicle (HGV) capable medium-range ballistic missile (MRBM).[19] In a regional conflict in the Western Pacific, it is estimated that China will have the advantage of being able to fight from its territory. This implies that while its own forces can be dispersed yet be logistically well disposed, the forces of its adversaries would be stretched logistically and be forced to operate in a concentrated manner from specific bases only. This gives China's rocket force and its plethora of hypersonic weapons a huge advantage.

Employment of Hypersonic Missiles in Joint Warfighting in India

It is evident from the above discussion that if the hypersonic missile system have to be weaponised by India in the Tri-services construct, these have to be produced in adequate numbers and that too indigenously. Proper selection of targets has to be done to get value for the cists invested. Like nuclear arsenal, these also have the huge potential of strategic signalling which has successfully attempted by Russia. Since, China has taken the lead in this field, India needs to galvanise the R&D, manufacturing and employment.

Conclusion

The ability to deploy and employ high manoeuvre hypersonic weapons with long ranges is a major strategic advantage for any country since they can evade current defence systems and be effective on their targets with great effect. However these weapons are not game changers unless reconnaissance strike integration of a high order is in place. Presently it is only China and Russia which have these weapons in their inventory. The US is in an advanced stage of testing them. North Korea has also carried out some tests of hypersonic weapons. Australia, India, France, Germany and Japan have the capability and technology to develop them and are in the process of doing so. In addition, Iran, Israel and South Korea are also carrying out some research in this field. As Hypersonic weapons are being developed, there is also a parallel development in defence against these systems. All in all, as the hypersonic system technology matures, these weapons will continue to dominate strategic thinking in years to come.

****

Lt Gen P R Shankar, PVSM, AVSM, VSM (Retd) is a retired Director General of Artillery. He gave great impetus to the modernisation of Artillery through indigenisation. He has deep knowledge, understanding and experience in successful defense planning and acquisition. The General Officer is now a Professor in the Aerospace Department of Indian Institute of Technology, Madras.,

Chennai. He is actively involved in applied research. He writes extensively on defence and strategic affairs at www.gunnersshot.com

NOTES

[1] DF-17 Dongfeng-17, (2024), " Mobile medium-range ballistic missile with hypersonic glide vehicle – China" , Army Recognitionhttps://armyrecognition.com/military-products/army/missiles/hypersonic-missiles/df-17-mobile-ballistic-missile-hypersonic-glide-vehicle-data-fact-sheet

[2] IISS, (2022), "China's 2021 orbital-weapon tests", URL: https://www.iiss.org/en/publications/strategic-comments/2022/chinas-2021-orbital-weapon-tests/#:~:text=In%20mid%2D2021%2C%20China%20launched,hit%20targets%20on%20Chinese%20territory.

[3] Congressional Budget Office, (2023), U.S. Hypersonic Weapons and Alternatives, URL: https://www.cbo.gov/publication/58924

[4] Tom Karako and Masao Dahlgren, (2022), "Complex Air Defense Countering the Hypersonic Missile Threat", CSIS, URL: https://missilethreat.csis.org/wp-content/uploads/2022/02/220207_Karako_Complex_AirDefense.pdf

[5] Congressional Budget Office, (2023), U.S. Hypersonic Weapons and Alternatives, URL: https://www.cbo.gov/publication/58924

[6] Shan Shaikh , (2021), "China's Hypersonic Future", Missile Threat, URL: https://missilethreat.csis.org/chinas-hypersonic-future/

[7] Science Direct, (2003), "I.E Combustion in Rocket Engines", URL: https://www.sciencedirect.com/topics/earth-and-planetary-sciences/air-breathing-engine

[8] Aero Notes, "Scramjet Engine", URL:https://aeronotes.weebly.com/scramjet-engine.html

[9] Adam B Peters et al, (2024), "Materials design for Hypersonics", Nature Communications, 15:3328, URL: https://www.nature.com/articles/s41467-024-46753-3

[10] Thomas Novelly, (2022), "Russia's Alleged Use of First Hypersonic Missile in Combat Downplayed by US Military and Allies", Military .com, ULR: https://www.military.com/daily-news/2022/03/22/russias-alleged-use-of-first-hypersonic-missile-combat-downplayed-us-military-and-allies.html

[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-evaluates-russias-use-of-hypersonic-daggers-in.html

12 Keshav Padmanabhan (2024), "'Impossible to defend against' — what is Zircon hypersonic missile that Putin says Russia used in battle", The Print, URL: https://Theprint.In/Theprint-Essential/Impossible-To-Defend-Against-What-Is-Zircon-Hypersonic-Missile-That-Putin-Says-Russia-Used-In-Battle/1983838/

13 Otto Kreisher, (2013), ""China's Carrier Killer: Threat and Theatrics", Airforce Magazine, URL: https://www.airandspaceforces.com/PDF/MagazineArchive/Documents/2013/December%202013/1213china.pdf

14 Congressional Budget Office, (2023), U.S. Hypersonic Weapons and Alternatives, URL: https://www.cbo.gov/publication/58924

15 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-evaluates-russias-use-of-hypersonic-daggers-in.html

16 David Vergun, (2023), "General Says Countering Hypersonic Weapons Is Imperative" , US Department of Defence, URL: https://www.defense.gov/News/News-Stories/Article/article/3391322/general-says-countering-hypersonic-weapons-is-imperative/

17 P R Shankar, (2023), "PLARF – China's Rocket Force Plagued By Poor Quality, Corruption; Bulk Of Missiles May Never See Action", Gunners Shot, URL: https://gunnersshot.com/2023/12/09/plarf-chinas-rocket-force-plagued-by-poor-quality-corruption-bulk-of-missiles-may-never-see-action/

18 Shan Shaikh , (2021), "China's Hypersonic Future", Missile Threat, URL: https://missilethreat.csis.org/chinas-hypersonic-future/

19 Department of Defence, (2021), "Military and Security Developments Involving the People's Republic of China", Government of the United States of America, URL: https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF

ADVISORY BOARD & EXECUTIVE COUNCIL
CENJOWS

Advisory Board

Shri Rajnath Singh, Raksha Mantri, Patron-in-Chief
Shri Sanjay Seth, Raksha Rajya Mantri
General Anil Chauhan, PVSM, UYSM, AVSM, SM, VSM, ADC
Chief of Defence Staff
General Upendra Dwivedi, PVSM, AVSM, ADC
Chief of the Army Staff
Air Chief Marshal VR Chaudhari, PVSM, AVSM, VM, ADC
Chief of the Air Staff
Admiral Dinesh K Tripathi, PVSM, AVSM, NM
Chief of the Naval Staff
Shri Giridhar Aramane, IAS, Defence Secretary
Lt Gen Johnson P Mathew, PVSM, UYSM, AVSM, VSM
CISC & Chairman CENJOWS
Vice Admiral Suraj Berry, AVSM, NM, VSM, C-in-C, HQ SFC
Shri Sugata Ghosh Dastidar, IDAS, Secy (Def/Fin)
Lt Gen HS Lidder, PVSM, UYSM, YSM, VSM (Retd)
Vice Admiral Shekhar Sinha, PVSM, AVSM, NM & Bar (Retd)
Lt Gen Satish Dua, PVSM, UYSM, SM, VSM (Retd)
Air Marshal BR Krishna, PVSM, AVSM, SC (Retd)

Executive Council

Lt Gen Johnson P Mathew, PVSM, UYSM, AVSM, VSM
CISC & Chairman CENJOWS
Vice Admiral Sanjay Vatsayan AVSM, NM, DCIDS (PP & FD)
Lt Gen DS Rana, AVSM, YSM, SM, DGDIA & DCIDS (Int)
Lt Gen Vipul Singhal, AVSM, SM, DCIDS (DOT)
Air Marshal Jeetendra Mishra, AVSM, VSM, DCIDS (Ops)
Air Marshal MS Sridhar, DCIDS (Med)
Brig AS Dabas, DACIDS (MS & SD)
Air Cmde Jagdeep Shetty, DACIDS (Adm & Coord)

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 further published & printed Sabre & Quill Publishers

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 SEP 24)

(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).**

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 2,500/-
<u>Note</u>: 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
