Issue Brief

July 2024
No : 402

Internet of Battlefield Things: Warfighting in Realtime

Major Gaurav V Mhetre

Internet of Battlefield Things: Warfighting in Realtime

Major Gaurav V Mhetre

Abstract

We are living in an era wherein "smart things" will dictate how we lead our lives. Internet of Battlefield Things (IoBT) will create a huge impact in gaining leverage over the adversary in a manner and magnitude that is difficult to comprehend. IoBT, with its ability to provide efficient situational awareness in the battlefield, can change the course of battles.

The concept of IoBT is still at a nascent stage and significant efforts are being made Research and Development (R&D) for practical implementation of IoBT all over the world —— the Army Research Laboratory, USA and National University of Defence Technology, China being the notable among them. Under the 'Atmanirbhar Bharat' slogan, several projects like NFS, iSentinel are in the pipeline in this field.

The Armed Forces need to focus on a 'bottom-up' approach and enable the smallest of teams to work with 'intelligent' systems. However, implementation of IoBT where human soldiers and machines form tailor-made units/teams for specific tasks, comes with numerous challenges that warrants various changes to approach, training, organisation etc.

Keywords: Niche Technology, IoBT, Robots, AI, Blockchain

Introduction

Internet has now become so much part of everyday life that its vulnerabilities are not realised easily. We are living in a time where every possible thing is getting smart and the days are not far when the machines or "smart things" will dictate how we lead our lives. The smart devices or "things" along with technology that facilitates communication between devices and the cloud constitutes 'Internet of Things' (IoT), applications of which are to be seen in many fields such as medicine, manufacturing, logistics, home appliances etc. IoT, when utilised for military applications, is going to create a huge impact and help in gaining leverage over the adversary in a manner and magnitude that is difficult to comprehend. Several modern militaries have incorporated niche technology in various fields for modernisation like drones, robots for medical support, cyber defence, integrated surveillance etc. Moreover, with the induction of 5G, weaponisation of "things (comprising both machines and the man behind machines)" for strategic advantage in cyber, air, land, space and maritime domain, will certainly accelerate the tempo of operations in both offensive and defensive postures. Therefore, it is certain that 'Internet of Battlefield Things' (IoBT) is the future of military operations and military strategists will have to incorporate its huge impact while envisioning the 21st century warfighting scenario.

IoBT will Change How War is Waged and How Peace is Maintained

Situational Awareness forms the bedrock of national security. For example, due to strong situational awareness of Israel and its allies coupled with supreme air defence technology, Iran's airstrike on Israel as part of 'Operation Iron Shield', was averted without much damage. Accurate situational awareness serves as the basis for planning operations followed by controlling them by observing and adjusting their effects. Excellent situational awareness depends on continuous surveillance provided by diverse sensors. To be effective, the surveillance systems must be connected with Command and Control (C2) Centres over a robust network and the C2 Centres must further be connected with fighting arms in real-time. These entities are distributed over space, mobile and are heterogeneous. They include aircrafts, long-range vectors, vehicles and troops on ground and must operate effectively together while fighting battles, maintaining defensive posture, assisting in humanitarian relief etc.

Coordination and control requires planning and continuous monitoring of a plan's execution. Yet, no plan can be considered as infallible. It is said that plan is the first casualty of war. The reason is not because parts of the plan fail as good commanders develop contingencies in their plans. Good plans fail because of what is called the "fog of war" (Clausewitz,1989)— the uncertainty regarding one's own capability, enemy capability and his intent during any operation or campaign which is primarily due to a breakdown of visibility and communication in the battlefield. The fog of war prevents a commander from knowing real-time details as to which part of the plan needs immediate attention. The attacking units and the entities supporting the operations lose track of the location and status of their reinforcements and supplies etc. In the future, IoBT promises more than just improved efficiency in ensuring command and control in the battlefield, and has the ability to change the course of battles. It can do so by physically altering the battlespace by dynamically joining vast numbers of smart, heterogeneous sensors, processors and actuators over robust and secure networks. Thus, IoBT has the capability to dispel the fog of war. Some of the main benefits of IoBT for defence and national security (Douglass et. al. 2022) are as under:-

- ***Increased Tempo of Warfighting.*** More autonomy in defence systems entails lesser time for flow of information and requirement of humans. Actions can go from sensors to C2 centres in milliseconds instead of seconds, minutes, or hours.
- ***Automated Weapons.*** IoBT increases automation and enables autonomous surveillance systems, weapons including long-range vectors to be employed effectively.
- ***Reducing Own Casualties.*** Owing to smart sensors accurately identifying the target and Precision Guided Munitions/ Target Guided Munitions (PGMs/TGMs) effectively engaging them, own casualties can be reduced to a great extent thereby achieving enhanced operational efficacy.
- ***Increasing the Probability of Destroying Targets.*** Onboard and off-board sensors in an IoBT network can guide PGMs/TGMs more accurately to their intended target. Automated control loops can modify flight paths more rapidly and more accurately than weapons that are manually sighted and fire dumb ammunitions.
- ***Intelligent Processing (AI and Big-data).*** IoBT provides intelligent processing to expand human ability to observe. As the future battlefield will be inundated with sensors, it will be important to filter, prioritise and abstract information of intelligence value, for commanders to make wise decisions. AI can further simplify the process by demonstrating human level intelligence in aspects of military operations, however, due caution must be exercised.
- ***Expands the View for Military Operations.*** IoBT networks can join large number of dispersed sensors covering wide areas. It can as well observe an area, event or activity in a more pervasive, multi-view and continuous manner. IoBT sensor networks support improved human interpretation of sensor data and deliver training data through the cloud for intelligent processing algorithms.
- ***Automation of Logistics.*** Logistic activities, such as resupply, deployment, and maintenance will become more efficient. With the induction of IoBT, a soldier can efficiently monitor where supplies currently reside and what resources are available to get those supplies delivered to the desired location

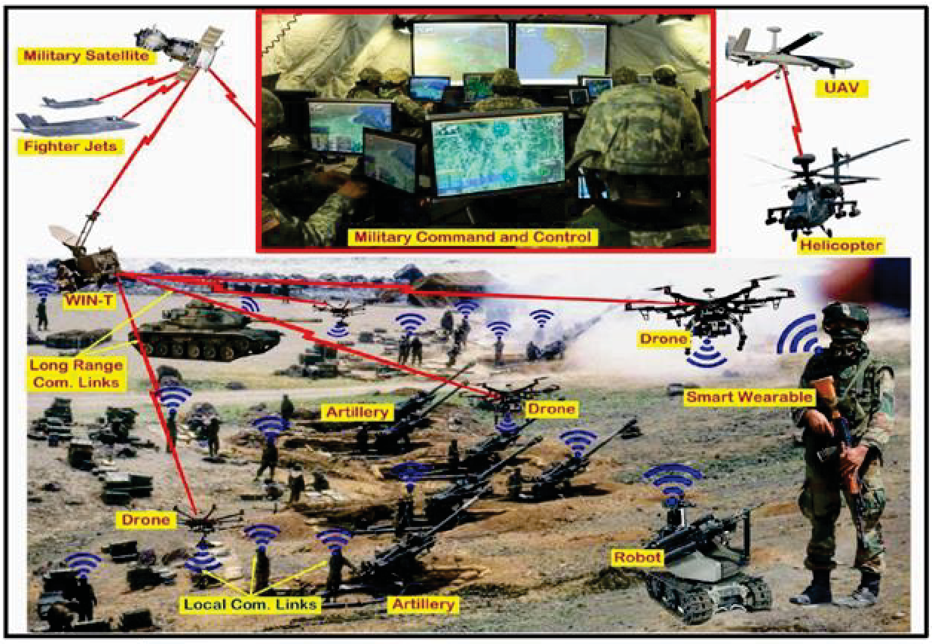
in time. This would optimise administration and logistics both in war and peace.

IoBT : Expanse in Military Operations

As even today, conflicts remain long-drawn affairs and battles have turned swift and lethal. This is so primarily because of long ranges of surveillance devices coupled with robust communication systems and long range vectors. However, smart systems and low latency of 5G (US DoD, 2024) will further enable remote operations to be monitored by the commanders in real-time thereby doing away with delay in operations caused due obtaining bunch of permissions. In the IoBT, sensing and surveillance resources such as satellites, drones, active and passive surveillance equipment as also soldiers on ground, are used to draw valuable information through various sensing equipment. Using cloud and edge computing, these equipments are further connected to create a cohesive fighting force, thereby enhancing operational efficacy. Having said this, it is pertinent to understand the expanse of IoBT (Frost and Sullivan, 2019) technology in the realms of battlefield. Various actions that can be carried out using the technology are:-

- Gathering Battlefield Data.
- Monitoring the Soldier's Health.
- Equipment and Vehicle Fleet Management.
- Identifying Adversaries.
- Smart Bases.
- Remote Training.

Figure 1: Components of IoBT



Source: https://x.com/DefenseCharts/status/1564984101207248896

IoBT: Challenges in an Uncertain Environment

Future warfighting will be characterised by effective cooperation between intelligent networked things and human fighters (machines and the men behind machines). A variety of artificially intelligent things connected to a network like guided missiles, unattended ground sensors, unmanned aerial vehicles etc. will dominate the battlefield and work in tandem with soldiers in a highly hostile environment. An extremely fast-changing battlefield will pose a real challenge wherein confusion, deception, etc. will be exploited to gain advantage over the adversary. Hence, IoBT must offer support for several application requirements:-

- ***Diverse Missions, Tasks, and Goals.*** IoBT should be specifically conditioned to meet the requirements for a mission. Tasks may vary from wide area persistent surveillance— tracking dispersed groups of targets moving throughout a cluttered environment, to local tasks such as monitoring the physiological and psychological state of soldiers. Tasks are not expected to start or end simultaneously and new tasks may emerge throughout a mission.

- ***Rapid Adaptation to Changing Tasks.*** To maintain operation tempo, goal-driven IoBTs must be composed and deployed rapidly— for instance, in a quickly formed forward assembly area/ release point. Once deployed, the dynamics of the battlefield will generate changes to missions, cause new tasks to emerge, and provoke commanders to change tactics. These changes make it necessary for the IoBT to be capable of maintaining synchronisation with the current mission needs and specifications and also provide effective support for new tasks that may simultaneously emerge.
- ***Highly Resource-Constrained Assets***. Many systems will be simultaneously deployed in IoBT and consist of disadvantaged assets with limitations on energy, power, storage, bandwidth, infrastructure (fixed infrastructure may not be available) etc. IoBT must be able to operate under these severe constraints without hindering their support for tasks with stringent time deadlines.
- ***Extreme Heterogeneity.*** Heterogeneity is seen across multiple dimensions of an IoBT. Variety of sensing devices creates multi-modal data and variety of computing devices create diverse processing capacities. Further, even adversaries would employ IoBT. Hence, it becomes very important to create a robust IoBT network that can withstand such heterogeneity and also provide reliable solutions.
- ***Contested and Adversarial Environments.*** Many IoBTs will be forward deployed with limited physical security. Much like today's electronic warfare, IoBT will be targeted by the enemy, while securing their own IoBT. This implies that own IoBT must be protected from sophisticated and persistent threats while trying to disrupt enemy IoBT to gain leverage over the adversary. Cyber/information security measures must be taken to protect IoBTs, and analytics must be able to deal with conflicting and deceptive data to safeguard their own systems.

IoBT: A Global Perspective

The concept of IoBT is still at a nascent stage and significant efforts are being made Research and Development (R&D) for practical implementation of IoBT all over the world.

Recently, a study was conducted at the National University of Defense Technology (Changsha, China) {Feng et. al. 2020} to study the robustness of IoBT in a directed network. Several important conclusions were drawn out and are as under:-

- The ability to maintain network connectivity under enemy attacks is a critical property of IoBT networks.
- Applying the network model, an analysis of the robustness of IoBT network under the optimal attack strategy was carried out, which provided insights into the development of effective strategies to ensure the security and sanitization of IoBT network despite enemy interference.
- The heterogeneity of devices and heterogeneous multi-layer networks would increase the complexity of IoBT.

Similarly, Army Research Laboratory strategically placed under the Army Futures Command, USA has instituted the Collaborative Research Alliance (CRA) for R&D of niche technology that includes IoBT, artificial intelligence, cyber security, robotics, etc. The IoBT CRA (DEVCOM) focuses on the augmentation of commercial IoT research, with interdisciplinary science, to address army complexities especially operations in highly dynamic, resource-constrained and adversarial environments.

Manifestation of IoBT in the Indian Armed Forces

Considering a threat to our national security, both from the West and the North, rapid modernization of our military capabilities is need of the hour. With overwhelming requirements of equipment modernisation and other operational and logistic challenges, employment of niche technologies comprising robotics, artificial intelligence (AI) and IoBT is yet to begin in a full-fledged manner. However, limited use of niche technology has started in some critical formations using commercial off-the-shelf equipment.

In the Indian context, IoBT R&D is still in nascent stages. This needs immediate attention considering the size of the economy and also the fact that India has arrived on the global stage and many nations especially, those belonging to the Global South, see India as their leader.

5G technology is the bedrock of implementing IoBT and the all-pervasive nature of 5G will be crucial for fast flow of information in the IoBT network. The testbed of Indian 5G research at IIT Madras (TOI, 2022), has achieved complete end-to-end solutions indigenously and is customisable including a secure NB-IoT Chip. There is a need for deploying indigenised

5G solutions across varied terrain configurations while utilising the existing radio, fibre, and satellite data links.

- ***Project Network for Spectrum (NFS).*** In 2012, under the Network for Spectrum (NFS) project, the Ministry of Defence (MoD) and Department of Telecommunication (DoT) conceptualised a network to connect critical defence locations. The project encompasses creating an optical fibre cable-based network exclusively for defence communication. OFC cables have been laid all across the nation in varied terrain profiles including intrusion-proof cable technology, network monitoring and GIS mapping, making it the most advanced and secure network for the armed forces. This can be further exploited for creating IoBT network exclusively for the armed forces.

Under the 'Atmanirbhar Bharat' slogan, several new projects are being implemented by the Department of Defence Production (MoD). As per reports of July 2022, several projects integrated with AI are being developed. Some of them are enumerated as under:-

- ***iSentinel - Intelligent Automated Threat Tracking and Identification System.*** Designed as a surveillance system for CI/CT environment, iSentinel is a deep learning-based threat detection and tracking system. It can be effectively incorporated with Anti Infiltration Obstacle Systems (AIOS) with an aim to address cross-border terrorism.
- ***Smart Helmets.*** To address the need for real-time situational awareness, the 'Smart Helmet' can capture 3D information of any unknown environment in real-time and assist in various decisions. The 'Smart Helmet' comprises of an optical sensor, mounted on the helmet of an active combat soldier, and can be effectively used for special operations in LC scenario and also in border management postures along the northern borders. This helps in tracking potential threats and also location of own troops inside an unknown environment thereby creating a comprehensive situational awareness for decision making.
- ***Permissive Block Chain Mechanism.*** The solution is intended to create a Trusted Communication Platform using Blockchain. The idea is to establish a secured network for data transfers between the entities. This technology will

form an inherent part of the IoBT network which is crucial for ensuring transparency, security and auditability among entities using the network.

Considering the ongoing progress in terms of developing niche technology under the ‘Atmanirbhar Bharat’ Project and Indian Army’s ‘Year of Technical Absorption’, there is a need to integrate outputs from sources like AI, Robotics, drones, deep learning, blockchain technology along with IoT, to come up with tailor-made solutions for specific problems such as operating in CI/CT grid or countering Chinese threat in High Altitude Areas (HAA) along the northern borders.

Implementation of IoBT in the Indian Army

Owing to the development of niche technology in warfighting, there will be substantial change in the way the Indian Army will operate in recent future. The armed forces need to focus on a ‘bottom-up’ approach and enable the smallest of teams to work with ‘intelligent’ systems. However, implementation of IoBT where human soldiers and machines form tailor-made units/teams for specific tasks, comes with numerous challenges and warrants various changes to approach, training, organisation etc., some of which are as under:-

- ***Approach to Warfare.*** There is a need to adopt a holistic approach to warfare and even maintain defensive posture that incorporates several changes to tactics, drills due to emerging technologies. It requires decision-makers, junior leaders as also the troops on ground to get abreast with handling the technology and operating the same in fast paced and vulnerable environment. At present, the Indian Armed Forces are driven by specific arms and services, but there is a need to break specific silos and focus on more jointness in operations in a well-connected IoBT network.
- ***Information Warfare.*** In today’s warfare, information is the most lethal weapon. Hence, there is a need to incorporate an Information-driven culture that emphasises specific procedures for collecting, collating and disseminating data using the IoBT network.
- ***Man v/s Machine.*** With the implementation of autonomous systems like robots, swarm drones and UAVs, there is a huge risk of taking humans ‘off the loop’. Human logic cannot replace machine intelligence to win wars. Hence, there is a need to reserve decision-making with commanders in the

Observe, Orient, Decide, Act (OODA) loop while creating an IoBT network infused with 'artificially intelligent' sensors and smart weapons capable of delivering immense firepower within a short span of time.

- ***Independent 'cloud' for the Armed Forces.*** The Indian Army has launched a highly encrypted 'Army Cloud', as part of its technology absorption initiative, in similar lines with 'Megh Raj' cloud service of National Informatics Centre. The 'Army Cloud' along with Network for Spectrum (NFS) project will revolutionise strategic decision-making at the highest level once the smart sensors are integrated to provide a comprehensive picture of the battlefield in real-time.
- ***Focus on Specialisation.*** Research and Development in emerging technologies demands officers to be specialised in the domain. Innovation, being an important aspect, requires individuals to work for a considerable time for a project to fructify. Recently, the Army introduced an HR policy (Dutta, 2024) wherein officers specialising in niche technologies can continue in the same domain on promotion to Colonel instead of getting posted out for command assignments. Such policies incentivizes R&D of niche technologies and help in speedy transformation into a technologically superior force. A similar effort can be undertaken at the tri-services level.
- ***Training Aspects.*** Along with R&D, it is also important to train the tactical commanders, junior leaders and troops on ground to effectively utilize niche technology while in active operations. Manual war gaming has been a method for a long time. However, emerging technologies requires a new approach to training. Computerized war games can be introduced that cater to various possible scenarios like cyberattacks, jamming, drone warfare, enhanced operations using IoBT network, etc.
- ***Cyber Security.*** As future battles will be fought with machines connected over various networks, cyber security assumes greater importance. We are already in an age where wars are fought on the field and also off the field, as we have seen in the case of the Russia-Ukraine war, the conflict in the Middle East or even COVID-19.

Conclusion

IoBT as a technology is certain to impact the future battlefield comprehensively. As a rapidly developing nation and also one of the strongest military might in the world, it is our responsibility to develop and incorporate this technology to our advantage at the earliest. Combining IoBT with other niche technologies would further act as a force multiplier and enable our Armed Forces to fight future battles in real-time.

Works Cited

Douglass, R., Gremban, K., Swami, A., & Gerali, S. (Eds.). (2022). *IoT for Defense and National Security*. John Wiley & Sons. Inc. https://onlinelibrary.wiley.com/doi/book/10.1002/9781119892199.

Dutta, A. N. (2024, January 15). Army to let Lt Cols who specialises in niche tech opt out of command posts. The Indian Express. https://indianexpress.com/article/india/army-to-let-lt-cols-who-specialise-in-niche-tech-opt-out-of-command-posts-9109427/.

Feng, Y., Li, M., Zeng, C., and Liu, H. (2020). Robustness of Internet of Battlefield Things (IoBT): A Directed Network Perspective. *Entropy* 22(10), 1166. https://doi.org/10.3390/e22101166.

Howard, M.E. and Paret, P. (Trans.). (1989). *On War* by Carl von Calusewitz, Princeton University Press. ISBN: 978-0691018546. Department of Defence Production. (2022, July 7). Artificial intelligence in Defence [Press release]. https://www.ddpmod.gov.in/artificial-intelligence-defence.

Internet of battlefield things (IoBT) CRA. *DEVCOM Army Research Laboratory*. https://arl.devcom.army.mil/cras/iobt-cra/.

(2022, May 17). Indigenous 5G test bed in telecom sector is an important step in India's self-reliance: PM Modi at Trai event. *The Times of India*. https://timesofindia.indiatimes.com/business/india-business/indigenous-5g-test-bed-in-telecom-sector-is-an-important-step-in-indias-self-reliance-pm-modi-at-trai-event/articleshow/91612406.cms.

Kulkarni, M. (2022, December 5). IoT at Battlefields will make life of Soldiers Safer and Easier. *Medium*. https://medium.com/@manas.kulkarni21/iot-at-battlefields-will-make-life-of-soldiers-safer-and-easier-63001928a368.

(2020, August 24). NFS: Optical Fibre Cable for Critical Defense. (*STL Tech*. https://stl.tech/blog/nfs-in-the-service-of-the-nation/.

(2019). US DoD 5G and IoBT Activities, Forecast to 2024. *Frost and Sullivan*. https://store.frost.com/us-dod-5g-and-iobt-activities-forecast-to-2024.html.

About the Author

Major Gaurav V Mhetre was commissioned in the Regiment of Artillery in 2018. He is an alumnus of RIMC, Dehradun, NDA, Khadakwasla and IMA, Dehradun. The officer has served in High Altitude Areas along LAC in Arunachal Pradesh and Sikkim. The officer has been nominated for Long Gunnery Staff Course at School of Artillery, Devlali.

No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from CLAWS The views expressed and suggestions made in the article are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.