MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Absorption of Emerging Technologies in Armed Forces

Akshat Upadhyay

March 01, 2023

Summary

Critical and Emerging Technologies (CETs) can be classified in terms of their use in war, i.e., as battlefield and over-the-horizon (OTH). Battlefield CET refers to those technologies that can be used for warfighting and used explicitly on the battlefield. OTH CET comprises technology which can be used in the non-kinetic domain and includes cyber-physical attacks, influence operations, big data analytics (BDA), among others. There is a need to rethink organisational structures in the Indian armed forces to optimally integrate CETs. Given that data is at the heart of CET, robust cyber security standards need to be put in place for data privacy and protection.

Introduction

The prototypes showcased at the recently concluded Aero India 2023 at Bengaluru are symptomatic of two major shifts underway within the Indian Armed Forces. The first is the move towards 'Atmanirbharta' or self-reliance, while the second is an added emphasis on critical and emerging technologies (CET). While self-reliance or indigenisation in defence has unlocked the entrepreneurial spirit of the Indian private sector and is essential for retaining the country's strategic autonomy, a move towards mainstreaming CETs is equally important given the changed nature of the battlefield facing India today. This Brief examines the importance of CETs in the military domain, the efforts undertaken by the Indian government and the Armed Forces in promoting the use of CETs and the optimum organisational structure for absorption of these technologies and finally recommends some steps that need to be undertaken so that these technologies can be utilised to their full potential.

Changed Nature and Character of War

It has become quite a cliché to talk about the changed character of war or HOW war is fought. The presumptive component is the unchanged nature of war or WHAT war entails. War, at its most basic and primal level, is understood as the calibrated use of violence to attain political objectives. It is taken for granted that at the foundational level this notion holds true, i.e., war is about violence and only the tools, organisation and application of violence for gaining political ends are bound to change. However, of late there has been a change in the way war is conceptualised. Warfare has become both non-contact and non-kinetic in its character and the nature of war has become diffused, i.e., violence is no longer the scaffolding on which war is visualised. This is due to a number of technological and historical factors. Due to the limited scope of this Brief, only the technological factors will be examined.

Three significant technological shifts have taken place since the end of World War II. Advances in semiconductor technology, creation of data through the process of digitisation and finally, systems integration have had a profound impact on the way war is imagined and fought. These three processes have combined to create a host of new technologies, collectively called critical and emerging technologies (CETs). The CETs include artificial intelligence (AI), quantum processing, advanced unmanned systems, internet of things (IoT) and cloud computing, among others. The common thread is electronics and data. Electronics and therefore, semiconductors, have become ubiquitous in the modern age.

Non-kinetic warfare, i.e., the use of non-violent methods of warfighting, has diffused with far-reaching effects. Disinformation and propaganda has become amenable to being individualised. Similarly, the dependence of countries on access to the latest electronics components for growth has created leverages for certain countries controlling chokepoints of the semiconductor supply chains.[1] Export controls and outright bans can be used,

[1] Henry Farrell and Abraham L. Newman, **"Weaponized Interdependence: How Global Economic Networks Shape State Coercion"**, *International Security*, Vol. 44, No. 1, July 2019, pp. 42–79.

again, as part of non-kinetic means of waging war. On the non-contact front, the precision revolution that started in the 1970s in the later stages of the Vietnam War and which reached its high point during the First Gulf war[2], has combined with the ongoing data revolution to create precise and deadly weapon systems supplemented by sensor-fusion, advanced intelligence, surveillance, target acquisition and reconnaissance (ISTAR) and the ability of joint fires without the need for massing forces. Both non-contact and non-kinetic means of warfighting are dependent on CETs.

Why are CETs Important?

CETs have become essential components in the warfighting domain due to the three shifts alluded to earlier. Advances in semiconductor technology has led primarily to generation of massive amounts of data. This has become possible due to the 'PC revolution'[3] which led to computers being mainstreamed in citizens' homes, followed by the advent of smartphones, pioneered by Apple and finally the current phase, which is dominated by 'wearables' such as smart watches, and IoT devices like smart bulbs, speakers, cameras, etc. At every stage, the cost per unit of these devices has decreased exponentially.[4] Then Intel Chief Executive Officer (CEO) Paul Otellini's 2013 prediction that the cost of personal computing devices will come down to as low as US$ 100 as sales rise exponentially, has indeed come true. Mainframe computers, for instance, initially costed tens of thousands of dollars since limited numbers were sold. He also predicted that the next generation of PCs would cost less than US$ 1000 per unit with more than 300 million units being sold and the future generation of computing devices would further be priced at close to US$ 100 per unit and sales estimated at 3 billion units.[5]

While the global shipment of smartphones in 2022 was 1.2 billion units,[6] the sale of tablets in the same period was 163.2 million units,[7] making it a total of 1.36 billion units. These are the figures of only one year. There is a significant percentage of the global population which already has slightly dated mobile phones. As per the World Bank estimates, the global internet penetration, calculated as the percentage of individuals with an active internet connection, is close to 60 per cent.[8] Also, the number of 'unique' mobile phone users in the world is now close to 5.5 billion.[9]

[2] Chris Miller, *Chip War: The Fight for The World's Most Critical Technology*, Scribner, New York, 2022, p.173.

[3] Jay Greene, **"The Computer Which Launched the PC Revolution"**, *CBS News*, 11 August 2011.

[4] Pushkar Ranade, **"History (and future) of Computing in One Chart"**, *Bits and Bytes*, 16 October 2015.

[5] Alexis C. Madrigal, **"Intel CEO Paul Otellini Draws the 'History of the Computer Industry' in 1 Chart"**, *The Atlantic*, 16 May 2013.

[6] Counterpoint Research, **"Global Smartphone Shipments Market Data (Q1 2021 – Q4 2022)"**, Counterpoint,8 February 2023.

[7] Federica Laricchia, **"Worldwide Tablet Shipments from 2nd Quarter 2010 to 4th Quarter 2022"**, Statista, 8 February 2023.

[8] **"World Development Indicators: Internet Users (per 100 people)"**, The World Bank.

[9] **"The Mobile Economy 2022"**, GSM Association Intelligence, London, 2022.

These figures highlight two important points: the world is increasingly becoming more connected through platforms and that a staggering amount of data is being produced, stored and processed around the world in real-time. As per an estimate, data produced in 2022 was 2.5 quintillion bytes per day.[10] This is ten followed by 30 zeros. All aspects of human activity including biometrics, social interactions, finances, entertainment, politics and ideologies are being moderated through these devices and platforms. The implications are wide. The possibility of affecting individuals across countries through influence, coordination and radicalisation are immense, creating vulnerabilities from a national security point of view. There are examples of election fraud[11] and genocide[12] by exploiting this connectivity. Similarly, civilian domains have been weaponised using non-kinetic tools of warfighting. Ban on Russian access to semiconductors,[13] export controls against China in the fields of semiconductor manufacturing equipment (SMEs) and chips for AI,[14] cyber-attacks against power grids[15] and disinformation campaigns[16] are some of the ways non-kinetic war is being waged by countries.

Four other advances due to the semiconductor revolution relate to the field of AI, quantum cryptography, precision munitions and sensor fusion/systems integration. The clustering together of increasing numbers of transistors within a single piece of chip has led to powerful processors such as graphics processing units (GPUs) and tensor processing units (TPUs) which have the capability of being 'trained' on vast amounts of data being generated, thereby creating stronger AI programmes. Similarly, the semiconductor revolution has also given rise to quantum cryptography which both holds the potential of ensuring impossible-to-hack communications as well as breaking erstwhile secure communications. [17] Precision munitions have the potential to target specific platforms and personalities and avoid collateral damage on the battlefield. The lethality of precision munitions is enhanced by increasing fusion of sensors, where data from a number of analog and digital sensors is fused through standards and plug-and-play platforms, edge computing and use of AI for creating strike options for the commanders.

[10] **"How Much Data is Created Every Day and How to Collect It"**, *CIO Bulletin*, 4 April 2022.

[11] Craig Silverman, Craig Timberg, Jeff Kao and Jeremy B. Merrill, **"Facebook Groups Topped 10,000 Daily Attacks on Election before Jan. 6, Analysis Shows"**, *The Washington Post*, 4 January 2022.

[12] Chad De Guzman, **"Meta's Facebook Algorithms 'Proactively 'Promoted Violence Against the Rohingya, New Amnesty International Report Asserts"**, *Time Magazine*, 28 September 2022.

[13] Zoya Sheftalovich and Laurens Cerulus, **"The Chips are Down: Putin Scrambles for High-tech Parts as His Arsenal Goes Up in Smoke"**, *Politico*, 5 September 2022.

[14] Mark Magnier, **"Semiconductor Export Curbs Hitting China to be Followed by Biotech and AI Restrictions: US Official"**, *South China Morning Post*, 28 October 2022.

[15] Binayak Dasgupta, **"Chinese Hackers Targeted 7 Indian Power Hubs, Govt Says Ops Failed"**, *Hindustan Times*, 8 April 2022.

[16] Himanshi Dahiya, **"How 'Chinese 'Social Media Warriors are Waging a War Against India"**, *The Quint*, 16 July 2020.

[17] Daniel J. Bernstein and Tanja Lange, **"Post-quantum Cryptography"**, *Nature*, No. 549, 2017, pp. 188–94.

The fourth technological shift, systems integration, has been in the making for a while. Systems integration can be classified into two parts: *within body* and *outside-body*. Outside-body integration comprises innovations such as the combined-arms manoeuvres during World War II where different platforms such as tanks, infantry and steep-dive bombers like the Stukas were integrated into a single fighting force through organisation and introduction of radio communication.[18] These were responsible for the *blitzkrieg*. Similarly, the navy and air forces have created formations where complementary capabilities fielded by different platforms are combined for battlefield effect, e.g., carrier battle groups (CBGs) and strike packages. These are held together by advances in communication and data integration where a command centre (static or mobile) with an array of encryption, communication and decision-making tools coordinates the operations of various platforms.

Within-body systems integration is a relatively new phenomenon. It is based on the recognition that the capabilities of conventional platforms can be enhanced by replacing or adding enabler modules. For example, the same unmanned aerial system (UAS) could use different payloads for executing vastly different missions. Cameras, missiles, infrared sensors and even compatible communication modules can lead to the UAS acting as an ISTAR or kinetic platform or wingman to a manned fighter. This modularity has been made possible due to the semiconductor revolution. Similarly, several modernisation programmes around the world have taken the infantry soldier as a system, adding upgrades that may heighten his cognitive capabilities, enhance his firepower range and allow him to communicate to nearby in-situ assets[19].

Categories of CETs

There have been attempts to classify CETs into categories to increase understanding about these technologies and highlight their utility. One such attempt is by the United States National Defense University (NDU), which classifies CETs under four heads namely, perception, processing, cognition; performance and materials; communication, navigation and targeting; and manufacturing, logistics and supply chain.[20] This Brief suggests another way of classification in terms of their use in war, i.e., as battlefield and over-the-horizon (OTH) CET. Battlefield CET refers to those technologies that can be used for warfighting and used explicitly on the battlefield. These include sensor fusion where data from analog and digital sensors is standardised and fed into a system generating a common operating picture (COP).

This data can be further used by creating multiple strike options using AI, similar to the ones being used by the Ukrainians in the ongoing conflict. Battlefield CETs also comprise

[18] Martin von Creveld, *Technology and War: From 2000 BC to the Present*, Touchstone, New York, 1991, p. 278.

[19] Kimball Johnson, **"Modernizing Soldier Lethality"**, *NCO Journal*, April 2018.

[20] Michael Raska, **"Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns"**, *Prism—Journal of Complex Operations*, Vol. 8, Issue 3, pp. 65–81, 9 January 2020.

advanced unmanned systems with multiple payloads such as infrared (IR) and/or light detection and ranging (LIDAR) sensors, combat cloud, edge computing, internet of military things (IoMT), space based ISR, electronic warfare (EW) and cyber warfare against military systems.

OTH CET comprises technology which can be used in the non-kinetic domain and includes cyber-physical attacks, social engineering, disinformation, influence operations, gene editing, big data analytics (BDA) and energy capture and storage. There are certain technologies which are common in both the sets, based on their usage since most are based on data and are dual-use in nature.

Acquisition of technologies for the Armed Forces is the first step towards operationalising them. The second and third steps, i.e., absorbing and scaling them, are more critical. Absorbing a particular technology within the Forces refers to the process of aligning the organisational structure with the technology for optimum results on the battlefield, in whatever manner it may be defined. Scaling refers to the mass production of the technology platforms so that it reaches the user in due time.

Matching Technology with Structure

The current organisational structure of the Indian Armed Forces has been created, conceptualised and honed to fight a particular form of warfare and in which the Forces have gained a professional edge. This form of warfare has certain attributes: focus on combined-arms operations, use of mechanised platforms in manoeuvre battles, emphasis on territory and/or attrition and hierarchical directives and orders. This is an ideal structure for fighting large-scale conventional wars. The two most recent conflicts, i.e., Armenia–Azerbaijan and the ongoing Russia–Ukraine one, have thrown up radically different interpretations of the use of conventional force in achieving political objectives. While military force was used in the former to force a political outcome in Azerbaijan's favour, the latter has highlighted the tenuous link between the use of violence and achieving political aims. As a result, one cannot discard the conventional warfighting paradigm.

However, there is a need to rethink organisational structures in terms of optimally integrating CETs. Certain steps have indeed been taken in this direction. For example, the Indian Army is in the process of inducting swarm drones into its mechanised forces,[21] at the same time reported to be procuring close to 2,000 drones through a variety of manufacturers—400 for logistical support and around 1,500 for ISTAR purposes.[22] Swarm drones, powered by AI and edge computing, have the capability to overwhelm enemy air defence systems, and saturate airfields and artillery gun concentrations, extending the range and target set of the force operating them.

[21] **"Swarm Drones being Inducted into Mechanised Forces of Indian Army"**, *The Print*, 26 August 2022.

[22] Paran Balakrishnan, **"Indian Army has Placed Orders for Nearly 2,000 Drones for Surveillance"**, *The Telegraph Online*, 8 January 2023.

However, the procurement of drones from multiple suppliers need to be coordinated in terms of software and firmware compatibility, standardised data formats, communication systems and cybersecurity. Swarm drones function on the presumption of autonomy, in selecting and neutralising targets. How much autonomy has been provided to the drones, whether it is limited only to collision avoidance and collaborative action in terms of recouping losses or is also extendable to the selection and neutralisation of targets, is a matter of conjecture.

For autonomous systems, a 'man-on-the-loop' as a failsafe measure always needs to be present. However, in a communication-contested environment, this may not always be the case. Serious discussion is, therefore, required on responsible AI and AI ethics. On the organisational front, there is a need to boost human autonomy by delegating actions to junior commanders and the structure of the forces needs to reflect this.[23] Modular forces capable of point air defence (AD) and supplemented by micro UAVs for local ISR and plug-and-play wearable modules for a broader operational picture may be one of the ways that the future force may be conceived of.

Similarly, for absorbing AI, there is a requirement of a data standards policy that fulfils two criteria: convert analog data within the Services to digital and; collection, collation and storage of the data, preferably in consonance with the National Data Governance Framework Policy.[24] In case of OTH CETs, the requirement is of collaborating with sister agencies for shaping common and reinforcing narratives, preventing information fratricide and knowledge sharing. Operations of this magnitude require certain capabilities of the Forces to be available in a supplementary manner. These are just some of the examples of major requirements for absorbing and then scaling technologies into the Armed Forces.

Recommendations

Root of Trust

Roots of trust are "highly reliable hardware, software and firmware components that perform specific, critical security functions. Since these are inherently trusted, they must be secure by design".[25] When translated into requirements for the military, this implies that all of the latest technologies and platforms being inducted into the Armed Forces must have roots of trust which are inviolable and rigorously vetted by designated agencies. All electronics components must be checked for hardware trojans and only certified components must be allowed to be used in the military.

[23] Akshat Upadhyay, **"Amid Changing Nature and Character of War, the Need for Tech-Oriented Military Commanders for India"**, Occasional Paper No. 390, Observer Research Foundation (ORF), 17 February 2023.

[24] **"National Data Governance Framework Policy (Draft)"**, Ministry of Electronics and Information Technology, Government of India, May 2022.

[25] **"Roots of Trust"**, Computer Security Resource Center, National Institute of Standards and Technology.

There have been instances in the US military where spurious chips in fighter jets have led to the death of US Air Force officers.[26] Similarly, the Russian military designates all electronics components through a centralised agency and stamps all components which can be checked through visual inspection.[27] In the case of software, common cybersecurity standards need to be laid down and implemented stringently. This assumes added importance since the defence sector has seen an influx of private players increasing the importance of coordinating cyber security measures.

Commonalities

Exploiting commonalities of requirements between separate ministries will ensure that private companies reach economies of scale and are able to deliver in a more expedited time frame. For example, drone airframes and propulsion systems are required not only by the Armed Forces but also by the state police forces, central armed police forces (CAPFs), and by other departments and organisations like the Archaeological Survey of India (ASI), National and State Disaster Relief Forces (N/SDRF), the Ministry of Agriculture among others. Combining the common requirements of these ministries will create a much bigger customer base for companies rather than catering to piecemeal requirements. Also, defence companies can explore the consortium method where they can combine their strengths to 'collaborate and compete' rather than merely competing. The consortium method has been extremely successful in certain cases, e.g., MBDA (Matra, BAe Dynamics and Alenia)—a multinational consortium of missile production companies with participants from France, Italy and the United Kingdom (UK).[28]

Project Managers

While the Project Managers (PMs) employed with the US Defense Advanced Research Projects Agency (DARPA) have a very wide charter, which includes scouting for talent in the science, technology, engineering and mathematics (STEM) fields internationally,[29] there is a requirement of the forces appointing similar project managers, not limited to their in-house personnel, to scout for talent in universities across the country. The list of these universities does not need to be limited to the Indian Institutes of Technology (IITs) or the National Institutes of Technology (NITs) but can be widened to look at colleges in the Tier 2 and 3 cities. Apart from this, bright talent can also be on-boarded from a young age through leveraging the Atal Tinkering Labs[30] and similar young science incubators.

[26] Rachel S. Cohen, **"An F-16 Pilot Died When His Ejection Seat Failed. Was It Counterfeit?"**, *Air Force Times*, 14 September 2022.

[27] David Gauthier-Villars, Steve Stecklow, Maurice Tamman, Stephen Grey and Andrew MacAskill, **"As Russian Missiles Struck Ukraine, Western Tech Still Flowed"**, Special Report, *Reuters*, 8 August 2022.

[28] Douglas Barrie, Bastian Giegerich and Tim Lawrenson, **"European Missile Defence - Unstructured Cooperation?"**, *IISS Blog*, 26 August 2022.

[29] William Boone Bonvillian, Richard Van Atta and Patrick Windham (eds), ***The DARPA Model for Transformative Technologies: Perspectives on the U.S. Defense Advanced Research Projects Agency***, Open Book Publishing, Cambridge, 2021, pp. 315–17.

[30] **"About Atal Tinkering Labs"**, Atal Tinkering Labs.

The prime focus of the PMs must be talent search and then matching the talent with a given project within a laid-down timeline. Once prototyping has been done, the technology needs to be copyrighted by the Forces, then given to a private company for scaling and production. Efforts have been made in this direction by the Defence Research and Development Organisation (DRDO) through their Technology Development Fund (TDF)[31] and the Department of Defence Production (DDP) through the innovations for defence excellence (iDEX) challenges,[32] as well as the respective services' innovation organisations such as the Army Design Bureau (ADB)[33] and the Naval Indigenisation and Innovation Organisation (NIIO).[34] There needs to be further coordination amongst these organisations with representatives from the private sector being on-boarded in advisory roles, something on the lines of the Defense Innovation Board (DIB) in the US.[35]

Data Policies

Most CETs described in this Brief have data as their base. As mentioned earlier, there is an increasing trend towards digitisation, i.e., the process of creating data out of daily analog activities which allows organisations to process data and delve further into the functioning of the modern world. As a result, data privacy and protection have become critical, especially in the face of major cyber-attacks. Within the forces, there is a need for a data governance policy, preferably aligned with the national data governance policy framework, but also firewalled from public interfacing to prevent inadvertent leak of sensitive data. As a result, data standards need to be laid down, cloud centres need to be designated and physically protected, and finally effective cyber security measures need to be ensured. All these need to be created at the tri-services level so that common data standards can be used in future warfare for joint operations.

Conclusion

Technology absorption is a function of both the organisational structure and the technology itself. Neither can be effective without the other. Technologies and their enablers are themselves products of the *zeitgeist* or the social milieu in which they are conceptualised and formed. Therefore, attempting to induct or absorb technologies without a corresponding change in structures may not yield the desired outcomes. Therefore, it is imperative that serious debates be undertaken within the forces regarding the future force structures necessary for winning in the competition continuum.

[31] **Technology Development Fund (TDF)**, Defence Research and Development Organisation (DRDO).

[32] **"Defence India Startup Challenges (DISC)"**, Innovations for Defence Excellence (iDEX).

[33] **"Army Design Bureau"**, Indian Army.

[34] **"Startup 20 Inception Meet—NIIO Showcase"**, Naval Indigenisation and Innovation Organisation (NIIO), Indian Navy.

[35] **Defense Innovation Board (DIB)**, Department of Defense, United States of America.

About the Author

Lt Col Akshat Upadhyay is Research Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Disclaimer: Views expressed in Manohar Parrikar IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the Manohar Parrikar IDSA or the Government of India.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses