CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 272 February 2021

Engagement or Estrangement: Gauging Indian Army's Relationship with the Emerging Technologies

Lieutenant Colonel Akshat Upadhyay is currently posted in the Army Headquarters. He is a prolific writer who has written for a number of think tanks including CLAWS, IDSA, ORF and USI. He has also published op-eds in The Hindu; Hindustan Times; The Daily Guardian; and The Tribune on a variety of topics such as radicalisation, social media, LC dynamics, emerging technologies and social movements. The author has also won a number of awards including a Gold Medal in the Essay Competition organised by USI (New Delhi).

"It isn't what an algorithm can do for you, but about whether you can expand your mind".

—Jaron Lanier

(Dawn of the New Everything, 2017)

Key Points

- The Indian Army is looking at adapting emerging technologies such as AI, Quantum Computing, Blockchain and Additive Manufacturing to gain edge over its adversaries, but also needs to think obliquely about support functions such as logistics, inventory management, education, health services and surveillance rather than focusing on kinetic capabilities directly.
- There is a need for thinking in terms of and creating a 'data-driven culture' within the organisation—one which facilitates flattening and spreading of structures.
- Understanding warfare by using a systems approach is required as emerging technologies work best in non-hierarchical flattened formats.
- There are number of technical and cognitive issues that need to be considered such as over-reliance on data, privatisation of warfare, humans in/on or out of the loop.
- Innovative solutions apart from structural ones includes creation of an Armed Forces' cloud (BADAL), creation of a Centre for Armed Forces Innovativeness (CAFI), longer posting tenures of officers, subsidising online courses for officers and a faster inception-procurement cycle.

Introduction

In March 2020, during a seminar organised by the Centre for Land Warfare Studies (CLAWS), the Chief of the Army Staff (COAS) of the Indian Army, General MM Naravane laid out his vision for the future. [1] Alluding to 'contested equality', he explained that technology had made 'previously unequal adversaries' equal and big-ticket items like tanks and fighter aircraft could, in the long run, become obsolete. [2] In a matter of months, his prediction rang true when Azerbaijan comprehensively defeated Armenia in the first conventional conflict of the 21st century — primarily using unmanned system.[3] In the ensuing euphoria over the role of technology in that conflict, certain assumptions have been made while some questions have been left

unanswered. The aim of this paper is to understand the relationship between the Indian Army and technology in general by using both theoretical and practical applications of niche technologies.[4] The paper will also attempt to address some inherent challenges and identify areas and procedures which need to be reimagined, if the Army aims to transcend its current philosophy of attritional warfare and truly embrace the post industrial age.

What is Technology?

Technology in simple words is a coherent set of instructions, methods and mechanisms used to shape the material world.[5] The role of technology has progressed from freeing humans from the mundaneness of physical labour to facilitating their cognitive development. Artificial Intelligence (AI) is the next step in this evolution which aims to emulate and then surpass human intelligence. Associated with AI are a number of technologies that aim to transform the nature of work itself. Indian Army needs to get onto this bandwagon fast in order not only to improve efficiency but also to change its own perception of the battlefield.
(For ease of understanding, 'technology' in the paper refers to 'digital technology').

Emerging Technologies

Emerging technologies differ from existing ones in five major attributes. These are *radical novelty*, *relatively fast growth*, *coherence over time*, *prominent impact across a number of sectors* and, *uncertainty & ambiguity pertaining to utility*.[6] An apt example of an emerging technology is the tank. Developed as a counter to the stalemated trench warfare during the First World War, the tank, supplemented by wireless communications (another emergent technology still in use), proved to be a game-changer when used *en masse* by the Germans during the Second World War. The next big revolution in current times is the increasing cognitive convergence between man and machine. AI has the potential to bridge this gap fast but requires a lot of 'prepping up' in form of large amount of training data (Big Data and Internet of Things (IoT), huge bandwidths (5G) and massive storage space (Cloud Computing). All these technologies have their own specialised literature but are mostly interdependent on each other. The Indian Army is looking at all these technologies apart from others such as Blockchain Technology, Additive Manufacturing and Quantum Computing.

What is Artificial Intelligence (AI)?

AI is the ability of machines to perform complex tasks. It has sub-fields like machine learning, machine vision, autonomous machines, expert systems, natural language processing, explainable AI and facial recognition among others. Contrary to common perception of sentient machines or killer robots wielding lethal power, AI has the potential of

transforming military effectiveness by intelligently applying AI to major administrative and decision making matters. This is the "AI+X" model, whereby adding AI to anything makes that particular model smart. While human functions, especially abstract thinking and vision, have the advantage of millions of years of evolution, researchers and scientists face challenges in designing algorithms which simulate this 'behaviour' in machines. Whereas the human brain is excellent in multitasking, non-contextual pattern recognition, machine learning is always purpose-built, problem-specific, and context-dependent.

Digital India

India has had substantial success with linking technological advancement to social development. The current government's emphasis on Jan Dhan, Aadhar and Mobile (JAM Initiative)[7], Direct Benefit Transfer (DBT), Public Distribution System (PDS) linkage to Aadhar [8], has made it possible for technology to truly improve human condition. Initiatives such as DigiLocker and UMANG, based on public cloud system, are attempts at using Big Data for providing last-mile services to a majority of the population. Tech industries in India too have made major strides in emerging technologies. A number of AI based startups such as GreyOrange[9], Ather Energy[10], CynLr[11] are likely to be commercially viable in the next 18-24 months[12]. However, significant challenges are still present. Most Indian IT companies provide non-deep tech services to major MNCs. Minor innovation in form of workplace or budgetary efficiency therefore takes precedence over R&D or major breakthroughs. There are lack of incentives in established tech companies to use these technologies apart from the low scalability of 'smart' products by startups. The current state of research opportunities in the country on emerging technologies are limited to top colleges and universities. Combined with uncertainty regarding data privacy & cyber security and ad-hoc state of digitisation limited only to a handful of sectors, substantial investment in these technologies is generally inhibited. This is further compounded by the absence of major data sets for training AI systems, absence of indigenous chip-making industries and almost zero network effect.[13]

Initiatives by the Indian Government towards AI

The Task Force on AI for India's Economic Transformation, in its report of 19 Jan 2018, identified 10 domains for the utilisation of AI and proposed the creation of an inter-ministerial National AI Mission (NAIM) with a funding of Rs 1200 crores, spread over a period of five years. One of these domains include national security with a passing reference to four non-connected areas of national security vis. autonomous surveillance and combat systems, adaptive communication systems, cyber attack mitigation and counter attack systems and, multi-sensor data fusion based systems.[14] The Ministry of Defence (MoD) also came out with its own findings within less than six months of the release of this report.

MoD Task Force

MoD's report titled *Implementation of the recommendations of the multi-stakeholder Task Force constituted by the Ministry of Defence for 'Strategic Implementation of Artificial Intelligence for National Security and Defence'*[15] was released in June 2018. It identified five areas for developing AI based solutions vis, *lethal autonomous weapon systems (LAWS)*, *unmanned surveillance*, *simulated wargames & training*, *cyber security & aerospace security* and, *intelligence & reconnaissance*. Two agencies were envisaged namely the Defence AI Council (DAIC) headed by the Raksha Mantri and comprising the three Service Chiefs, Chief of Integrated Defence Staff to the Chairman Chiefs of Staff Committee or CISC (with creation of the Chief of Defence Staff or CDS, this composition may undergo a small change) along with the Defence Secretary and the National Cyber Security Coordinator. The other agency was the Defence AI Project Agency (DAIPA) under the Secretary (Defence Production).[16] While DAIC has been established as an overall guiding body on policy decisions concerning use of AI in the defence forces, DAIPA —which has the task to implement the policy decisions of DAIC and provide pragmatic solutions in collaboration with DRDO, academia and industry — is yet to be created.

Flattening and Spreading

Any major policy decision emanating from the Army headquarters passes through a bureaucratic structure. The major function of bureaucracy is efficient distribution of resources - a task which requires adequate internal checks and balances, time for deliberation and subdivisions organised for administrative efficiency. Due to percolation of organisational cultures and 'in-group/out-group' dynamics, most bureaucracies harden into silos. Decision-making process therefore is piecemeal and time-consuming. As most digital technologies have been designed with an aim to create a horizontal distribution of specialised work and a collaborative mindset, government bureaucracies must either reorient and restructure themselves or adapt the technology to suit the organisation. This leads to one of two things: either technology itself is designed or used in a manner that mirrors/ replicates the daily routines of administrative manners or the bureaucracy 'flattens' and 'spreads' over a period of time. Flattening and spreading in relation to armed forces can be thought of as sequential processes. While 'flattening' is part of the cognitive realm and refers to the breaking of silos and acceptance of a more open and collaborative model of functioning, 'spreading' is the physical counterpart when the actual coordination between departments happens. This can lead to a new organisational culture with more emphasis on functionality without compromising the organic strength of the Army.

Interface between Man and Machine

Technology in the Army is necessarily complex due to the need for strong encryption standards, ruggedisation and employment of complicated algorithms. However, that does not mean that the user interface has to be equally esoteric. Donald A Norman in his seminal work *The Design of Everyday Things* contended that, those who designed things did not make it from the point of view of consumers. As a result, there was always a tension between added functionality and added complexity. [17] Most of the technology designed for use in the forces has an unwieldy interface. As a result, technology's absorption is limited to only select personnel. This is a far cry from the design of smartphones which, while containing increasingly strong processors and a host of complex technologies, are simple to use and understand. The armed forces need to focus on the accessibility and usability of any platform that utislises the latest digital technology , as technology is only useful if it is scalable and permeates down to the last soldier especially in networked warfare. Military technology also needs to be on the lines of 'lean back' in terms of being easily understandable, accessible and intelligent as compared to 'lean forward' where the human element predominates.[18]

Time to Change?

Why is AI Required?

One can always argue that the use of AI and other niche technologies by the Indian Army is only inevitable in view of the considerable Chinese investments in the same fields. However, 'emulation is not innovation'. Technology should not be used just for its own sake. It must serve a purpose that enables its users to enhance their productivity. While Blockchain enables process automation and removal of unnecessary intermediaries, quantum computing allows one to think of ultra-fast computers that can simulate complex scenario-building using parallel computing in extremely miniaturised devices. Additive and 3D manufacturing can fill the voids in our own design and manufacturing capacities while unmanned platforms can be put to multiple uses. The common features of these technologies include networking, reliance on data and, removal of humans one step away from decision making. Within the Indian Army, though there has been an increased focus towards platforming number of services for the ordinary soldier, ideally the use of emerging technologies should have been based on the foundations of 'Digital Army', based on standardising and cleaning pre-existing data sets.

What areas should the Army focus on?

Entrenched global norms of securitisation constrict one's views of technology when used in context of armed forces. Technology is often viewed as enhancing the coercive component of the armed forces. However, one must not lose focus on the supplementary systems that enable the forces to function the way they do. The Indian Army needs to focus on a 'bottom-up' approach of automation and then 'intelligentisation' of the supporting services such as medical, inventory management, logistics, repair & maintenance and professional military education, progressing to surveillance and analysis to finally autonomous combat capability, if desired. Though some of these processes can run concurrently, attempting to insert AI directly into combat systems may have unforeseen results. Some of the uses of AI and other niche technologies within the Army are detailed below:-

- **Project BEEHIVE**. The Corps of Electronic and Mechanical Engineers (EME) has already started to work on Project BEEHIVE that aims to serve as a centralised real-time database of all equipment repairs being carried out by almost 2000 Army workshops across the country as well as terrain-related criticalities.[19] This first step of automation now needs to be made smart thereby eliminating the need for human entry of data and creating models of 'Predictive Maintenance' in place of the current forensic and preventive maintenance. Machine vision can be utilised in EME workshops for undertaking repairs of vehicles in conjunction with natural language processing (NLP) modules like VADER[20] (Virtual Assistant for Data Entry and Recording) which converts a mechanic's real-time verbal description of his work into text, extract relevant information from it and update it into the BEEHIVE cloud. A number of officers are currently looking into combining condition - based monitoring of equipment and machine learning through digitisation of logbook data to predict patterns of breakdown in different equipments, using multiple data points.[21]
- **Medical Healthcare.** The Army Medical Corps' (AMC) centralised database *Dhanvantri* has an automated data entry system thereby allowing all military hospitals on the network to access each other's patients' medical history. AI can be integrated in AMC to reduce the load on its limited personnel, automate reading of X-rays and reports and improve the quality of medical health care by being holistically preventive rather than prescriptive. A number of health startups like PreCog (cloud based ECG monitoring company) [22] and SigTuple (intelligent screening solutions using AI powered analysis of visual medical data) are good models to follow. A smarter use of AI diagnostic tools will reduce the rush and facilitate faster reaction during the 'Golden Hour'.[23] Data gained from these diagnoses can also be correlated with the terrain, demographics, palate, lifestyle of an individual soldier— to create a customised health plan.

- **Using AI Against Cyber Attacks.** AI based algorithms can be trained to automatically detect malwares in networks and take countermeasures against them. On an ambitious note, AI can be trained to write code against malignant software, something on the lines of Generative Pre-Trained Transformer 3 (GPT-3).
- **AI on the LC.** An important feature of life on the LC is the uncertainty of ceasefire violation (CFVs). Casualties are results of unpredictable firing and lack of institutional memory especially during turnover of units. An integrated cloud based AI system can effectively eliminate these shortcomings. Combining data from multiple sensors—audio and visual— including intelligence reports from higher formations, a pattern of CFVs, calibre of weapons used, approximate ammunition used by the adversary per engagement (counting the gaps in firing using audio sensors) and likely timings of firing can be eked out. The same algorithm's accuracy can be further enhanced by feeding data regarding political events in the state, local elections and festivals. The more the number of data points, the more detailed a correlation of data will be. The major shortcoming of this model is that with increasing number of data points, the model might identify correlation as causation leading to different conclusions.
- **Use of Unmanned Platforms.** While robots will come in handy in defusing Improvised Explosive Devices (IEDs) in counterinsurgency/ counterterrorist (CI/CT) areas — the Indian Army can learn from the experiences of the US Army in using robots such as Talon[24], iRobot[25], Packbot[26] in Iraq and Afghanistan. Use of 'robotic mules is one such example.[27] UGVs can be used as part of smart convoys during conventional operations however; manned-unmanned teaming (MUMT), currently in use by the US Air Force, will have maximum impact when it comes to deploying a mix team of soldiers and robots to undertake specialised missions.[28] MUMT can also be used in 'mosaic warfare' which envisages a systems battle or the ultimate networked warfare. The adversary is overwhelmed with multiple sensor and weapon platforms where each sensor and shooter fits seamlessly as a part of a mosaic.[29]
- **Offensive Use of Niche Technologies.** Combining AI based solutions with unmanned systems can actually produce potent and dynamic responses, short of conventional war.[30] However, on the LC, there is a need to bring in the paradigm of small war. Commercial off-the-shelf (COTS) drones and

quadcopters, equipped with grenades, can be used with devastating effect. The operationalisation of drone swarming, has the potential of overwhelming the enemy defences and troop concentrations, especially in the short- war format.[31] The same AI which detects patterns and correlated data can also be programmed to control the drone in real-time and based on the density of individuals gathered at the post at a particular time, drop grenades causing maximum destruction.

Need for a Different 'Organisational Culture' in the Army?

The Armed force of any country is essentially technologically and ideologically conservative, in terms of retention of existing norms and means of waging war. Only a 'top- down approach' can shake these relatively complacent notions. US' Goldwater-Nichols Act (1986) for 'inculcating jointness' and Gen Sundarji's 'mechanisation and introduction of digital technology in the army' are apt examples of a top-down revolution rather than a bottom-up evolution. There is a need to create a 'data-driven' culture in the Indian Army which lays emphasis on standardisation of protocols for collecting, collating and storing data. Though some work was done in this field during the 'Digital Army' phase, the applications created and run on the Army Data Network (ADN) are, unfortunately, incompatible with each other and therefore cannot interact. This has resulted in massive data being stored in silos by different branches and directorates of the Indian Army. Applications such as ARMAAN, Computerised Inventory Control Project (CICP) and Human Resource Management Suite (HRMS) as holders of training data are not suitable, in their current avatars, for providing training data for AI and other technologies. On the other hand, units and sub-units also generate a huge amount of data which can be used for generating extra data points, however an overarching backbone with a common set of protocols need to be designed to do so. As of now, all these systems are stuck in Faraday-cages like structures that do not contribute to the automation or intelligentisation of the Army. The Indian government's e-governance standards, especially the Metadata and Data Standards can be looked upon for further study.[32]

Automation or Autonomy?

Automation is just the start of a process that leads to autonomy. The Indian Army does not have any choice in choosing between the two. For a potent force of an emerging power, the Indian Army needs to tailor make technologies for its requirements. Ideally, a foundation should have been laid with the 'Digital Army' initiative and common protocols for data creation, collection, collation and dissemination set for the Army. The first step after this will require on-boarding of all data sets, albeit in standardised formats, to start the process of

Big Data analysis and machine learning. Also, a common agency should handle the generation of data, training data and implementation of various niche technology applications.

Challenges

Though network centric warfare is the ideal aim, however, one should aim higher and think of networked warfare where humans and machines form tailor-made units/ teams for specific tasks. This concept also takes into account the gradual melting of the human machine interface which, for now a remote possibility, will happen in the near future. However, one must take a look at the challenges that the Army currently faces and may face in the future while implementing such changes, as well as the shortcomings associated with over-reliance on data:-

- ***Systems Approach to Warfare.*** A holistic approach regarding technology in general and emerging technologies in particular is missing. Though steps have been taken to involve the academia and private players, all these actions are happening as per an old paradigm where the major focus is on platforms and attrition warfare. Even procurement of platforms has generally been piecemeal and behind the technology curve. A systems approach which focuses on networked 'systems', i.e. humans and platforms, either in conjunction or in standalone mode, forming part of an interconnected web of task- specific nodes, is a much better and required mode of approaching warfare rather than seeing it from either a human or equipment centric view. It obviates major deficiencies in individual platforms and divides (weighted) cognitive and coercive load between the humans and machines. The concept of warfighting within the Indian Armed Forces is based on arms and service specific silos. The Department of Military Affairs (DMA) and CDS need to play a major role in first breaking these silos, then integrating them, based on both equipment and technologies, and not merely allocating resources from the services and distributing them across geographical commands.
- ***Understanding of Knowledge Warfare.*** Even after the successful airstrikes against Pakistan in Balakot, India was lagging behind as far as narrative warfare was concerned, due to institutional challenges in its response. The Indian Army needs to embrace a more flattened structure of command and control if it wants to prepare for the next war. A flattened command structure with maximum autonomy afforded to smaller units and formations also mimics 'cybernetics' and 'biological systems'.[33] With centralised oversight, the military

can accomplish its objectives in a more efficient and time effective manner.

- ***Encoding Abstractions and Biases into Code: A Work in Progress.*** Algorithms are basically steps to carry out certain processes in order to get results. An algorithm for an AI is in the form of mathematical functions. However, the way the algorithms are written, they generally try to encode abstractions into mathematics. As a result, they are also the product of the coder's or the company's inherent assumptions and biases[34] about the way the things function. A recent spat within Google wherein an AI researcher, qualified in facial recognition had to leave the company because of her paper where she summarised, with mathematical evidence, that the current facial recognition technology was much more adept at classifying white people rather than people of colour (POC).[35] Although ethics in AI is not an issue currently within the Indian Army, it may become so in the future with algorithms unfairly painting individuals in undesirable categories. This will matter in case AI is used in the Indian Army's legal or human resource management system such as postings, gradings and annual reports.

- ***Human Intuition v/s Machine Logic.*** While there are many advantages of the usage of AI in the Indian Army, one has to remember that having data or using AI is part of a holistic process—AI cannot replace intuitive human decision making. While the prime task of the armed forces is to win wars, it is a fact that wars are emotional ventures. While requiring precision in their conduct, wars are primarily political in nature. As a result, their overall conduct should never be left to machines or algorithms. The future of warfare needs to be practical with only a smattering of the fantastic to enable ambitious long term thinking. AI, Big Data, IoT are being used in much more mundane and pragmatic real world applications in the military than what is envisioned in experimental pamphlets.[36]

- ***Injecting Malicious Code into Data.*** A paper written for Microsoft by a group of researchers at the Berkman Klein Center for Internet and Society (Harvard University) brought out new issues with training of algorithms for AI.[37] These ranged from introducing false and malicious training data, either intentionally (adversaries) or inadvertently (incorrect entries), to the algorithms identifying optimisation functions not in sync with the desired end result. Utmost care has to be taken to select and input data in the algorithms.

- ***Vulnerabilities of a Networked System.*** A fully networked system is also vulnerable in part due to its complexity. Electromagnetic interference and

trackability are some of the likely issues that will be faced. Passage of information may lead to swamping effect in networks where every entity is fighting the battle of the bandwidth.

- ***Ethical Issues.*** Certain ethical issues also need to be looked at when thinking about niche technologies:-
    - **Ethics of using (or not using) LAWS.** Advantages of unmanned systems include alleviating battlefield stress thereby providing stability, sustainability and longevity. However, using autonomous systems or robotics, purely for combat, is an issue which needs a huge public debate especially for LAWS. One may be tempted to assume that LAWS removes the weakest link in war i.e. the fallible human being. Besides questions of ethics, this mentality raises two important issues: ending the nature and character of war as it is understood and; removing the question of using violence to subdue the adversary by raising costs. If the adversary itself is unmanned —robotics alter the identity of who fights —then there is no cost of inflicting violence on the adversary on the battlefield. Automatically, war moves on to cities or 'counter value' targets.
    - **Humans In, Out or On the Loop?** There is a tendency for taking humans 'off the loop' in autonomous systems. While the idea of replacing tired and judgmental human beings from the decision matrix and replacing them with indefatigable machines working on maths and logic may sound enticing, the reality is much more complex. The downing of an Iran Air Flight 655 by USS Vincennes in 1978[38] and shooting down of an RAF Tornado by a Patriot missile battery in 2003[39] are all reminders that humans need to be 'on-the-loop' atleast.
    - **Privatisation of Warfare.** The most obvious repercussion of the proliferation of technology is the rise of non- state actors. Availability of COTS drones, hacking software and other implements, enable individuals to challenge the state's monopoly on violence. Edward Snowden's revelations regarding the companies' (i.e. Facebook & Google) culpability in passing huge amounts of data to the National Security Agency (NSA) under domestic and international surveillance programs such as PRISM and STELLARWIND[40] are a grim reminder that this power can be turned against any nation state in the future.

Way Ahead

The solution lies in first strengthening existing capacities, concurrently creating new ones to harness the fourth industrial revolution. The Indian Army has to focus on three core areas:-

- ***Cyber Security.*** This is a much abused yet barely understood term especially concerning military systems. Cyber security is a holistic concept involving two major components vis. offense and defense. While 'offense' looks into pre-emption, 'defense' protects leakage of information. The current methods of air-gapping computers, disabling USB ports and mandatorily installing cryptography software within units, are only one part of cyber security. The Indian Army's near universal acceptance of the Linux based indigenous Bharat Operating System Solutions (BOSS) for its day to day functioning is a great step, that needs to be strengthened by regular updates. The recent hacking of Solar Winds through Microsoft 365 [41] is a grim reminder that digital technologies have to be indigenous. The offense part needs to be equally capable of mounting attacks on adversarial networks. Once the systems and network are secure, data functions can be implemented.
- ***Data Generation.*** Data generation forms the bedrock of most emerging technologies. The current model of functioning needs to be more conducive to allow innovation in the methods of generating data. With an assortment of modern and legacy equipment, there is a deliberate need for slowly and steadily transcribing all forms of data into the digital format. All this needs to be done under an overall common architecture.
- ***Inception to Action.*** Indian defence procurement has generally followed technology instead of being in sync with it. Due to bureaucratic red tapes and inordinate delays, most procurement is piecemeal and ad-hoc resulting in voids in capability development. Technology adoption cannot follow this route. The entire cycle of inception-conception- validation-scaling-action (ICVSA) must be expedited and completed in time.

Apart from these core areas, following practical steps may be taken:-

- ***Incubators or Intubators.*** The current format of officers spending two-three years in a 'specialised' appointment is not suitable for the completion of projects in the niche technology field. While the creation of appointments for interacting with IITs, academia and the industry is laudable, there are two major lacunae—the appointed officers are neither subject matter experts (SMEs) nor necessarily technically or public policy qualified. Also, once an officer is involved in a project, a timeline of two to three years is not sufficient enough to reach the deadline. The idea of an incubator can be created at the tri-services level and called the Centre for Armed Forces

Innovation (CAFI). CAFI should consist of officers who are SMEs in emerging technologies or with a technological bent of mind. The tenure of the officers should be long enough to ensure completion of specific projects. The major aims of this organisation will be to convert theoretical ideas regarding emerging technologies into workable projects, and coordinate with the academia and DRDO. CAFI should also scout for talents in college for both short term and long term projects and offer sponsorships. Liaisoning can be done with MNCs and big corporate houses for unpaid internships of short and medium durations, to learn data mining, labelling/ annotating, cleaning and classifying.

- ***Audit by Third Party.*** A non-partisan think tank can provide advisory services and keep tabs on the progress of the projects recommended by CAFI and approved by higher authorities. DAIPA should expand its mandate and encompass other emerging technologies namely blockchain, IoT, Big Data Analysis and Deep Learning. DAIPA should also coordinate with DRDO's Centre for AI Research (CAIR) to ensure that products are made as per the requirements of the armed forces within deadlines and thereafter complete the ICVSA cycle. There should be adequate latitude within both CAFI and DAIPA to abandon 'non-functioning projects'.
- ***Online Courses.*** Number of courses are being offered by top universities like Harvard and Stanford through Massively Open Online Courses (MOOCs) on websites such as Coursera, edx and Udemy. Such courses can be subscribed on an institutional basis and offered to interested personnel.
- ***BADAL - A Cloud for the Armed Forces.*** The Armed Forces can develop their own cloud, and name it BADAL (Bulk Accumulation of Data for Automation and Learning). Currently, some applications of the Indian Army are being run from the Indian government's cloud service, MeghRaj[42], while the rest are either run from local clouds or Army Headquarters. All these disparate data sets need to be 'on-boarded' to BADAL which will be possible with the operationalisation of the Network for Spectrum (NFS) project and creation of multiple data centres. BADAL will seek to integrate the data of entire MoD including all three services' classified and unclassified data separated and segregated by strong encryption and accessed through biometric embedded data— either as part of a new identity card or a thumb drive. The entire setup will be indigenous leading to data localisationand sovereignty. If implemented, BADAL will revolutionalise strategic decision making at the highest level by making available a comprehensive picture of the battlefield and providing a top oversight during the conflict. In peacetime, BADAL could be used for training algorithms based on both simulated and actual data.

Conclusion

Though India and the Indian Army are late entrants into the field of AI and other emerging technologies, however, India can always learn from others' mistakes and devise much more robust systems to create better and responsive AI systems. India has already joined the 14 member Global AI Community and hosted its first ever virtual summit on AI called RAISE (Responsible AI for Social Empowerment) 2020 from 05 to 09 Oct 2020. The seriousness of the Indian Government however has to be translated into equal seriousness within the Army and the above steps need to be adopted earnestly in order to make the Indian Army a truly modern Army.

End Notes

1 Philip, Snehesh Alex. "Tanks, Fighter Aircraft Will Soon Be on Their Way out like Sony Walkman: Army Chief." *ThePrint* (blog), March 4, 2020. https://theprint.in/defence/tanks-fighter-aircraft-will-soon-be-on-their-way-out-like-sony-walkman-army-chief/375386/. Accessed December 17, 2020.

2 ibid

3 Gupta, Shekhar. *What Azerbaijan's Spectacular Victory over Armenia Tells Us about the Future of Modern Warfare*. Video Presentation. Cut the Clutter Ep 618. New Delhi: The Print Studio, 2020. https://www.youtube.com/watch?v=KDmDi_QN3kE. Accessed November 16, 2020.

4 Rajat Pandit. "Indian Army: Amid LAC Face-off, Army to Study Lasers, Robotics & AI for Warfare." News Website. Times of India, August 8, 2020. https://timesofindia.indiatimes.com/india/amid-lac-face-off-army-to-study-lasers-robotics-ai-for-warfare/articleshow/77425169.cms. Accessed December 17, 2020.

5 Agar, Jon. "What Is Technology?" *Annals of Science*, October 11, 2019. https://www.tandfonline.com/doi/abs/10.1080/00033790.2019.1672788. Accessed December 17, 2020.

6 Daniele Rotolo, Diana Hicks, and Ben R. Martin. "What Is an Emerging Technology?" *Research Policy* 44, no. 10 (July 7, 2015): 44. https://doi.org/10.1016/j.respol.2015.06.006. Accessed August 9, 2020.

7 PMO. "Leveraging the Power of JAM: Jan Dhan, Aadhar and Mobile." PM India. Accessed December 17, 2020. https://www.pmindia.gov.in/en/government_tr_rec/leveraging-the-power-of-jam-jan-dhan-aadhar-and-mobile/.

8 Daiji World. "'Adhaar' Most Sophisticated ID Programme in the World : World Bank," March 16, 2017. http://www.daijiworld.com/news/newsDisplay.aspx?newsID=442948. Accessed December 17, 2020.

9 GreyOrange. "Inventory in Motion for the Age of Immediacy." Accessed December 18, 2020. https://www.greyorange.com/.

10 Ather Energy. "Ather 450X." Accessed December 18, 2020. https://www.atherenergy.com/.

11 CynLr. "CynLr - Cybernetics Laboratory." Accessed December 18, 2020. https://cynlr.com/.

12 Harichandan Arakali. "Why India's Deep Tech Startups Are In The Deep End." Forbes India, December 17, 2020. https://www.forbesindia.com/article/innovation/why-indias-deep-tech-startups-are-in-the-deep-end/65029/1.

13 Sriram Sharma. "Here's Why India Is Likely to Lose the AI Race." Factor Daily, August 18, 2017. https://factordaily.com/artificial-intelligence-india/. Accessed December 14, 2020.

14 V Kamakoti. "Report of the Artificial Intelligence Task Force." Government Brief. New Delhi: Ministry of Commerce and Industry, 2017. https://dipp.gov.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf. Accessed December 14, 2020.

[15] Ministry of Defence, India. "Implementation of the Recommendations of the Multi-Stakeholder Task Force Constituted by the Ministry of Defence for 'Strategic Implementation of Artificial Intelligence for National Security and Defence.'" File No. 8(19)/2018-D(Coord/DDP). New Delhi: MoD, February 8, 2019. https://www.ddpmod.gov.in/sites/default/files/AI.pdf. Accessed December 14, 2020.

[16] Ibid

[17] Donald A Norman. *The Design of Everyday Things*. 2013 ed. US: Basic Books, 1988.

[18] Helen E Katz. The Media Handbook: A Complete Guide to Advertising Media Selection, Planning, Research, and Buying. Seventh. Routledge Communication Series. Taylor and Francis, 1995.

[19] Shaurya Karanbir Gurung. "Indian Army: For Better Operations, Army Developing Real-Time Equipment Database." News Website. The Economic Times, October 14, 2019. https://economictimes.indiatimes.com/news/defence/for-better-operations-army-developing-real-time-equipment-database/articleshow/71574345.cms?from=mdr. Accessed December 18, 2020.

[20] Kukla, Jim, Adam Huganir, Jeehye Yun, Jennifer Sleeman, and Aaron Bridgeman. "VADER - Virtual Assistant for Data Entry and Recording The Best Time to Capture What *was* Done Is When It's *getting* Done." Devpost.com. Accessed November 16, 2020. https://devpost.com/software/honeybadger-r13qbp#updates.

[21] Interaction with EME officers undergoing MTech at IIT Kharagpur

[22] Sriram Sharma. "Here's Why India Is Likely to Lose the AI Race." Factor Daily, August 18, 2017. https://factordaily.com/artificial-intelligence-india/. Accessed December 14, 2020.

[23] The Golden Hour is the period of time during which human and medical intervention is required to save lives after injury of any form.

[24] Singer, P. W. Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century. New York, NY: Penguin Books, 2010.

[25] Ibid

[26] Ibid

[27] David Neyland, DARPA TTO. "Legged Squad Support System (LS3)." Industry Day Agenda: Presentation on DARPA's LS3 presented at the Industry Day Agenda, Arlington, Virginia, November 12, 2008. Accessed December 14, 2020.

[28] David Neyland, DARPA TTO. "Legged Squad Support System (LS3)." Industry Day Agenda: Presentation on DARPA's LS3 presented at the Industry Day Agenda, Arlington, Virginia, November 12, 2008.

[29] DARPA Official Website. "DARPA Tiles Together a Vision of Mosaic Warfare." Accessed December 18, 2020. https://www.darpa.mil/work-with-us/darpa-tiles-together-a-vision-of-mosiac-warfare.

[30] The Economic Times. 2020. *Focusing On Dynamic Response That Is Below Threshold Of All-Out War: Indian Army Chief*. [online] Available at: <https://economictimes.indiatimes.com/news/defence/focusing-on-dynamic-response-that-is-below-threshold-of-all-out-war-indian-army-chief/articleshow/74471547.cms?from=mdr> [Accessed 6 January 2021].

[31] David Hambling. "Indian Army Shows Off Drone Swarm Of Mass Destruction." Forbes, January 19, 2021. https://www.forbes.com/sites/davidhambling/2021/01/19/indian-army-shows-off-drone-swarm-of-mass-destruction/?sh=1e7f45ae2384.

[32] "Metadata And Data Standard | E-Governance Standards, Standards For E-Governance Applications". 2021. *Egovstandards.Gov.In*. http://egovstandards.gov.in/metadata-and-data-standard.

[33] Anil Ananthaswamy. "Deep Neural Networks Help to Explain Living Brains." Accessed December 14, 2020. https://www.quantamagazine.org/deep-neural-networks-help-to-explain-living-brains-20201028/?mc_cid=598581e9a8&mc_eid=95deaabb89&utm_source=newsletter&utm_medium=email&utm_

campaign=newsletter_axiosfutureofwork&stream=future.

[34] Cathy O'Neill. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Second. London: Penguin Allen Lane, 2017.

[35] Schiffer, Zoe. "Google Fires Prominent AI Ethicist Timnit Gebru." The Verge, December 3, 2020. https://www.theverge.com/2020/12/3/22150355/google-fires-timnit-gebru-facial-recognition-ai-ethicist. Accessed December 9, 2020.

[36] Lindsey R Sheppard. "The Future of War: Less Fantastic, More Practical." ORF Online, February 1, 2020. https://www.orfonline.org/expert-speak/the-future-of-war-less-fantastic-more-practical-60935/. Accessed December 14, 2020.

[37] Ram Shankar Siva Kumar, David O'Brien, Jeffrey Snover, Kendra Albert, and Salome Viljoen. "Failure Modes in Machine Learning." Berkman Klein Center for Internet and Society at Harvard University, November 11, 2019. https://docs.microsoft.com/en-us/security/engineering/failure-modes-in-machine-learning#how-to-use-this-document. Accessed December 14, 2020.

[38] Ann, Kristen. "Systematic Analysis of Complex Dynamic Systems : The Case of the USS Vincennes," n.d., 263.

[39] Agencies, Staff and. "Coroner Condemns 'glaring Failures' That Led to US Missile Killing RAF Crew." the Guardian, October 31, 2006. http://www.theguardian.com/uk/2006/oct/31/military.iraq. Accessed December 19, 2020.

[40] Gellman, Barton. Dark Mirror:Edward Snowden and the Surveillance State. First. London: The Bodley Head, 2020.

[41] Bing, Christopher. "Suspected Russian Hackers Spied on U.S. Treasury Emails - Sources." *Reuters*, December 14, 2020. https://www.reuters.com/article/us-usa-cyber-treasury-exclusive-idUSKBN28N0PG. Accessed December 19, 2020.

[42] Cdr Amrut Godbole. "Scale up National Cloud for AI in Defence." Indian Council on Global Relations (Gateway House), April 9, 2020. https://www.gatewayhouse.in/national-cloud-ai-defence/. Accessed December 14, 2020.