PINNACLE

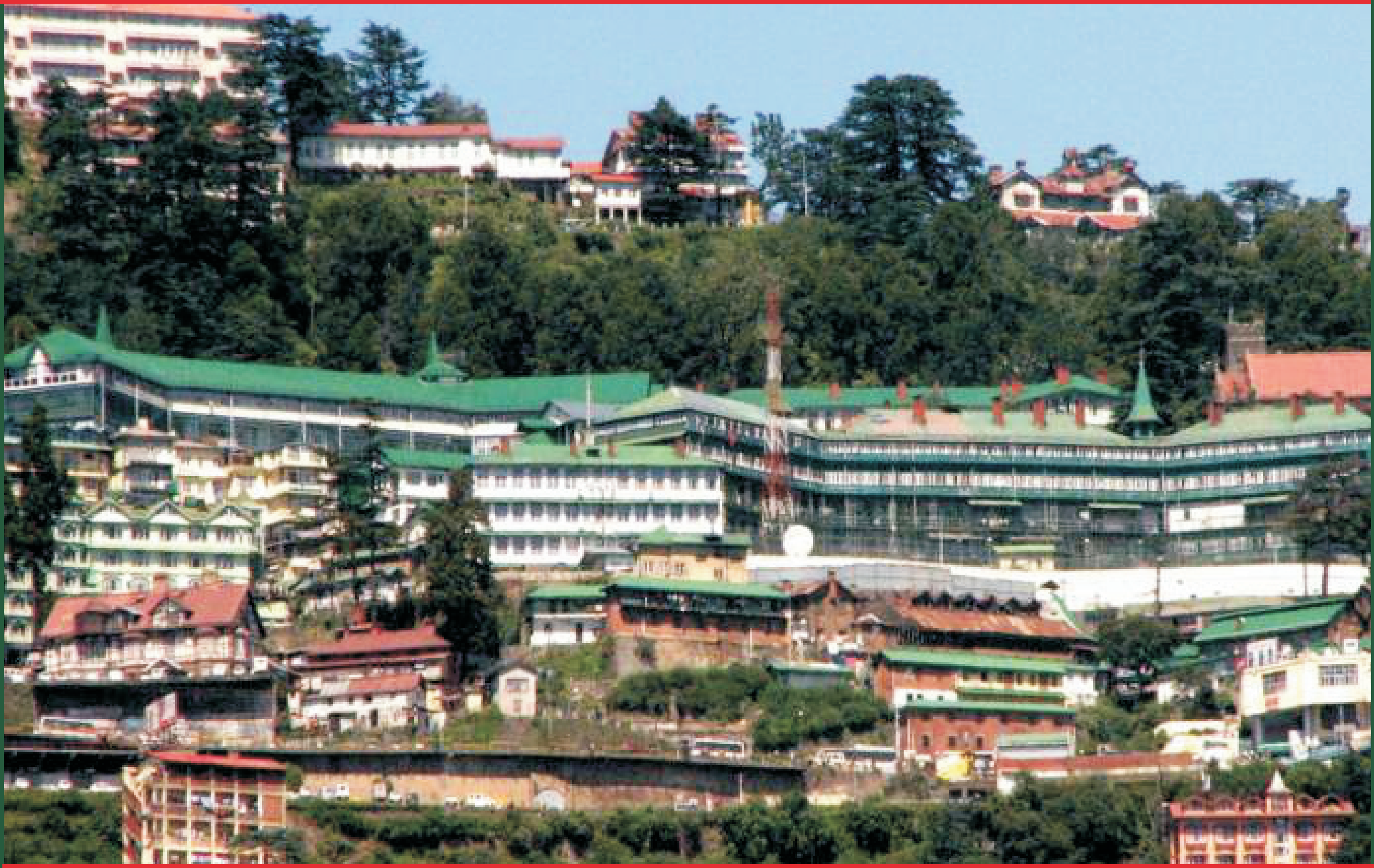
The ARTRAC Journal

Army Training Command, India

VOL 21

2022

ARTIFICIAL INTELLIGENCE AND THE FUTURE OF WARFARE: ROADMAP FOR THE INDIAN ARMY



''युध्द कला शास्त्रे च श्रेष्ठता''

"Excellence in the Art and Science of War"

MISSION

"To offer a vibrant forum for serving and retired members of the armed forces, civil services, police organisations, members of government and academia to exchange the views and express mature professional thoughts on contemporary national and international security matters, art and science of warfare, military strategy, leadership, management and other topics of vital national interest".

PINNACLE - THE ARTRAC JOURNAL

PINNACLE is one of the leading professional journals of the Indian Army. Published from the alma-mater of all conceptual studies for future warfare, the journal offers a vibrant forum to all serving and retired members of all three Services to share military thoughts on contemporary security and defence matters at the conceptual, directional and functional levels.

The Indian Armed forces, like all other modern armies, have been influenced by Information Warfare and Revolution in Military Affairs. The strategic thinkers and military intellectuals need to explore the impact of these emerging technologies on the doctrines and concepts and visualize as to how it will affect the method of waging wars in future.

In this era of ever changing battlefield environment, it is incumbent on the part of the servicemen as well as the military intelligentsia to remain abreast with the developments. The resultant changes in doctrines, strategies, concepts, organisations and tactics need to be evolved continuously. PINNACLE provides an ideal forum to offer your valued comments on how best we can adapt to the changes and improve our military effectiveness.

PINNACLE is published every year. Copyrights of all published articles rest with the Editor, PINNACLE. No part of this publication may be reproduced or transmitted in any form without the written permission from the Editor.

The views expressed in the articles are solely those of the authors in their individual capacity. They do not represent the views of the Headquarters, Army Training Command or the Indian Armed Forces or any other agency of the Government of India.

PINNACLE is registered with the Indian National Scientific Documentation Centre, with the International Standard Serial Number, 0972-4044, allotted to it. The title PINNACLE is also registered with the Office of the Registrar of Newspapers for India in terms of the Proviso to Section 6 of the Press & Registration of Books Act, 1867, vide their letter No HPENG 00169/08/1/2001-TC dated 03 Jan 2002.

PINNACLE

Published By
Headquarters, Army Training Command, Shimla (HP), India

VOLUME 21 **INDEX** **2022**

ARTICLES

FOREWORD

Science and Warfare share a symbiotic relationship. While Geopolitical considerations and Nature of War have proved enduring and timeless, technology has shaped profound changes in the Character of War. In the 16th Century, science was used to develop field fortifications and to calculate ballistic trajectories. It was however, in the 20th Century that technological inventions in the internal combustion engine and electronics made their presence felt in unprecedented ways.

Warfare since the 1950s has been transformed by convergence of information and computing prowess of the computer chip. Network Centric Warfare which facilitated the convergence of sensors and communications often overwhelmed the decision makers with information. Artificial Intelligence (AI), currently at nascent stage has already made profound impact in administrative and logistics functions. AI also has the potential to complement human cognitive functions, thereby, assisting commanders to take decisions on the battlefield. In its evolved form, AI would reduce the human cognitive **Observe – Orient – Decide – Act (OODA) Loop** into a more proactive and nonlinear **Anticipate – Act – Adapt** paradigm, thereby transforming warfare.

Even as predicting the future is subject to probabilities, trends suggest that the number of variables that could impact warfare in the future are likely to be greater than the previous wars. Change in any one variable could create an exponential impact on the outcome of the battle and even the war itself. Appreciating and monitoring the complex interplay between large number of military and non-military variables are likely to transcend beyond human cognitive abilities. In future wars, therefore, exploitation of AI to supplement human cognitive abilities could represent the difference between the winning and losing side.

Our Nation and the Armed Forces in particular have laid impetus in developing AI enabled solutions. Institutions and framework have been established to incorporate this niche technology in military operations to leverage the opportunities available to own advantage in future battlefield. It gives me immense pleasure to release Pinnacle 2022 edition, themed '**Artificial Intelligence and the Future of Warfare: Roadmap for the Indian Army**'. The journal has articles and book reviews highlighting various facets of AI and its applicability in warfare. I sincerely thank all authors for providing an insight on the contemporary subject making it an interesting read.

JAI HIND

(SS Mahal)
Lt Gen
GOC-in-C, ARTRAC

From the Editor

Dear Readers, the Editorial Team has the singular privilege of putting forward this edition of Pinnacle with the theme '**Artificial Intelligence and the Future of Warfare: Roadmap for the Indian Army**'. Overwhelming response to the theme is a clear indication of the relevance of the topic in the current scenario. We are also grateful to all the readers who provided us with their valuable feedback on our previous issue on '**Employment of Offensive Cyber as a Multiplication Tool for Defensive and Offensive Operations by the Indian Army**'.

In the current issue, contributions have been made by a wide spectrum of authors with varied service experience. The facets of '**Artificial Intelligence and the Future of Warfare: Roadmap for the Indian Army**' that has been covered in the Journal include application of Artificial Intelligence in operations to enhance the combat efficiency of Indian Army. The journal highlights aspects of incorporating Artificial Intelligence in cyber, communications, logistics, R&D and it's applicability in future wars. The quality and content of each article received demanded that they be published; however, due to constraints of space, the Editorial Team had to contend with only 16 articles. Some of the articles have been edited to conform to the size and to avoid repetition. We have also included two reviews of the books 'Artificial Intelligence and the Future of Power: 5 Battlegrounds by Mr Rajiv Malhotra" and AI by Design – A Plan for Living with Artificial Intelligence by Catriona Cambell' respectively.

Team Pinnacle expresses its sincere gratitude to our esteemed subscribers, authors and readers for their keen interest in the Journal and look forward for the contributions for our next issue based on the theme '**Changing Character of War'.**

Happy Reading

- Editor

Theme for PINNACLE 2023 Issue

CHANGING CHARACTER OF WAR

The Indian Army is a battle-hardened force renowned for its professionalism. The rich experience gained in varied terrain and different operations of war will undoubtedly be beneficial as the Indian Army prepares for future conflicts. Leaders familiar with battlefield conditions are more likely to appreciate, describe and lead their units and formations to success. However, leaders would also need to relate their experiences within the context of a broad understanding of the Nature and Character of War.

It is unlikely that experiences of the past conflicts will be fully applicable in the future. Fog, friction, uncertainty and complexity have been intrinsic to the Nature of War since times immemorial and are likely to remain so in the future. However, the Character of War, which in essence is the form in which violence is applied on the battlefield, has seldom been the same. Wars are a contest of wills in a given social, cultural, political and economic backdrop; all of which continue to evolve. Besides technology, structures and doctrines also influence the Character of War. Leaders at all levels therefore, need to consider what experiences of the past will be relevant in the future. This assessment will assist leaders in placing their training/education as well as experiences in context to develop understanding of the continuities and discontinuities of war.

Studying the evolving Character of War is important to ensure that the Indian Army prepares for the right kind of war. Accordingly, Changing '**Character of War**' has been identified as the theme for the next publication. The publication would be divided in four themes with subthemes to ensure greater granularity and insights into the Character of War. A note on Changing Character of War has also been included along with guidelines for contributing authors for reference at the end of this journal.

The professional journal being an unclassified venture and published on the open domain, invites articles confined to the norms of unclassified domains of the theme & sub-themes. I am extremely grateful to all the eminent authors for sending in their contributions for the current edition on the theme '**Artificial Intelligence and the Future of Warfare: Roadmap for the Indian Army**' and would solicit similar support for the next issue.

- Chief Editor

DISCLAIMER

The views expressed and suggestions made in the articles are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with the author.

ARTIFICIAL INTELLIGENCE AND ITS EXPLOITATION IN FUTURE WARFARE

- Brigadier (Dr) Navjot Singh Bedi

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

- Alan Turing

Introduction

The above quote by *Alan Turing* is a stark reminder of what awaits us as regards predicting ***Singularity***. Despite that, among the newer generation technological developments, Artificial Intelligence (AI), Quantum Computing and Big Data Analytics hold greater promise for their applications in the Defence and Security Forces. These largely computer science-based technologies are inspired by the relentless research undertaken in the US and followed equally seriously in China, Europe, Japan, Russia, and Israel. India has also made credible strides and a Bengaluru-based DRDO Laboratory, Centre for Artificial Intelligence and Robotics (CAIR), has developed several technologies for applications in Defence Forces. The Indian Army has set up a centre for AI at the Military College of Telecommunication Engineering (MCTE), Mhow for undertaking research in this field. AI has the potential to revolutionise the way future wars will be fought. To quote Ray Kurzweil, American inventor, and futurist, "***Artificial intelligence will reach human levels by around 2029. Follow that out further to, say, 2045, and we will have multiplied the intelligence – the human biological machine intelligence of our civilization – a billion-fold***."

On 18 November 2021, while delivering the keynote on India's technology evolution and revolution at the inaugural Sydney Dialogue, Hon'ble Prime Minister Narendra Modi said that it is a "great honour" for India and that this indicates India's central role in the Indo-Pacific region and in the emerging digital world. He said that "*We are in a time of change that happens once in an era. The digital age is changing everything around us. It has redefined politics, economy and society. It is raising new questions on sovereignty, governance, ethics, law, rights and security. It is reshaping international competition, power and leadership*". The same is equally true for AI and the changes it will usher in the field of Defence.

Modern Warfare

Modern warfare refers to the concepts, methods and technologies that have come into use during and after the Second World War and the Korean War. The Gulf War (Operation Desert Storm) and the wars in Afghanistan, Iraq and Russia-Ukraine are indicators of the shape of things to come. The concepts and methods have assumed complex forms of the 19th and early-20th-century antecedents, largely due to the widespread use of highly advanced information technology, and modern armies must modernize constantly to preserve their battle-worthiness.[1] Although total war was thought to be the form of international conflict from the experience of the French Revolutionary Wars to the Second World War, the term no longer describes warfare in which countries or nations use all of their resources to destroy another country's or nation's organised ability to engage in war. The practise of total war, which had been in use for over a century as a form of war policy, has changed dramatically with greater awareness of tactical, operational, and strategic battlefield.

Drivers of Change

The primary drivers of change in the way wars will be fought in times to come will be the Economy, the Public Pressure/ Public Opinion, the Punitive Cost of a Nuclear Strike, and the Impact of Emerging Technologies. In the present-day context, due to the emphasis on economic development and the prohibitive costs associated with wars, the likelihood of a full-scale war is extremely remote. Moreover, due to the availability of nuclear weapons, full-scale war carries with it the prospect of total annihilation, which is a no-win situation for all concerned. In addition, no government relishes the prospect of its soldiers dying in combat and being answerable to the public for the same. Lastly, the multitude of technological developments that have taken place, including those that are on the drawing board, have revolutionised the way wars will be fought.

As such, conflicts since WWII have by definition been "low intensity" conflicts,[2] typically in the form of proxy wars fought within local regional confines, using what are now referred to as "conventional weapons," typically combined with the use of asymmetric warfare tactics and applied use of intelligence and high technology weapon platforms. The impact of AI in future warfare has been analysed in subsequent paragraphs.

Introduction and Attributes of AI

Definition AI is an umbrella term for smart technologies that are aware of and can learn from their environments, enabling them to subsequently take autonomous action. Robotic process automation, machine learning, natural language processing, and neural networks, all incorporate AI into their operations. AI enables machines to respond autonomously to inputs from the external world,

[1] *International Congress Innovation &Technology XXI: Strategies & Policies Towards the XXI Century, & Soares, O. D. D. (1997). Innovation and technology: Strategies and policies. Dordrecht: Kluwer Academic.*

[2] *Creveld, Martin Van (2000). "Technology & War I:To 1945". In Charles Townshend. The Oxford History of Modern War. New York, USA: Oxford University Press. p. 206. ISBN 0-19-285373-2. And Creveld, Martin Van. "Technology and War II:Postmodern War?". In Charles Townshend. The Oxford History of Modern War. p. 349.*

inputs that programmers do not directly control and therefore cannot always anticipate[3]. AI is thus a collective term for computer systems that can sense their environment, think, learn, and take action in response to what they are sensing. Forms of AI in use today include, among others; digital assistants, chat bots and machine learning.

Types of AI AI works in four ways, namely, **Automated Intelligence** which deals with the automation of manual or cognitive and routine or non-routine tasks; **Assisted Intelligence** which helps people to perform tasks faster and better; **Augmented Intelligence** which helps people to make better decisions and **Autonomous Intelligence** which leads to automating decision making processes without human intervention.[4] *A brief description of a few technical terms usually employed in AI literature often leads to a better understanding of its potential applications.*

Approaches to AI In an article titled "Some Specific Tech Aspects of Artificial Intelligence", André M. König, has described two vastly differing approaches to AI[5] namely: **General** and **Narrow** AI, also called **Strong** and **Weak AI**. Strong AI is a hypothetical machine that exhibits behaviour at least as skilful and flexible as humans, and there is a research programme to build such an artificial general intelligence. A strong AI builds its own models based on raw input. The principle behind Strong AI is that machines could be made to think or could represent human minds in the future. Those machines will have the ability to reason, think, and perform all functions that a human is capable of doing. Weak AI, on the other hand, uses models of its problem domain assigned to it by programmers. In Weak AI, machines can be made to act as if they are intelligent, like a computer playing chess with a human player based on pre-programmed moves by the humans

Machine Learning (ML) and Deep Learning (DL) ML uses algorithms to parse data, learn from it, and then decide or predict something pertaining to the data. The machine is trained using large amounts of data and algorithms that give it the ability to learn how to perform the task. Computer vision is an application for machine learning, though it still requires a great deal of hand-coding to get the job done. **Deep Learning** (DL) is a branch of ML based on a set of algorithms that attempt to model high-level abstractions in data. Simply put, one can have two sets of neurons: ones that receive an input signal and ones that send an output signal. When the input layer receives an input, it passes on a modified version of the input to the next layer. In a deep network, there are many layers between the input and output, allowing the algorithm to use multiple processing layers,

[3] *Chris Curran and Anand Rao; PWC Briefing: Artificial intelligence; http://usblogs.pwc.com/ emerging-technology/briefing-ai/.*

[4] *ibid*

[5] *Andre M Konig, "Some specific tech aspects of Artificial Intelligence"; https://www.linkedin.com /pulse / some-specific-tech-aspects-artificial-intelligence.*

composed of multiple linear and non-linear transformations. DL is part of a broader family of machine learning methods based on learning representations of data.

Data Science Jim Gray imagined data science as a ***fourth paradigm*** of science (empirical, theoretical, computational and now data-driven) and asserted that everything about science is changing because of the impact of information technology and the data deluge.

AI Development Trends

Messrs Rao, Voyles and Ramchandani have listed **Deep Reinforcement Learning (DRL)** and **Generative Adversarial Network (GAN)** as emerging AI trends in their paper on this subject[6] and also indicated their likely future applications. **DRL** involves interacting with the environment to solve business problems. DRL has been used to learn gaming strategies. **GAN** is a type of unsupervised deep learning system that is implemented as two competing neural networks. One network, the generator, creates fake data that looks exactly like the real data set. The second network, the discriminator, ingests real and synthetic data.

Global AI Developments in Defence Applications[7]

Russia In 2017, Russian President Vladimir Putin declared that whichever country becomes the leader in AI "*will become the ruler of the world*." Russia has been working on AI guided missiles that can decide to switch targets mid-flight. Reportedly, there already exist completely autonomous AI operation systems that provide the means for UAV clusters to fulfil missions autonomously, share tasks between them, and interact. Russia believes that it is inevitable that swarms of drones will one day fly over combat zones. Russia has been testing several autonomous and semi-autonomous combat systems, such as Kalashnikov's neural net combat module, with a machine gun, a camera supported by AI that can possibly make its own targeting judgments without human intervention. The Russian government has strongly rejected any ban on Lethal Autonomous Weapons Systems (**LAWS**), suggesting that such a ban could be ignored. The AI subsidiary of MTS,[8] Russia's largest telecom operator, has launched a US$ 100 million venture capital fund for start-ups, to include upto $20m in individual projects & start-up accelerator investing up to $100,000 per project.

[6] *Anand Rao, Joseph Voyles and Pia Ramchandani;Top 10 artificial intelligence (AI) technology trends for 2018; http://usblogs.pwc.com/emerging-technology/top-10-ai-tech-trends-for-2018/.*

[7] *Artificial intelligence arms race; https://en.wikipedia.org/wiki/Artificial_intelligence_ arms_race.*

[8] *https://developingtelecoms.com/telecom-business/telecom-investment-mergers/11904-russian-operator-mts-launches-us-100m-ai-investment-fund.html*

China China sees itself as a close competitor to the United States in AI. The Chinese military intends to achieve an advantage through changing paradigms in warfare with military innovation. The close ties between Silicon Valley and China, and the open nature of the American research community, have made the West's most advanced AI technology available to China. The Chinese industry has numerous home-grown AI accomplishments of its own, such as Baidu passing a notable Chinese-language speech recognition capability benchmark in 2015. By 2030, China aims to make great strides in various AI technologies like Big Data and Autonomous Intelligent Systems. As of 2017, China's roadmap aims to create a US$150 billion AI industry by 2030. China often sources sensitive emerging technology such as drones and AI from private start-up companies. The Japan Times reported in 2018, that private Chinese investments in AI were under US$7 billion per year. In 2020, private investments in AI from China amounted to almost US$ 9.9 billion in funding, ranking it second after the USA. China's AI start-ups received nearly half of the total global investment in AI in 2017. Of late, Chinese institutions have filed for nearly five times as many AI patents as Americans have.

By 2025, China plans to achieve major breakthroughs in AI to reach a leading level, with AI becoming a primary driver for China's industrial advancements and economic transformation. By then, China intends to become a leading player in research and development while widely using AI in fields ranging from manufacturing to medicine to national defence. China's core AI industry is likely to surpass 400 billion RMB (about US$ 59 billion), with AI-related fields exceeding 5 trillion RMB (about US$ 740 billion). The Chinese leadership is advocating an "innovation-driven" strategy for civilian and military development, aiming to become the world's "premier innovation centre" in AI by 2030.

China's recent advances in Swarm Intelligence—which involves autonomous cooperative behaviour among masses of distributed robots—have been on prominent display in official media. In June 2017, China Electronics Technology Group Corporation, a state-owned defence conglomerate, successfully flight-tested a swarm of 119 drones—a new record. In a conflict, the PLA could use swarms to target high-value U.S. weapons platforms, such as aircraft carriers. In addition, China plans to achieve progress in the creation of laws and regulations, as well as ethical norms and policies, along with the establishment of mechanisms for AI safety assessment.

United States of America United States believes that the rapid advances in AI will define the next generation of warfare. According to Deltek[9], identifiable federal spending on AI rose to **nearly US $1 billion in 2020**, up 50 percent from FY-2018, making it one of the fastest-growing emerging tech investment areas. In 2020, private investments in AI in the US amounted to almost $ 23.6 billion. Drones, motherships, protective exoskeletons, unmanned vessels,

[9] *https://crsreports.congress.gov/product/pdf/IF/IF11150.*

and combat are some military-based AI applications in the US. A few other military AI combat programmes of the US are the Sea Hunter autonomous warship, which is designed to operate for extended periods at sea without a single crew member, and to even guide itself in and out of port.

The USA government is spending billions of dollars preparing for the next stage in warfare that it believes will be defined by advances in AI. Concepts like motherships of drones releasing little baby drones from the air and the sea, infantrymen and women sporting exoskeletons and wearable electronics loaded up with combat apps, and lone mission commanders directing swarms of unmanned vessels to carry out operations are already being tested at MIT’s Computer Science and AI Laboratory.

A new National Science and Technology Council (NSTC) Subcommittee on Machine Learning and Artificial Intelligence was formed on 03 May 2016 to help coordinate federal activity in AI. On June 15, 2016, NSTC directed the subcommittee on Networking and Information Technology Research and Development (NITRD) to create a National Artificial Intelligence Research and Development Strategic Plan. A NITRD Task Force on Artificial Intelligence was then formed to define the federal strategic priorities for AI R&D, with particular attention to areas of national security that private industry is unlikely to address. In the last few decades, one of the largest sources of funding for AI research came from the Defence Advanced Research Project Agency (DARPA).

Israel Most remarkably, Israel has seen investments in AI start-ups go from 5% of all equity invested in start-ups in 2011 to 25% by mid-2018. The Israel Innovation Authority (IIA) has launched a national programme to promote AI and data science at a total cost of 5.26 billion shekels (US$ 1.63 billion). The goals of the programme are to promote high-level research to create an ecosystem that will enable the continued development and competitiveness of industry, academia, and the public sector. It also aims to develop critical applications for Israel's security and to assimilate the use of AI in industry, services, and government ministries. Israel has designed Harpy anti-radar fire and forget drone that is to be launched by ground troops and autonomously fly over an area to find and destroy radar that fits pre-determined criteria.

Military Applications of AI[10]

Adopting AI tools in defence enhances the processing and utilization of data which in turn improves the speed of decision-making on the battlefield. Below are few applications of AI in the military:-

- **Computational Military Reasoning** Computational military reasoning solves military problems that humans face and focuses on

[10] *https://acadgild.com/blog/applications-of-ai-in-military.*

making the right battlefield decisions. It analyses the area of conflict and acts on the data it receives from the set of orders (known as the "Course of Action" or COA). In controlled settings like military labs, this application can exploit the weaknesses of the enemy successfully.

- **Intelligent and Autonomous Unmanned Weapon Systems** Unmanned vehicles that are used by armed forces, as well as the most sophisticated weapons and robotics, are some of the direct uses of AI. These weapon systems have the requisite intelligence to observe, pursue and destroy enemy targets distinctly.

- **AI-Enabled Information Processing and Intelligence Analysis** Deep learning algorithms can be used to effectively process sensor data and raw intelligence that has been collected from satellite imagery. This information can aid in making accurate decisions during military operations.

- **Communications and Computers** Communication is the core of all military activities, providing improved visibility. The non-availability of real time information can hamper the decision-making ability of soldiers fighting the war. In future, the success on the battlefield will depend on maintenance of network connectivity and management of information, especially using agile cognitive networks, from a large variety of sources, which will be considerably enhanced due to AI.

- **Cyber Defence and Cyber Warfare** Cyber-attacks can be detected and curbed through pattern matching, statistical analysis, machine learning and big data analysis. Offensive cyber operations can unleash large scale destruction of cyber networks in a matter of minutes. Considering the speed at which AI works, it serves as a counter-intuitive force against malicious cyber threats. Generative Adversarial Networks (GAN) are likely to be employed in cyber detection applications in future.

- **Electronic Warfare (EW)** EW employs the electromagnetic spectrum (that includes radio waves, infrared signals, or radar) to sense, protect, and communicate data. It can also be used to block adversaries from using electronic equipment. In India, Adaptive Radar Countermeasures (ARC) and Behavioral Learning for Adaptive Electronic Warfare (BLADE) are direct applications of AI. ARC enables airborne EW systems to automatically generate effective spontaneous countermeasures against unknown radars in real time. This is done intelligently in the presence of other signals, which could be either hostile or neutral. On the other hand, the BLADE program develops machine learning algorithms to rapidly detect new radio threats and dynamically generate new countermeasures that are similar to ARC even in the most tactical environments.

- **Pattern Recognition** Pattern recognition is the area of research that studies the operation and design of systems that identify patterns in data. When a program makes observations of some kind, it is often programmed to compare what it observes as a pattern, e.g., face, fingerprint, or handwriting recognition. Important application areas are image analysis, character recognition, speech analysis, man-machine diagnostics, and personnel identification, all of which have applications in the military.

- **Bioinformatics** Bioinformatics is the application of computer technology for the management of biological information. AI provides several powerful algorithms and techniques for solving important problems in bioinformatics. Approaches like Neural Networks, Hidden Markov Models, Bayesian Networks and Kernel Methods are ideal for areas with more data but very less theory. The goal in applying AI to bioinformatics is to extract useful information from the wealth of available data by building good probabilistic models.

- **Data Mining** An AI-powered tool that can discover useful information within a database that can then be used to extract patterns from data. Data mining is seen as an increasingly important tool by modern businesses to transform data into business intelligence, giving an informational advantage. It is currently used in a wide range of profiling practices, such as marketing, surveillance, fraud detection, and scientific discovery. Profiling and surveillance have applications, especially in CI/CT operations.

- **Expert Systems** An expert system is a computer program that represents reason with knowledge of some specialist subject with the view of solving problems or rendering advice. It is essentially a knowledge-based system, having several modules, sub-modules, and sections. The knowledge-based applications of AI have enhanced productivity in almost all fields, such as business, science, engineering, and the military. Today’s expert systems clients can choose from dozens of commercial software packages with easy-to-use interfaces. Diagnosis and troubleshooting explain the development and testing of a condition-monitoring sub-module of an integrated plant maintenance management application based on AI techniques.

- **Robotic Surgery**[11,12&13] This has the potential to relive surgeons to perform other lifesaving tasks/supervise robotic surgery and has immense potential in posts at remote/inaccessible areas.

- **Powered Exoskeleton**[14] AI coupled with robotics can facilitate development of Future Force Warrior (like Iron-man). This will not only aid heavy lifting but will also provide a solution for paralysis/muscle related diseases, warfare, construction, LOPES (exoskeleton), Re Walk, Human Universal Load Carrier.

- **Body Implants, Prosthesis, Regenerative Medicine** Brain implant, retinal implant, prosthetics, rejuvenated soldiers & life extension may soon be possible due to AI. This will greatly augment the combat potential and staying power of the armed forces.

- **Self-Reconfiguring Modular Robot (SCMR)** AI will enable SCMR to be a reality which may change the way we make many physical structures and machines.

- **Swarm Robotics**[15] AI enabled swarm intelligence, autonomous robotics, nanorobotics, particle swarm optimization, multi-agent systems, behaviour-based robotics have the potential to ensure autonomous cooperative behaviour among masses of distributed robots. In a conflict, swarms of drones can be used to target high-value weapons platforms of the adversary, such as aircraft carriers, as well as to confuse and evade enemy radar.

- **Cloak of Invisibility**[16&17] AI has the potential to provide camouflage cloaking microscope tips at optical frequencies, thus addressing one of the challenges that has perplexed armies since time immemorial.

[11] *"Doctors grapple with the value of robotic surgery". Houston Chronicle 16 September 2011. Retrieved 24 December 2011.*

[12] *"Robotic surgery making inroads in many medical procedures." The Jakarta Post 8 March 2011. Retrieved 24 December 2011.*

[13] *"Doctors Perform First Fully Robotic Surgery". PC World. 21 October 2010. Retrieved 24 December 2011.*

[14] *Christopher Mims (2009). "Exoskeletons Give New Life to Legs". Scientific American. Retrieved 21 April 2009.*

[15] *"Riders on a swarm". The Economist. 12 August 2010. Retrieved 21 April 2011.*

[16] *Rachel Kaufman (28 January 2011). "New Invisibility Cloak Closer to Working "Magic"". National Geographic News. Retrieved 4 February 2011.*

[17] *"Breakthrough in bid to create 'invisibility cloak' as 3D object is made to vanish for first time". Daily Mail. 26 January 2012. Retrieved 3 March 2012.*

- **Immersive Virtual Reality** AI can also provide an artificial environment where the user feels just as immersed as they usually feel in consensus reality. This will add a realistic feel to the conduct of war games and simulations and may end up economising expenditure on formation exercises.

- **Social Media based IW** With social media sites overtaking TV as a source for news for young people and news organisations increasingly reliant on social media platforms for generating distribution, major publishers now use AI to post stories and generate higher volumes of traffic. The same rationale can be used by the ADG PI in furthering a favourable narrative.

- **Logistics** Various models of operations research have been employed in effective management of logistics operations. AI has great potential in assisting in planning and keeping the supply chain effective and efficient. In 1991, US forces deployed a Dynamic Analysis and Re-planning Tool (DART), using AI planning techniques, during the Gulf War to undertake automated logistics planning and scheduling for transportation, which allowed a plan to be generated in hours rather than weeks.

Tactical Applications of AI[18] The advent of AI could fundamentally change the character of war, resulting in transformation from today's "informatized" ways of warfare to future "intelligentized" warfare, in which AI will be critical to military power. Few tactical applications of AI are as under:-

- Mine sweeping drone bots that use feature maps to analyse and identify mines, to deactivate them or carry them away.

- Enemy segmentation detection - identify enemy tanks in different situations.

- Combat simulations using virtual reality, can help train soldiers for a more realistic battlefield environment.

- Combat helmets with visors help analyse battlefield environment and provides wide vision.

- Analysing location of missiles fired, akin to satellite defence grid systems to shoot down the correct missile.

[18] *Military Applications Of Artificial Intelligence; March 17,2018 By Deepak Kumar Gupta (http://www.claws.in/1878/military-applications-of-artificial-intelligence-deepak-kumar-gupta.html).*

- **Screenless Display**[19] **(Virtual Retinal Display, Bionic Contact Lens), Eye Tap** Augmented reality, virtual reality, Eye Tap could allow user to reference the blueprints like in a construction yard, in a 3D manner, Head-mounted display, Head-up display, & adaptive optics for the next generation soldier.

- **Electronic Nose**[20&21] Detecting spoiled food, chemical weapons and explosives and detection of contagious pandemic affected people.

- **Memristor**[22&23] AI enables the development of smaller, faster, lower power-consuming analogue electronics, which has immense potential in equipment used at the tactical level.

- **Machine Vision**[24] Biometrics, controlling processes (driverless car, automated guided vehicle), detecting events (visual surveillance), interaction (non-human-computer interaction), and robotic vision.

Niti Ayog Roadmap The national AI task force at NITI Aayog of India has also set up a road map for the AI development employing intelligent machines enabling high-level cognitive processes like thinking, perceiving, learning, problem solving and decision making, coupled with advances in data collection and aggregation, analytics and computer processing power. NITI Aayog has decided to focus on five sectors that are envisioned to benefit the most from AI in solving societal needs:-

- Healthcare: increased access and affordability of quality healthcare,

- Agriculture: enhanced farmers' income, increased farm productivity & reduction of wastage,

- Education: improved access and quality of education,

- Smart Cities and Infrastructure: efficient and connectivity for the burgeoning urban population and

[19] *"Google 'to unveil' hi-tech Google Glasses that put a screen of information over the world." Daily Mail 20 December 2011 Retrieved 22 December 2011.*

[20] *"Tuberculosis breakthrough as scientists get funds for 'electronic nose'". The Guardian. 07 November 2011. Retrieved 4 December 2011.*

[21] *"Now, a mobile phone that can smell". The Times of India. 7 November 2011. Retrieved 04 December 2011.*

[22] *"Remapping Computer Circuitry to Avert Impending Bottlenecks". The New York Times. 28 February 2011. Retrieved 27 April 2011.*

[23] *"Memristor revolution backed by HP". BBC News. 2 September 2010. Retrieved 27 April 2011.*

[24] *"The big plan to build a brain". The Telegraph. 21 June 2011. Retrieved 18 November 2011.*

- Smart Mobility and Transportation: smarter and safer modes of transportation and better traffic and congestion problems.

AI Commercial Infrastructure[25] Key trends of AI commercial infrastructure are:-

- AI Industry in India was around US$180 Million annually in revenues as on 2018. India's AI market is expected to reach **$7.8 billion by 2025** growing at a CAGR of 20.2%, as per an International Data Corporation (IDC) report. AI software segment would dominate the market and grow from $2.8 billion in 2020 at a CAGR of 18.1% by the end of 2025.

- There are approx one lakh AI personnel working in India across enterprises and sectors – this represents a 20% jump in personnel from 2021 (91000 AI personnel) & from 29,000 in 2018. According to a 2018 report the need for AI skills has more than doubled in the past three years, with job postings going up by a whopping 119%. The average work experience of AI professionals in India is 7.6 years.

- University of Mumbai, BITS (Pilani), IITs (Kharagpur, Delhi, Mumbai, Kanpur, Roorkee), University of Pune & Delhi are the top universities that are undertaking professional AI graduate/ post graduate courses.

Conclusion

AI will eventually manifest in all dimensions of warfare. A comprehensive long-term vision will help formulate a mission oriented long-term policy for critical strategic AI technologies. Since the locus of innovation has shifted to the private sector, the government should facilitate to create closer public-private partnerships, with an emphasis on "Make in India". Human resource needs to be trained and cultivated for military applications of AI.

Home to the world’s third largest start-up ecosystem, elite science and technology institutions like the IITs, robust and ubiquitous digital infrastructure, and millions of newly minted STEM graduates every year, India is well-positioned to become a global leader in the development of artificial intelligence. Industry analysts predict that AI could add up to $957 billion to India’s economy by 2035.

In the spirit of *Sabka Saath Sabka Vikas*, Prime Minister Shri Narendra Modi plans to leverage AI for inclusive development, representing the country's “AI for All' strategy. Directed by the PM’s vision, India will soon stand out in the international community not just as a leader in AI, but also as a model to show the

[25] *Military Applications Of Artificial Intelligence; March 17, 2018 By Deepak Kumar Gupta, (http://www.claws.in/1878/military-applications-of-artificial-intelligence-deepak-kumar-gupta.html).*

world how to responsibly direct AI for social empowerment. In his words ***"India is one of the leading nations in Artificial Intelligence and Machine Learning, especially in human-centred and ethical use of artificial intelligence. We are developing strong capabilities in cloud platforms and cloud computing. This is key to resilience and digital sovereignty*."**

AI has the potential to transform national security. It is also seen that AI is essentially a dual-use technology. While it can fuel technology-driven economic growth, it also has the potential to provide military asymmetry. India has strong IT industry and huge talent pool of engineers which are advantages which need to be leveraged.

Bibliography

1. *Niti Ayog National Strategy for AI: Discussion-Paper; June 2018.*

2. *Artificial Intelligence And The Future Of Defense Strategic Implications For SmallAnd Medium-Sized Force Providers; The Hague Centre for Strategic Studies-2017.*

3. *Warfighting 2018 & Beyond; CENJOWS Aug 2013, by Col Navjot Singh.*

4. *Artificial Intelligence and the Future of Warfare; Research Paper M. L. Cummings International Security Department and US and the Americas Programme January 2017.*

5. *Artificial Intelligence in Military Operations: Technology & Ethics Indian Perspective; Lt Gen RS Panwar, AVSM, SM, VSM, PhD (Retd); January 2019 - March 2019.*

6. *Artificial Intelligence In War: Human Judgment as an Organizational Strength and a Strategic Liability; Avi Goldfarb and Jon Lindsay November 2020; The Brookings Institution publication.*

7. *Future Warfare and Artificial Intelligence- The Visible Path; Gp Capt Atul Pant; IDSA Occasional Paper No. 49; August 2018.*

8. *Military Applications of Artificial Intelligence; Ethical Concerns in an Uncertain World; by Forrest E. Morgan, Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima, Derek Grossman; RAND Corporation, Santa Monica; 2020.*

9. *International law & the military use of unmanned maritime systems Michael N. Schmitt & David S. Goddard; International Review of the Red Cross (2016), 98 (2), 567–592. War & security at sea*

10. *Final report of National Security Commission on AI- Mar 2021 Report; Eric Schmidt –Chair & Robert Work Vice Chair.*

11. *Scope for Use of AI in Security: Opportunities and Challenges; 31st IISSM Annual Global Conclave- 2021; Maj Gen PK Mallick, VSM (Retd); 16 December, 2021.*

12. *Artificial Intelligence (AI) and Its Applications For Defence; CENJOWS/ Indian Def Conclave Seminar; Brig (Dr) Navjot Singh Bedi; Dec 2018.*

STRATEGY TO EVOLVE ARTIFICIAL INTELLIGENCE IN TACTICAL OPERATIONS FOR THE INDIAN ARMY

- Colonel Bikramjeet Singh

"We can evade reality, but we cannot evade the consequences of evading reality"

- Ayn Rand

Introduction

Despite an early start in the year 1950, the real development in the field of Artificial Intelligence (AI) started only around 2010 due to the confluence of three major enablers in the field: availability of big sources of data; massive improvement in computing and processing power; and most importantly, the massive improvement in machine learning science. AI today is being heavily invested in and researched upon in the scientific and commercial world. It is already showing up for nascent commercial usage in many gadgets and devices, search assistance, requirement prediction, data analysis and validation, modelling and simulation, linguistics, psychology etc.

AI now is also termed the Industrial Revolution 4.0 is bringing significant transformations in the commercial as well as military domains. In December 2021, the Chief of Army Staff, General M. M. Naravane, said, "Future wars will be fought with inventive methods and AI." As our needs converge toward the use of AI in the commercial domain, we must also pay attention to the use of AI in military training, warfare, and wargaming. The potential of AI lies in how effectively one can combine human interpretation, data, and algorithms to produce results, enhance the effectiveness of training and operational readiness of the Indian Army. This article will try to analyse the key facets of the same.

Use of AI During Tactical Operations in Modern Day Warfare

As we grow in the domain of AI, there is a requirement for developing, integrating, and enabling advanced AI-based systems that will help the military or the armed forces in combat at the tactical level. While it is known that cloud-based AI systems can be used at operational or theatre level, these systems lack proximity to the tactical edge. Several advanced states or countries have conducted research to make effective use of AI in the tactical domain, and as a result, certain applications where such systems can be used have been discovered. Such applications of AI in tactical operations are listed in the succeeding paragraphs.

- **Autonomous Machines** The use of robotics for taking complex decisions, which are human-like, is mostly done using autonomous machines. The development of autonomous vehicles has been progressed on this concept. Various applications include obstacle recognition, navigation and explosive decanting, etc.

- **Mules** Robots which can work along with armed forces in the forward areas may be a far-fetched dream as of now. However, in some countries, research has already gone into the provision of logistic-based robots which can perform tasks like evacuation of casualties, delivering heavy loads or acting as mules (e.g. the BigDog project of Defence Advanced Research Projects Agency (DARPA)). Defence Research and Development Organisation (DRDO) is also looking forward to develop a Multi Agent Robotics Framework (MARF) which can be used for surveillance and casualty evacuation in Counter Terrorism (CT) operations.

- **Swarming of Drones** AI-based cooperative behaviour, or swarming, is a unique subset of autonomous vehicle development, with concepts ranging from large formations of low-cost drones designed to overwhelm defensive systems to small squadrons of drones that collaborate to provide electronic attack, fire support, and localised navigation and communication nets for ground-troop formations. AI technology may also be adapted for defending harbours, hunting submarines, or scouting in front of a formation of larger navy ships and tanks.

- **Logistics** The validation and audit of transportation decisions and their optimal utilisation for the logistics requirements of armed forces can be done through AI-based programs. Similarly, meeting logistics requirements, including movement of troops or material, is a herculean task, especially in high-altitude areas and difficult terrain. This task, if automated with AI, will reduce a huge amount of effort at the operational level. Knowledge Resource and Intelligent Decision Analysis (KRIDA), an application which aims to facilitate military logistic movements at large scales using extensive knowledge base and data editing systems, is one of the major projects taken up by Centre for Artificial Intelligence and Robotics (CAIR) & DRDO.

Use of AI in Defence and Global Military Conflicts

- **Armenia and Azerbaijan War** In 2020, the news channels were bloated with the conflict between Azerbaijan and Armenia, not only because the conflict was over the Nagorno-Karabakh region, but for Azerbaijan's overwhelming and decisive defeat of Armenia by using AI-based complex military hardware. The country demonstrated how the use of technology such as armed drones can enable minor adversaries to outmanoeuvre a well-equipped enemy on the battlefield. During the conflict, Armenian soldiers apparently anticipated fighting a war as they fought in 1994, using Russian-built T-72 tanks covered by an intimidating network of extremely effective S-300 high-alt air defence missile systems. However, the Armenian forces were outright annihilated by the Azerbaijani forces, which were already prepared for the war of the future.

- **Russia** Drone swarming of the combat zone is inevitable in future wars. According to reports, Russia has developed AI systems capable of performing autonomous or shared missions via drone clusters. They are on the path of achieving AI guided missiles, which have the capability of midflight target switching. Semi-and fully automated combat systems, such as Kalashnikov's AI neural net combat module integrated with a machine gun and a camera for target recognition, are also being tested. Russia is following the aggressive policy of no ban on the development of lethal autonomous weapons.

- **China** Deep ties between China and Silicon Valley technology firms have allowed Chinese home-grown technology firms access to the most advanced AI technology available. Number of AI patents held by Chinese institutions is five times more than what is held by American. Also, drone and AI technology are sourced from private firms by China. In 2015, Chinese homegrown search engine Baidu was able to crack the speech recognition capability benchmark. By 2030, China is on the path of creating a $150 billion AI industry. As per a 2018 report by the Japan Times, Chinese private annual investment in AI is close to $7 billion.

- **Israel** Fire and Forget drone, "Harpy," developed by Israel, has the capability of autonomous flying over an area to find and destroy enemy radars that fits a predetermined criterion.

- **United States of America** The US is working with the commercial sector to harness AI at the tactical level. In 2021, US private investment in AI was close to $100 billion. IBM is analysing the United States Army’s Logistics Support Activity (LOGSA) transportation of spare parts. AI combat programmers such as sea hunters’ autonomous warships have been designed which enable crew-less operations at sea for extended periods with the ability to guide themselves in and out of ports.

- **Russia-Ukraine War** Despite being quantitatively weaker, Ukraine has put up tough resistance against Russian invasion with the use of advanced drones facilitated by Elon Musk’s Starlink satellite system, which is enabling reconnaissance missions by providing uninterrupted internet connectivity. Turkey’s AI-based TB2 Bayraktar drones have been put to effective use by the Ukrainian force. In retaliation, the Russian Army is also exploiting Orion combat drone system which was also used in the Syrian conflict in 2015.

Status of AI in Indian Armed Forces

AI can be used anywhere and everywhere; however what one needs to understand is that the effort required for developing the same is immense. The figure below shows us two solution spaces for AI, i.e., our defence requirements and solution space available for development. The exact requirement lies between the intersection of both the spaces, as depicted in Figure 1. This, however, is an abstract issue as effort, time, and cost vs. the need are certain issues that need to be taken into consideration while developing or undertaking defense-related projects in Robotics and IA. AI has a typical ‘dual-use’ description. The situation is not about humans vs. machines but about interface between humans and machines to make better decisions.

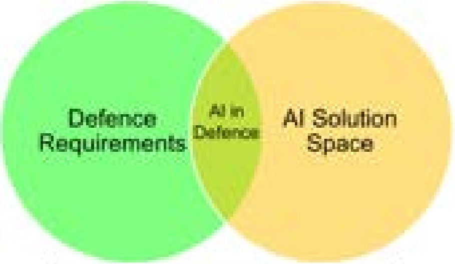


Figure 1: Abstract Areas for AI

Lethal Autonomous Weapon Systems (LAWs) No country has currently deployed fully autonomous weapon systems. However, all global leaders recognised a need to address issues concerning the morality of these weapons and their status under international humanitarian law. The United Nations (UN) has been arguing for a preemptive ban on the development of such weapons. However, countries like the United States have argued that autonomous weapons have benefits, including reducing casualties and improving efficiency in defensive capabilities.

AI Roadmap for India The AI roadmap by the Indian government was published in the year 2018 by the AI task force, which was constituted by the Ministry of Commerce and Industry and the national strategy for artificial intelligence under the stewardship of Niti Aayog. While acknowledging the need to promote AI, governments at different levels, along with their various instrumentalities, should adopt proactive measures to accelerate AI adoption in various processes. However, the report of the task force on AI does recognise AI as a major force multiplier and suggests development military applications. The report has clearly given and identified that the cost of technology and system management capability are major challenges towards developing military applications for AI.

Doctrines Though the doctrines for integrated warfare exist with the Indian armed forces, stringent policies exist for evolving any integrated procedures for data infusion. This will result in inconsistent logic in algorithms, which eventually forms the backbone of any AI-based systems. Also, the rapid changes in Tactics, Techniques and Procedures (TTPs) of the Armed Forces is a major aspect that needs to be kept in mind to avoid incorrect decision making by AI systems.

Foreign Acquisition The acquisition process for any AI-related project will include the sharing of database and TTPs, which will have security related issues. Dummy data will have impact accuracy of AI solutions. Moreover, present acquisition processes are not agile enough for fast-paced development in AI.

Hardware and Microelectronics The power of AI comes from the hardware and the microelectronics chips being used in it. Thus, we need to fabricate microchips to ensure secure and cost-effective AI-based systems that will shape the future battlefield.

Strategy for Evolving AI based Defence Capabilities for the Indian Army

AI is a technology that will provide the Indian Army with greater advantages than any other technology. Other technologies such as big data, cryptography, and cyber aspects can also be proliferated to the next level using AI. However, to fully exploit AI, there is a requirement to go ahead with certain requirements shown in Figure 2 that will come a long way in the future. Some of them are highlighted in the succeeding paragraphs.

- **Data Storage** AI data storage and its scaling is one of the biggest contemplations as the volume of data for AI keeps on growing. As organisations concoct AI stratagems and build the essential structure, storage must be of the utmost precedence. Storage will include ensuring the appropriate storage capacity and consistency to deal with the enormous data required for AI. Typically, the storage may depend on factors which include the level of AI, real-time decisions, and the source of data. As databases cultivate with time, organisations need to monitor capacity and plan for expansion as needed. Moreover, for military data, this data needs to be secured to prevent any misuse.

- **Data Availability and Integrity** AI algorithms need to be trained on large datasets. If a technologically capable adversary is aware of the dataset used by AI, they will have an advantage in deciphering ways to defeat it. In case the enemy inserts false data into our systems, the AI will learn the untrue version of reality that the adversary desires. Under these circumstances, it will be very dangerous, especially because the victim will not realise that their own AI dataset is incorrect and may continue trusting the incorrect results. Moreover, the availability of data for training the AI-based tactical operations is also questionable.

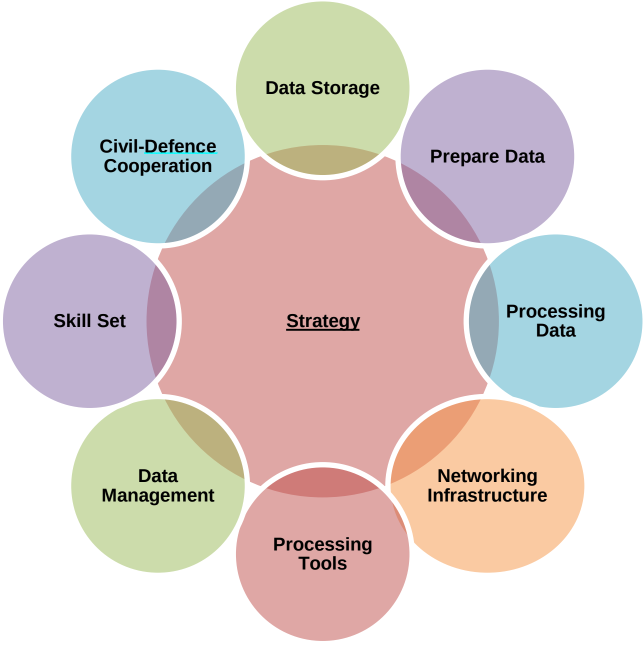


Figure 2: Strategy for Evolving AI based Defence Capabilities

- **Networking infrastructure** One of the key components of the AI infrastructure is its networking infrastructure. AI learning algorithms are highly dependent on communications and enterprise networks will be essential to keep pace with the demand as AI efforts expand. AI systems will require high-bandwidth and creative architectures. The Network for Spectrum can be a stepping stone towards the primary needs for AI networking infrastructure.

- **Processing and Preparing AI Data** Not only is there a need to plan storage, movement and processing of data for AI, but we need to choose how to prepare the data for use in AI applications. This is one of the critical steps for cleansing the AI data and is sometimes also called data scrubbing. This process includes updating or removing data from a database that is inaccurate, incomplete, improperly formatted or duplicated. Thus, adequate infrastructure in terms of manpower, hardware and tools must be procured for preparing the AI data.

- **Data Management and Governance** Another important factor is data access. An organisation must have proper mechanisms in place to deliver data in a secure and efficient manner to the required users. A data management strategy is needed to ensure that human users and machines have easy and fast access to data via wireless networks. Access also raises several privacy and security issues, so data access controls are important. We need to look at technologies such as identity and access management and data encryption tools as part of data management and governance strategies.

- **Skillset** Training and skills development are vital for any endeavour. AI will need data analysts, data scientists, developers, cyber security experts, network engineers, and IT professionals with a variety of skills to build and maintain their infrastructure to support and use AI technologies.

- **Civil Military Fusion** There is a need to synergise efforts towards understanding, finding, and implementing AI-based technology by major players in defence, academia, and civil industry. There is also a requirement for laying down an adaptive roadmap with priorities to ensure the best future technologies are incorporated into the armed forces.

- **Timelines** The above-mentioned capabilities will take time to develop as they require changes in policy and decision-making. Thus, there is a requirement to prioritise a clear roadmap defining the goals required to be achieved in the future. Various goals to be achieved may be divided into short-term, medium-term, and long-term solutions as given under Figure 3.

  ➢ **Short Term (2022-2025)**

  ❖ Awareness at the technical level.

  ❖ Reduction of payload carrying capacity.

  ❖ Introduce soldier borne sensors.

  ❖ Autonomous robots for route clearance and Improvised Explosive Device clearance.

  ❖ Start maturing policy & improve data storage.

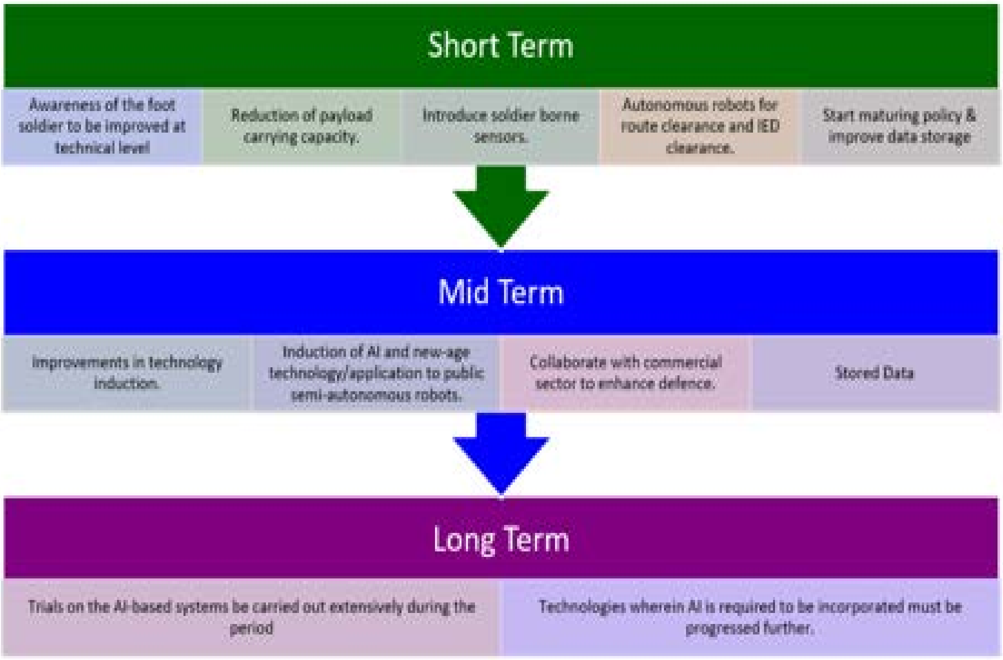

Short Term
Awareness of the foot soldier to be improved at technical level
Reduction of payload carrying capacity.
Introduce soldier borne sensors.
Autonomous robots for route clearance and IED clearance.
Start maturing policy & improve data storage
Mid Term
Improvements in technology induction.
Induction of AI and new-age technology/application to public semi-autonomous robots.
Collaborate with commercial sector to enhance defence.
Stored Data
Long Term
Trials on the AI-based systems be carried out extensively during the period
Technologies wherein AI is required to be incorporated must be progressed further.

Figure 3: Timelines and Goals for AI in Indian Armed Forces.

➢ **Mid Term (2025-2030)**

❖ Improvements in technology induction.

❖ Induction of AI and new-age technology/applications for semi-autonomous robots.

❖ Collaboration with commercial sector.

➢ **Long Term (2030 and beyond)** The research facilities, data and the lessons learnt would have matured, thus trials on the AI-based systems could be carried out extensively and AI technologies progressed further.

Conclusion

The Indian Army is converging towards IBG-isation as one of the responses to the progressive changing dynamics of war. The creation of these forces and tailor-made structures is a right step towards achieving the military and operational objectives of the nation. As we progress towards learning, weighing and comparing the pros and cons of employment of AI-based systems in the Indian Armed Forces, the AI market for India in the civil domain is rapidly rising. As an example, India was ranked third in the G20 countries for AI-based start-ups.

The Indian defence forces should realise the dual nature of AI and make necessary amendments in the policies to enhance the participation of AI-based start-ups in defence.

Bibliography

1. *Artificial Intelligence: Autonomous Technology (AT), Lethal Autonomous Weapons Systems (LAWS) and Peace Time threats By Regina Surber, Scientific Advisor, ICT4Peace Foundation and the Zurich Hub for Ethics and Technology Pp 5.*

2. *Hoadley D,Lucas N, Artificial Intelligence and National Security, April 2018.*

3. *https:// www. c4isrnet.com/ ome/ 2017/ 09/ 07/army – logistics – integrating – new – ai - cloud-capabilities/.*

4. *https://www.drdo.gov.in/sites/default/files/drdo-news-documents/NPC_10-12_April_2021_ 0. pdf.*

5. *H Michael, Artificial Intelligence, International Competition, and the Balance of Power, Texas National Security Review: Volume 1, Issue 3 (May 2018).*

6. *T Chand, AI and its applications for defence and security forces, Synodos Paper Vol - XII NO-7/Jun 2018.*

7. *The Global Race for Artificial Intelligence: Weighing Benefits and Risks, IDSA Issue Brief, 23 Feb 2018 by Munish Sharma.*

8. *Discussion Paper NITI Aayog National Strategy for Artificial Intelligence June 2018.*

9. *Report of The Artificial Intelligence Task Force, Ministry of Commerce and Industry (Govt of India).*

10. *https:// www. c4isrnet. com/ ome/ 2017/ 09/ 07/army – logistics – integrating – new – ai - cloud-capabilities/.*

11. *T Chand,AI and its applications for defence and security forces, Synodos Paper Vol - XII NO-7 / JUN 2018, PP 6.*

12. *The Global Race for Artificial Intelligence: Weighing Benefits and Risks, IDSA Issue Brief, by Munish Sharma.*

13. *India and the challenge of autonomous weapons R. Shashank reddy.*

14. *Report of The Artificial Intelligence Task Force, Ministry of Commerce and Industry (Govt of India) Pp 25.*

15. *https://searchenterpriseai.techtarget.com/feature/Designing-and-building-artificialintelligence infra-structure.*

ARTIFICIAL INTELLIGENCE: IMPACT ON WARFIGHTING AND PERSPECTIVE PLANNING

- Colonel Harish Totade

The nation that leads in AI will be 'the ruler of the world

-Vladimir Putin

Introduction

The term "Artificial Intelligence" (AI) generally means that those tasks which humans could do with organic intelligence will be executed by machines, viz., identifying a pattern, learning by repetition, making a conclusion, or acting in a particular manner.[1] It is about the study of computations that makes it possible to perceive, reason, and act. In addition to hardening the mechanisms to counter threats to important infrastructure like medical assets, power grids, stock markets etc., AI can optimise our combined abilities to identify, respond, and forecast threats from a variety of sources. If we turn to AI, the prevailing definitions typically denote a wide range of capabilities covered by human intelligence that includes these elements. In a military context, the United States Defence Science Board states that AI is "the capability of computer systems to perform tasks that normally require human intelligence." Together, these provide relevant building blocks of a definition of AI.[2]

The rapid development of technology and its spread is altering the character of war and international polity. AI has already permeated a wide range of fields, both civil and military, making inroads and paving the way for transformation. However, AI in isolation is not the key element of change; it's application in the realm of military routine tasks can hasten decisions, regulate speed of operations and someday, may push conflict beyond human cognitive ability.

Specific to the military requirements, the vast applications of AI assure better early warning models for the onset of conflict, enabling decision makers to pre-empt and/or prevent it. It can help save the lives of soldiers through better on-site medical diagnosis. In fact, AI may put fewer soldiers in direct combat by employing unmanned systems. AI applications may automatically repair faults in software-driven weapons in real time, which would otherwise take humans a prolonged period.[3] With maturing technology, AI is already shaping new doctrines and will continue to influence strategy for the future. Conventional weapon systems powered by AI may destabilise strategic assets and the balance of power by making the fog of war denser there by creating confusion or escalation, prompting the start of nuclear confrontation.

Current Capabilities and Trajectory in Future

AI is already a military reality and since it is not one particular application but a whole system, as such, it can be said that the armed forces of the world are seeing it's inroads in some form or the other. For example, weapon-guidance systems can make independent decisions irrespective of human input (barring the setting up parameters before launch) and large datasets can be analysed to identify patterns. Peculiarly, AI systems with networked computers will have autonomous decision-making in a rapid, sequential, and uncertain environment. Intelligent systems adept at drawing inferences on the basis of random data will likely be on the battlefield and learn from previous actions and from those of parallel machines.[4]

At the cutting edge of AI research, there is rapid development in algorithms for self-learning even with limited data coping with vague and nonlinear data. In general, ongoing AI research is focused on areas other than defense, such as civilian vehicle manufacturing, the internet, and healthcare.[5] Overall, the developed capability to categorise asymmetric information and its utility as a decision-making basis have numerous tactical applications. Early studies promise that AI will be employed across the spectrum from tactics to strategy.[6]

It is expected that autonomous systems will be more flexible and deploy optimally than those guided by human decision-making in the near future. Already, AI systems can outshine pilots in simulated air-to-air combat.[7] The scope of AI will additionally be expanded to include administration, human resources (postings and profiling), weapon development, etc. These apparent tactical actions have the potential to collectively transform a nation's strategy. AI presently is narrow in the sense that it can continue in its own field and not expand into other functions on its own.

Inspite of the recent developments, certain thinkers point out to the recurrent cycle of optimistic progress in AI, followed invariably by failure to deliver and a virtual plateau as concepts fail to achieve results in autonomous decision-making[8]. However, the full extent of its influence on reshaping armed forces cannot be predicted with certainty.

Technology and Impact on Strategy

Even though there is considerable development in the field and advent of many promising technologies are envisaged in the near future, there seems to be no clear approach to it in most nations as to where and how it will be implemented in the military. Whether it will be limited to only tactical level applications or be used in a way that doctrines and strategy will have to be re-written is a matter of speculation. The military advantage in AI will go to the nation with the most focused investments and the most comprehensive enabling environment.

Throughout the history of warfare, it has been seen that the advent of new technology has a profound impact on strategy. Character of war was transformed by inventions like gun powder, rifles, tanks, or steam power, but they affected strategy moderately at best. These changes, however, did not affect the primacy of fundamental principles like surprise, concentration of force in space and time, etc.[9] Inspite of the previous technological advancements transforming war and society, they did not change psychology as such, i.e., the primacy of evolved human mind in strategy.[10]

Theoretically, the AI system should differentiate between combatants and civilians based on pre-fed parameters and further choosing to apply lethal force accordingly. However, these systems, like humans, will always have the potential for confusion and error. Due to its speed, precision, accuracy, and unbiased nature, AI is likely to be more favourable for offensive actions. Though the attribute is equally applicable for defence, the balance is shifted by two factors. By definition, offensive acts have the initiative, and enemy infrastructure may be overwhelmed by a mature AI ecosystem. As per Clausewitz, the culminating point in warfare is a psychological factor in defence as well as attack. Humans are risk averse, likely to gamble more when losing and will value in-hand possessions rather than perceived victory.[11]

Transformation of Key Processes

AI systems will optimise core activities such as reconnaissance, manoeuvre, and deceive enemy forces through precise fires and rapid concentration at both tactical and operational levels, increasing lethality and lowering risk on the battlefield. The developed armies will see their military power optimised and enhanced exponentially compared to the rest, way beyond the advancements gained through the information revolution, which will surely change the power balance.[12] They shall have multiple impacts on processes as listed below:-

- AI will reduce the risks, especially because own casualties will be lower, and thus lower the threshold for countries that would otherwise avoid conflict. The risk-averse state may now find it affordable to wage war due to perceived affordability. Contrarily, AI may negate aggression by a rogue nation seeking easy gains that are no longer below the interventional threshold.[13]

- AI shall shape military actions holistically instead of distinguishing between conventional and grey zone warfare. The thoughts and methods for distinguishing the two and exercising restraint need greater deliberation and definition right from the inception stage.

- Accuracy in decision-making and prognosis of battle scenarios can be corroborated by AI-enabled war-gaming and advanced simulations.

Additionally, deterrence capability can be furthered by autonomous platforms and hypersonic smart missiles.[14]

- When exploited, AI can filter clutter from large unorganised datasets and derive actionable intelligence, which may prove mission critical to the commanders on the ground.[15]

- The enemy's Air Defence may be overwhelmed by smart drones, thereby increasing the effectiveness of own air interdiction operations, amphibious ground assaults, long-range vectors, and maritime operations in degraded, contested, and denied environments.[16]

- The employment of AI in military is not devoid of its challenges. To be reliable, the systems need to be trained on large datasets.[17] It may predictably overrate the existing threat, transforming the nature and contours of the situation.[18] Such vulnerabilities would derive mostly from the risk posed by the enemy employing means to deceive, disrupt, or impair Command and Control (C2) systems[19] and hence bring out the need for inbuilt security.

- Based on the various scenarios and likely future military application, a brief summary was put up by Niklas Mashur which analyses the advantages and likely disadvantages of AI.[20]

Factors	Benefits and Potential Advantages	Disadvantages and Risks
Strategic Decision making	• More precise, faster situation assessments and analysis. • Offsetting emotions and prejudices. • Rational behaviour in crisis situations.	• Low crisis stability due to acceleration of decisions. • Prejudices can be inherent in algorithms. • Problems regarding the balance of power within states, for example between the military and the civilian leadership.
Training and Organization of Armed Forces	• Personalized training, fair assessments and promotions. • More realistic exercises, manoeuvres and simulations. • Credible simulations of future technologies and their applications.	• Overestimation of AI-generated results. • Cultural and personnel problems due to incompatibility between military culture and values held by specialized personnel. • Military cast system due to higher technical specialization
Military Operations	• More efficient processing of data from different sources. • Reduction of administrative and staff work through forward-looking logistics. • Reduced risks for troops through autonomous logistics. • Improvement of support and reconnaissance systems.	• Potential dependencies that cannot be replaced in the field. • Risks in supply chains due to lack of inventories and reserves. • Unclear whether autonomous vehicles can be used in complex scenarios. • Reduction of strategic stability.

Advantages and Disadvantages of AI in the Military Field

In other words, AI provides the potential to employ systems lethally, unconventionally, and asymmetrically without responsibility, given the absence of firm international law and ambiguous rules of engagement. Robotic systems when deployed with Electro Magnetic (EM) jammers can cloud jammers, confuse enemy Command, Control, and Communication (C3) systems, penetrate hostile systems, as well as provide layered defence. The doctrines and concepts are likely to undergo changes consequent to the speed and nature of war due to the presence of weapons like autonomous robots.[21]

Roadmap and Implementation

There is a definite requirement in the Indian context to first accept the requirement of AI in Armed Forces. As per the NITI Aayog Discussion Paper 2018, the applications of AI in India have referenced utilisation in various sectors but makes no mention of military applications. However, the current confrontation with China raises concern and necessity to match research and development (R&D) for use of AI in the Armed Forces. Simple changes in the present organisation and planning may be needed, which shall entail:-

- A broad thought on the possible usage and formulation of a tri services doctrine. The fact that AI is needed in the armed forces needs acceptance at the highest levels including policy makers.

- Leadership at the strategic level, which appreciates the potential of AI needs to create policy, allocate resources and ensure charting of a roadmap. Ultimately, AI technology needs to be involved into products and processes to solve challenges in the battlefield. This shall also entail training and adaptations in Tactics, Training and Practises.

- AI advancements will initially occur in bits and processes will eventually merge to form a system. Hence, the need to have in place scaling at all levels and intra organisational transparency will be a prerequisite. This will require creation of a common platform for shared data, reusable tools, frameworks, software standards, cloud and edge services.[22]

- Developing AI into products and process would require employing a pool of best talent available in the country, not only to harness the existing systems but also to develop them with the contemporary changes in the field as well as the changing strategy and operational construct. This will necessitate the involvement of leading organisations such as the Centre for Artificial Intelligence and Robotics (CAIR), National Association of Software and Service Companies (NASSCOM), Army Design Bureau (ADB), Simulator Development Division (SDD), and others, as well as internal oversight for ethical application, particularly in weapon-related infrastructure.

- Establishment of a focal point to handle all AI-related issues, as well as a link between the doctrinal approach, development, current strategy, and most importantly, implementation and integration at all levels[23], with a feedback mechanism for continuous updating and refinement.

- Priority in fielding AI systems, firstly those systems that enhance the capabilities of humans by replacing strenuous cognitive or physical tasks in the Indian Armed Forces context and introducing new ways of working. This requires multi-disciplinary technological development in an iterative way closely associated with all users.[24]

- Forming partnerships in both academic and innovative fields is another key aspect. The leading think tanks in AI and strategic study organisations need parallel studies to entice new talents in both fields to match the technology to tactics and vice versa.

- Development in present war-gaming modules and test them in real situations in parallel to assess their potential for offering advice/planning susequent or immediate actions/relocating resources/ change in logistics/ predicting enemy actions etc. Development of virtual reality applications that would reduce the cost of peacetime training while increasing its realism and facilitating integration.[25]

- Bringing together all present cyber organisations to focus on the applications of AI in a phased manner with definite timelines of development. Concurrently, the technological threshold of rank and file needs upgradation with careful planning.

- Technology, being fast paced, will need constant upgrades in hardware as well as software. This has to be addressed in the procurement model and paced accordingly. The hurdles due to the prolonged loop at grassroot level have to be mitigated.

Ethical Concerns and Security

The quantum of research in AI technology is nearly similar in volume to that of its ethical concerns and has centred broadly on the issues of control and accountability.[26] This compounds the problems of system management, technical expertise integration, and requirement of black or white language demarcating ethics of AI. In this context, AI systems will inevitably reduce boots on the ground (though extremely unlikely in the Indian context given the border issues with both neighbours) and change channels of command. New relationships between a society in general and its army will likely emerge.[27] In any event, it is commonly agreed, ethically and politically that man has to be in the decision-making loop and be the executive authority in any event. Robert Work, the US Deputy Secretary of Defence stated in 2016 that the US Department of Defence (DoD) ‘will not delegate lethal authority to a machine to make a decision' in the use of force.[28] The most often repeated question which remains unanswered is that of accountability in case of a mistake by the machine leading to fatal errors.

Though it is certain that the majority of the algorithms and software on which AI runs are dual use, with both military and civil contexts, with codes and machines potentially replicated and commercially used in all fields. Therefore, once a specific AI application is working, it will be comparatively easy and cheap to produce similar systems as opposed to the cost of traditional military hardware, which is inherently expensive.[29] There are significant implications for the question of how production, proliferation, and the use of a wide variety of AI applications can be controlled by states. Hence, AI is multi-purpose, multifaceted, not necessarily easily controllable and is likely to have both long-term and short-term effects that are respectively disruptive and incremental in nature.[30]

The inclusion of AI in existing military capability can upset the military balance of power by making traditional systems and doctrines obsolete. The political costs of going to war are likely to be lower if fewer humans are sent to the front, thereby reducing an important constraint to going to war. However, immature AI applications rushed into military platforms can lead to spiral dynamics if they perform wrong actions due to battlefield environment, similar to problems in financial trading.[31] The study conducted by Research and Development (RAND) Corporation regarding risks and concerns related to AI in military lists certain factors repetitively and they are illustrated below in Figure 1.

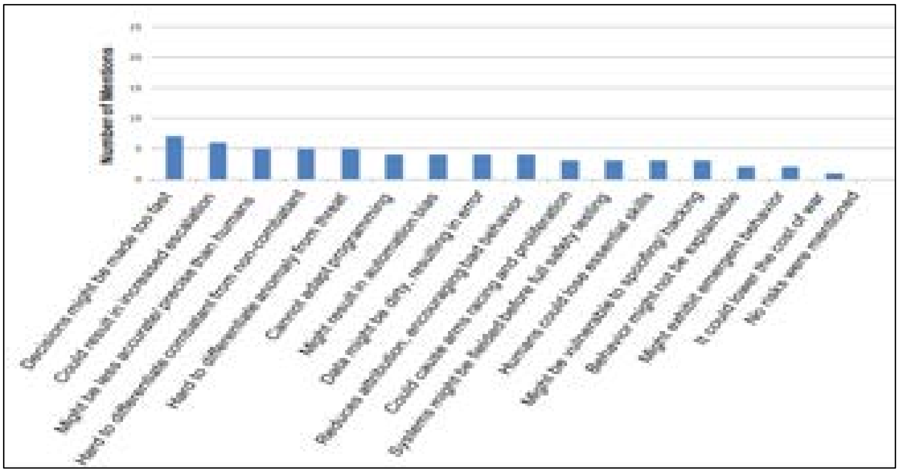


Figure 1

Conclusion

Hitherto, the introduction of AI into military systems is limited. Yet, irrespective of the timescale, an adaptive AI for decision-making matters does presage a prominent shift in strategy that may be more radical in nature as compared to the nuclear revolution.[32] As compared to humans, the AI scores majorly in being non-susceptible due to its great speed and accuracy in processing information. Concurrently, the AI will continuously enhance all tasks by being devoid of human cognitive tendencies.[33]

History bears testimony that any technological advantage means little unless war fighters complement the technology with a comprehensive enabling environment. The British first invented the tank and led the development of the technology, however, the Germans developed training, doctrine, concept of operations and organisational structure to use tanks effectively, resulting in German tank battalions regularly outmanoeuvring allied forces in the early years of World War II. As AI transforms military warfare, the advantage will go to the nation with the most strategically focused investments *and* most inclusive and comprehensive environment.

By accelerating decision-making, shortening the Observe, Orient, Decide and Act (OODA) loop and optimising Command, Control, Communication, Computer, Information, Surveillance, and Reconnaissance (C4ISR) capability, AI can provide a cutting edge to the armed forces. However, until solving the mystery of unpredictability, inflexibility, and brittleness in nature of AI, this phenomenon will continue to "outpace strategy and human error'.[34] Transparency in these decisions is extremely useful as a confidence and security building measure.[35] Until there is a doctrinal and focused thought with specific time-bound goals that are neatly implemented, the gap between what could have been possible and what is available will continue to grow.

Bibliography

1. *Summary of the 2018 Department of Defense Artificial Intelligence Strategy, Harnessing AI to Advance Our Security and Prosperity.*

2. *Artificial Intelligence and Its Future Impact on Security. Testimony prepared by Dr. Tim Sweijs for The Committee on Foreign Affairs and the subcommittee on Security and Defense of the European Parliament. Bruxelles, ro October 2018.*

3. *Ibid.*

4. *Sergey Levine, Timothy Lillicrap and Mrinal Kalakrishnan, 'How Robots Can Acquire New Skills from Their Shared Experience', Google Research Blog, 10 March 2016, ttps://research.googleblog.com/2016/10/how-robotscan-acquire-new-skills-from.html.*

5. *Kenneth Payne. Op cit pp 14.*

6. *Kareem Ayoub and Kenneth Payne, 'Strategy in the Age of Artificial Intelligence', Journal of Strategic Studies, vol. 39, nos 5–6, 2016, pp. 793–819, https://doi.org/10.1080/01402390.2015. 1088838. See also Michael Horowitz, 'Artificial Intelligence, International Competition and the Balance of Power', Texas National Security Review, 15 May 2018, https://tnsr.org/2018/05/artificial-intelligenceinternational-competition-and-thebalance-of-power/; and Paul Scharre, Army of None: Autonomous Weapons and the Future of War (New York: W.W. Norton, 2018).*

7. Nicholas Ernest et al., ‘Genetic Fuzzy Based Artificial Intelligence for Unmanned Combat Aerial Vehicle Control in Simulated Air Combat Missions’, Journal of Defense Management, vol. 6, no. 1, 2016, https://doi.org/10.4172/2167-0374.1000144.

8. Payne loc cit.

9. See Beatrice Heuser, The Evolution of Strategy: Thinking War from Antiquity to the Present (Cambridge: Cambridge University Press, 2010).

10. Payne op cit pp 4.

11. Kenneth Payne, ‘Prospect Theory and the Defence in Clausewitz’s “On War”’, paper presented to the annual meeting of the International Studies Association, Atlanta, GA, 16March 2016, http://web.isanet.org/ Web/Conferences/Atlanta%202016/ Archive/968b741d-130c-4912-a4ee-997345a57ce1.pdf.

12. Ibid.

13. Ibid.

14. Linda Lastovych. Op cit pp 5.

15. James s. Johnson. Op cit pp.

16. Linda Lastovych op cit pp 6.

17. Michael C Horowitz and Paul Scharre, ‘AI in international Stability: Risk and Confidence Building Measure (Centre for New American Security 2021) pp5.

18. James s. Johnson, ‘Artificial Intelligence and Future Warfare: Implications for international Security (2019) pp 35 Defence & Security analysis pp147.

19. Mark Fitzpatrick, ‘Artificial Intelligence and Nuclear Command & Control 2019 pp 61.

20. Niklas Mashur. AI in military Enabling Applications. CSS Analyses in Security police no 251 Oct 2019 pp 3.

21. Ibid.

22. Summary of the 2018 Department of Defense Artificial Intelligence Strategy op cit pp.

23. The US DoD has already established a Joint Artificial Intelligence Center (JAIC) to accelerate the delivery of AI-enabled capabilities, scale the Department-wide impact of AI, and synchronize DoD AI activities to expand Joint Force advantages.

24. Ibid.

25. Atul Pant, Artificial Intelligence The Visible Path, IDSA Occasional paper. No 49, Aug 2018.

26. Ugo Pagallo, ‘Robots of Just War:A Legal Perspective’, Philosophy &Technology, vol. 24, no. 3, September 2011, pp. 307–23, https://doi.

27. Ibid.

28. Linda Lastovych op cit pp 6.

29. *Dr. Tim Sweijs. Op cit pp 5.*

30. *Ibid.*

31. *Ibid.*

32. *Ibid.*

33. *Payne op cit pp 22.*

34. *James s. Johnson. Op cit pp.*

35. *Draft Guidelines on Developing National Defense Policy And Doctrine Papers ("White Papers") (Approved by the Committee on Hemispheric Security at its meeting held on October 22, 2002).*

ARTIFICIAL INTELLIGENCE IN CYBER SPACE: TOWARDS MODERN WARFARE

- Miss Khyati Singh

Introduction

The AI currently available to us is called ‘Narrow AI’, and its evolution would lead us to ‘General AI’, which has the power to revolutionize military operations. However, the presently available AI is more evolutionary than revolutionary which facilitates decision making. Currently, AI is being developed, and used in cyberspace & military operations in all three domains - air, water and land, and for strategic placement of weapons which also involves decision-making. Despite the multifaceted use, the strategic planning in and around AI has been obscure and lacks quality R&D. A repetitive mistake has been labeling slight technological modifications as AI. This has created an environment of misinformation where basic coding and system advancement is dubbed as “AI”. Consequently, it broadens the bracket of AI without any depth, and keeps the human resource involved in petty technological projects. The core aspect of AI being a ‘replica of human mind’ has been relegated to the sidelines. The sole fact that makes AI ‘revolutionary’ is that it aims to ‘replicate human brain’. The cognitive skills are what puts it apart from every technological ace the world has developed till date. As scholars worry about and populate the existing literature on a possible ‘AI arms race’, they miss out on the basic questions of AI, and its implication. Narrow AI, is comparatively less complex, and has fair share of technological limitations along with the constraint to undertake multitasking. However, General AI would fix these challenges as it will be organized along more complex structures that will be of great advantage to military operations and intelligence. For instance, Harpy drone is being used by Israel to counter enemy operations, Governments are utilizing AI to extract big data for counterterrorism, while the New Zealand Navy is using it for logistics. China too has worked on drone swarm technology that is beneficial in bypassing the enemy defense base.[1]

Weaponization of AI in Cyberspace

The speculation of AI being weaponized and causing drastic changes has become a reality of late. Weaponization altered conventional warfare weapons used in the air, sea, land, and space. Moreover, this weaponization of nuclear and chemical materials has been linked to space usage and climate manipulation. The presence of weaponized AI in cyberspace is alarming. It corrupts the system and adds malicious data that can be used to hinder its smooth functioning and send across rigged messages. Weaponzied AI has been defined as *“Malicious AI algorithms that can degrade the performance and disrupt the normal functions of benign AI algorithms, while providing technological edge attack scenarios in both cyberspace and physical spaces.”*[2]

Cyberspace operates on data, and with its exponential growth, the data it works upon will also increase. This will make it next to impossible to keep it in check through a human agency alone. This is where the element of AI comes in. AI helps in assuring the security of cyberspace along with managing the enormous data. However, tampering with the hardware and software can be extremely dangerous. For instance, autonomous systems based on AI models can be used to disguise or divert people. Researchers at UC Berkeley firm developed a model based on this feedback. They devised a false stop sign for the autonomous driver, which confused fellow drivers and almost caused a road accident. Inducting this prototype into the military can be worrisome. Enemies can hack into the systems of army vehicles and alter the settings.

Weaponized AI cyberspace can either be directly integrated into battles or be inducted into military operations that deal with computing, data analysis, systems operation, decision making, etc. The latter aspect is more prevalent given the current scenario since it involves real-time decision making, maintenance of prominent supply chains and doing jobs that humans refrain from doing. All these factors together affect the power dynamics of conventional warfare. The power of "big data analysis" is crucial to any operation. This big data is referred to as ‘mass’, and the bigger the 'mass', the better performance AI has. Another aspect that is often considered easy with AI is decision making. However, the present-day AI does not afford that comfort. Human agency is integral to the process. The aim of AI remains to replicate human brains with the same cognitive capabilities, but that is a far-flung goal. Present day reality requires human intervention because machines do not understand the human codes of morals and rationality. Their algorithms work on a designated pattern. Hence, when it comes to cyberspace, human agency has to be given more attention and the required edge.

Conventional vs Modern Cyberattacks

Conventional cyber-attacks are devoid of AI, whereas the modern cyber-attacks are backed with AI. The conventional methods, or the most common ones are Distributed Denial of Service attacks (DDoS), Denial of Service attacks (DoS), Phishing, Man in the Middle (MitM) attacks, injections of Structured Query Language (SQLI) and Cross-site Scripting (XXS), Malware attacks, Ransomware attacks, Eavesdropping attacks, Scarce attacks, etc.[3] A variety of these are also being used in the Ukraine-Russia war. However, they did not qualify as AI powered attack. AI powered attacks include data misclassification, data analysis and synthetic data generation. The technology deployed to tweak these factors can be applied to various other warfares.

Trail of events for AI development

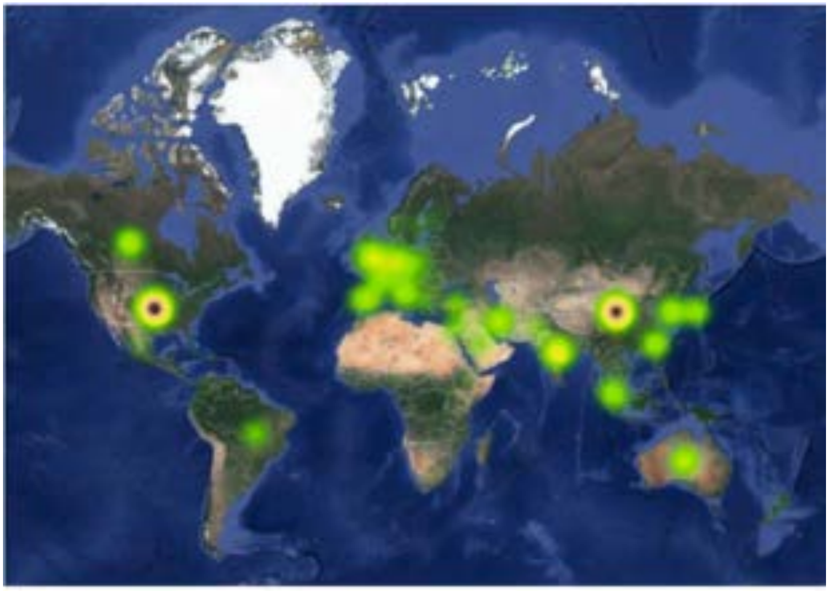
AI advancements are not new and have been in the works since the 1950s, However, the current rate of progress is unprecedented. The Defence Advanced Research Projects Agency (DARPA) [4] led the research in AI and paved the way for nuclear powered AI supersonic jets. Likewise, the induction of AI into cyberspace is in the pipeline and just one step away from the breakthrough that everyone looks forward to. It was with the development of AI in the military with projects like the "Survival Adaptive Planning Experiment" that was tested for AI decision making. It was concluded that though AI decision making will become feasible with time, the real challenge will arise when the power of decision-making rests both with humans and AI[5]. It might create a conflict that either collides or diffuses the actions. Moreover, the lack of an accepted definition for addressing what "autonomous" means has been a cause of concern. Initially, the autonomous tag meant little human intervention, but gradually, as the advancements in AI are taking place, it is being envisioned as something that has no human variable to it.

In addition, the other issue that encircles the development of AI is that of ownership and creation. It was the private sector that led the development of AI and not the government. Private firms have a model that is at ease compared to the government, which falls prey to regulations and turf battles, along with the money that goes into these developments. Private agencies could produce the same or better results in little time as compared to government agencies. This regulation-free operation makes it easy for the private sector to produce and sell the technology, which might end up with either a rogue state or a terrorist organization.

Even as the trend towards exploitation of AI for military purposes cannot be rendered, there is a need to manage it effectively. It has already penetrated various domains of operations, and it now focuses on cyberspace. Most AI-powered attacks in cyberspace take place by inducing noise in machine learning algorithms that pave the way for adversarial machine learning. It corrupts the network and creates a ruckus. This can be defended by modifying the neural network that has additional classifiers along with the data that constitutes the defensive domain. [6]

Mr Vasisht Duddu, a researcher from the Indraprastha Institute of technology[7] undertook a survey in 2018 that studied adversarial machine learning in cyber warfare. He identified a series of threat models and defensive strategies. The adversarial machine learning attacks included model inversion attacks, equation solving attacks, path finding attacks, evasion attacks, member inference attacks, transferability attacks, and black box attacks. Furthermore, he pinpointed the vulnerabilities in machine learning algorithms, encompassing supervised, unsupervised, and reinforcement learning algorithms. The defence mechanisms available for these attacks were privacy-preserving algorithms and processing techniques that safeguard machine learning-based algorithms.

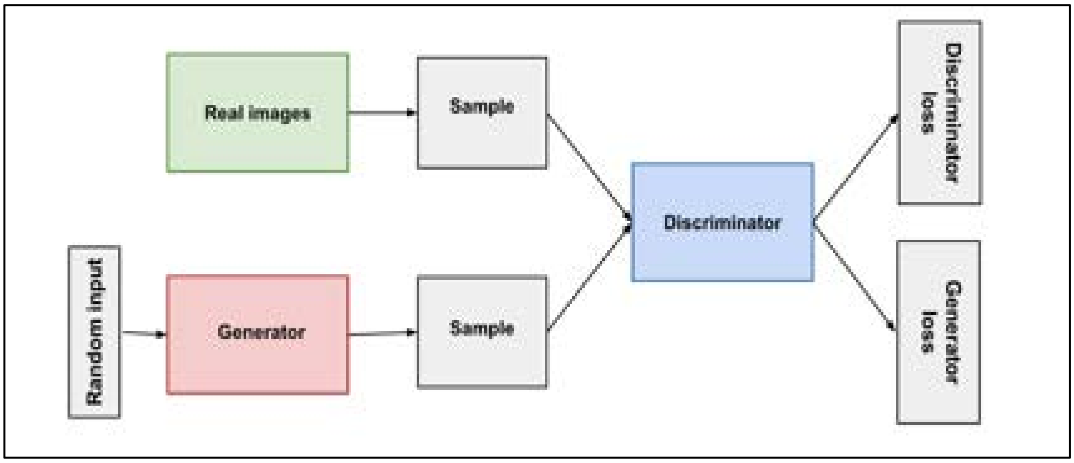
Mr Naveed[8] also conducted a survey in September 2019 that charts the countries that are leading the AI battle in cyberspace. China topped the list followed by Iran, Singapore, the US and India. However, majority of the research that these countries and their universities were doing aimed at data mining[9], network traffic classification[10], fraud detection[11], adversarial machine learning[12], and anomaly detection[13]. The following figure[14] shows what has been dubbed "AI hotspots". These are the countries that are leading the research on AI in cyberspace.



Researchers came across **Generative Adversarial Network (GAN)**[15] that proved to be a breakthrough in deep learning. GAN along with its medical imaging applications, works like a neural network model where two networks are trained at the same point of time. One of it focuses on image generation while the other on discrimination. For AI powered cyber- attacks, GAN is of immense importance. The main function of GAN falls under data generation in terms of visual, textual, and audio content. The range of applications include audio synthesis, super resolution, text mining, drug discovery, video in painting, synthesizing data for training which can be used for further training deep networks.

GAN has two prominent agents, namely, ***generator and discriminator***. Both of them are deep networks but have different loss functions. The generator network first learns the dissemination of data and then produces samples for the discriminator network. Further, the discriminator is given two kinds of samples: one that comes from the generator and the other that is the original data. Therefore, it is the job of the discriminator network to identify whether the generator sample has been sourced from the original network or from the generator network. The training is devised to train the generator to trick the discriminator by replicating original samples, while the discriminator is trained to identify the original sample. This is an end-to-end training network that ends when it acquires ***Nash equilibrium***[16]. In the context of networks, this equilibrium works when the loss of the generator, that is, the number of times it failed to trick the discriminator, is equal to the loss function of the discriminator, that is, lack of discrimination between the two samples.

However, reaching such an equilibrium is a tall order since the loss functions oscillate. The following picture[17] is a pictorial representation of the GAN diagram.



AI Induced Cyberattacks

Research has tried to identify machine learning strategies' relationships with cybersecurity strategy and functioning. Machine learning relies on algorithms that work on the feedback gained from previous experiences to comprehend repeating patterns in place of programming the patterns themselves. Machine learning helps find solutions to the same problems. [18]. Two types of algorithms that can be deployed in machine learning are ***supervised and non-supervised algorithms***.

To solve the issue of cybersecurity, military bases can deploy these methods of machine learning. Militaries can induct regression, classifications, generative models, clustering, and association rule learning. By applying regression in cybersecurity defensive measures, fraud or detection of any suspicious activity can be outlined. Classification helps in organising or categorising data based on the training that is being provided that contains a category for known membership observations. Whereas clustering is a tool of unsupervised learning using which data points can be employed or populations can be grouped. Meanwhile, generative models stimulate real data by devising a model that creates a list of information parameters that evaluate specific applications for injected vulnerabilities.

Machine learning also plays it's part both as an offensive and defensive actor. On the offensive end, cyber security tools like spearfishing, evasive malware and botnets can be used. While on the defensive front, machine learning tools like malware detection is being used. The hacker needs to crack the code just one time, and that one single access can help in corrupting the entire system. Military intelligence needs to be on their toes 24x7 and must work with 100% accuracy to block these attacks. To facilitate this, machine learning can imitate human behavior and prepare a database that gives out possible services based on the set of behavior. This can even help in preventing attacks that have not yet taken place. However, leakage of data is very much a possibility in machine learning systems. Big companies like Google and Amazon have had such experiences. A shadow training technique has been devised to resolve this issue. This helps in filtering the actual data from nosy interference data.

AI powered tools which deploy data analysis for offensive operations in cyberspace are numerous. The most common ones are DeepHack[19]- a tool that creates injection attack patterns that can be applied to database, DeepLocker[20]- emulates an Advanced Persistent Threat (APT) to facilitate the launch of complex cyber-attacks, GyoiThon[21]- which is used for gathering information and automatic exploitation, EagleEye[22]- uses facial recognition algorithms for information reconnaissance for social media, uriDeep[23]- generates domain names that are fake but can be used in various attack scenarios and works as a proxy, Deep Exploit[24]- automates Metasploit for gathering information, exploitation and post exploitation, and Deep Generator- which works for web applications by producing injection attack patterns. These tools that are completely AI driven can help counter the hackers that feed false information into the machine learning models, or at times evade detection using technology codes that crack through the systems. To keep pace with such nefarious activities, deployment of AI tools in military cybersecurity space is extremely crucial.

On the audio front, deep fakes are increasingly becoming an attack force to reckon with. An attacker no longer needs a voice actor or performer to mimic or copy the desirable voice. Deep Fake generates the exact voice that can be used to give commands. In warfare, or in military operations in general, orders come via various audio devices owing to the different locations of operations. Under this scenario, fake voices imitating the actual person in charge can cause confusion throughout the entire operation. These kind of fake audio-induced attacks are known as 'vishing'[25].

Future Course of Actions

In cyberspace, it is an open war of AI vs AI. It would either end in a draw or might end up favouring the one with greater might. Offensive AI in cyberspace looks for the loopholes and penetrates vulnerabilities to cause harm. At the defensive level, the proposed AI would figure out these loopholes to cover up vulnerabilities and keep them from further damage. This, in the sense, is also a question of timely interjection. For instance, the Defence Advanced Research Projects Agency (DARPA) cyber grand challenges[26] make AI-based cyber defenders and attackers compete. This helps the government track the possible threats and their feasible solutions. The Indian military can too adopt such innovative methods that help in strengthening their systems. Likewise, in adversarial machine learning, GAN can be used both in defense and offense. The biggest challenge that AI faces is the acquisition of required data that facilitates the creation of accurate models. This the military can resolve by expanding their resource base and incorporating more data analysis tools. Furthermore, with the introduction of new and advanced technologies like 5G/6G, better infrastructure will be required.[27]

Another set of security systems that can help counter security breaches in cyberspace are: **signature-based,** which try to map out all the cyber-attacks with those attacks' specific signature or pattern; **anomaly-based**, which keep track of regular machine behaviour and raises an alarm if there is any deviation from the normal sense; **hybrid based,** is a combination of the previous two, that is, anomaly and signature. It keeps an account of the intrusion rate and thereafter tries to bring down the range of unknown attacks.[28]

Cyber attackers often exploit the overfitting attribute of GAN where the algorithms learn the distribution of the training data accurately; however on the validation set they lack precision. This overfitting is easier to deal with in the case of convolutional neural networks, Boltzmann machines and auto encoders, but when GANs are involved, it becomes rather challenging. Hackers exploit this aspect to produce data to foul the networks. The way to deal with such a threat is through 'network regularization' which aims at developing sophisticated regularisation. Moreover, a generalised model can be more helpful in mitigating these odds.

It is also important to secure AI classification models that are generally exposed to 'Evasion', 'Poisoning' and 'Stealing'. In 'Evasion', the data that works as an input for the AI algorithm is manipulated; this allows it to bypass the classification mechanism. Likewise, in 'Poisoning', the training data is tampered with to affect the classification pattern. Lastly, in 'Stealing', the input and output analysed by the AI algorithm are accessed to understand the model properties and then create a model that counters those safeguards. Deep-pawn[29] is one such system that was developed in 2016 and can be deployed to tackle the aforementioned attacks.

These attacks can be on multiple levels, but the military of any country, for example, needs to recruit AI measures for cyber defence. These include anti-phishing measures[30], kill chains, attack visualization, etc. Phishing is the most prevalent method of stealing data using the internet. Military operations rely on information, and during wartime, any information leakage proves to be detrimental to the entire operation. This needs to be tackled at all levels. Researchers have tried to develop machine learning algorithms that train the model to detect phishing attacks. The current AI-based techniques include the Synthetic Minority Over-Sampling Technique (SMOTE) algorithm for detecting phishing. Furthermore, there are attacks that are taking place on the grid systems and essential infrastructure. These are generally controlled by human operators, but has its limitations, and are generally erroneous. It is important to devote resources to the development of effective technologies to counter such attacks. The attacks on cyberspace have started penetrating the system, and with AI, the devastation would be unparalleled.

Conclusion

It was initially just the development of AI that the world was dealing with, but as technology climbed the ladder of development, it got clubbed with cyber space as well. Cyber-attacks are not new to humans. What is new about them is their clubbing with AI. This has unfolded a new dimension, where the attackers are accessing the capabilities faster than the defenders. Moreover, the fact that AI has not been autonomous to the extent it was believed to be, has further made it difficult to define a definite trajectory. Therefore, timely involvement, active measures, and sincere R&D concerning AI in cyber space is the need of the hour. Militaries are primarily trained in conventional warfare. It is crucial to understand that, with the changing dynamics of war, it should be our obvious action to upgrade and update our modes of operation. To provide more cyber training to the personnel, develop systems and machine learning algorithms that could safeguard the system. In a war of AI against AI, only technology will win.

Bibliography

1. *China Releases video of new barrage swarm drone launcher. 2020, https://www.forbes.com/sites/davidhambling/2020/10/14/china-releasesvideo-of-new-barrage-swarm-drone-launcher/#484d44822ad7.*

2. *Weaponized AI for cyber attacks Muhammad Mudassar Yamin a,∗ , Mohib Ullah a , Habib Ullah b , Basel Katt.*

3. *Yamin Muhammd Mudassar, Katt Basel, Kianpour Mazaher. Cyber weapons storage mechanisms. In: International conference on security, privacy and anonymity in computation, communication and storage. Springer; 2019, p. 354–67.*

4. *Defense advanced research projects agency. 2019, https://www.darpa.mil/.*

5. *Geist Edward Moore. It's already too late to stop the AI arms race—We must manage it instead. Bull At Sci 2016;72(5):318–21.*

6. *Li Jian-hua. Cyber security meets artificial intelligence: a survey. Front Inf Technol Electron Eng 2018;19(12):1462–74.*

7. *Duddu Vasisht. A survey of adversarial machine learning in cyber warfare. Def Sci J 2018;68(4):356–66.*

8. *Abbas Naveed Naeem, Ahmed Tanveer, Shah Syed Habib Ullah, Omar Muhammad, Park Han Woo. Investigating the applications of artificial intelligence in cyber security. Scientometrics 2019;1–23.*

9. *Bekerman Dmitri, Shapira Bracha, Rokach Lior, Bar Ariel. Unknown malware detection using network traffic classification. In: 2015 IEEE conference on communications and network security (CNS). IEEE; 2015, p. 134–42.*

10. *Ullah Mohib, Ullah Habib, Khan Sultan Daud, Cheikh Faouzi Alaya. Stacked lstm network for human activity recognition using smartphone data. In: 2019 8th European workshop on visual information processing (EUVIP). IEEE; 2019, p. 175–80.*

11. *Abdallah Aisha, Maarof Mohd Aizaini, Zainal Anazida. Fraud detection system: A survey. J Netw Comput Appl 2016;68:90–113.*

12. *Biggio Battista, Roli Fabio. Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognit 2018;84:317–31.*

13. *Ullah Habib, Altamimi Ahmed B, Uzair Muhammad, Ullah Mohib. Anomalous entities detection and localization in pedestrian flows. Neurocomputing 2018;290:74–86.*

14. *Abbas Naveed Naeem, Ahmed Tanveer, Shah Syed Habib Ullah, Omar Muhammad, Park Han Woo. Investigating the applications of artificial intelligence in cyber security. Scientometrics 2019;1–23.*

15. *Yi Xin, Walia Ekta, Babyn Paul. Generative adversarial network in medical imaging: A review. Med Image Anal 2019;101552.*

16. *Nash John F, et al. Equilibrium points in n-person games. Proc Natl Acad Sci 1950;36(1):48–9.*

17. *https://developers.google.com/machine-learning/gan/gan_structure.*

18. *Chachra Anjali, Sharma Deepak. Applications of machine learning algorithms for countermeasures to cyber attacks. 2019, Available at SSRN 3370181.*

19. *BishopFox/deephack: PoC code from DEF CON 25 presentation. 2020, https: //github.com/BishopFox/deephack.*

20. *CyberWarefare/DeepLocker: DeepLocker - Deep learning based malware. 2020, https:// github.com/Cyber Warefare/DeepLocker.*

21. *Gyoisamurai/GyoiThon: GyoiThon is a growing penetration test tool using Machine Learning. 2020, https://github.com/gyoisamurai/GyoiThon.*

22. *ThoughtfulDev/EagleEye: Stalk your friends. Find their Instagram, FB and Twitter Profiles using Image Recognition and Reverse Image Search. 2020, https://github.com/ ThoughtfulDev/EagleEye.*

23. *Mindcrypt/uriDeep: Unicode encoding attacks with machine learning. 2020, https://github.com/mindcrypt/uriDeep.*

24. *Machine_learning_security/DeepExploit at master. 13o-bbr-bbq/machine_ learning_security. 2020, https://github. com/13o-bbr-bbq/machine_learning_ security/tree/master/DeepExploit.*

25. *Griffin Slade E, Rackley Casey C. Vishing. In: Proceedings of the 5th annual conference on information security curriculum development. ACM; 2008, p. 33–5.*

26. *Avgerinos Thanassis, Brumley David, Davis John, Goulden Ryan, Nighswander Tyler, Robert Alex, et al. The mayhem cyber reasoning system. IEEE Secur Privacy 2018;16(2):52–60.*

27. *Ali Sher, Ahmad Ayaz, Faheem Yasir, Altaf Muhammad, Ullah Habib. Energyefficient RRH-association and resource allocation in D2D enabled multi-tier 5G C-RAN. Telecommun Syst 2019;1–15.*

28. *Yamin Muhammad Mudassar, Katt Basel, Sattar Kashif, Ahmad Maaz Bin. Implementation of insider threat detection system using honeypot based sensors and threat analytics. In: Future of information and communication conference. Springer; 2019, p. 801–29.*

29. *Deep-pwning - Metasploit for Machine Learning. 2020, https://www. kitploit.com/2016/ 11/deep-pwning-metasploit-for-machine.html.*

30. *Sundararajan Aditya, Khan Tanwir, Aburub Haneen, Sarwat Arif I, Rahman Shahinur. A tri-modular human-on-the-loop framework for intelligent smart grid cyber-attack visualization. In: SoutheastCon 2018. IEEE; 2018, p.1–8.*

FUTURE OF ARTIFICIAL INTELLIGENCE APPLICATIONS IN THE INDIAN ARMY COMMUNICATION NETWORK

- Colonel PS Mehta

"Artificial Intelligence is about replacing human decision making with more sophisticated technologies."

- Falguni Desai

Introduction

Artificial Intelligence (AI) was introduced as an academic discipline in 1955 and, since its introduction, has experienced several waves of optimism followed by periods of disappointment. After 'Alpha Go' defeated a professional Go player in 2015, AI once again attracted widespread global attention. AI techniques have now become an essential part of the industry and are being used to extensively solve challenging problems in software engineering, communication technology, and computer science.

AI is being introduced in the defence communication sector in a big way, with the aim of providing new services, improving network efficiency, and enhancing user experience. Some pioneering work has already been carried out in the defence communication field using AI, and its advantages in learning, understanding, and reasoning have been used to develop Software Defined Networks (SDNs) and Network Functions Virtualization (NFV). In addition, Deep Packet Inspection (DPI) and Service-Aware Network technologies are in the process of development.

Inclusion of AI in Army Communication Network

The Army Communication Network has a varied set of needs that include diversity, security, and ruggedisation. With the smart soldier concept being introduced in armed forces across the world, it is all the more necessary to introduce AI in the army communication network. This will assist the soldier in taking timely decisions based on inputs received through communication devices or equipment. The outcome of an operation or battle will depend on the availability of better and more advanced communication equipment, to equip the soldier with all the necessary inputs to take a timely decision to influence the outcome of the battle. In addition, a lot of surveillance and intelligence data is available as inputs to a commander. It is important to sort the data into useful and generic information so that only that information is fed to the commander that is relevant to him, so as to assist him in passing necessary directions timely to his subordinates. Trends in the field of communication, which necessitate the inclusion of AI in the Army Communication Network, are given in the succeeding paragraphs.

- **Characterised Requirements** With the increasing number of users and growing size of the Army Communication Network, differences in preferences, habits, and the informational needs of subscribers are gradually exposed. The demand for customised networks and services is now becoming stronger with the varied requirements of data users. In the near future, there will be complex communication network requirements whose implementation would be unmanageable without an intelligent tool.

- **Multimedia Services** Army users have now also become information producers, as well as information consumers and are producing more and more information. User generated content increases traffic at an unbelievable speed. Under these circumstances, both storage and transmission are great challenges. The inclusion of AI bolsters our ability to handle this challenge in the Army Communication Networks.

- **Precision Management** The various dimensions and granularities in today's wireless traffic models should be considered in the Army Communication Networks. With the development of the technologies of network function virtualization and software-defined networks, the management of the communication network has become more precise. Virtualization is not only at the level of network elements but also at the level of components such as the CPU, memory, ports, bandwidth, etc. AI based technologies will allow operators to setup on-demand networks.

- **Predictable Future** The expansion of data requirements and increasing numbers of end users has ensured that the gap between the peaks and troughs of Army Data Network usage is becoming greater. It is therefore required to predict the future status of Army Data Networks more accurately to satisfy users' demands and improve their experience.

- **Network Performance** The increase in network equipment and user terminals, the expansion of network size, the increase in the number of users, and the complexity of the Army Communication Network have resulted in the network management becoming more difficult to maintain with an acceptable Quality of Service (QoS). In addition, due to expanding capacity by introducing more equipment as part of Project Network for Spectrum (NFS) in the Indian Army, there is a requirement to enhance network performance with smart tools and intelligent technologies enabled through AI.

- **More Attention to Security and Safety** Data breach and Cyber Security violations are growing and becoming severe in the Army Communication Network. These events have resulted in significant consequences, including compromise of operational data. AI can be introduced into several layers to establish strong security protection and behavioural analysis based on machine learning which will significantly improve the ability of network detection attacks, automatic analysis of data, and the identification of relationships between isolated behaviours.

Advantages of AI in Army Communication Network

- **Abilities of Learning** Intelligent decisions are required to manage dynamic traffic to accurately describe the Army Communication Network traffic characteristics. Fortunately, AI has entered the cognitive age wherein deep learning can be exploited. Through deep learning, the machine system can use the existing training data to process large amounts of data through data mining. AI can be utilised to carry out Army data traffic management and maintenance. Through these efforts, the accuracy of analysis can be enhanced and the intelligent management of Army Communication Networks can be realized.

- **Abilities of Understanding and Reasoning** Due to the changing dynamics of the Army Communication Network system, the state of information source may have changed when it is transmitted to the network management system. Therefore, the network management can only know the local state information without knowledge about the system's internal state. Machine learning happens to have the strength to deal with this kind of fuzzy logic and uncertainty in reasoning. In order to make the classification or prediction easier, deep learning constructs a multi-hidden layer model and uses the hierarchical network structure to transform the feature representation of the sample into a new feature space, layer by layer. In particular, AI does not need to describe the mathematical model of the system accurately and therefore has the ability to deal with the uncertainty or even "unknowability" that is peculiar to the Army Communication Network.

- **Ability of Collaborating** The structural complexity of Army Communication Network is rapidly increasing as the network expands in both scale and size. Concepts such as distribution and hierarchy are often talked about in network management. Management tasks and controls are distributed to the entire network. As a result, we must deal with issues such as task distribution, communication, and collaboration between Army Communication Management Nodes. If we introduce the multi-agent collaboration of distributed AI into the Army Communication Network Management, we can expect the ability to collaborate between network managers distributed at every layer.

- **Use of AI in Management, Monitoring and Maintenance of Army Communications** Since the era of Time Division Multiplexing (TDM) automatic switched to IP based communication on networks, it has been the pursuit of the Army Communication Engineers to introduce intelligence into network operations, management, and maintenance. Software–Defined Networking (SDN), Network Functions Virtualization (NFV), etc, coupled with integrated network management systems, can directly issue orders which can be executed by network equipment, and it is possible to realise real-time monitoring of Army Communication Networks and services. To monitor the real-time information of the Army Communication Network, Deep Packet Inspection (DPI) system can collect information such as the running state of network equipment, the usage of resources, and the quality of services. With the big data obtained from the DPI system, the AI system can rapidly analyse and find if there are or will be abnormity within the information. For example, if AI system finds a burst of continuous traffic, it can suspect a Distributed Denial of Service (DDoS) attack in the network, analyse the package characteristics and orchestrate an inspector collaboration task to drop all packages with the suspected characteristics to avoid damage.

- **AI in Traffic Prediction** AI can be applied to Army Communications traffic demand prediction during the planning process, where it is used to predict and analyse traffic demand. Traffic tendencies can be divided into two types: ***short-term tendencies***, such as temporary traffic increase during motion exercises; and ***long-term tendencies***, from which anomalous tendencies such as temporary traffic increases during events have been removed. In AI-driven traffic prediction, we make AI learn the short and long term traffic tendencies that have totally different factors causing traffic fluctuations and mechanisms in order to predict both short and long term traffic demands.

- **AI in Spectrum Management** Spectrum is a valuable asset in Defence Communication Networks and needs to be utilised judiciously. Piecemeal optimization of applications such as spectrum monitoring are manpower intensive. It entails efforts to hand-engineer feature extraction and selection that often take months to design and deploy. By employing powerful machine learning algorithms, AI can be utilised to efficiently carry out assigned tasks. In addition, the design complexity of Radio Frequency (RF) systems can be reduced by improving RF parameters such as channel bandwidth, antenna sensitivity, and spectrum monitoring.

Conclusion

Indian Army recognises the qualitative edge AI systems will provide in near future, and will assist commanders faced with unconventional adversaries in high-speed engagements. AI system will augment analysis and decision-making capabilities of commanders and speed up learning and improve their ability to act with discretion, accuracy and care under uncertain and changing conditions.

Use of AI systems will transform traditional Army Communication Network into intelligent network. Predictive mechanisms will enable users to take faster and better data driven decisions. Intelligence built on huge amount of historical network data will provide a pattern for network anomalies. Using AI models, Army Data Network administrators can detect network failures, forecast traffic patterns, understand traffic congestion, and build intelligent security. Use of AI in Army Communication Network, thus, will enable commanders at all levels to obtain timely information and further disseminate information to subordinates, based on analysis available using AI systems to ensure timely action.

Bibliography

1. *G. E. Hinton, R. R. Salakhutdinov, Reducing the Dimensionality of Data eith Neural Networks, Science, Jul. 2006, Vol. 313:504-507*

2. *N. Kojic, et al. Neural Network for Optimization of Routing in Communication Networks, Facta Universitatis (NIS) Ser: Elec. Energ. Aug. 2006, Vol. 19, no.2:317-329.*

3. *SUI Dan, JIN Xian-Hua, Network Cognition Control Method Based on Artificial Intelligence, Computer Simulation, Sept. 2011, vol. 19, no.2:317-329.*

4. *Sandra Sendra, et al, including Artificial Intelligence in a Routing Protocol Using Software Defined network, ICC2017: wt04-5th IEEE International Workshop on Smart Communication Protocols and Algorithms (SCPA 2017).*

5. *Sahebu, K.M. Artificial intelligence approach to planning and managing communication networks, International Conference on Electromagnetic Interference on Electromagnetic Interference & Compatibility, 2002: 193-202.*

6. *Open Networking Foundation (ONF), Software-defined Networking: The New Norm of Networks [EB/OL], http://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-nownorm.pdf.*

7. *Chiosi M. et al. Network Functions Virtualization: An Introduction, Benefits, Enablers, Challenges and Call for Action [EB/OL], http://www.etsi.org.*

8. *M.Al-Hisnawi, M. Ahmadi, Deep Packet Inspection Using Quotient Filter, IEEE Communications Letters, 2016, 20 (11):2217-2220.*

9. *XU Guibao, A technological architecture of artificial intelligence, Telecommunication Network Technology, Dec. 2016, no. 12:1-6.*

10. *J. Holland, Can there be a unified theory of complex adaptive system?, in: The Mind, the Brain and the Complex Adaptive Systems, H. Morowitz and J. L. Singer, Eds., Addison-Wesley, 1995.*

EMPLOYMENT OF ARTIFICIAL INTELLIGENCE TO ENHANCE EFFICACY OF ARTILLERY

- Major Sharad Sagar Joshi

Introduction

In wars of the future, the side with shorter and effective Observe, Orient, Decide and Act (OODA) loop will be able to achieve effect based application of its lethal and non-lethal assets to break the enemy's will to fight. A shorter OODA loop can be achieved by ensuring seamless command and control architecture with targeting capability of firepower assets providing the cutting edge. The ultimate role of artillery aims at effective application of all firepower assets to achieve the desired degree of neutralization, suppression and destruction. This entails multifarious tasks, primarily including rapid deployment, handling of Artillery Target Intelligence (ATI), establishment of surveillance grid, target acquisition, target analysis, allotment of most suitable firepower asset for engagement and Post Strike Damage Assessment (PSDA). There are well established procedures for these functions and automated systems such as ACCCS (Artillery Combat Command and Control System) have been employed to perform these tasks to some extent. Since the process of handling ATI is tedious involving handling of overwhelming data and considerations of various variables simultaneously, Artificial Intelligence (AI) has the potential to increase the efficacy of artillery in the battlefield.

India's Conundrum

India's efforts at AI R&D, particularly defence R&D, are comparatively nascent. This lag in AI is surprisingly glaring when viewed with respect to the size of its economy and defence needs. India's current AI industry is estimated to be around $180 million annually. According to one study, India had only about 6 per cent of the world's companies and about 29,000 AI professionals in the civilian sector. In August 2016, Carnegie India published a research paper titled "India and the Artificial Intelligence Revolution"; the paper highlighted the fact that India needs to view AI as a critical element of national security in view of the advancement the world has achieved, and especially in view of neighbour China's rapid progress in the field calling India's entry into the domain as "late".[1]

In an ambitious initiative, the Indian Government has started work on incorporating AI to enhance the operational preparedness of the armed forces in a significant way that would include unmanned tanks, ships, aerial vehicles and robotic weaponry. An AI task force has been created to formulate a concrete

[1] *Pant Atul, Future Warfare & Artificial Intelligence, The Visible Path, IDSA Occasional Paper, August 2018.*

strategy and framework for employment of AI for national security and defence needs in the years ahead.

Operational Functions

The armed conflicts during the recent times have ushered in major changes in war fighting philosophy which now seek to defeat enemy by shattering his morale and physical cohesion, his ability to fight as an effective whole, rather than to destroy him physically through incremental attrition. Firepower is going to play a crucial role, more important than ever before, and contribute substantially in achieving success in operations. The essence of optimal exploitation of such an asset of immense firepower lies in certain prerequisites. These are the operational functions mentioned below which artillery needs to undertake in order to perform its operational role in the battlefield:-

- Establishment of gap free surveillance grid.

- Handling of ATI (Target acquisition, Analysis and Allotment of Firepower Asset).

- Passage of engagement orders to all concerned resources & engagement.

- PSDA and re-engagement, where necessary.

- Operational logistic functions, primarily related to ammunition management.

Operational Functions and Application of AI

All the above mentioned functions are presently based on human intellect. The capability of human mind to analyse voluminous data simultaneously, considering all variables within short duration is limited. Thus, AI presents scope in each of the above mentioned functions for its employment and enhancing the overall efficacy of artillery. Present methodologies to perform these functions and identify the shortcomings which can be overcome with the application of AI.

- **Deployment Plan** In today's fluid, crowded battlefield, the movement and positioning of field artillery units is a very complicated process that includes location selection, terrain management, movement planning, the coordination of survey support for firing and target acquisition. The present methodology for formulating deployment plan considers the factors like **Range, Line To Shoot Down To, Crest Clearance, Required Gun Density and Survivability** against enemy artillery, air and ground forces. This results in considerable time spent in recce and selection of gun areas, resolving the issues of availability of route and Battle Space Management. Some form of assistance is provided by ACCCS which employs GIS based platform to assist in identification of induction routes and deployment areas. However, it is an automated system and does not consider all the above mentioned factors in entirety. AI integrated GIS will allow consideration of various aspects of terrain and would be able to handle large data obtained from the attributes of the terrain. These attributes when analaysed with various variables factors for Artillery deployment will enable evolution of most optimum deployment on the theatre grid. As the complexity of AI systems matures, AI algorithms may provide commanders with viable courses of action based on real-time analysis of the battle-space, which would enable faster adaptation to future events.[2]

- **Surveillance Grid** The deployment of surveillance assets to obtain ATI involves detailed recce to identify or select the most suitable location for deploying an asset. Moreover, it requires analyses of availability, characteristics, capabilities and limitations of surveillance equipment for generating the deployment plan. Further, sensors deployed across the battlefield generate a large amount of data pertaining to artillery targets. This data is required to be analysed in near real time for prompt engagement. Presently, the procedure is based on human intellect and is limited to the capability of human mind. An AI based system will enable quick analyses of the area of interest, identify most probable course of enemy action and identify the likely locations of the enemy elements. While BFSRs and EO devices will be ab-initio deployed as per the plan, thereafter, side stepping based on the progress of the operations and predicted future locations of the enemy, will be autonomously monitored, analysed and predicted by AI.

- **Target Acquisition and Analysis** In the present system, a target is acquired using manual observation, using Electro Optical (EO) devices like Thermal Imaging Integrated Observation Post Equipment (TIIOE), Long Range Reconnaissance and Observation System (LORROS), aerial platforms, satellite imageries and Weapon Locating Radars (WLRs). Large number of targets acquired by the sensors need to be analysed in near real time on various parameters to include **location, size, description and characteristics** to identify the most suitable resource for engagement. Presently various ad-hoc organisations are established at various levels to carry out this analysis, relying on human intellect. However, the process is time consuming and thus owing to the limited human capability manifests in sub optimal results. AI can carry out these tasks autonomously to **analyse, prioritise and allot** the most suitable firepower asset. This aspect when combined with an integrated environment of sensors and shooters, controlled by AI will shorten the Sensor to Shooter link. These

[2] *Hoadley D,Lucas N, Artificial Intelligence and National Security, April 2018, Pp 10.*

type of systems can utilise AI to automatically pursue, distinguish, and destroy enemy targets and should compose of information collection and management systems, knowledge based systems, mission implementation systems, etc.[3] For example, Defence Advanced Research Projects Agency's (DARPA) Target Recognition and Adaption in Contested Environments (TRACE) program uses machine learning techniques to locate and identify targets with the help of Synthetic Aperture Radar (SAR) images.[4]

- **Engagement Orders and Communication Systems** After analysing the targets, prioritising them and allotting the most suitable firepower assets, the engagement orders are issued. Presently, some form of automation has been achieved with ACCCS. However the system is not AI supported, based on conventional means of communication (Line and Radio) which causes a delay in passage of engagement orders. The limited capacity of the media being used, interruptions due to enemy Electronic Warfare (EW) and the distances involved between the firepower assets and decision making organisations may render this system ineffective in an intense battle. AI compatible cognitive radios with dynamic spectrum management to enhance communications, while pursuing offensive EW capabilities through the application of machine learning to learn and rapidly devise countermeasures are the future.[5]

- **Ammunition** The assessment of the optimum quantum of ammunition required to be delivered on the target to achieve the desired effect is a crucial aspect. With large number of variables like quantity of fire units, types of equipment, different types of terrain and different types of ammunition systems, the assessment of the scale of ammunition required to be fired on the target, cannot be left to the judgement of the observer. Presently, Ammunition Tables (AMTAB) are used to calculate the ammunition required to be delivered on the target to achieve the desired degree of effect. AMTAB allowance is based on limited trials carried out almost half a century ago. AI based system can carry out analysis of the target characteristics, lethality of the ammunition and various other variables involved. AI can be employed to analyse the target characteristics just by visual acquisition and through photographs. Thereafter, it can carry out target to weapon matching and based on the availability of most suitable asset, it can then suggest the quantum of the ammunition to be delivered on the target to achieve the desired effect.

- **Counter Bombardment and Survivability** The ability of producing effective counter bombardment fire depends on the accuracy of

[3] *Hoadley D,Lucas N, Artificial Intelligence and National Security, April 2018, Pp 10.*
[4] *Ibid .*
[5] *Ibid .*

location of hostile guns, accuracy of the fire which is being applied for engagement of these locations and availability of resources for engagement. The procedure involves detection of hostile gun locations by WLRs, aerial assets, crater examination and manual acquisition by troops operating behind enemy lines. The present system is time consuming and does not ensure full proof integration of all sensors with shooters. Further, in a dynamic and fluid situation, allotment of resources for this task will be a challenge. AI based sys will enable quick engagement of enemy gun areas. Crater examination, shell report and bomb report process can be automated by utilising AI based system. Just the visual input of the crater or image of the crater would suffice for the system to decipher the location of the hostile gun position. This, when combined with the ability to learn patterns, terrain analysis of own and enemy area, will enable the system to suggest safe deployment areas to obviate the threat of counter bombardment by the enemy.[6]

- **Ammunition Replenishment and Transportation** To ensure that no fire power asset is idle at any point of time, it is essential that the supply of ammunition is continuous. The system presently relies on manual monitoring and updating for carrying out ammunition replenishment. AI can be employed to autonomously monitor available stock of ammunition in various logistics echelons. AI can lower transportation costs and reduce human operational efforts. It can also enable military fleets to detect anomalies and predict component failures.

Conclusion

The dynamics of the present and future battlefield demand near real time combat intelligence and engagement, which existing systems cannot provide. The proliferation of sensors and fluid battlefield situation will generate enormous volume of information, which will be humanly impossible to process. It is therefore imperative to develop a fully automated, autonomous and intelligent system, which will receive information from directly interfaced system, carry out target identification and situational assessment, present a cohesive picture and nominate the firepower resources for near real time engagement of targets.

[6] *Thesis on Artillery Survivability Model performed by MOVES Institute.*

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING: THE WAY AHEAD FOR FUTURISTIC IMAGERY INTERPRETATION

- Captain Shreya Sood

"Artificial Intelligence is in a 'Golden Age' and solving problems that were once in the realm of science fiction."

- Jeff Bezos, Founder and Chairman, Amazon

Introduction

Artificial Intelligence (AI) and its subset, Machine Learning (ML) is a trailblazing technology that can mimic the capabilities of the human brain in machines. It is the main driver of emerging technologies like big data, robotics, and Internet of Military Things (IoMT), and will continue to act as a technological innovator for the foreseeable future.

Interpretation of space and satellite images is one of the sectors being changed by AI and ML. The ever-growing number of satellites in space has resulted in massive amounts of data received by ground stations on a regular basis, increasing the requirement for skilled manpower, training, and technological resources to process it. The use of AI and ML in this field will be a viable option as it reduces processing time and effort while enhancing productivity and error-free outputs. Geospatial tools enable the prediction, monitoring, and countering of such threats, as well as the planning and support of field operations.

AI and ML in Satellite Imagery Interpretation

Every day, millions of photos are shot in space and returned to Earth by ever-increasing number of satellites. Satellite imaging enables unprecedented degrees of remote surveillance of an adversary's locations, movements, concentration, training drills, naval manoeuvres, damage assessment, and so on. They assist military observers and commanders in detecting changes in hostile terrain across a large area. Satellites are now transmitting significantly more data for processing and analysis. As a result, AI might be utilised to automate the study of this data from various sources and alert analysts to unusual events that require their expertise.

In light of this, one of the most significant advancements in Imagery Interpretation (IMINT) is the use of software and AI algorithms to analyse satellite imagery. Despite the ever-growing volume of photos, the algorithm now in use allows an interpreter to detect, recognise, and identify aeroplanes, vehicles, and ships. In addition to assisting experts in their task of looking for information and hints on photos, this technology also enables them to enhance the study of activities of previously chosen geographic locations. It helps to lighten the load on human analysts so they can handle the growing amount of imagery data being collected.

Apart from better clarity and visualization, ML lets us interpret images in many ways and from different vantage points. The scope of using ML in satellite imagery is not restricted to a narrow field but could be used for modelling, separating images or extracting useful information. The process is complex but the final results are worth the long process. Some of the other cutting-edge benefits of application of AI and ML to satellite imagery have been enumerated below:-

- Numerous applications that demand a significant amount of spectral and spatial data for pattern recognition benefit from ML and remote sensing technologies.

- ML combines algorithms using Computer Vision (CV), computer systems, and deep learning techniques to collect and classify features quickly and accurately.

- ML and CV, can help the end-user to process the data collected to find solutions from remote sensing data. It can also improve the overall accuracy of the data classification and enhance the reliability and assessment – IMINT analysis.

- To overcome the limitations of remote sensing data, ML techniques through neural networks can enhance the analysis of broad areas in order to classify objects, identify temporal change, data fusion, cloud removal, and spectrum analysis from satellites or aerial pictures.

- For areas with complex feature distribution, such as in the applications of environmental monitoring and management, mineral mapping, agriculture, disaster management, climate change, and wildlife conservation, images collected by satellites or Unmanned Aerial Vehicles (UAV) using ML techniques can provide near real-time reports.

Applications of AI and ML in Satellite Data Modern AI and ML techniques, particularly deep learning, have made it simpler to perform tasks such as object identification, item counting, semantic segmentation, and general picture classification. Following are a few examples of AI and ML applications in satellite imagery: -

- **Object Detection Using ML** Object detection is a Computer Vision technique for locating instances of objects in images or videos. Object detection algorithms typically leverage ML or deep learning to produce meaningful results. This happens when Computer Vision techniques are used to identify various features of an image, such as the colour histogram or edges, to identify groups of pixels that may belong to an object or any changes within the same. These features are then fed into a regression model that predicts the location of the object along with its label. Object detection is not just a requirement for contemporary combat but also a key factor in the development of early strategic warning systems. A large dataset is needed in order to train an AI model to recognise military artefacts. There must be a significant number of photos with labels in the dataset. Analysts can automate detection and analysis of activity-based data by combining electro-optical satellite imagery with advanced algorithms to detect and flag objects with high accuracy to include trucks, tanks, ships, and aircraft.

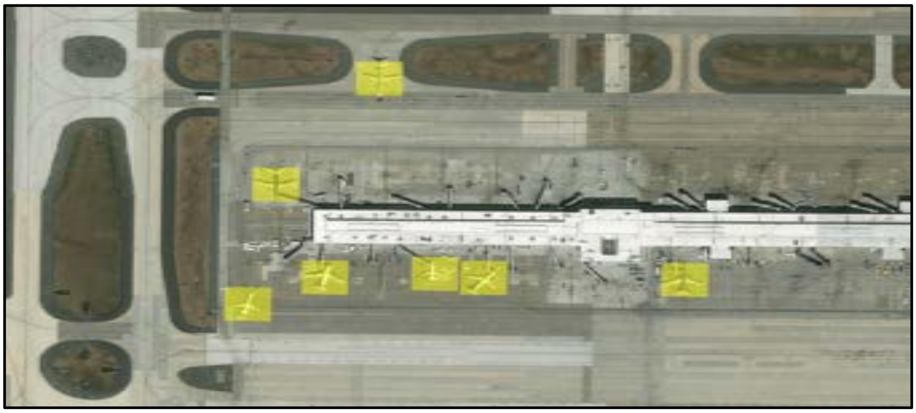
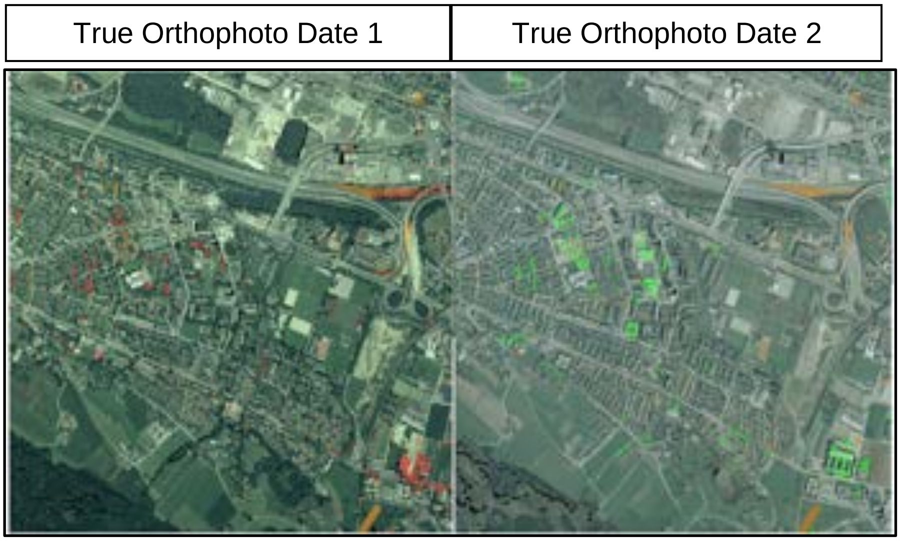


Figure 1: Automated Algorithms Detect Airplanes in High-Resolution Satellite Imagery

- **Change Detection Algorithms** It is defined as the process of identifying differences in the state of an object or phenomenon by observing it at different times.

  - This process is usually applied to detect changes in earth surface at two or more times. The primary source of data is geographic and is usually in digital format such as satellite imagery, analog format (aerial photos), or vector format (feature maps). Ancillary data (historical, economic, etc) can also be used.

  - Actual information comparing buildings, road segments, troop concentration, new construction, concentration of weapon systems, mobilisation, etc is extremely important from a military point of view. Technically, the goal of a change detection algorithm is to create a map in which changed areas are separated from unchanged ones, and the value of AI is in replacing visual interpretation with automatic or machine interpretation, which would increase the amount of data being processed while simultaneously decreasing the amount of human intervention or probability of error.



True Orthophoto Date 1

True Orthophoto Date 2

Figure 2: Time-Series Analysis and Change Detection Algorithm Demonstration. Changes in Buildings and Roads Highlighted Red (Before) to Green (After)

- **Terrain Analysis** By combining stereo satellite imagery and terrain elevation databases, it is feasible to create true-color 3D terrain visualization models of any location. Detailed knowledge of the terrain is a key factor for successful military operations. Stereo satellite map data is a source of reliable, regularly updated information that gives a realistic and objective view of the terrain which is indispensable for mission planning.

- **CV Techniques** The fundamental use of satellite data is to enable CV to detect diverse objects. CV is a branch of AI that allows machines and programs to extract useful data from virtual photos, videos, and other sensory inputs. CV can also participate in executing certain measures to make predictions based on that data. Municipalities, government bodies, emergency crews, the armed forces, and other civil authorities require reliable information on structures, route sections, and urban area boundaries.

- **Automated Response System** AI onboard satellites can enable the collection and transmission of information in near real time. On-orbit, ML algorithms may be used to detect anomalies and initiate responses. Tasking another imaging satellite to collect pictures at a specific timestamp or coordinating a co-collection activity of several data kinds in the same region of interest are examples of autonomous replies. Inter-satellite communications links would be used to send tasking directives and data acquired. Algorithms can analyse, categorise, or combine massive amounts of data on-orbit with enough on-board processing gear on each satellite to offer insights straight to end users when they need them.

- **Estimation of Global Oil Inventory** Employing the basics of interpretation and trigonometry, this is achieved by interpreting shadows. As most of the fuel tanks have a floating top, it is possible to calculate its volume and the amount of oil in it, utilizing simple trigonometry. Also, knowledge about the locations of all such oil tanks (extracted from other satellite imagery or gathered from different database) can assist in area/region-wise calculation of global oil inventories.

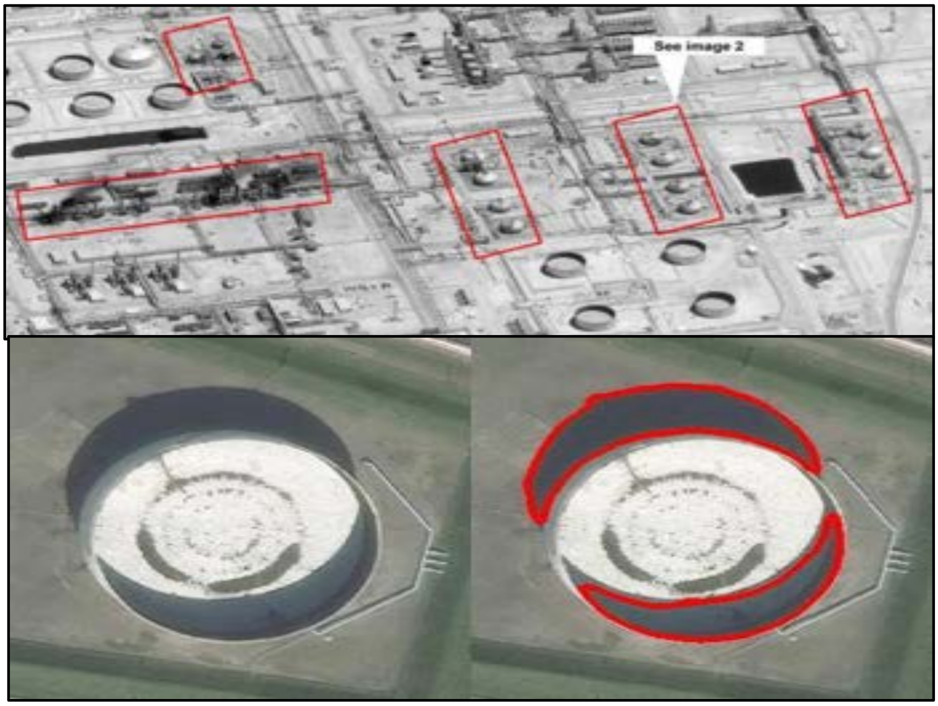


Figure 3: Measuring Oil Inventory by Interpreting Shadows

- **Monitoring National Activities** Another application which can be said to combine all the other applications given above is monitoring the economic and military activities of various countries across the globe. If independent satellite-powered measures of cities' development, such as car density, construction rates, electricity consumption through nighttime illumination, import and export operations through ship count and sizes, and aircraft count in airports, combined with traditional surveys, statistics, and media data are indexed/catalogued, it can generate a comprehensive report on the economic, financial, and social health of the country or region which is otherwise off-limits.

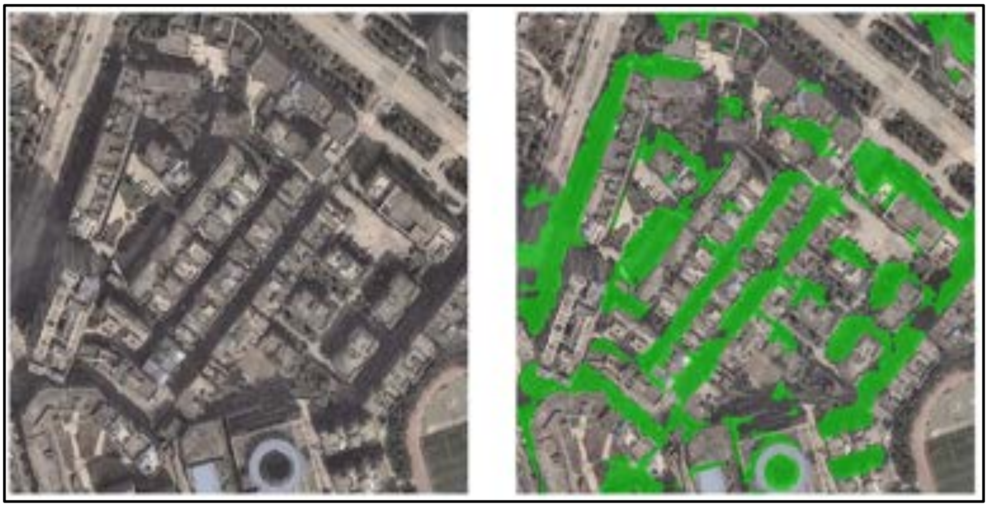


Figure 4: Construction rates monitoring via shadow detection

- **Creation and Use of Synthetic Data** To build an effective AI system, engineers need to feed massive amounts of training data to ML algorithms, images of the type of objects they want them to find, so they can automatically find those objects when presented with new images. To compensate for the shortage of such data, real world data is often supplemented with synthetic data, which is artificially created but designed to look like the real-world data the machine is being built to work with. Most AI algorithms are trained on both real-world images and synthetic images.

- **Quantum of Imagery Data** There is a large amount of imagery and other types of data transmitted by satellites to reception stations on Earth. It can neither be looked at nor exploited in its entirety by traditional means. Hence, actions like counting objects in imagery, monitoring different places, etc. it can be processed by AI/ML. The military and intelligence setups of many countries, such as the USA, Israel, Russia, France, etc., are keen on using AI tools to sift through the vast torrent of data created by an ever-increasing number of sensors and pick out the most important information for human analysts.

AI Based Software in Satellite Imagery Interpretation

Some tools and software in vogue or under development for both military and civil use have been covered in the succeeding paragraphs. Such tools allow armies to increase their surveillance and intelligence capabilities by processing the growing volume of data coming from new sensors and by relieving experts of repetitive tasks. The army thus has greater efficiency in situation assessment and decision-making. Analyzing images is a crucial issue, and a well-coded AI can generate alerts as soon as predefined parameters are observed. As a result, it is not surprising that security laws are being enforced zealously to prevent pilferage or unintentional sharing.

- **Planet Labs** International aerospace and data analytics firm Planet of the USA has a dedicated solution for ML called Planet Analytics. This uses ML algorithms for processing daily satellite imagery, detecting and classifying objects, locating topographic and geographical features, and consistently monitoring even the most infinitesimal change over time. The information feed is seamlessly integrated into the workflows and provides insights on virtually any location on the planet.

- **Descartes Lab** Satellite imagery refining start-up Descartes Lab based in USA has a cloud-based platform that applies ML forecasting models to petabytes of satellite imagery that is drawn from a number of sources.

- **Google** One of the pioneers utilising the prowess of ML in satellite photography is Google. Google has released a tool named PlaNet that can pinpoint the precise geographic location of any image taken anywhere on the planet. Convolutional neural networks and mapping technologies are the foundation of the PlaNet project, which harnesses the potential of ML, offering knowledge that is priceless and unmatched in both qualitative and quantitative ways.

- **Preligens** The French company Preligens employs a tool that compiles data (commercial and open source) from a variety of sensors (satellite images, air and ship transponder data, infrared imagery, social networks, etc.) and notifies analysts in the event of unusual changes in the situation at a specific theatre of operations. In particular, it can track the development of a critical site and automatically detect armoured vehicles, aircraft, or ships. When a nuclear submarine departs from a military port or when an unusual concentration of armour is found, the AI can notify a human analyst.

- **Project Maven** It is a United States Department of Defense program to create an AI-powered investigation system for UAVs to prepare predictive analytics of drone footage.

- **OneAtlas** Project OneAtlas is prepared by Airbus. The software provides a collaborative environment to easily access very high-resolution imagery, performs large-scale image processing and extracts industry specific insights. The services include infrastructure change detection, vehicle detection & counting and will soon cover aircraft detection and land use change detection as well.

- **Raster Vision** Raster Vision is an open source framework for Python developers building computer vision models on satellite, aerial, and other large imagery sets (including oblique drone imagery). There is built-in support for chip classification, object detection and semantic segmentation.

- **Pulse Satellite** Pulse Satellite is a tool to analyze satellite imagery assisted by neural networks. It has been developed by United Nations Satellite Centre.

Challenges and Concerns

The challenges associated with geospatial data are regarding its processing and analysis. Some of these challenges have been enumerated below:-

- **Size** The size of objects in satellite imagery is usually very small (~20 pixels), yet the size of the input images is vast (often hundreds of megapixels). The algorithms outlined above are not tuned to detect minute objects in huge images and frequently perform poorly when applied to Earth observation data due to a relative lack of training data. Although this field of study is still relatively new, adapting these methodologies to the many scales and objects of interest in satellite imagery shows considerable promise.

- **Amount of Data and Storage** According to research, the expanding fleet of imaging satellites transmits back to Earth over 80 gigabytes of data daily. This information is unprocessed and binary in nature. Professionals who access the data must be aware of their search criteria. Additionally, the cost of storing such data is substantial. In order to distil the layers of data included in the images into coherent information that is helpful to other academics, politicians, or funding organisations, additional processing power and enhanced human experience are needed.

- **Normalisation of Images** Another complexity is that all images in the dataset should be normalised to be ready for input into the change detection process. Building change detection solutions requires competence in ML and strong experience with remote sensing data.

- **Automatic Target Detection** Due to the target object's varied size, orientation, scale, and background, this is a difficult task that largely relies on pre-existing data that will be used in AL/ML techniques. In addition, very clear and concise attributes are present in the edge information of objects in satellite photography. AI systems can automatically detect changes in satellite photos while taking into account the image's radiometric properties. However, accurate interpretation of the change as well as accurate identification of targets of military relevance requires human participation. The same will only reveal the locations of the temporal changes in the image. A well-defined and extremely particular data set must be developed and supplied to the machine in order to minimise or eliminate human interaction in interpretation and identification using AI. Further, such military data will also be strictly classified. This is a major problem because creating a repository of such a classified data pertaining to military information of foreign or hostile military forces is extremely difficult and time-consuming. Such data will be dynamic in nature, and therefore inaccuracies in the same is a probability which cannot be overlooked. Even if acquired, it will be sensitive and classified due to its inherent nature, creating additional concerns about its handling and dissemination.

- **Type of File** Most popular deep learning architectures are not designed for imagery that is often a gigabyte or larger, may contain over a dozen channels (most of which are not in the visible spectrum), and is stored in spatially referenced file formats like GeoTIFF and JPEG2000. Hence, for professionals interested in applying these techniques to satellite imagery, there remain many obstacles to even basic workflows.

Prognosis

The Armed Forces cannot remain oblivious to such technological advancements in the field of Satellite IMINT and therefore will have to devise methodologies to keep pace with such cutting-edge technologies. The same would entail a combined and synergized effort of all concerned departments and stakeholders.

A holistic approach towards the creation of capability and imbibing of such cutting-edge technology by combining the efforts of all concerned lead agencies dealing with the subject is the need of the hour. While attempts are being made to develop the same, there is overlap between the activities of several entities working on related projects. All interested parties must build a shared roadmap for creating AI and ML-based solutions for imagery interpretation in the armed forces. This would entail inter-agency or departmental synergy and involvement of subject experts from both within and outside the organization. Creation of a pool of subject experts within the organisation would therefore assume priority.

National institutions such as ISRO, the DRDO's Centre for Artificial Intelligence and Robotics (CAIR), and others should be approached to take the lead in this regard. Involvement or inclusion of select indigenous private players or startups in the subject industry could also be considered, with due security vetting. The National Geo Int Framework, designed by the NTRO as a tool to assist in decision making and analysis by concerned stakeholders at the national level, on aspects concerning National Security, is expected to roll out by October 2022. Ibid tool will also result in creation of a repository of data from all sources of intelligence, especially data of military significance. Such data will be highly classified with the necessary security protocols for access. Such information will be extremely useful to all Armed Forces, including the Defence Space Agency (DSA). Utilisation of above for creating a framework for introduction of AI and ML should be thought about and planned by the NTRO in consultation with DSA and the three services.

Bibliography

Publications/ Books

1. *Du, E., Ives, R., van Nevel, A. et al. Advanced Image Processing for Defense and Security Applications. EURASIP J. Adv. Signal Process. 2010, 432972 (2011).*

2. *Military Intelligence Satellite, Dr Manish Chandra, Surendra Publications, 2018, New Delhi.*

3. *Artificial Intelligence: A Guide for Thinking Humans, Melanie Mitchell, Pelican Publications, 2019, UK.*

4. *A fast military object recognition using extreme learning approach on CNN by International Journal of Advanced Computer Science (IJACSA) and Applications, Vol. 11, No. 12, 2020.*

5. *Artificial Intelligence and the Future of Power: 5 Battlegrounds, Rajiv Malhotra, Rupa Publication, 2021, New Delhi.*

Web Links

1. *https://www.geospatialworld.net/blogs/machine-learning-in-satellite-imagery/.*

2. *https://earthobservatory.nasa.gov/features/OrbitsCatalog.*

3. *https://medium.com/vsinghbisen/ai-applications-for-satellite-imagery-or-satellite-images-dataset-3b1a2499c5e5.*

4. *https://techfastly.com/satellite-imagery-and-ai/.*

5. *https://emerj.com/ai-sector-overviews/ai-applications-for-satellite-imagery-and-data/.*

6. *https://www.coe.int/en/web/artificial-intelligence/history-of-ai.*

7. *https://opendatascience.com/the-history-and-future-of-ai-with-michael-i-jordan/.*

8. *https://www.geospatialworld.net/blogs/difference-between-ai%EF%BB%BF-machine-learning-and-deep-learning/.*

9. *https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation /Artificial_intelligence_in_space.*

10. *https://concisesoftware.com/history-of-machine-learning/.*

11. *https://insights.regenesys.net/how-is-artificial-intelligence-transforming-business/.*

12. *https://web.archive.org/web/20130719163905/http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002006.htm.*

13. *https://cloud.withgoogle.com/build/data-analytics/explore-history-machine-learning/.*

14. *https://www.ibm.com/in-en/cloud/learn/what-is-artificial-intelligence.*

15. *https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html#industries.*

16. *https://insights.regenesys.net/ai-and-machine-learning-the-relationship-explained/.*

17. *https://concisesoftware.com/history-of-machine-learning/.*

18. *https://insights.regenesys.net/how-is-artificial-intelligence-transforming-business/.*

19. *https://www.fritz.ai/object-detection/.*

20. *https://www.pixxel.space/technology.*

21. *https://www.mdpi.com/2079-9292/7/10/216/htm.*

22. *https://www.popularmechanics.com/military/research/a37014065/how-to-spy-on-military-bases-use-satellite-imagery/.*

23. *https://wsimag.com/science-and-technology/64215-artificial-intelligence-has-changed-our-world.*

24. *https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/.*

25. *https://whatis.techtarget.com/definition/AI-code-of-ethics.*

26. *https://www.brookings.edu/research/how-to-address-ai-ethical-dilemmas/.*

27. *https://orbitalinsight.com/geospatial-solutions/defense-intelligence.*

28. *http://interactive.satellitetoday.com/via/october-2020/10-ways-ai-is-making-a-difference-in-the-satellite-industry/.*

29. *https://arxiv.org/pdf/1812.05815.pdf.*

ARMY DESIGN BUREAU - CONNECTING CAPABILITIES IN ARTIFICIAL INTELLIGENCE FOR NEW AGE WARFARE

- Colonel Amandeep Singh Bains

"*Victory will smile upon those who anticipate changes in the character of war, not upon those who wait to adapt themselves after changes occur*."

- General Giulio Douhet, The Command of the Air (1921)

Introduction

In recent times, the impact of ***technology has assumed an altogether new and disruptive dimension***. Science & Technology has a central role in the defence eco-system as it drives strategic national capability and is central to countering emerging threats. Our modernisation strategy for developing Artificial Intelligence (AI) needs to focus on **information and data at the core**. As we modernise, we will embrace **information-centric technologies**, recognising that it will be the application of a combination of technologies like **processing power, connectivity, AI, automation, robotics, autonomy, and quantum** that will achieve the disruptive effect we need. [1]

In the realm of National Security, AI presents huge **military opportunities** and its **associated challenges**. As conflicts increasingly leverage technologies like **AI and Big Data**, *military relevance will rest heavily on the paradigm where technology will achieve strategic objectives, while preventing the adversary from doing the same*. It is important to understand how **AI** will develop over time in **New Age Warfare**, its ***impact on operations and capability*** and their applications on **military concepts and organisational structures**.

AI Enabled Battlefield

The underlying technologies themselves (the internal combustion engine, radio communications, radar etc.) as well as the new military systems to which they gave birth (airplanes, tanks, amphibious landing craft, aircraft carriers, radar and so forth), formed only a part of the innovations.

Military capability is not only dependent on fielding weapon systems with superior technology. History has shown that improving military effectiveness requires organizational and doctrinal innovation*. For example, German Blitzkrieg was a military concept that combined organizational and doctrinal innovations*.[2] *One still had to integrate advanced weapons systems with appropriate tactics, operational*

[1] *https://www.gov.uk/government/speeches/chief-of-the-defence-staff.*

[2] *Emerging Technologies and Military Capability Dr Andrew D. James.*

concepts and doctrines in order to realize the full potential of new ways of fighting (see box)[3]*.* ***This is where the challenge to integrate AI into systems and war fighting lies.***

Technology has come to dominate the discourse of military strategists in the aftermath of the recent conflicts in **Israel**, **Armenia-Azerbaijan** and **Russia-Ukraine war**. The Israeli military is calling '**Operation Guardian of the Walls**', the **first AI War**[4], where AI was a key component and force multiplier. Israeli Defence Forces used advanced program '**Alchemist**', '**Gospel**' and '**Depth of Wisdom**'[5] during the fighting where '**Alchemist**' used AI to alert troops of possible attacks and '**Gospel**' generated recommendations for aerial targets. ***It is believed that AI helped shorten the duration of the fighting, having been effective and quick in identifying targets****.*

Emerging technologies will shift the balance between ***quality and quantity****, as well as between* ***offense and defense****. For example, low-cost drone swarms could overwhelm defensive systems, providing a greater advantage to the attacker, while Counter-Drone systems could easily neutralize such attacks, and*

At the same time, the recent events in **Saudi Arabia, the Azerbaijan-Armenian conflict** over the contested **Nagorno-Karabakh** region, and **Ukraine** are reminders of the **paradigm** and showed how UAVs/Drones can dominate ground operations and inflict crippling losses. **Future wars will also involve low technology**, which is easy to obtain but difficult to defeat. Since World War II, high-tech militaries have been consistently thwarted by low-tech opponents. ***Thus, there is a need to maintain a balance while infusing technology into our inventory and doctrines****.*

AI - Enabling Fourth Industrial Revolution Technologies

AI is playing a predominant role in connecting **Fourth Industrial Revolution (4IR)**[6] The development of 4IR-enabled military capabilities raises a critical analysis in the difference between **four important concepts that sit roughly on a continuum ranging from science to technology to capability to effect**.

<u>4 IR Technologies</u>

- *AI*
- *Robotics*
- *IoT and Cloud Computing*
- *Quantum Computing*
- *Blockchain*
- *Big-data Analytics*
- *Novel materials*
- *Additive manufacturing*
- *Bio Technology*
- *Smart Sensors*
- *VR & AR*
- *Energy Storage*
- *Space Technologies*

[3] *Barry Watts and Williamson Murray in Military Innovation in the Interwar Period (In experimentation: The Road to Discovery - Tom Greenwood and Jim Greer, 2018).*

[4] *Anna Ahronheim in 'The Jerusalem Post" on 27 May 21.*

[5] *Younis Dar in 'Eurasian Times' on 29 May 21.*

[6] *SIPRI Report on Emerging Military and Security Technologies.*

Moving from technology to capability requires a range of non-technological innovations while moving from technology to effect is largely a matter of effective implementation.[7] We need to appreciate that **'Uncertainty'** is a key characteristic of technological change and the process from the emergence of a technology to its having an impact on military capability is a long one. [8]

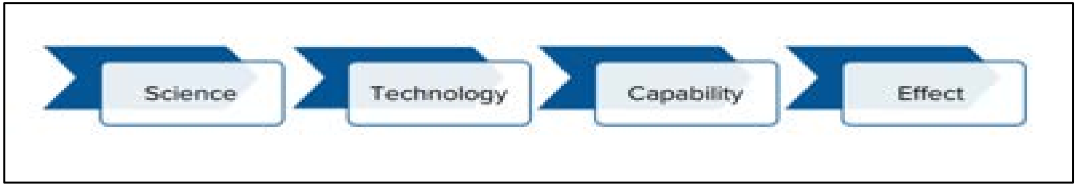


Figure 1: Continuum of Niche Military Technology Capability Development

Army Design Bureau: Focus Areas for AI Capability Development

Future combat outcomes will rest on the development and deployment of AI-based military capabilities and applications. Today, when we are looking at the contours of future warfare, the development of weaponry and other systems is being done keeping in mind the predominant play of AI.

The emerging battlefield environment will be dynamic, multi-dimensional, and technologically intensive, characterised by enhanced battlefield transparency, real-time connectivity, and extreme lethality. In order to maintain a technological advantage across key capability areas, certain AI use cases that are being developed by the **Army Design Bureau** through **the Indian industry, start-ups, and academia** are highlighted.

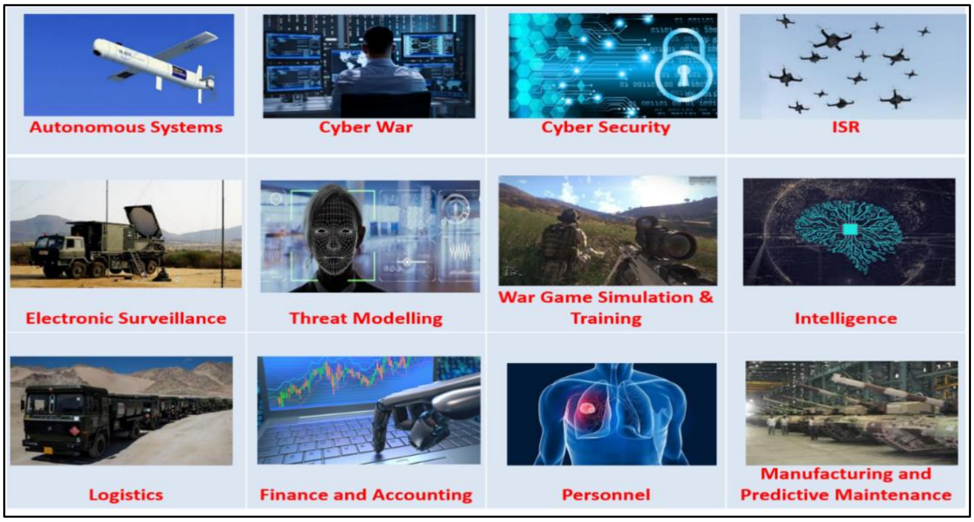


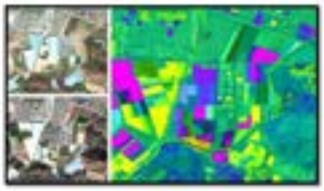
Figure 2: AI Domains

[7] *Atlantic Council Report on Emerging Technologies.*

[8] *Emerging Technologies and Military Capability Dr Andrew D. James.*

- **Natural language Processing** Development of **bi-directional English to Mandarin devices**, to develop ruggedised '**Wearable Translators**' which are custom designed to work in the edge.

- **Autonomous Systems** The use of AI for autonomous systems is a priority and the **Swarm Drone demo** witnessed during the **Army Day celebrations in 2021** was only a beginning. The applications for **manned unmanned teaming**, **Unmanned Ground Vehicles** (**UGVs) for Intelligence, Surveillance and Reconnaissance (ISR), Combat and Support applications** are being developed.



- **ISR Satellite and UAV imagery** analysis has huge potential and projects which will enable **automatic identification and change detection to enable event alerts,** will be extremely useful in defending our borders.

- **Threat Modelling** Use cases like aerial threats from drones and suspicious vehicle detection in Counter Insurgency are a focus area for development.

- **Logistics AI has tremendous utility in the field of military logistics**. It is a priority area for capability development in **Supply Chain Management** and **Inventory Control**.

- **Health** AI can play a predominant role in **health care**. A unique use case which focuses on identifying early indicators in the development **High Altitude Illness** and will help in **reduction in morbidity and mortality of troops** is underway.

Given the reality of short technological cycles, the rapid pace of obsolescence, and rising costs, it has become imperative today to align our AI technological aspirations with the civilian domain. *The **Army Design Bureau is matching the Indian Army's aspirations with what the industry can realistically deliver*** and thereafter progressing AI use cases through **multiple**

routes, including initiatives like collaborating with Defence Public Sector Undertakings (DPSUs) **like BEL in co-development of AI use cases**. Today, in all future **procurements and upgrades**, we are considering the incorporation of AI for all Qualitative Requirements (QRs).

Routes for AI Development

- *MAKE II*
- *iDeX (Def Innovation Org)*
- *Army Tech Board/R&D*
- *Tech Devp Fund (DRDO)*
- *Capital Procurement*
- *Collaboration with DPSUs*

Data - Strategic Asset for AI Capability

The ability to undertake Algorithmic Warfare heavily rests on computing technology, which is dependent on **Processing Power, Big Data** and **Cloud Technology**.[9] Our modernisation strategy needs to focus on **information with data at the core**. As we modernise, we will embrace **information-centric technologies**, recognising that it will be the application of combinations of technologies like *processing power, connectivity, machine learning and artificial intelligence, automation, robotics, autonomy and quantum computing* that will achieve the disruptive effect we need.

The Indian Army is **graduating from an '*era of log books*' to standard data management framework. The need of the hour is *to improvise on the fly to breed a data centric culture*, which will allow us to provide training data for AI Engines.** ***Today,*** capability exists to derive a trained AI model from general data, which can be '**rebuild and retrained**' by methodologies like '**transfer learning**' and ***techniques that convert unstructured data to the required format to train AI engines.***

AI systems will be the future enablers for the Armed Forces to operate in the future **Multi Domain Operations** where AI-infused autonomous weapon systems will become **Force Multipliers** and be *the* ***fulcrum around which Big Data will be turned into actionable intelligence and a decision advantage***. We in the Army realise that AI needs data for the development of intelligent machines, and ***we need to breed a culture in which we recognise and value data as a strategic asset!***

Army Design Bureau - Facilitating Experimentation and Risk

The 21st Century is a '**risk-on' environment** and does not reward timidity - if we remain cautious then we carry significant risks. **AI and Big Data** will have a disruptive impact on war fighting and we have to pay adequate emphasis on AI technologies that have dual use and are being driven by commercial entities and innovations. However, **predicting changes will be challenging, so we will have to take risk and accept some failures**.

[9] *'Algorithmic Warfare - Applying AI to War fighting' - Peter Layton.*

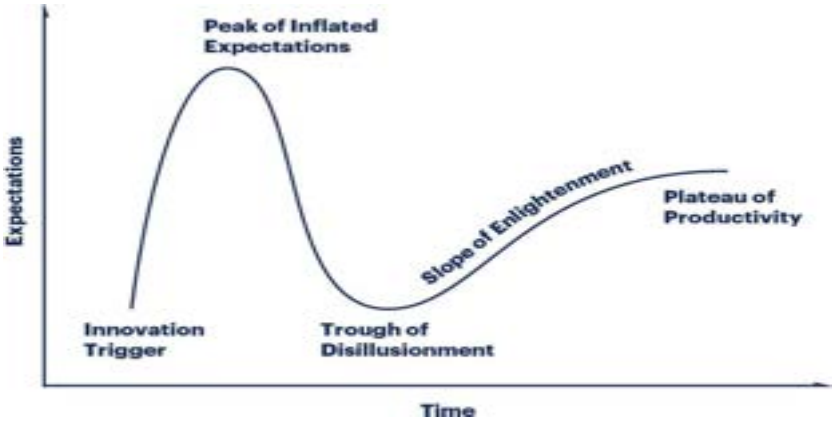


Figure 3: Hype Cycle - AI Innovations[10]

The above graph figure shows a pattern that arises with each innovation/ technology. *In the Army as we integrate AI, we will also have our breakthroughs in AI technology, buzz around the potential operational expectations, failure & frustration when use cases are delayed, experience benefits of commitment in few AI use cases and finally **Capacity Enhancement and Capability Development in critical AI domains***.

Technological development requires **experimentation and failure,** and there is a need to incorporate a **greater appetite for risk-taking into our innovation pipeline**. We have to realise that *technological development requires experimentation,* and in order to leverage technological advantage, there is a need to incorporate an appetite for risk-taking to support start-ups. There is substantial progress in ***R&D in niche areas along parallel routes*** so as not to lose time if one fails or stumbles, which would put the clock back a few years.

Army Design Bureau - Connecting Capabilities in AI

The Indian Army has been advocating the need for *increased self-reliance in the defence sector as only **indigenous technologies will be available during conflicts***. In order to take advantage of new government policies to foster a robust defence industry in emerging technologies/systems and realise our **Atmanirbhar Bharat Vision**, the **Army Design Bureau** *is at the forefront of all initiatives.*

Innovation is a key tenet to maintain operational advantage and to make defence an attractive innovation partner, the **Army Design Bureau** is finding ways to **share risk and reward**, **provide clarity on intentions** and make **contractual processes** less daunting in order to ***encourage and incentivize technology/***

[10] *Steinert, Martin. "Scrutinizing Gartner's hype cycle approach". Research Gate. IEEE Xplore, September 2021.*

innovations. The **Indian Army** is striving to ensure that we do not let go of **potentially impactful advancements in AI** languishing in the **'Valley of Death' between invention and adoption**.

The **Indian Army** established the **Army Design Bureau** as a single point of contact with all innovators, industrial houses, DRDO and budding entrepreneurs. The ADB has initiated a focused **Outreach Program in AI applications** with the **Industry and Academia** and significant progress has been made. Initiatives in getting **Industry, Academia, R&D establishments & Start Ups together** have started bearing fruits towards rapidly advancing technological needs. ADB is also looking at establishing mechanisms for **technical cooperation** and **co-development of AI Technology** through **strategic alliances**. The time is now apt where there is a need to **augment the private sector** with enabling provisions and facilities to make them the **starting blocks of R&D in AI**.

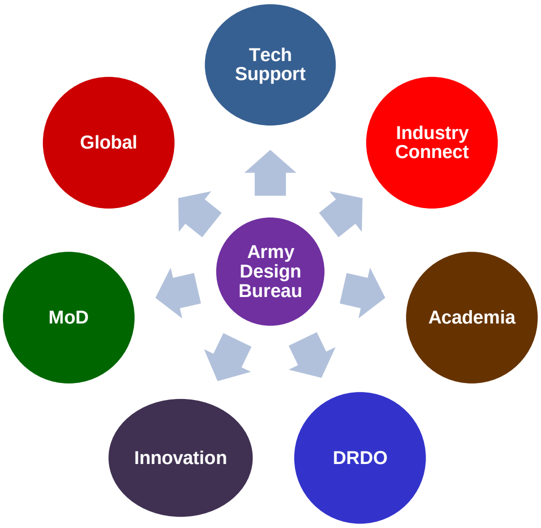


Figure 4: Army Design Bureau: Connecting Capabilities in AI

The rate of technological change, places a premium on **agility and responsiveness of the acquisition system** and the need of the hour *is to* ***gravitate towards an open model of defence innovation*** for faster infusion of technology into the Army. We are also looking to have a ***dedicated capability*** *that will* ***crystal gaze and identify how AI military applications will impact warfare and which AI domain is worth investing*** **in**. At the same time, we also need to ensure that if the **desired military capability** is not being met within our defined **timelines, resources and budget** then it is time to **rethink that technology/equipment concept**.

As the **R&D interface of the Indian Army**, the **Bureau is creating an innovation culture in AI** for startups through steps like facilitating **trials in field conditions**, establishing **Cells at Indian Institute of Technologies (IITs)** with

Service Innovators posted, reaching out at various forums like **ARTECH, DefExpo/AeroIndia** etc. This all has been achieved by working with an open mind with the academia, industry, in-house innovators, investors etc and having a critical, decisive, failure absorbing, agile and responsive technology development model.

Conclusion

The **Chief of Army Staff** has often highlighted the **impact of disruptive technologies in warfare** and emphasised that our current modernisation drive is focused on upgradations with **available indigenous technologies**.[11] Today, the ***domain of 'Non-Contact Warfare' is as important as 'Contact Warfare'***; and the virtual fight is assuming as much salience as the physical fight - that is where **AI will play a big role**.

The envisaged **contours and trends of future warfare in the era of AI** are evolving and we need to be agile to adapt to it. Timely infusion of technologies like **AI, Machine Learning and Big Data Analytics** is crucial, so that we are not left behind the technological curve. The **Army Design Bureau** is focused on **developing technologies and capabilities in AI**, by imbibing an **innovation culture** for harnessing emerging technologies and building an effective **Services-Industry-Academia interface**.

[11] *https://pib.gov.in/PressRelease, August 20.*

ARTIFICIAL INTELLIGENCE IN MODERN WARFARE: DRONE DETECTION USING MACHINE LEARNING

- Captain SBS Bhullar

Introduction

There have been numerous incidents of hostile or terrorist strikes using drones for surveillance. These are just a few of the numerous potential applications for these devices, so it's important to identify and monitor drones in locations where potential assaults can take place. These aircrafts have the capacity to fly both very low and very high[1]. These platforms provide a serious threat since they can move stealthily and unobserved. The drones consequently become the perfect tool for compromising security, putting lives in danger, inflicting damage or unauthorized entry into one's own area, as well as monitoring military activity.

Factors of Drone Detection

- **Appearance and Operation of Drones** Some drones include a light device on the lower half of their bodies, which can make detection more successful, especially in low-light situations. The way that a drone operates is another characteristic that sets it apart. The movement's goal is to take the drones from its stabilised position to its final destination, where it will be stabilised once more. The movement of drones is recognised for its predictability. The drone does not make any of these motions, in contrast to a bird gliding or flapping its wings.

- **Basic Approaches** Two categories-visual and acoustic can be used to categorise the fundamental methods of drone detection. Visual detection uses camera systems which capture a two-dimensional image on how the drone appears or moves, or perhaps on both. Acoustic approaches employ microphones[2] to capture acoustic signatures even if they are not visible.[3] Combining these two strategies will result in a hybrid

[1] *Norouzi Ghazbi, S.; Aghli, Y.; Alimohammadi, M.; Akbari, A.A. Quadrotors Unmanned Aerial Vehicles: A Review. Int. J. Smart Sens. Intell. Syst. 2016, 9, 309–333.*

[2] *Case, E.E.; Zelnio, A.M.; Rigling, B.D. Low-cost acoustic array for small DRONES detection and tracking. In Proceedings of the 2008 IEEE National Aerospace Electronics Conference, Dayton, OH, USA, 16–18 July 2008.*

[3] *Busset, J.; Perrodin, F.;Wellig, P.; Ott, B.; Heutschi, K.; Rühl, T.; Nussbaumer, T. Detection and Tracking of Drones Using Advanced Acoustic Cameras. In Unmanned/Unattended Sensors and Sensor Networks XI; andAdvanced Free-Space Optical Communication Techniques and Applications; International Society for Optics and Photonics: Bellingham, WA, USA, 2015; Volume 9647.*

detection system.[4] For instance, a radio-frequency jamming device, radio-frequency sensor, and video are all necessary components of an anti-drone system.

- **Object Characteristics** Algorithms for object recognition and classification are based on the properties of the objects being taken into account. This implies that the traits are determined by their behaviour and movement patterns in addition to how they look. The challenge of identifying drones in the sky centres on both the drones themselves and other items that could appear in the sensing area. One of a drones most glaring visual features is its form. From a tricopter to the octocopter, every form of drone resembles the others in their respective categories. A quadcopter is shaped like a square, a tricopter like an equilateral triangle, etc. Each drone also consists of a hard structure with recognisable visual traits. Depending on the number of propellers, the control board is often positioned in the centre of the structure and has three to eight arms. Each arm has a motor at the end, which is attached to the propeller. The most fundamental drone appearance pattern is this one, and it may be used on practically every drone.

- **Long Range Surveillance and Armed Drones** There is another kind of drone that has a different size, weight, and top speed than multi-rotor models. They are known as fixed-wing drones. Due to their characteristics, they are commonly used in applications like meteorology, quality inspection, and environmental and area mapping (with the capacity to further analyse and generate three-dimensional data). Additionally, important benefits include their flight safety and operational range.

- **Onboard Components** The inclusion of a variety of distinctive components is another way that drones are differentiated. Some drones, for instance, provide protection to the machine by enclosing the entire circumference in a ring. On the other hand, some components of other drones kinds are entirely accessible. On some drones models, an additional covering ring that is situated close to the machine propellers may be used. A camera is a standard feature on most drones. The drone's body can be modified to conceal the camera, minimising its external visibility. However, on drones with higher-quality cameras, the camera is mounted on the underside of the drones, where it is clearly visible. The existence of additional electronics helps to distinguish some drone types.

[4] *Shi, X.; Yang, C.; Xie,W.; Liang, C.; Shi, Z.; Chen, J. Anti-drone system with multiple surveillance technologies:Architecture, implementation, and challenges. IEEE Commun. Mag.* ***2018****, 56, 68–74. [CrossRef].*

Existing Methods of Image Processing

- **Contour Searching** Creating a curve that encloses the objects in the image is the main idea behind employing contours in image processing. This object bounding method can only be used successfully if picture preprocessing techniques like image smoothing and morphological procedures are used. The image must only be split into positive and negative regions,[5] whose edges can be visualised as delimited objects, in order to use contour searching. A contour is a collection of points that depicts a curve in a picture. These curves are shown as sequences, with each record storing information for the subsequent point on the curve. Due to the way it is structured, the contour searching function might produce a "contour tree." Thus, it can be determined which contours are child contours and which contours are root contours.[6]

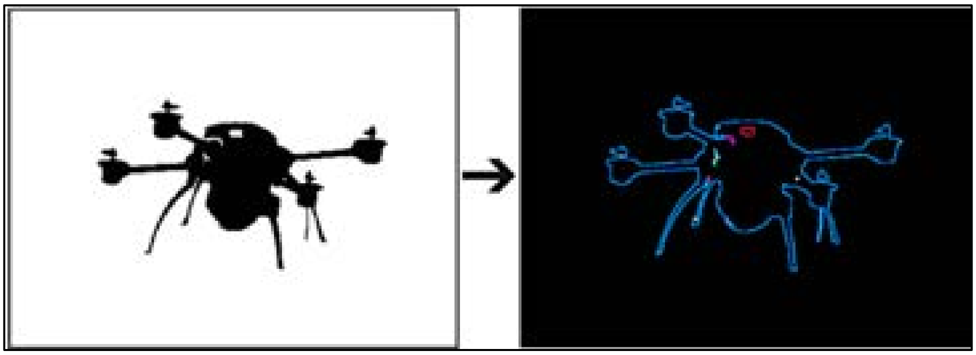


Figure 1: Contour Searching

- **Selective Searching** An algorithm called selective searching is one of the most successful ways to discover sub-regions in an image that contain an object. This method is based on three key assumptions[7]:-

  - ➢ **Capturing All Possible Scales in the Image** Selective searching employs a hierarchical approach to account for all possible object scales.

  - ➢ **Diversification** Selective searching does not utilise a uniform technique for a subregion search since objects in the

[5] *Bradski, G.; Kaehler, A. Learning OpenCV: Computer Vision with The OpenCV Library; O'Reilly Media, Inc.:Newton, MA, USA, 2008.*

[6] *Koniar, D.; Hargaš, L.; Štofan, S. Segmentation of motion regions for biomechanical systems. Procedia Eng.**2012**, 48, 304–311. [CrossRef].*

[7] *Uijlings, J.R.; Van De Sande, K.E.; Gevers, T.; Smeulders, A.W. Selective search for object recognition. Int. J.Comput. Vis. 2013, 104, 154–171. [CrossRef].*

studied area are subject to variable changes such as illumination, shadows, and other factors.

➢ **Calculation Speed** This approach is meant to speed up the computation performance because the phase of sub-region searching is merely a preparation for the object recognition step.

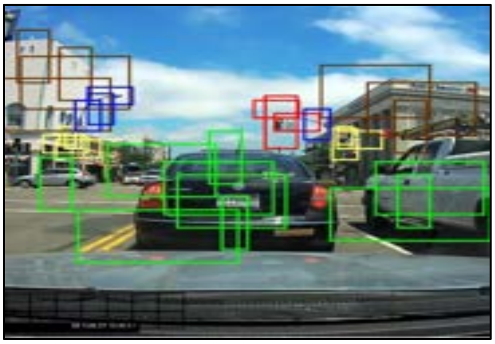


Figure 2: Selective Searching

- **Background Subtraction** One of the most basic techniques for identifying things in an image, particularly in terms of usability, is background reduction. The backdrop model must be accurately determined for this method to be effective. The known background components are then subtracted from the background model before it is compared to the current image. The foreground items that are not eliminated are almost certainly recent additions. Typically, any stationary or sporadically moving aspects of the scene are considered the background. Time-varying elements may be present throughout the entire scene, such as moving or static tree leaves. Systems that monitor objects with a static camera frequently include a module that removes the background to distinguish stationary objects from moving ones. Keeping the backdrop model intact is a crucial and challenging step in the background removal process. Situations where it is challenging to read or detect the background include uneven and variable lighting of the scene, changing spectral characteristics of the illumination, and, as a result, different colours of the objects, overlapping objects, different camera angles, and object variations within one category.

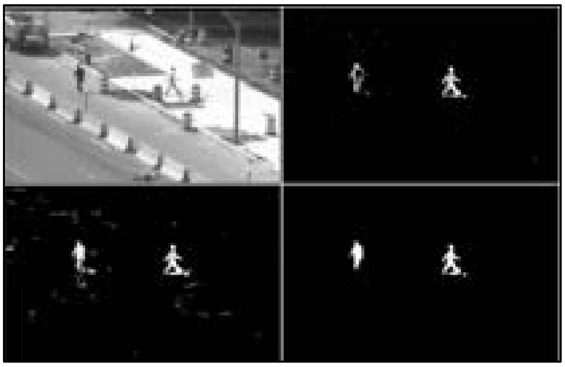


Figure 3: Background Subtraction

- **Support Vector Machines (SVM)** SVMs are appropriate for assigning items to N groups since they work by projecting data into multidimensional space. SVM looks for and determines the plane in which data is divided into groups. For example, if a vector of features has a dimension of 2500, SVM will represent it as a point in a space with 2500 dimensions. Talking about SVM working in vectors of features in 2D, Figure 4 shows the pictorial representation of SVM decomposition.

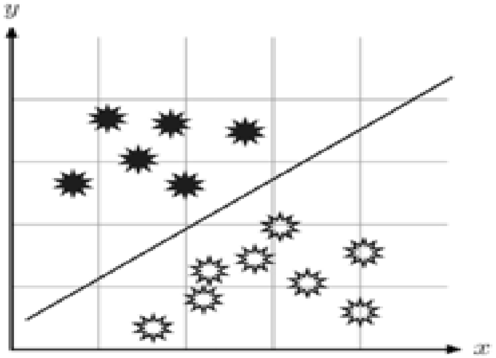


Figure 4: Support Vector Machine (SVM) Principle

- **Cascade Classifier (Haar-Like Features)** The classification of stable objects is the main purpose of this classifier. One may discuss the human body's figure or the face, for instance. The proportions of the human body, including the hands, legs, head, and other body parts, are generally the same as those of the face. The shape analysis of the drone demonstrates that it does not belong in this group of objects. For two main purposes, a Haar classifier is used to recognise objects[8]. One benefit is that, unlike when using insufficient training data, Haar-like features can accurately describe a region of interest. In comparison to raw pixels, Haar

[8] *Chen, Q.; Georganas, N.D.; Petriu, E.M. Real-time vision-based hand gesture recognition using haar-likefeatures. In Proceedings of the 2007 IEEE Instrumentation & Measurement Technology Conference IMTC2007,Warsaw, Poland, 1–3 May 2007.*

features might, depending on their characteristics, increase or decrease the variability of data that does or does not belong to a similar class.

The value of the light-to-dark ratio in a scene can be recognised and defined with accuracy using Haar characteristics. They excel at common computer vision problems including diverse scenes and changing lighting. The speed of this classification method is the second justification for using it, as handling Haar characteristics is thought to be quite effective.

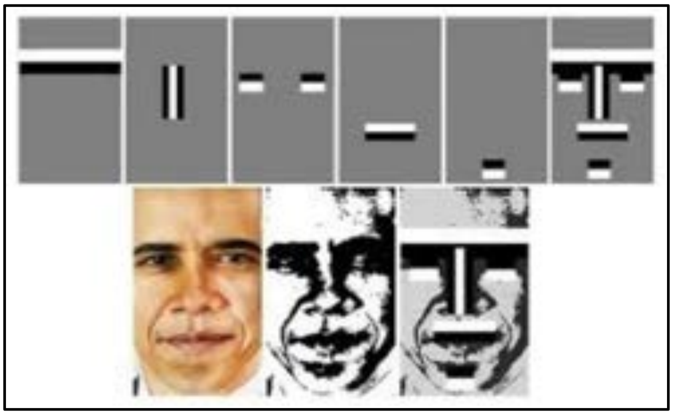


Figure 5: Cascade Classifier

- **Machine Learning and Neural Networks** It is a complicated situation when neural networks are used for object recognition. It requires a sizable set of data to represent the object that has to be recognised in order to employ a neural network for this task. Some neural network techniques also require data samples in which the target object is absent. The weights of the neurons are changed in response to an error that happens when neural networks classify an object, which causes the network's total error to decrease over time. This method of training is also known as the error propagation algorithm. When the network reaches the selected error threshold, network training is terminated. Another choice is to halt the training after a specific number of iterations. However, this method does nothing to address the general inaccuracy of the training.

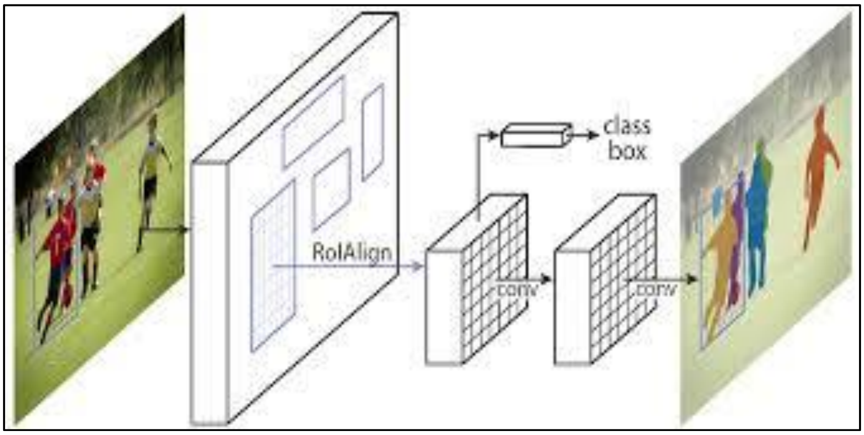


Figure 6: Neural Networks

- **Tensor Flow (TF)** Open-source machine learning platform TF is used in a wide range of applications [9 & 10]. A tensor is a multidimensional generalisation of vectors and matrices. By using n-dimensional coordinates of basic data types, TF represents tensors[11]. Google released this artificial intelligence-based solution in 2015 (for free use). The dataflow graph technique is used by TF to depict the calculations. Calculating units are represented by graph nodes. The edges of the graph, which are communicated between nodes as tensors (multidimensional arrays)[9 & 10], show the amount of data used or generated by the algorithm[12]. The architecture of this system makes it possible to deploy computation on a range of platforms, including multicore CPUs, graphics cards, and Tensor Processing Units, quickly and affordably (a computer system also developed by Google designed primarily for machine learning). A neural network must be trained using large number of calculations, in order to classify and recognise objects[9]. With the help of TF's features, users may efficiently execute computationally taxing activities like categorisation.

[9] *Abadi, M.; Barham, P.; Chen, J.; Chen, Z.; Davis, A.; Dean, J.; Devin, M.; Ghemawat, S.; Irving, G.; Isard, M.;et al. Tensorflow: Asystem for large-scale machine learning. In Proceedings of the 12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16), Savannah, GA, USA, 2–4 November 2016.*

[10] *Abadi, M.; Agarwal, A.; Barham, P.; Brevdo, E.; Chen, Z.; Citro, C.; Corrado, G.S.; Davis, A.; Dean, J.;Devin, M.; et al. Tensorflow: Large-scale machine learning on heterogeneous distributed systems. arXiv**2016**, arXiv:1603.04467.*

[11] *Creative Commons (CC) License. Tensors. Available online: https://www.tensorflow.org/ programmers_ guide/tensors (accessed on 28 April 2018).*

[12] *Creative Commons (CC) License. Graphs and Sessions. Available online: https://www.tensorflow. org/ programmers _guide/graphs (accessed on 28 April 2018).*

Machine-Learning Approach

- Finding a neural network that is effective at recognizing multi-rotor drones is the goal of using machine learning techniques. We have selected the TF machine learning platform for this since it is both readily available and cutting-edge. The aim is to select a suitable type of network, overtrain it using adequate network parameters, and then assess its success rate in classifying objects moving in the sky into the required classifications. The phases of the suggested solution are listed below:-

    - ➢ Preparing data for training and evaluation.
    - ➢ Selection of detection model.
    - ➢ Files for training/Big Data Analytics.
    - ➢ Training.
    - ➢ Export of the trained model to a frozen graph format.
    - ➢ Creating an application to test the detector.

- **Preparing Data for Training and Evaluation** A sizable data set is needed for neural network training to be successful. Photographs of the subject should be taken in various lighting, spatial, and other conditions. It's also crucial that the data shows every form of drone that has been defined in different contexts, rotations, and circumstances. The amount of data gathered ought to be enough to train the network and identify the target item. Annotations specifying the precise location of the object in the scene are necessary in addition to the data collected.

- **Selection of Detection Model** Since building new identification model would require a lot of time and resources to get the desired results, detection models trained on the "Common Objects in Context dataset" are to be used after evaluating the alternatives. Approximately 2,000 annotated photographs of various classes (such as aeroplanes, birds, kites, and so on) that can be used in instruction should be included in this collection. On the other hand, the drone is not one of them. Since all of the training parameters would be suited to distinct detection, developing our own detection model would probably be more reliable than using a model that has already been trained. These models each have a configuration file that serves as the model's training data source. It is crucial to keep the application in mind when selecting the model's input parameters. Models like Faster Regions with Convolutional Neural Networks (R-CNN) use the selective search strategy to find likely objects in a scene when the detector has to be more accurate. These models, however, give less importance to processing time. This model will be used in this instance of automated drone detection. On the other hand, Single Shot MultiBox Detector (SSD) models give processing time priority.

- **Files for Training/Big Data Analytics** There must be enough data for the model to be trained correctly. About 2000 drone images will therefore be acquired from freely available online resources. The next step is to create an annotation for each photograph that features the drone, which serves as the object of interest. 80 percent of the data should be used for model training, and the remaining 20 percent should be used for model testing. The publicly available labelling tool can be used to annotate and creates a file called an.xml. This file is used to extract the information that was used to create the Tensor Flow Record (TF Record) file. The TF training library uses a simple binary file for this purpose. It is thereby housed in a single memory block, enabling quicker data access. A.csv file is used to save the data. This file displays the name of the file where the drone object is placed, as well as the object's height, width, class name, and coordinates.

- **Training** The training script was provided by the library's creators and can be found in the official Github source. An average of one second was needed to complete one training step (using TF in Google Colab Pro Plus with GPU support). After a total of 5,000 steps, a model with enough reliability and viability can be produced (about six training days).

Conclusion

- The TF library was used to create a reliable multi-rotor drones detection system. The Common Objects in Context dataset was utilised for this. In ideal conditions, a successful detection rate of 99.3% was attained. The proposed detection principle was found to work well in the tested scenarios. The trained detection system performed well in almost every scenario that it was tested in. An issue did not appear until there were objects with features shared with objects of another class. The detection model's statistical analysis revealed that the detection rate in this instance was only 61.7 percent. Since birds should also be unnoticeable, a different detection model was used. This model was able to discriminate between drones and birds, two different types of drones. The tests showed that the detector was much more successful at detecting items if it was trained on many things.

- This leads us to the conclusion that the presence of items with identical characteristics is the biggest obstacle to drone detection. A bird, an aeroplane, a parachute, or a paragliding wing are examples of something like drones. These things are less common, therefore, a large dataset could be used to train the detection model. This kind of detector may be even more efficient than one that has taken two classes of training. On the other hand, a detection rate of 97 percent of detectors trained in two classes is adequate for basic security applications. The system's reliability and success can be compared to those of a regular human observer. Based on the provided data and settings, this paper suggests a practical approach for multi-rotor drone detection under ideal flight conditions. Future research using this methodology might focus on other instances where the detector could act as both a common observer and a complex detection system that can be applied in challenging settings.

COMBAT “AI-EFFECTIVENESS”: ROLE OF ARTIFICIAL INTELLIGENCE IN COMBAT EFFECTIVENESS

- Colonel G Praveen, SM

“Extensive opportunities in Artificial Intelligence (AI) and Data Analytics calls for the Indian Armed Forces to prepare a perspective plan to embrace these technologies and place greater thrust on training its personnel to learn these technologies and also reskill service and civilian personnel with advanced training and learning management systems”.

- General MM Naravane

Introduction

The battlefields of the future will be dynamic, chaotic, unpredictable, and uncertain. In such interlinked battlefields in multiple theatres and domains, commanders would be sifting through a multitude of data and striking a balance between their leaders and subordinates for the timely provision of information, decisions, and feedback. In such a time-constrained operational environment obscured by the Clausewitzian fog of war, effective and unbiased decision-making by a leader will be a battle-winning factor. Capabilities offered by the latest technology will aid decision makers and troops in various domains.

The famous Observe, Orient, Decide, and Act (OODA) loop will have technology-assisted inputs at each stage of Observe, Orient, Decide, and Act. Faster processing capabilities of Big Data and inferential analytics and seamless integration of inputs by machines would simplify the complexities associated with the five Vs of Big Data, ie, Volume, Velocity, Veracity, Value, and Variety. A complex dynamic of man-machine interaction is the future, which would mandate increased trust in a machine in a similar manner to that between two soldiers in the same team. Human machine teams and xAI, or explainable Artificial Intelligence (AI), are working towards improving this **"Trust" factor,** which would impact Combat Effectiveness.

Some Definitions

AI is a branch of computer science that brings together multiple disciplines with the aim of creating smart machines-devices and systems capable of performing complex tasks that often require human intelligence, but in a manner that equals or exceeds the capabilities of humans. Essentially, the aim is to make intelligent machines that can replicate human behaviour and intelligence in every sense. Howard Gardner proposed eight types of intelligence and a ninth one called existential intelligence; a machine which is equipped with at least one of them can be called intelligent. As we are aware, amongst the three types of AI, present capability is in the first level of Weak AI, where a machine or a system like Alexa or Siri can perform a series of predetermined and defined activities repeatedly. In day-to-day life, the interaction is with one of the sets or subsets associated with AI, like Big Data, Machine Learning, etc, even though all are loosely termed as AI.

The essential effect of AI will primarily be on the **Combat Effectiveness** of the Armed Forces. Combat Effectiveness is defined as the readiness of a military unit to engage in combat based on behavioural, operational, and leadership considerations[1]. It is a combination of tangible and intangible factors like force (numerical), equipment availability, morale, leadership, training standards, etc. In other words, combat effectiveness is the capacity of a military force to succeed in its mission, or task. Since the components of combat effectiveness are quite a few, the paper will focus on two major aspects; Decision Making and Training.

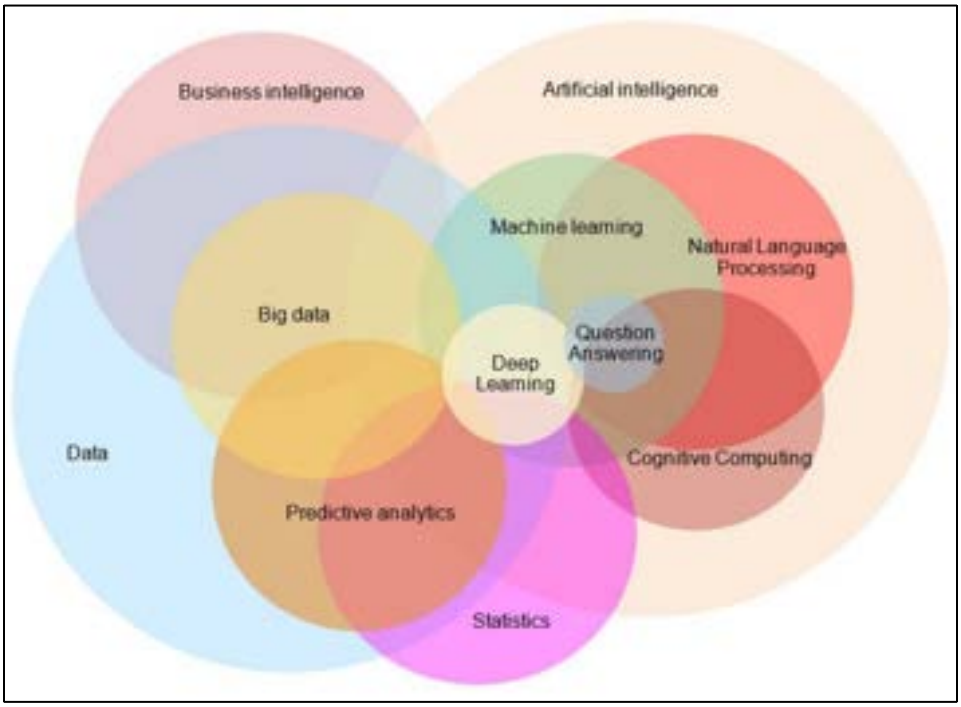


Figure 1: Specturm of AI

Developments in AI

Countries like the United States of America (USA), China, and Russia have made rapid progress in the realm of AI in various domains, including that of military capability. India has undertaken a series of steps to develop and exploit the capabilities of AI, which include setting up a national level structure and Centres of Excellence at various institutes. The Defence AI Council and the Defence AI Project Agency have been established, and efforts are being made to

[1] *Encyclopedia Britannica at https://www.britannica.com/topic/combat-effectiveness.*

identify and develop projects across multiple domains. Ten Centres of Excellence and two dedicated laboratories of the Defence Research Development Organisation (DRDO) are focused on identifying and developing key technologies and applications. The Indian Army has set up the AI Centre of Excellence at Military College of Telecommunication Engineering (MCTE), Mhow and added AI-oriented curriculum at various training institutes.

Even as new technologies are adopted, ethical and moral concerns, including concerns about privacy, need to be duly factored in. The subsets of Machine Learning and Deep Learning require huge datasets for establishing a referential framework. In the present setup, with levels of confidentiality and limited sharing and recording of events, having a viable training dataset and an algorithm that can cater for multiple contingencies becomes a challenge. The famous "Death Algorithm" concept, wherein an algorithm for a self-driving car should save the occupants or a pedestrian in case of the likely occurrence of a crash, gives one word datasets insights into the challenges in devising AI systems.

AI can be used to exponentially improve performance in the fields of Training, Surveillance, Intelligence Collation, Logistics (including Supply Chain Management), Cyber Security, Arms & Ammunition, etc. A Manekshaw Paper on "Leveraging AI for the Military" mentions the domains of situational awareness, lethality, HR, training, survivability, cyber, Information and Electronic Warfare (EW) and mobility in which AI can focus on.[2] The present thoughts are, however, silent on three important aspects which must be kept track of while incorporating the various facets of AI; Bias, Trust and Interoperability.

Decision Making and AI Assisted Debiasing

Cognitive biases in human decision-making and judgement are well documented. Daniel Kahneman spoke of the System 1 and 2 types of brain, wherein the fast and intuitive System 1 attempts to hijack the slow and analytical System 2 brain, thereby leading to an increased propensity for mental shortcuts or heuristics and thereby biases. Though there are ways and means for removing and mitigating biases (debiasing), the awareness of a bias does not always result in the removal of bias from the decision loop. What is more damaging is the lack of knowledge of implicit biases that normally occur when the brain adopts one of those shortcuts (heuristics) in a limited time window under conditions of uncertainty and risk. In addition to having policies and processes at various levels in the organisation for systematic debiasing and having feedback mechanisms, there is a need to adopt "Data Driven Decision Making." This would entail common data sharing platforms and standard algorithms that can decipher inputs and analyse both structured and unstructured data to offer insights to a leader or

[2] *Jadhav, Ajinkya, Leveraging AI in the Indian Army, Manekshaw Paper, 10 June 2021, available at https://www.claws.in/publication/leveraging-artificial-intelligence-in-the-indian-army/ accessed on 15 February 22.*

decision-maker at various stages of the decision-making process. Biases can be mitigated in the "Observe" phase of the OODA loop by having machines synthesise large volumes and varieties of inputs to offer a collated intelligence picture. In the "Orient" phase, when a decision-maker is going through the "sense-making" paradigm of the decision loop, a collated and synthesised set of analytic inputs will help in framing and orienting in a faster timeframe. The "Decide" phase duly supported by a machine learning based Decision Support System can supplement the experience and intuition of a leader to arrive at a better decision in a faster manner, which is essential in a futuristic multi-domain battlefield with no clear boundaries in the cognitive and physical domains.

On the other hand, increased dependence on AI-enabled systems could further amplify inbuilt biases in the algorithm or existential biases in the training datasets. Even though there are checks and balances to systematically review algorithms for bias and to prevent implicit biases from occurring due to training on incomplete datasets, the probability and likelihood of human cognitive biases getting incorporated into the design stage cannot be ruled out. Though some argue that a biased algorithm will still suggest a more balanced "Course of Action" than a biased human decision maker, the aspect of "debiasing" deserves far greater attention than what is being given today. It can be said that both humans and machines can enter into a "**mutually beneficial debiasing strategy**" to improve the quality of decision-making.

Human-Machine Teaming and Trust

In any fighting unit or subunit or what could be called a team, each team member, over a period, having trained together, is aware of the strengths and weaknesses of the other. Camaraderie and *esprit de corps* amongst the team members finally make the team a combat-effective, cohesive unit. Much more than anything, a key factor amongst the team members is "trust," which gets validated when the team has to operate under enemy fire, wherein the life of one is dependent on the covering or supporting fire from the other member or mate. The introduction of a machine, a faceless, emotionless member into such a cohesive unit, impinges on the trust factor. Human beings traditionally resort to anthropomorphism, which is a habit of ascribing human emotions to other beings, which is commonly seen at homes with pets. A machine that would exhibit human-like features, habits, and emotions has greater chances of winning over trust in a team.

Another trust-winning factor could be transparency in actions. As compared to a teammate and his or her known likely reactions and outputs under various conditions, the output from a machine is more mechanical and devoid of any explanation as to why that output was suggested. XAI, or explainable AI[3] is one

[3] *Explainable AI (xAI) techniques, utilizing abstractions or explanations that provide the user insight into the AI's rationale, strengths and weaknesses, and expected behaviour, can supply the human*

field wherein the actions and deliberations undertaken by a machine will be more transparent to the other teammates, which in the long run is expected to increase the trust factor, which is an important element for battle winning and thereby being combat effective. In future warfare scenarios wherein, enemies will target the cognitive domain as part of the Information Warfare spectrum, this factor will become a key ingredient.

Jointness and Interoperability

For a Battalion or a Regiment or a Ship to be truly combat effective, it must have a minimum basic awareness of the others will to fight or operate. At a point wherein the Services are debating the implementation of Theatre Commands and exploring more joint avenues to operate together, the AI-assisted technologies of Augmented and Virtual Reality offer the participants a more integrated chance to train together. The scenarios and settings can be dynamically changed as per evolving strategies and weapon profiles of the adversaries, while own processes can be systematically addressed through such joint simulations and AI-assisted wargames.

The diminishing number of field firing ranges, ever expanding urban landscape along the periphery of traditional training areas, cost-cutting measures, etc can be succinctly overcome by adopting the AI assisted Joint Wargaming and Simulation. This methodology will bring in much needed awareness, dynamism, and a purple mindset at various levels of leadership. AI-enabled systems can also assist in identifying key personnel to operate specific platforms right from recruitment and training stage which will at some stage obviate the biases or prejudices that are found in identifying the right man/woman for the job.

AI-Effectiveness in a Battalion/Regiment

Researchers usually consider a set of tangible and intangible factors to measure combat effectiveness: army size, physical and mental prowess of troops, leadership, the quality of arsenal and tactical aptness in using weaponry, logistics, intelligence, medical care, knowledge of topography, etc. Measuring the intangible factors with high accuracy is difficult, and it is the synergy of many contributing factors that determines combat effectiveness, and researchers cannot eliminate perceptual, perhaps non-measurable elements[4]. Despite having details of weapons systems, it is impossible to use reliable quantitative criteria to evaluate the actual skills of military personnel in using those systems, or the cumulative

teammate a representation of the collaborative robot's behaviour policy and may assist in the human teammate's ability to predict and develop a collaboration plan. Available at https:// proceedings.neurips.cc/paper/2021/file/05d74c48b5b30514d8e9bd60320fc8f6-Paper.pdf accessed on 15 March 2022.

[4] *Value and Methods of Measuring Combat Effectiveness: A New Approach, available at https://assets. researchsquare.com/files/rs-408649/v1_covered.pdf?c=1631861993*

effect of weaponry efficiency and tactical efficiency. The Lanchester model[5] used for combat modelling, only considers numerical changes in forces deployed, but the troop strength must be complemented with skills and morale to estimate the combat effectiveness of an army. In a traditional attack and defence model, certain research also focuses on the capability of a unit to hold or capture ground as a measure of Combat Effectiveness.

Existing System Many factors, including camaraderie and cohesion, play a major role in the Combat Effectiveness of a unit. Presently, a yearly Administrative Inspection certifies a unit as "Fit for War" after checking a series of parameters of performance, including firing, battle preparedness, running standards with loads and level of subunit leadership, to name a few. During actual operations, which often occur in some counterinsurgency settings, Combat Effectiveness of a unit is taken as the capability of that unit to achieve success in any operation, which effectively has many sub domains, including area domination, intelligence awareness and collation, zero fatalities, etc. Depending on the terrain and place of operations, the quantification of combat effectiveness also varies. Though the intangible factors can be quantified to a large extent using various models, aspects like skill, morale and leadership remain quantification challenges. Even standards of training, which can be measured at laid down levels, fail to comprehensively quantify or capture the Combat Effectiveness of that unit.

AI at Battalion/Regiment Level At various levels and stages, AI and its associated tools and capabilities can be introduced at various levels and stages to both enhance and measure skills and standards, while simultaneously being amenable to further modifications as per dynamic demands of an ever-evolving battlefield and operational challenges. Mental and physical immersion though Virtual Reality (VR) and Augmented Reality (AR) combined with haptic technology[66] can add realism and dynamism to training, while simulations and wargaming models can reduce costs, improve adaptability, and improve inter-operability. VR can be used in the domains of education, medical, and combat training. The COVID pandemic saw large scale increase in online teaching platforms, with many educational institutions using the available technology to make learning more immersive. Complex concepts could be explained using 3D online models, while VR systems could help soldiers achieve multiple levels of education and skill development. Healthcare aspects including combat medical care can be better learnt and practised by all soldiers. Using the capabilities of Natural Language Processing, conversational AI systems can be set up that can engage a soldier on various issues ranging from basic documentation, aspects of

[5] *https://www.maa.org/press/periodicals/loci/joma/an-interactive-use-of-the-lanchester-combat-model-the-lanchester-combat-model.*

[6] *https://www.smithsonianmag.com/innovation/heres-what-future-haptic-technology-looks-or-rather-feels-180971097/.*

field craft and tactics, basic medical clarifications, tenets of Professional Military Education (PME), etc.

Anthropomorphising, or the human tendency to attribute human feelings and emotions to other beings, is both a boon and a bane. While it helps in developing an intimate bond with an otherwise emotionless machine, it could have a psychological impact similar to how it was described in the movie "Her", where a lonely human falls in love with a machine which is replicating human emotions based on backend neural networks and reinforced learning. ELIZA, a psychotherapist chatbot developed by Weizenbaum in the 1960s, replicated responses based on key words typed in by the patient but had the capability to reduce stress levels as the human beings felt they were conversing with someone who paid attention to their thoughts. Though the capabilities on offer by such systems which can replicate human responses are tremendous in terms of trust building and stress busting, the psychological aspects need to be factored in.

Capability Spectrum Many articles have already identified and suggested the domains in which AI can make an impact in the Armed Forces. Situational awareness, lethality, Human Resource (HR) management, training, survivability, cyber, information and EW and mobility are some of them. What needs to be simultaneously developed is in the psychological domain by agencies like the Defence Institute of Psychological Research (DIPR) to analyse the impact and evolve mitigation measures regarding the impact of AI systems on a soldier's psyche.

The Future

The moot point is about what will actually change at Battalion/Regiment level. Will it change the way we work and operate presently? There will indeed be paradigm shifts in the way we work and operate in terms of efficiency and transparency. There will also be concomitant demand for change management and technological skill enhancement. There is a need to set up **Human-Machine Interface Teams (HMiT)** at each level, which will facilitate this transition. Starting from Services Selection Board and Recruitment Centres, AI-assisted software can help in identifying individuals with the right aptitude and uptake to work in such human-machine interface teams. These teams can then work in synergy to identify actionable sections or domains at each level and then collaborate with various Centres of Excellence to produce need-based machines or systems.

The capabilities of AI and the roles of all associated systems of AI need to be introduced as part of **PME at tri-services level**. An integrated multi-domain fighting force, which is the demand of future battlefields, cannot have commanders who are unaware of the capabilities that these emerging technologies can offer. PME needs to address these requirements at the level of officers, JCOs, and troops. Even as agencies like DIPR devise psychological measures to embrace machines and systems, there is a need to revamp the present **training**

methodology at unit/subunit level, which focuses on Mission Essential Tasks (MET) and Mission Essential Task Lists (METLs). The HMiT can identify various stages where technology can enhance and augment success in operations or for various tasks. After all, success in a task is one of the prime determinants of Combat Effectiveness.

Even as AI in its present form transforms from "Weak AI" to a stronger variant with deep learning, neural networks, etc, concepts like "artificial intuition" and "quantum cognition" will gain more traction. A future-ready force preparing for multi-planar, multi-domain operations has to be **Combat AI-effective** and this can become a reality through systematic, sustainable, incremental yet parallel, nudges at various levels of the organization. Trust amongst the members of a team is essential, though an intangible factor like morale needs to transcend to human-machine trust with adequate safeguards against systemic and implicit biases.

Bibliography

1. *Thomas B Allen, War Games: The Secret World of the Creators, Players, and Policy Makers Rehearsing World War III Today: New York, McGraw Hill, 1987.*

2. *Kritika Roy, Advances in ICT and the Likely Nature of Warfare: KW Publishers, 2019.*

3. *Leonard Mlodinow, Subliminal: Penguin, 2012.*

4. *Daniel D Wheeler, Irving L Janis, A Practical Guide for Making Decisions: The Free Press, 1980.*

5. *Ed. GJ David Jr, TR McKeldn III, Ideas as Weapons: Pentagon Press, 2009.*

6. *Mehrabi, Ninareh and Morstatter, Fred and Saxena, Nripsuta and Lerman, Kristina and Galstyan, Aram, A Survey on Bias and Fairness in Machine Learning, 2021 available at https://dl.acm.org/doi/abs/ 10.1145/3457607 accessed on 14 Feb 2022.*

7. *Implementing a Software Modeling - Simulation in Military Training, available at https://www.proquest.com/scholarly-journals/implementing-software-modeling-simulation/docview/881226834/se-2?accountid=139958.*

8. *Tomalin, M., Byrne, B., Concannon, S. et al. The practical ethics of bias reduction in machine translation: why domain adaptation is better than data debiasing. Ethics Inf Technol 23, 419–433 (2021). https://doi.org/10.1007/s10676-021-09583-1.*

9. *AI Is Biased. Here's How Scientists Are Trying to Fix It, 19 Dec 2019 available at https://www.wired. com/story/ai-biased-how-scientists-trying-fix/.*

10. *Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making, available at https://royalsocietypublishing.org /doi/ 10.1098/rsta.2018.0087 accessed on 20 Mar 2022.*

11. *National Strategy on AI available at https://indiaai.gov.in/documents/pdf/National Strategy-for-AI-Discussion-Paper.pdf accessed on 14 Mar 2022.*

12. *Rohan Paleja, Muyleng Ghuy, Nadun R. Arachchige, Reed Jensen, Matthew Gombolay, The Utility of Explainable AI in Ad Hoc Human-Machine Teaming, available at https://proceedings.neurips.cc/paper/2021 /file/05d74c48b5b30514d8e9bd60320fc8f6-Paper.pdf.*

13. *Williams, M. B. S., 2010. Heuristics and Biases in Military Decision Making. Military Review, 5(September-October), pp. 40-52.*

14. *Saini, C. S., 2008. Role of Intuition in Military Command. Journal of Defence Studies, 1(Winter), pp. 75-87.*

15. *Jr, M. P. T., 2014. Shaping and Adapting : Unlocking the Power of Colonel John Boyd's OODA Loop. [Online] Available at: http://www.pogoarchives.org/straus/shaping-and-adapting-boyd-20150422.pdf[Accessed*
15 July 2021].

16. *Jung, C., 1971. Psychological Types. First ed. New Jersey: Princeton University Press.*

17. *Kahneman D, S. P. T. A., 1982. Judgement under uncertainty : Heuristics and Biases. First ed. Cambridge: Cambridge University Press.*

18. *Kahneman, D., 2011. Thinking Fast and Slow. First ed. New York: Farrar,Straus and Giroux.*

19. *Kahneman, D., 2012. Thinking Fast, Thinking Slow [Interview] 2012.*

LEVERAGING ARTIFICIAL INTELLIGENCE (AI) FOR FURTHERANCE OF MILITARY OPERATIONS IN THE INDIAN ARMY

- Brigadier S Balakrishnan and Lieutenant Colonel Bikash Biswakarma

> *"Computers will overtake humans with AI within the next 100 years. When that happens, we need to make sure the computers have goals aligned with ours".*
>
> \- Stephen Hawking

Introduction

Artificial intelligence (AI), a niche technology is rapidly growing and is capturing the attention of commercial investors, defence intellectuals, policymakers, and international competitors as evident by its wide application in virtual assistance in the form of "Alexa" to Information Warfare (IW) in the form of 'Deepfake' in recent Russia-Ukraine conflict. Even in the Approach Document published by NITI Aayog on "**Responsible AI for all**" in February 2021, it has been brought out that the National Strategy for Artificial Intelligence (NSAI) has successfully brought AI to the centre-stage of the reform agenda of the Government by underlining its potential to improve outcomes in sectors such as healthcare, agriculture, and education. Furthermore, the NSAI underlines the need for a robust ecosystem that facilitates cutting edge research to not only solve societal problems and serve as the test bed of AI innovations, but at the same time enables India to take a strategic global leadership by scaling these solutions globally. AI is acknowledged to be one of the foremost dramatic technological game-changers of our age. It is also referred to as Industrial Revolution 4.0, and the Government of India has formulated a Task Force to prepare our country for the upcoming revolution. Defence and security will not be an exception.

Leveraging AI

Leveraging upon AI could fundamentally change the character of warfare and cause a shift in focus from **'information'** to **'intelligence'**. Assuming that IA can leverage the opportunity by the year 2025, then the time to incubate and induct AI is now, as the gestation period for project development in such niche technology is phenomenal. Therefore, a review of certain *pre-requisites, enablers*, and *implementation challenges* in the context of AI would be appropriate. Elaboration follows as under:-

- **Pre-requisites** The pre-requisites include infrastructure, datasets, organisational structure, matching financial support and enabling policy framework.

- **Enablers of AI** Enablers of AI include *inter alia* Government initiatives to promote AI, a robust and participative data sharing culture, a deep pool of national talent in science and technology, scope for Public-Private-Partnership (PPP) and an indigenous R&D/industrial base. Strategic partnerships for transfer of technology/knowledge coupled with spread of digital awareness will only act as catalysts.

- **AI-Implementation Challenges** A number of challenges besiege the early implementation of AI in the Indian Army (IA). These include the promulgation of an enabling policy framework; organisation and HR issues; technology base and infrastructure to include datasets; and the need for synergy amongst stakeholders. AI applications will require sustained R&D, handholding by the industry and academia, and will involve substantial gestation periods for tangible yields. Also, like any other exciting but nascent technology, AI too will course through inherent uncertainties and the associated risk of failure, which needs to be accepted.

Implementation Strategy

- Army Headquarters Computer Centre (AHCC) to take on large projects with extensive R&D, field trials and finally implement AI solutions pan Army. The organisation will be responsible to define problem statement, working out scope and reach of projects and carry out R&D.

    ➢ **HR Management** It is necessary to empower the proposed organisation created under the Directorate General of Signals for AI implementation with quality manpower. Talented individuals can be identified and trained with advance courses to enhance their capabilities. Post-graduation in AI has already started and officers are being trained by premier institutes like the Indian Institute of Technology (IIT). It is necessary to create a pool of talented experts to work on specific projects with timelines. The provision of hiring and employing a few talented individuals from outside the IA should also be enabled.

    ➢ **Creation of Infrastructure** Having created an organisation with talented manpower, it is necessary to develop infrastructure for undertaking AI Projects. Following issues need to be addressed while creating top-class infrastructure (some of it is already in the pipeline):-

        ❖ **High Powered Computing Lab** AI engines and algorithms require high processing and computing Graphical Processing Unit (GPU). It will be necessary to create a facility with number of high powered engines. A central facility should be created for all R&D and field trials.

❖ **Data Management** Data forms the building block for any AI application. The dataset must be tru, authentic, possess high degree of integrity to provide tangible inputs to the AI enginge. Different applications like MISO, CICG, FPMIS and similar other tools generate and store enormous data, which can be used for the development of AI engines. However, there is a need to harmonise the available data through a well-defined framework and make data available with the "right" data flowing out as the Single Source of Truth (SSOT) at the right time in a secure manner to the rightful user. Various systems, such as IA Certifying Agency (IACA) for token-based access control and Identification and Authentication Management (IAM) for role-based access control, are also in place or in the pipeline to ensure the authenticity, confidentiality, and integrity of data. Once Network for Specturm (NFS) is implemented, all data management will be handled by the one Central Data Centre (CDC) and the six Regional Data Centres (RDCs). Data will reside at the CDC and RDCs in a distributed manner and will be accessed over the NFS backbone. The proposed management of data in IA for AI application is depicted in Figure 1.

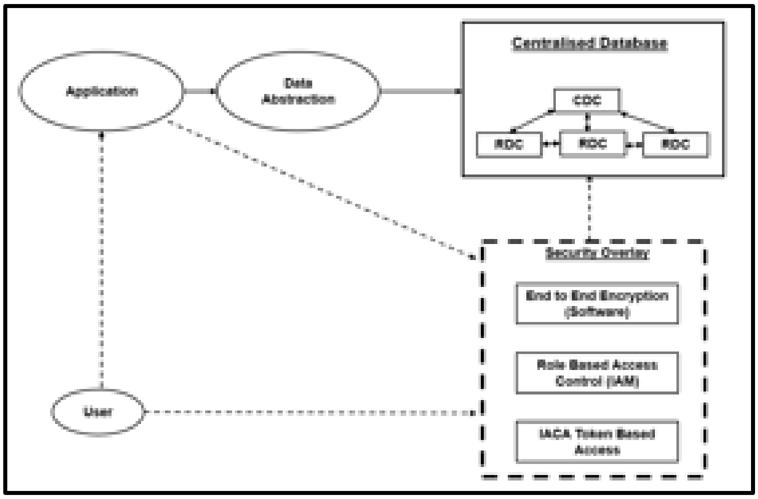


Figure 1: AI Application to Ride Over Complete Database

Areas for Project Development in AI

Intelligent Decision support system (IDSS) The DSS inherently provides technical insight and prowess, primarily through a software-related interface. It provides military commanders an excellent tool for dealing with initial checks of decision making along with comprehensive assistance later in analysing key concept data filtering and structuring, relieving the human element of the mundane, routine, and repetitive tasks. When AI techniques are utilised in the development of alternatives, the resulting system is referred to as an Intelligent Decision Support System (IDSS). AI attempts to mimic human decision-making in some capacity. Advances in AI have shown significant promise in assisting and improving human decision-making, particularly in real-time and complex environments. With the advancement of AI related technologies, the AI powered DSS will, to some extent, venture into the autonomous region. Thus, the system can take independent decisions in a limited way. This has the added advantage of compressing the OODA loop.

AI tools such as Fuzzy Logic, Case-based Reasoning, Evolutionary Computing, Artificial Neural Networks, and Intelligent Agents, when combined with DSS, provide powerful aids in solving difficult applied problems that are often real-time, involve large amounts of distributed data, and benefit from complex reasoning. One way of looking at intelligence is that it is primarily concerned with rational action, so that an intelligent system would take the best possible action in a situation. IDSS could be effectively implemented in IA at all verticals to assist in decision making during fog of war.

Command and Control (C2) With the growing complexity of military C2 in the future battlespace, modelling the C2 is recognised as one of the most challenging areas. AI will play a vital role in optimising the complexity of command and control models, which involve reasoning, decision-making, planning and other high-level intelligent behaviour. In recent years, AI has played an increasingly important role within modelling C2, which includes the following: -

- Representing C2 domain knowledge.
- Providing ‘intelligent’ simulated environments.
- Facilitating the coordination and communication of agents.
- Determining the validity and reliability of model.
- Interpreting simulation results.

C2 modelling is knowledge intensive. The knowledge includes command rules according to regulation of battle, the higher level of command orders, information of battlefield, weapons and equipment manuals, domain-related documents and experiences, and related experimental data etc. Agent-Based Modelling (ABM) is a recent simulation modelling technique that consists of modelling a system from the bottom-up. Such a bottom-up approach captures the interactions taking place between the system’s constituent units. The primary benefits of using agent models are that emergent behaviour can be produced from the interactions of individual entities, that are easy to manipulate and thus can cover a large portion of the analytical landscape, and that they eliminate the logistical headaches associated with conducting human-based experiments. AI, agents include reflex agents, goal-based agents, utility-based agents, and learning agents, etc. The structure of the command entity is shown in Figure 2 that captures the key C2 processes.[1]

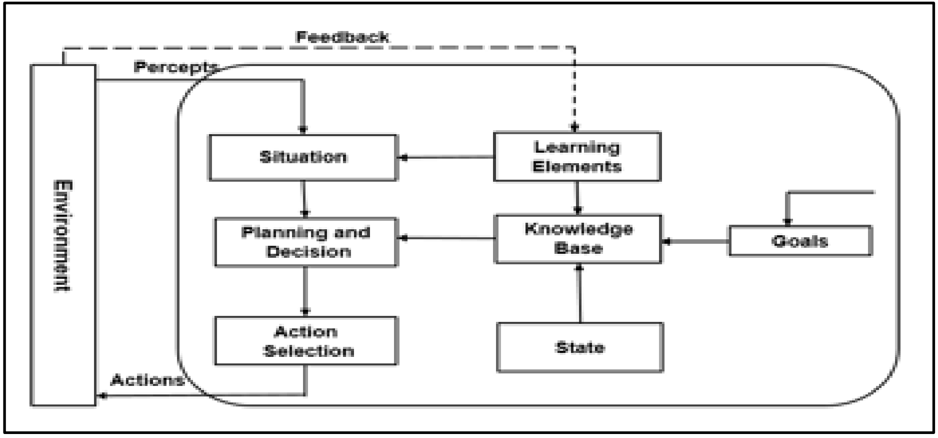


Figure 2: Structure of Command Entity

With the development of machines with human-like intelligence, more advanced AI techniques will be applied in the context of C2. In this way, IA can take forward research initiatives and, in collaboration with academia and industry, implement AI models for C2 structure. In the age of hybrid warfare and grey zone operations, these AI models too could be utilised to assess the capabilities of an adversary in terms of kinetic, Electronic Warfare (EW), Information Warfare (IW), and cyber domains to arrive at the most suitable option to commanders. The AI engine could access its own and adversary capabilities and suggest the most suitable options during various brainstorming sessions like war games, and the same algorithms can be further trained in real-world scenarios. Adversary capability, including intangibles, can be factored to work out an impact affecting various stages of battle.

Cyberspace Operation AI is likely to be a key technology in advancing military cyber operations. Conventional cyber security tools look for historical matches to known malicious code, so hackers only have to modify small portions of the code to circumvent the defences. On the other hand, AI-enabled tools can be trained to detect anomalies in broader patterns of network activity, thus presenting a more comprehensive and dynamic barrier to attack.[2] AI-enabled cyber tools can be developed with AI algorithms which could autonomously detect, evaluate, and patch software vulnerabilities before they exploit the network, all within a matter of seconds rather than the usual months. Progressing on similar lines, Army Headquarters Computer Centre (AHCC) has conceived a project on Security Information and Event Management (SIEM) wherein the flow of device logs from all the network devices and endpoints of the Army Data Network (ADN) has been integrated into the hierarchical structure from units to higher formations to Army Headquarters. Based on use cases, anomalies are being detected and suggestive measures are recommended for ensuring a robust defensive posture of ADN. Implementation of Security Orchestration and Automatic Response (SOAR) to streamline security operations of an organisation is one of the suggested methods for threat and vulnerability management, incident response, and security operations automation. The AI-enabled cyber tools could provide a distinct advantage in defending our networks in future cyber operations.

Information and Electronic Warfare

- **Information Warfare** AI might also play a vital role in the information war. Many fear that AI techniques such as Deepfakes—audio, video, text, and images that are created to show something that did not necessarily happen, or never occurred—will be a game changer in today's warfare. Application of Deepfake as a weapon of IW for misinformation has been observed in the recent Russia-Ukraine war where videos of the Russian President are circulating on social media with comments which were never made. This AI tool is a potent weapon which could change the course of war and has to be diligently used. A digital footprint to include purchase history, social media like Twitter, Facebook and openly available information of senior officials and their relatives of adversaries could be used to create a comprehensive behavioural profile and used for targeted information operations. Surveillance networks along the borders could be used to gather information and create a comprehensive database of adversaries, and AI techniques could be used to derive intelligence, which could help in IW.

- **Electronic Warfare (EW)** EW is one of the most important characteristics of modern battles. EW can affect a military force's use of the electromagnetic spectrum to detect targets or to provide information. Recent developments in AI suggest that this emerging technology will have a deterministic and potentially transformative influence on combat power. AI-driven algorithms can be very effective in diverse domains of EW, like processing radar signals for efficient recognition and classification of emitters, detecting jammers and their characteristics and developing efficient anti-jamming algorithms. AI techniques can also enable EW systems to operate autonomously. Appropriate application of AI in EW can help to mitigate the attempts by adversaries to hinder their communication networks, including GPS, satellite signals, etc. AI can reduce the cognitive burden and improve EW effectiveness for multi-domain operations. This will rank the incoming data quickly and accurately in order of priority to the war fighter so that less important signals can be removed. It is also useful in processing large volumes of data, thereby recognizing its patterns and deriving meaningful information.[3] A generic block diagram of an AI-enabled EW system is shown in Figure 3. Cognitive technology plays an important role in the electromagnetic spectrum and has to be leveraged as an independent AI module development project, not only for the radio frequency but also throughout the entire spectrum.

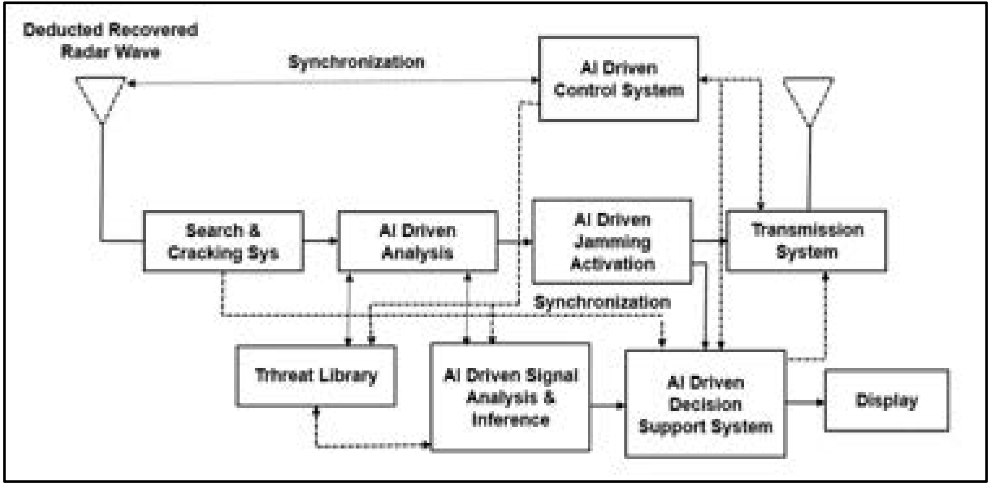


Figure 3: Basic Block Diagram of an AI Based EW System

- **Algorithmic Targeting** Another major use case of particular value in a tactical context, is the use of AI in developing rapid and accurate Automatic Target Recognition (ATR) systems: This is useful since visual identification of targets by human pilots requires flying at close approach, putting aircraft at risk from anti-aircraft systems; conversely, although radar in principle enables the identification and engaging of ground targets at a standoff distance, this comes at the cost of unacceptably high false-alarm rates or collateral damage. ATR systems can thus, combine the best of both worlds, providing highly accurate aircraft fire support from a standoff distance. Key tactical requirements for such a capability are that it can offer low false-alarm rates in complex environments-ensuring it is not easily thrown off by decoys or mistakes-and that it can rapidly improve its learning capabilities on the basis of sparse or limited training data. DARPA‘s Target Recognition and Adaptation in Contested Environments (TRACE) research program is already researching on a machine learning based ATR programme.

- **Situational Awareness and Understanding** Although drones have greatly aided force application in asymmetric conflicts, they have a number of operational limitations including low flying speed and vulnerability to air defence systems. Increasing the autonomy of unmanned systems will strengthen their survivability, enable higher-end performance, and improve their effectiveness in patrolling or monitoring areas. This feeds into an increased ability for militaries or states to cover far greater areas with sensors at a greater cost-effectiveness than human troops. The enhanced situational awareness enabled by more autonomous and survivable drones can strengthen the security of bases and experts have suggested, could potentially lead to greater stability between states by enhancing monitoring of contested areas, reducing the viability of covert or hybrid operations.

- **Target Systems Analysis (TSA)/Target Audience Analysis (TAA)** TSA and TAA are intelligence-related methods used to develop a deep understanding of potential areas for operations. They involve the analysis of reports, documents, newsfeeds, and other forms of unstructured information. Further, field AI systems could provide probabilistic forecasts of enemy behaviour, anticipate and flag bottlenecks or vulnerabilities in supply lines before they occur, and suggest mitigation strategies; draw on data (eg, weather conditions collected by drones) to examine factors affecting operations and assess the viability of different mission approaches. Natural language processing programmes can filter social media and news to identify strategically salient themes-or, conversely, can text-mine the mission reports of their own and allied forces in order to identify common themes or patterns in engagements. Projects could be developed in NLP which can recognise and translate languages like Mandarin and associated dialects in real time. This will not only help in interpretation during high-level meetings with adversaries but also be an efficient tool for IW.

- **Electronic Medical Records Analysis and Optimizing Medevac** Narrow AI agents could aid in the medevac of injured personnel from combat zones. Such systems can query up-to-date databases and cross-reference these against live intelligence from other forces in the area. Combining information on the severity of injuries, the length and security of available exfiltration routes, landing sites, and weather conditions, and the projected rate of medical emergencies in the coming days, such a system can perform a preliminary triage and determine the optimal means of evacuating casualties, increasing the efficiency and safety of medical evacuations and saving lives. Also, medical records can be digitised and, based on the profile posting of an individual, a detailed forecast of the force level available to operate in High Altitude Area (HAA) could be available at any instance of time. The data will also help in accessing the requirements of various types of medicines required to be stocked at different places both during operations and peacetime.

- **Documents Classification and Crypto-Preserving Intelligence Sharing** During and after operations and exercises, defence organisations have a need to move information between security domains. This requires the careful checking of the content to ensure no highly classified data or information will be moved or revealed to a less highly classified user or system. While aspects can be automated, the checking often requires a human to conduct the check. This can be very time-consuming and is prone to inaccuracy. Algorithms may be developed to more accurately read, understand, and verify if the content is safe to send from one domain to another. It also helps to minimise data aggregation risks and reduce the risk of inadvertent leaks.

- **Logistics Management** Large quantities of data are required to be shifted to make decisions regarding supply, transport, communications, and so on. Using AI and Machine Learning (ML) in one or more areas of logistics could help speed up that process and make it more agile.[4] Few areas where AI could be leveraged to optimise logistics management in IA are as under:-

    - **Cloud Service** A central repository of information might sound like a bad idea for the military, but in the world of logistics, it breeds efficiency. It means savings in time, effort, and money if logisticians have all the information they need to make informed decisions when moving supplies and equipment to support troops. The NFS, CDC and RDCs will assist in the same.

    - **Supply Chain Management** AI will have a future utility in the field of military logistics. Sensors can be placed at critical locations/shipments and AI based algorithms can be utilised to analyse supply chain flows for repair parts distribution, attempting to determine the most time-and cost efficient means to deliver supplies. This will potentially generate even greater cost savings in a shorter period of time. The same can be incorporated in existing applications of IA.

    - **Driverless Resupply** Drones are attracting attention in the AI space, but mostly for surveillance. We can look for self-driving vehicles to resupply outposts and bases, as being done by the US Department of Defence (DoD) under the Autonomous Ground Resupply program. This would spare human drivers from the hardships and risks. Robotic mules could also be used at different stocking places and warehouses to optimise manual labour efforts. There are efforts underway in the IA in this field as well.

Conclusion

AI technologies, though still in nascent stages, hold great promise for facilitating military decisions and enhancing the combat potential. The need of the hour is to catalyse the development of AI-based systems, utilising the best available expertise with due indulgence of all stake-holders. It becomes imperative that the Indian Military take note of the developments in this field and get on board as soon as possible to derive the advantages that technology will offer in future. Not only the military but it is also the responsibility of the Government to embrace this technology and provide the industry and academia necessary impetus for utilisation of AI in every possible military domain is essential.

Endnotes

1. *J. Liu and X. Li, "Artificial Intelligence in Modeling Command and Control," 2010 Second International Conference on Computer Modeling and Simulation, 2010, pp. 383-386, doi: 10.1109/ICCMS.2010.449.*

2. *Scott Rosenberg, "Firewalls Don't Stop Hackers, AI Might," Wired, August 27, 2017, https://www.wired.com/story/ firewalls-dont-stop-hackers-ai-might/.*

3. *'Mayhem' Declared Preliminary Winner of Historic Cyber Grand Challenge," August 4, 2016.*

4. *Article on "Artificial Intelligence for Military Logistics – Current Applications" by Millicent Abadicio published on https://emerj.com/ai-sector-overviews/artificial-intelligence-military-logistics/ as accessed on 26 March 2022.*

ARTIFICIAL INTELLIGENCE – RELEVANCE IN AIR DEFENCE BATTLE

- Major Akhand Pratap

I believe there is no deep difference between what can be achieved by a biological brain and what can be achieved by a computer. It, therefore, follows that computers can, in theory, emulate human intelligence - and exceed it.

- Stephen Hawking

Introduction

AI is not a recent phenomenon. Computer scientists like Alan Turing, Marvin Minsky, and John McCarthy contributed significantly to its theoretical and technological foundation during the previous 70 years. We are already at the beginning of the exponential age of AI as businesses learn to unlock the value locked in massive amounts of data thanks to nearly unlimited computer power and falling prices for data storage. As a result, by gathering and analysing images, sound, and speech, computer vision and audio processing may actively comprehend the environment around them.[1] The AI system can analyse and comprehend the information gathered with the help of the natural language processing and inference engines. A machine learning system can also act physically or through technologies like inference engines and expert systems. These human capacities are enhanced by our capacity for lifelong learning and adaptation. As these skills become more sophisticated, AI systems are being used in a wider range of organisations to supplement them. But regardless of the kind of AI being applied, every application starts with a substantial amount of training data. Statistical regressions, rule-based data analytics algorithms, and early "expert systems" were once responsible for this type of performance. However, the proliferation of robust deep neural networks has given AI the capacity to perform unanticipated tasks, something that a simple programme lacks.[2]

Evolution of AI

In the history of AI technology, waves of hope have been followed by setbacks and "AI Winters," or periods of inaction. Previous innovations have never been able to fully live up to the anticipation they created, and none have been able to propel the technology into the mainstream. Today's major shift is that we are seeing a moment of unparalleled technological advancement in a wide range of industries, leading us to believe that the "AI Spring" has not only begun but will continue.[3]

[1] *Author: Virtul Mittal, https://sharedservicesforum.in/think-big-start-small/.*

[2] *Discussion Paper National Strategy for AI NITI Ayog 2018.*

[3] *Author: Virtul Mittal, https://sharedservicesforum.in/think-big-start-small/.*

Exponential increase in digital data is a key factor that accounts for this optimism. International Data Cooperation (IDC) predicts that by 2025, the amount of data generated worldwide would increase to 163 (ZB), or a trillion gigabytes, or ten times the 16.1 ZB generated in 2016.

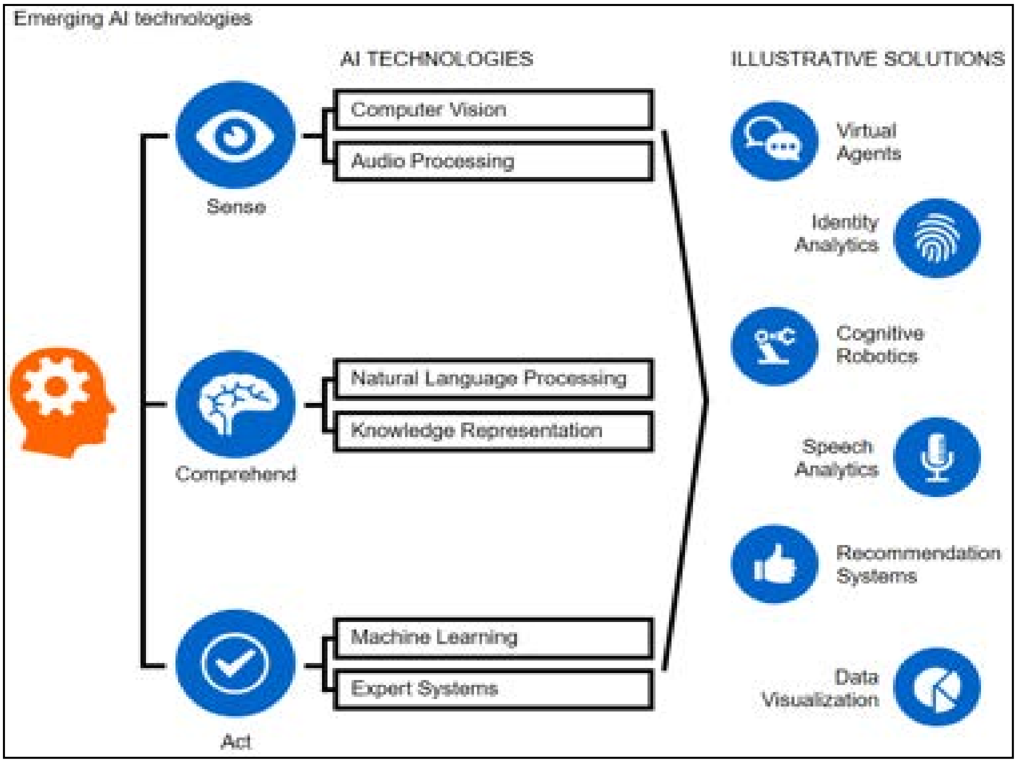


Figure 1: What is Artificial Intelligence[4]

Data is to AI what nourishment is to humans, according to Barry Smyth, professor of computer science at University College Dublin. As the world becomes increasingly digital, AI advances are continually being fuelled by the exponential rise of data. Additionally, General Bipin Rawat stated that "the military is the repository of big data, and there is a need to preserve and institutionalise the information and conduct predictive analytics utilising AI."

The Chinese government unveiled a roadmap outlining its goal of dominating AI by 2030 on 20 July 2017. Vladimir Putin openly declared Russia's intention to pursue AI technologies less than two months later, saying, "Whoever becomes the leader in this field will govern the world." Similar to this, the January 2018 release of the U.S. National Defence Strategy named artificial intelligence as one of the critical technologies that will "guarantee the United States to be able to fight and win the battles of the future."

[4] *Source: Accenture*

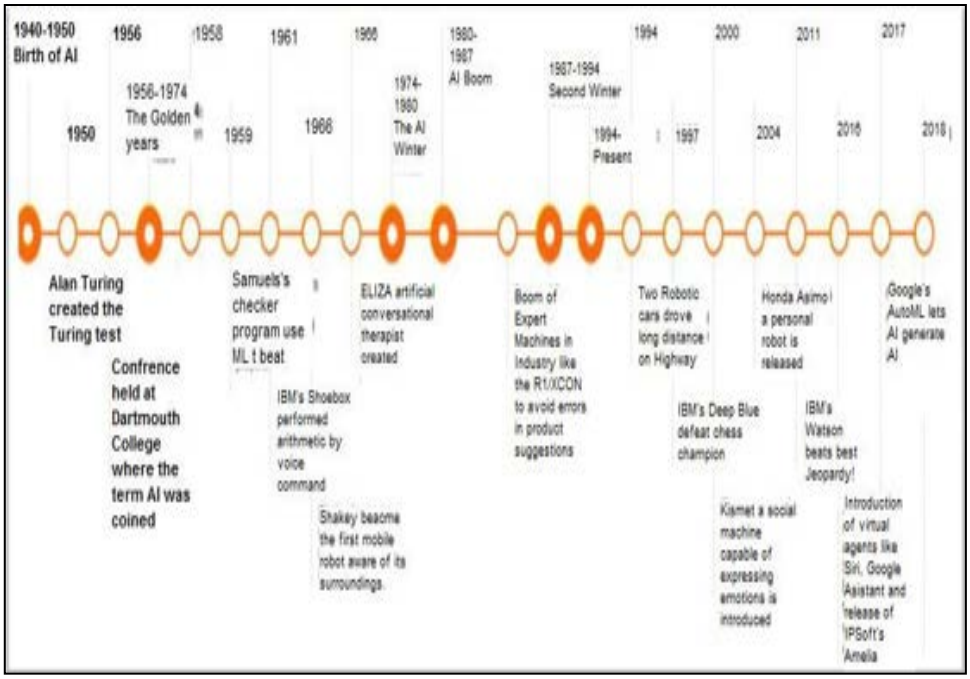


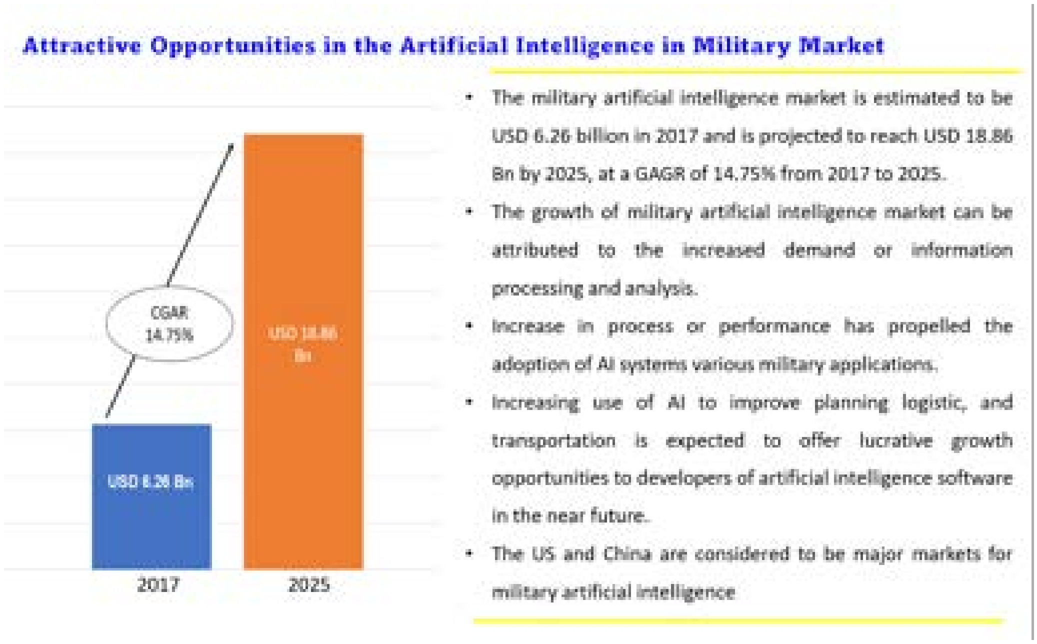
Figure 2: Evolution of AI[5]

Scope of Use of AI in Military Operations

Almost every imaginable sector of the civil sector has been affected by AI. It has revolutionised how people live and conduct business, and it is now swiftly advancing to play a crucial role in contemporary combat. Investment in this area is the highest in some of the most developed countries when compared to other sectors.

This investment is mostly used for thorough research and development of cutting-edge technologies for military purposes, including AI. Military systems with AI are capable of efficiently handling large amounts of data. Due to their enhanced computation and decision-making powers, such systems have also increased self-control, self-regulation, and self-actuation. The market survey and report from markets, which states that the AI in Military Market is projected to grow from USD 6.26 billion in 2017 to USD 18.86 billion by 2025, at a CAGR of 14.75 percent. In the upcoming years, the AI in military market is anticipated to be driven primarily by big data analytics, artificial neural networks, and advanced analytics.

[5] *Source: Discussion Paper National Strategy for AI NITI Ayog 2018.*



Attractive Opportunities in the Artificial Intelligence in Military Market

- The military artificial intelligence market is estimated to be USD 6.26 billion in 2017 and is projected to reach USD 18.86 Bn by 2025, at a GAGR of 14.75% from 2017 to 2025.
- The growth of military artificial intelligence market can be attributed to the increased demand or information processing and analysis.
- Increase in process or performance has propelled the adoption of AI systems various military applications.
- Increasing use of AI to improve planning logistic, and transportation is expected to offer lucrative growth opportunities to developers of artificial intelligence software in the near future.
- The US and China are considered to be major markets for military artificial intelligence

Figure 3: Prediction of AI in Military Market

Use of AI in Militaries around World The United States of America (USA), China, and Russia are some of the front-runners in implementing cutting-edge technologies to bolster their military capabilities. The United States Department of Defence published its first AI policy in 2019. It called for boosting the use of AI systems across the military, from problem prediction to decision-making, by investing in and partnering with private institutions in AI research. Project Maven, Defense Advanced Research Projects Agency's (DARPA) Squad X Experimentation Program, and the OFFSET programme are some of the most well-known AI-based programmes that have previously been implemented in the US military.

The Chinese government has also pushed for more advancements in military technologies that are based on AI and machine learning. Military-civil fusion style innovation, as advocated by President Xi Jinping, has also been included in Chinese National Plan. The "Military-Civil Fusion National Defence Peak Technologies Laboratory," established by Tsinghua University, is one of the projects under development. Another initiative is the creation of the Blowfish A2 model in cooperation with Ziyan Unmanned Aerial Vehicle (UAV). The company claims that its Blowfish A2 model can automatically carry out difficult combat tasks like fixed-point time detection and precise target strikes. Notably, China published its State Council AI Plan in 2017, outlining the nation's ambitious initiative to build an AI sector valued at 150 billion RMB.

Russia is renowned for its military might. The Foundations for Advanced Research Projects is the nation's version of DARPA. Higher hierarchies have been seen supporting the development of AI-based technology on the front of AI for the military. According to reports, in order to conduct more effective Information Operations, the Russian defence forces are considering leveraging AI, big data, and machine learning. Currently, Russia makes significant investments in AI for the commercial and defence sectors in order to detect, analyse, and refute misinformation.

India is implementing AI-based innovation in its combat and surveillance initiatives in small increments. The Ministry of Defence created the high-level Defence AI Council (DAIC) in 2019 with the purpose of giving strategic guidance for the adoption of AI in defence. Leading the collaboration between the government and the industry for the application of such technologies is one of DAIC's main responsibilities.[6]

Domains of AI in Military

- **Training** Multidisciplinary domains like training and simulation use systems and software engineering ideas to build models that let soldiers practise using different fighting systems that are used in military operations. Numerous sensor simulation programmes have already been started by the US Navy and Army. Additionally, simulations for training can be made that are efficient, realistic, and dynamic using techniques from augmented and virtual reality. Both real soldiers and virtual agents benefit from improved combat training thanks to reinforcement approaches.

- **Surveillance** The extraction of useful intelligence from linked equipment, such as radars and automatic identification systems, can be aided by AI with geographical analysis. By alerting the appropriate authorities, this information can assist in the detection of any unlawful or questionable activity. Target identification and classification can also be assisted by AI-powered and IoT-connected robots using computer vision.

- **Arms and Ammunition** Modern weapons now have AI technology built in. For instance, advanced missiles can analyse, identify, discriminate, and prioritise targets without human assistance.

- **Cyber Security** As a new dimension of warfare, cyberspace is currently regarded in defence circles as the third warfront. The security of the entire region could be seriously jeopardised by a corrupted and malevolent network. Machine learning is being used by defence agencies to anticipate threats and guard against unauthorised breaches.

[6] *https://analyticsindiamag.com/what-are-the-scope-and-challenges-of-using-ai-in-military-operations/*.

Categorizing the network as normal or intrusive is the typical method for performing this intrusion detection. AI-based methods aid in improving the categorization accuracy.

- **Logistics** The success of a military operation is largely dependent on a number of crucial aspects, one of which is logistics. The amount of effort, time, and error is reduced by integrating geospatial analysis and machine learning with the military's logistics systems.

IMPACT ON AIR DEFENCE BATTLE

AI Enabled Air Threat and Weapons AI is likely to impact future military aviation becoming part of the next generation hybrid, rotary and fixed wing unmanned systems. It will challenge the conventional monolithic systems thus redefining air power strategy. Salient aspects of Air Threat envisaged are listed below: -

- **AI Enabled Fighters** A within-visual-range, air-to-air combat drone that leverages AI for tactical decision making appears to be a simple engineering problem.[7] In fact, the United States Air Force (USAF) intends to replicate the AI-piloted aircraft versus human-piloted aircraft experiment from 2020 in 2024, but this time using real tactical aircraft rather than simulations. An operational, enhanced AI-enabled short-range, dog fight capable drone might be cheaper, smaller, and lighter than a crewed aircraft, and it might not even need to be armed to defend against an approaching enemy air attack.[8]

- **Precession Guided Munitions and Missiles** Long-range precession missiles and munitions are seen as being a significant threat in addition to conventional air attack because they may travel greater distances unnoticed and are difficult to neutralise because of their small size. Once they have reached their intended target, these missiles may identify and select their target more quickly and precisely, reducing the time and chance for air defence system to engage.

- **SWARM Attack** A Swarm of drones capable of communicating with one another, combined with an AI-based targeting and identification

[7] *Joseph Trevithick, "Navy Establishes First Squadron to Operate Its Carrier-Based MQ-25 Stingray Tanker Drones," The Drive, 1 October 2020, https://www.thedrive.com/; Kyle Mizokami, "Russia's 'Hunter' is Unlike Anything in America's Arsenal," Popular Mechanics, 10 August 2020, https://www.popularmechanics.com/*

[8] *Patrick Tucker, "An AI Just Beat a Human F-16 Pilot in a Dogfight — Again," Defense One, 20 August 2020, https://www.defenseone.com/; and Secretary of Defense Dr. Mark T. Esper, "Secretary of Defense Remarks for DoD Artificial Intelligence Symposium and Exposition," US Department of Defense, 9 September 2020, https://www.defense.gov/*

system, would wreak havoc on adversaries. It has the potential to attack any target, including bunkers, people, and equipment.

AI based Sensor Fields and Command & Control Model[9]

The system envisages deploying a significant number of inexpensive Internet of Things (IoT) sensors on land, sea, air, space, and cyber domains throughout the combat zone to keep a close watch on adversaries' activities. The Integrated Air Defence System (IADS) concept, consists of a network of surface-based radar stations augmented by Airborne Early Warning and Control Aircraft (AEW&C) to detect high and low-flying aircraft, already implements this principle.

- This idea involves using a significant number of AI-enabled small, low-cost surface and airborne sensors in addition to the current, expensive, limited-number sensor deployment. The partially processed data is transferred through the cloud to a fusion centre and subsequently to the command-and-control system.

- These networked Air Defence grid would involve numerous short range radar transmitters and passive IOT sensors capable of detecting emissions in the acoustic, Ultraviolet (UV), Infrared (IR) extending upto entire spectrum

- These low cost, small sensors may have low individual performance, however, the integrated outputs of hundreds of these sensors, would be able to provide a gap free, coherent air picture which would allow for tracking, identifying and subsequent engagement of enemy aircrafts.

- Air Defence IoT sensors on surface may be stationary and persistent, whereas drones with integrated sensors may have endurance ranging from a few hours to a day. High-altitude balloons, miniature and pseudo-satellites are just a few of the new IoT platforms that have the potential to significantly extend this endurance.

[9] *https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2548127/ai-enabled-war-in-the-air/.*

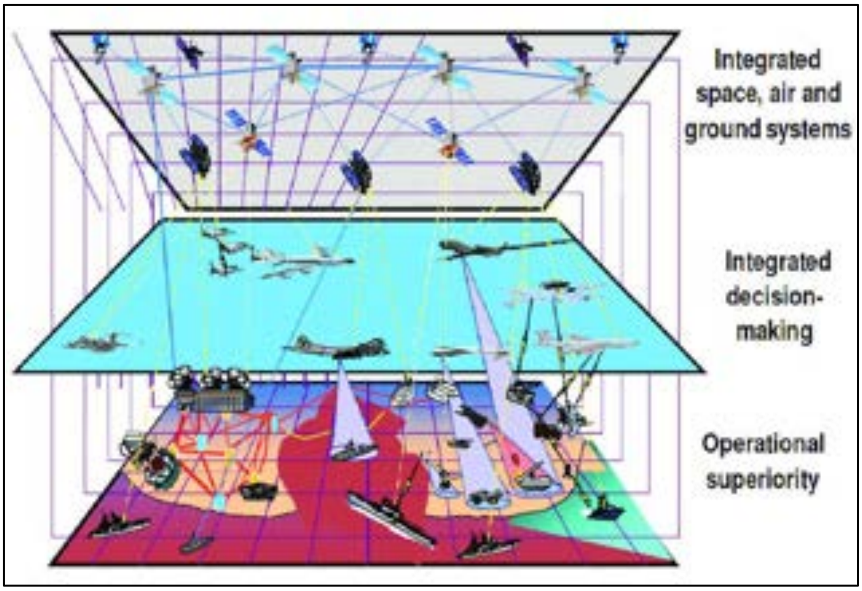

Integrated space, air and ground systems
Integrated decision-making
Operational superiority

Figure 4: AI Based Sensor Fields and Command and Control System

- Intruding aircraft will have to avoid using transmitting equipment like radars, data linkages, and communications systems to evade detection as a significant number of these IoT sensor employ passive detection technique. However, typical aircraft emissions like noise, heat, and visual signatures may still make an aircraft vulnerable to detection by a broad IoT sensor field. Aircraft may perform manoeuvres to reduce these emissions, particularly those from the forward section of the aircraft when it approaches a recognised sensors field. A deep sensor field would allow identification of a penetrating aircraft from flanks and rear section, even if it has not been picked up during ingress.

- A fusion facility would receive partially processed data from the extremely vast IoT sensor field enabled by AI and send it to the cloud for further processing by AI. The Observe-Orient-Decide-Act model can be used to process these sensor outputs. The IOT sensors, coupled with processing of data at fusion centres would form part of the first two stages of Observe and Orient stage. AI would not only create a comprehensive air picture in near real time but would also forecast adversaries' courses of action and movements.

- The next AI layer handling "Decide," would send a prioritised list of approaching air targets to engage, the best cross-domain assault strategies to use, relevant timings, and any disengagement considerations to the human commander for approval. Humans would continue to be actively involved in this through in-the-loop or on-the-loop control.

Following human approval, the following AI layer would automatically allocate the chosen weapons to each target, delivering the necessary targeting data, assuring friendly force disengagement, confirming when the target was engaged, and even commanding weapon munition resupply. Act, the last stage, would mostly be a human function.

Solutions with Available Technology A limited number of AI applications can be implemented right away because they are being developed in business industries, such as:-

- **Automated Air Sentry** With help of pattern recognition and machine learning independent cameras can be installed at difficult and un-accessible terrain, where sustenance of radars is difficult due to power requirements and high-altitude constraints. In our context high altitude areas of Ladakh and Northeast can be covered by such Air Sentries.

- **Data Management Systems with AI Processing** The air defence battle requires a large number of reports and returns to be generated for correspondence to provide near real time data of tactical and logistic situation to higher headquarters to include number of aircrafts shot down, requirement of ammunition, casualty report etc. This data is crucial for success in any battle as it provides commanders with a clear picture of battlefield and allows them to take informed decisions. This data can be transmitted, stored, and processed with an AI enabled central server and can allow for accessing it in a blink of an eye. For example, imagine an **Alexa** kind of application in office which can carry out all staff check and provide accurate data without delay and chances of human error.

- **AI Enabled Anti Drone Systems**. The vulnerability of static installations like airfields, refineries etc. has been adequately highlighted in recent attacks on such installations across the world. These installations are now guarded with state-of-the-art Anti Drone Air Defence Systems. IOT sensors on the periphery of such installations integrated over an AI based algorithm with passive and active anti drone systems would assist in neutralizing these attacks effectively.

- **AI Based Simulators** Air Defence missiles are extremely expensive and therefore it is a costly proposition to make large number of missiles available for training. Similarly, train radar operators on techniques of Electronic Counter Measures and Electronic Counter Counter Measures there is a need to coordinate with fighter aircraft flying. AI based missile gun and simulators would allows saving huge training cost an allow large number of gunners and operators to be trained simultaneously. Real time jamming operations can be generated on radar simulators thereby improving training standards.

Challenges in the Future The investment of time, money, and expertise required to use AI-based technology is a major challenge. India is a growing economy and requires concentrating its resources for development of human resource index: access to knowledge, a decent standard of living, and long and healthy life. A big difficulty is determining how much resources we can afford to offset for development of such technologies for military. There is a need to identify essential and dual use technologies which can assist in country's development as well as security.[10]

An ethical conundrum is also raised by the deployment of AI in kinetic domain. Global organisations and experts have boosted this technology, unintentionally exacerbating international tensions. One of the arguments is that if an AI system doesn't work as designed, it could have disastrous consequences. In reality, a number of human and civil rights organisations want a complete ban on autonomous defence equipment, particularly weapons.

Recommendations Implementing AI based Air Defence System would require the following: -

- Development of expertise for producing AI based systems and understanding of AI for operating such systems.

- Creating a group or organisation within services for faster and better understanding of user problems.

- Framing Policies for supporting AI and to understand and address the ethical, legal and societal implications of AI.

Conclusion

Air Defence battle requires management of greater amount of data handling in limited time frame being short, intense and time critical which further shortens the decision cycle. AI however, shows promise in providing solutions for data acquisition, fusion and analysis thereby enhancing the situational awareness of commanders and reaction capabilities of shooters at the tactical level. AI integrated Air Defence systems would allow real time identification of friend and foe (IFF) and would reduce fratricide thereby providing enhanced freedom of operation to friendly aircrafts. As the air threat envelope enhances from low cost drones to sophisticated 4th & 5th generation aircrafts, ballistic and cruise missiles a focused approach in Research and Development is required for incorporating AI in Air Defence Systems.

[10] *Author: Shraddha Goled, https://analyticsindiamag.com/what-are-the-scope-and-challenges-of-using-ai-in-military-operations/.*

Bibliography

1. *Allan, M Din, "Arms and Artificial Intelligence", Oxford University Press, 1987.*

2. *Bostrom, "Superintelligence".*

3. *Clayton M Christensen, "The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail".*

4. *Topychkanov, Impact of AI on Strategic Stability and Nuclear Risk.*

5. *Zachary, S Davis, "Artificial Intelligence on The Battle Field – A realistic appraisal of AI, Big Data & Machine Learning".*

6. *Discussion Paper on National Strategy on AI by NITI Ayog 2018.*

7. *Artificial Intelligence and Its Impact on the Indian Armed Forces by Maj Gen PK Chakravorty.*

8. *Cummins ML, Article on "Artificial Intelligence and The future of Warfare"- Defence Technology (January 2017, Number 128).*

9. *Gronlund Kirsten, Article on "State of AI : Artificial Intelligence, the Military and Increasingly Autonomous Weapons", Future of Life.*

10. *Kulshrestha S, Dr Rear Admiral, Article on " Indian Armed Forces Approach To Managing ISR Big Data",IndraAstra Oct 2016 Edition.*

11. *Talwar Surjeet Singh, 'Disruptive Technologies : Impact on Warfare and Their Future in Conflicts of 21st Century – Centre for Land Warfare Studies (CLAWS)', accessed 12 September 2020.*

12. *Article on "What are the Scopes and Challenges of using AI in Military Operations".https:// analyticsindiamag.com/what-are-the-scope-and-challenges-of-using-ai-in-military-operations/.*

13. *Article on "AI in Air Combat Indian Air Force leads the Defence". https://www.financial express.com/defence/artificial-intelligence-in-air-combat-indian-air-force-leads-the-defense-initiative /2228352/.*

14. *Article on "Using Artificial Intelligence in Big Data" by Analytics Insightchttps://www.analytics insight.net/using-artificial-intelligence-in-big-data/, accessed on 07 Oct 20.*

15. *Article on AI enabled War in the Air https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2548127/ai-enabled-war-in-the-air/.*

16. *Article on "Navy Establishes First Squadron to Operate Its Carrier-Based MQ-25 Stingray Tanker Drones" https://analyticsindiamag.com/what-are-the-scope-and-challenges-of-using-ai-in-military-operations/.*

17. *Joseph Trevithick, "Navy Establishes First Squadron to Operate Its Carrier-Based MQ-25 Stingray Tanker Drones" The Drive, 1 October 2020.*

18. *Article on Russias Hunter is unlike Anything in America's Arsenal https://www.thedrive.com/, Kyle Mizokami, "Russia's 'Hunter' is Unlike Anything in America's Arsenal," Popular Mechanics, 10 August 2020, https://www.popularmechanics.com/.*

19. *· Patrick Tucker, "An AI Just Beat a Human F-16 Pilot in a Dogfight - Again," Defense One, 20 August 2020, https://www.defenseone.com/; and Secretary of Defence Dr. Mark T. Esper, "Secretary of Defense Remarks for DoD Artificial Intelligence Symposium and Exposition," US Department of Defense, 9 September 2020, https://www.defense.gov/.*

ARTIFICIAL INTELLIGENCE AND FUTURE OF WARFARE: ROADMAP FOR THE INDIAN ARMY

- Lieutenant Colonel Deepak Kumar Tiwari

Introduction

C4I2STAR (Command, Control, Communication, Computers, Information, Intelligence, Surveillance, Target Acquisition, and Reconnaissance) is the acronym for systems that form the cutting edge of today's warfare. These systems define the technological superiority of any nation. The network centric approach to warfare means utilising information age concepts to integrate and undertake a different range of missions to improve both the efficiency and effectiveness of operations.

Recently, the integration of computers and revolution in the field of information has led to concepts such as the Internet of Things and Big Data Analytics. This pool of data is best used by autonomous machines and programs. Every nation with significant military might has declared budgets for research and development on artificial intelligence (AI) and its military applications in recent years. This genre of technology is likely to revolutionise elements of C4I2STAR. The command and control (C2 of C4I2STAR) system was always human-in-the-loop and required input from the other technologies (communication, computers, information, intelligence, surveillance, target acquisition, and reconnaissance). Today, every system is on the verge of using autonomous systems to work in tandem or remove the human-in-the-loop.

Automatic and Automated System

Before understanding Artificial Intelligence (AI), it is important to understand automatic and automated systems. Automatic systems are simple machines that do not exhibit much in the way of "decision-making." Automated systems are more complex and may consider a range of inputs and weigh several variables before taking action. An automated system is one in which a computer reasons by a clear if–then–else, rules-based structure and does so deterministically, meaning that for each input, the system output will always be the same (except if something fails). An autonomous system is one that reasons probabilistically given a set of inputs, meaning that it makes guess about the best possible course of action given sensor data input. Unlike automated systems, when given the same input, autonomous systems will not necessarily produce the exact same behaviour every time; rather, such systems will produce a range of behaviours.

AI is programmed to do something similar. A computer senses the world around it, and then processes the incoming information through optimization and verification algorithms, with a choice of action made in a fashion similar to that of humans. The technology envisages applications in both civil and military domains alike. AI has shown many applications in the contemporary world. AI-empowered cars are already under rigorous testing and they are likely to be common on the road. In 2017, the social humanoid robot Sophia became a citizen of Saudi Arabia in 2017. Natural language processing by machines is revolutionising mobile phones. Autonomous weapons can execute military missions on their own, identifying and engaging targets without any human intervention. AI enables intelligent machines that can execute functions similar to human abilities like speech, facial, object, or gesture recognition, learning, problem solving; reasoning; perception; and response.[1]

Investment in AI has seen a remarkable rise in the past few years (Figure 1). However, the spike in funding and focus is not restricted to the civilian domain. The United States, Russia, China, and other countries are increasing their investments in artificial intelligence. Russia and China have published their national strategies on artificial intelligence, and by 2030 they want to become leaders in AI technology. The Ministry of Commerce and Industry of India has set up a task force on Artificial Intelligence to kick-start the use of AI for India's economic transformation. The report was released on 20 March 2018. One focus area suggested by this report is National Security.

Integrating AI weapon systems into military platforms has a broad range of applications but numerous concerns, both practical and ethical. Autonomous weapon platforms have the potential to significantly reduce the manpower required to perform a myriad of tasks. This is important given that some of these tasks, like patrolling and mine clearing, are exceptionally dirty, dull, or dangerous. Autonomous weapon systems can perform the same task for longer durations more reliably. They lack human limitations such as fatigue, boredom, and injury. Furthermore, when placed in a combat situation, an autonomous system would have the ability to rapidly analyse data and react without human limitations, including panic and injury. Paradoxically, many of the same benefits can be interpreted as causes of concern.[2] While there is a strong consensus that Artificial Intelligence will be a game-changer and a key factor in development, there is a concurrent need to arrive at frameworks that will promote its deployment, taking all risk factors into account.

Applications of AI in Military

- **Force Structuring** Because of the military's large structure and the constant revision of concepts in war fighting, a continuous review of formation structuring, and employability is required. This process is done

[1] *Sharma Munish,The Global Race for Artificial Intelligence: Weighing Benefits and Risks, IDSA Issue Brief, 23 February 2018.*

[2] *https://ww2.kqed.org/education/2016/09/14/are-artificially-intelligent-military-systems-worth-the-risk/ accessed on 29 June 18.*

manually, and in countries with large armed forces, this process takes a long time. Successful implementation of AI in force structuring might lead to new concepts of operation that could influence how militaries organise themselves and plan operations.[3]

- **Intelligence, Surveillance and Reconnaissance (ISR)** Due to the availability of large amounts of data in ISR field, AI has found extensive utility. AI is planned to automate the work of human analysts who currently spend hours analysing videos and images for valuable information. AI may reduce the workload of analysts and improve their efficiency by allowing them to take timely AI-based solutions. The intelligence agencies have sponsored projects such as image recognition or labelling to predict future terrorist attacks or civil unrest based on wide-ranging analysis of open-source information.[4]

- **Logistics** IBM Watson is an AI processor that can validate and audit transportation decisions to optimise modes of transport for logistic requirements to reduce cost. The movement of troops and material in a country as vast as India is a complex task. In the Indian scenario, a trivial decision of troop transport in valleys based on available effort and available time for movement needs deliberation and analysis. This task, if automated with AI, will reduce effort at the operational level. The concept is to employ AI to determine whether air, land, or sea is the more rational mode for a given shipment.[5]

- **Maintenance** AI has also found unique applications in preventive maintenance, stocking, inventory management etc. Aircraft maintenance involves conducting repair tasks when an aircraft snags or has a planned schedule with inherent delays. Predictive aircraft maintenance based on AI would allow technicians to perform maintenance on individual aircraft on a need-basis. This kind of application would need real-time data from sensors and a large data pool to substantiate decisions for the system. Such sensors could be embedded in the aircraft's engines and other on-board systems and further feed them into a predictive algorithm to determine when technicians need to accomplish inspections or replace parts.[6]

- **Cyberspace** Conventional cyber-defence tools look for matches to previous malicious code, so intruders have to modify small portions of that

[3] *Artificial Intelligence: Autonomous Technology (AT), Lethal Autonomous Weapons Systems (LAWS) and Peace Time threats By Regina Surber, Scientific Advisor, ICT4Peace Foundation and the Zurich Hub for Ethics and Technology Pp 5.*

[4] *HoadleyD,Lucas N, Artificial Intelligence and National Security, April 2018, Pp 9.*

[5] *https://www.c4isrnet.com/home/2017/09/07/army-logistics-integrating-new-ai-cloud-capabilities/ accessed on 10 December 18.*

[6] *HoadleyD,Lucas N, Artificial Intelligence and National Security, April 2018, Pp 9.*

code to defeat this defence. AI-based cyber-defence tools can be taught to distinguish these minor variations from patterns or behaviour in a network and detect anomalies. Thus, AI-based cyber defence will present a more wide-ranging barricade to previously vulnerable attack strategies. These AI-based tools will allow defenders to be protected against new and creative means of cyber-attack instead of the simple mechanisms of the past.[7]

- **Command and Control** In the immediate future, AI may be used to fuse data from sensors in all of these domains to create a single source of information for decision makers, also known as a common operating picture. The information available to decision makers comes in diverse formats from multiple platforms, often with redundancies or unresolved discrepancies. A common operating picture enabled by AI would combine this information into one display, providing an intuitive picture of friendly and enemy forces, and automatically resolving variances from input data. Later, AI may be used to identify communications links cut by an adversary and find alternative means to distribute information. As the complexity of AI systems matures, AI algorithms may provide commanders with viable courses of action based on real-time analysis of the battlespace, which would enable faster adaptation to unfolding events.[8] In the long run, analysts believe this area of AI development will likely be especially consequential, with the potential to improve the quality of wartime decision-making and accelerate the pace of conflict.

- **Autonomous Vehicles** All the military services are incorporating AI into various types of autonomous vehicles. AI applications in this field are similar to commercial self-driving vehicles, which use AI technologies to perceive the environment, recognize obstacles, fuse sensor data, plan navigation, and even communicate with other autonomous vehicles.AI-based cooperative behaviour, or swarming, is a unique subset of autonomous vehicle development, with concepts ranging from large formations of low-cost drones designed to overwhelm defensive systems to small squadrons of RPAs that collaborate to provide electronic attack, fire support, and localised navigation and communication nets for ground-troop formations.[9]

- **Lethal Autonomous Weapon Systems (LAWS)** LAWS are a special class of AI systems capable of independently identifying a target and employing an onboard weapon system to engage and destroy it with no human interaction. LAWS require a computer vision system and advanced machine learning algorithms to classify an object as hostile,

[7] *ibid, Pp 10.*

[8] *HoadleyD,Lucas N, Artificial Intelligence and National Security, April 2018, Pp 10.*

[9] *ibid Pp 11,12.*

make an engagement decision, and guide a weapon to the target. LAWS, once activated, would, with the help of sensors and computationally intensive algorithms, identify, search, select, and attack targets without further human intervention. Whether a human being can still overpower or veto an autonomous weapon's 'decision' in order for it to be called LAWS is also being debated. From a military perspective, LAWS have many advantages over classically automated or remotely controlled systems. LAWS would not depend on communication links; they could operate at an increased range for extended periods. Their higher processing speeds would suit the increasing pace of combat.

Progress of AI in Military Domain

Global investments in artificial intelligence for economic and national security purposes are increasingly described as an arms race. China published a national strategy on artificial intelligence in 2017 that said AI represents a "major strategic opportunity" and proposed a coordinated strategy to "build China's first mover advantage" and lead the world in AI technology. Russia is investing heavily as well, especially in the military domain. Reports suggest that the Russian military is designing autonomous vehicles to guard its ballistic missile bases as well as an autonomous submarine that could carry nuclear weapons. In robotics, Russia is deploying remotely piloted tanks, such as the Uran-9 and Vehar, on the battlefield. China and Russia are not the only actors outside the United States interested in national security applications of AI. The character of AI technology, like robotics, makes many countries well-positioned to design and deploy it for military purposes. Commercial incentives for AI developments and the dual-use character of many AI applications mean that countries with advanced information economies are poised to be leaders in AI or at least fast followers. In Southeast Asia, Singapore is on the cutting edge of AI investments (both military and non-military). Other Southeast Asian nations are making advances in AI research as well. In the military domain, South Korea has developed the SGR-A1, a semi-autonomous weapon system designed to protect the demilitarised zone from attack by North Korea. AI also provides opportunities for capital-rich countries, which creates incentives to develop the technology. Israel, a classic example of an advanced economy with more capital than labour, also funds military AI investments that would predict rocket launches and analyse video footage.[10]

Status Update of AI in India

AI has a distinctive "dual-use" nature. While its benefits for humanity are immense, they all come with a multitude of risks from a multitude of factors. The situation is not about humans vs. machines but about harnessing camaraderie

[10] *H Michael, Artificial Intelligence, International Competition, and the Balance of Power, Texas National Security Review: Volume 1, Issue 3 (May 2018).*

between humans and machines to make better decisions. Today, AI has opened up a geopolitical debate and intense competition among nation-states.[11]

- **Ethical and Legal Concerns from LAWs** Autonomous weapons function with minimal to no human intervention, selecting and engaging targets by themselves. Fully autonomous weapons do not yet exist, but an increasing number of countries are developing or deploying near-autonomous systems. While no country has acknowledged deploying autonomous offensive weapon systems, even defensive systems will profoundly change the way nations think about wars and will directly affect a variety of areas, including trade and the balance of power. A small but fierce global debate has generated issues related to the morality of these weapons and their status under international humanitarian law. A consensus has not yet emerged, but parties such as the United Nations (UN) special rapporteur on extrajudicial executions and the state of Pakistan have already put forward arguments calling for a pre-emptive ban on the development of such weapons. Other parties, such as the US Air Force, have argued that autonomous weapons have benefits, including reducing casualties and improving efficiency in defensive capabilities. Only the United States and the United Kingdom have released official documents that clearly lay down their respective positions on autonomous weapons.[12] The other countries expressed their positions at the three gatherings of the Convention of Conventional Weapons (CCW) Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS) held at Geneva in April 2016. The primary issues debated were whether a pre-emptive ban is justified and what should be the way forward for autonomous weapons in the international arena. India has projected a need for increased systemic control over international armed conflict in a manner that does not widen the technology gap amongst states or encourage the increased resort to military force in the expectation of fewer casualties or that use of force can be shielded from the dictates of public conscience. India has also highlighted the issue of international security in the case of the proliferation of such weapon systems, arguably to non-state actors. India has noted that there is a wide divergence on the key issues of definition and "mapping autonomy" and that there is a need to resolve these issues.[13] ***India has emphasised the fact that such technology has both peaceful and military applications, and that the CCW will be a relevant and acceptable framework for addressing any issues of concern in future.***

- **Flexibility** The Indian armed forces are still evolving in terms of integrated procedures and data infusion. However, doctrines for the integrated nature of warfare in the future are made, but not time-tested.

[11] *The Global Race for Artificial Intelligence: Weighing Benefits and Risks, IDSA Issue Brief, 23 Feb 2018 by Munish Sharma.*

[12] *India and the challenge of autonomous weapons r. Shashankreddy.*

[13] *Ibid.*

This will result in inconsistent logic in algorithms, which eventually form the backbone of any AI-based system. ***Whenever ready, this backbone will decide the exact timelines for application. Also, the nature of rapid changes in tactics in armed forces owing to hybrid threats is one thing which needs to be kept in mind to avoid incorrect decision making by these AI systems if implemented.***

- **Dependence on Foreign Technology** The military may need to adjust the acquisition process to match timelines and progress in other countries and the civil domain. The availability of a valid and correct database is a must for any application of AI. Procuring this technology from any foreign country means a compromise of this database. If a solution is chosen to use dummy data for application development, it will still lead to teething problems for such a complex technology, and reliability will always be in question. Also, our defence acquisition processes are not agile enough for fast-paced development in AI, which will affect its war fighting capability. Considering the progress of AI development in India vis-a-vis the development of other nations, India is way behind the race. This will cause Indian military equipment to become obsolete more quickly, despite not conforming to conventional definitions of aging. ***Thus, perforce, we may have to resort to foreign technology, as we have seen in the past decade of military procurement in India. This dependence will only deter the Indian military from asserting its will when desired and has an inherent vulnerability to information***.

- **Challenges in Development of AI for Military** From the Cold War era until recently, most major defense-related technologies were first developed by government-directed programmes and later spread to the commercial sector. Examples include nuclear technology, the Global Positioning System (GPS), and the internet. In contrast, civilian companies are leading AI development, with the military domain adapting their tools for national security functions. ***Today, AI development in the commercial sector is leading the military sector. This reversal of the tradition of strategic technology development is a concern. In India, the development is still in a very nascent stage and military applications are done piecemeal***.

- **Software Error/Lack of Subjectivity** During the Cold War, and each side was capable of a nuclear strike. An example to explain the subjectivity involved in decision making is illustrated in the following paragraph.

> *Lieutenant Colonel Stanislav Petrov was on a night duty in bunker outside Moscow and his responsibility was to report the missile launch up the chain of command to his superiors. In the bunker, sirens blared, and a giant red backlit screen flashed*

> *"launch," warning him of the detected missile, but Petrov was uncertain. Why would the United States launch only five missiles? It didn't make sense. A real surprise attack would be massive, an overwhelming strike to wipe out Soviet strategic targets. Petrov was not convinced the attack was real. But he wasn't certain it was a false alarm, either. He was right and there was no attack. Sunlight reflecting off cloud tops had triggered a false alarm in Soviet satellites. Humanity was saved from potential Armageddon by a human "in the loop." The AI machine would have done whatever it was programmed to do, without ever understanding the consequences of its actions.*

Some decisions in conflict situations are straightforward. Sometimes the enemy is easily identified, and the target is clear. Some decisions, however, require understanding the broader context. The Indian armed forces have yet to mature enough to make these artificial intelligence-based decisions. ***Currently, every important military action has the nod of higher authorities due to seamless communication in each service. Changing the command structure and losing the broader perspective due to AI will definitely take a long time to employ in our environment.***[14]

- **Potential Weapons Arms Race** The armed forces of the US and China have already invested billions of dollars in developing LAW, intending to gain strategic and tactical advantages over each other. This runs the risk of an arms race. Similar to the support of chemists and biologists for international agreements prohibiting chemical and biological weapons, leading robotics and AI pioneers have called on the United Nations to ban the development and use of LAWs. ***In the swelling competition for AI technology progress, India fares average. Research output from India in international journals ranks at 7, and the numbers are one fifth of that of China.***[15] Given the predictable national security value, some analysts subscribe to AI technology as a game changer. Several analysts have cast the increased pace and magnitude of AI development as a "Sputnik Moment" that may spark a global AI arms race. Analysts warn that if military units rush to field the technology prior to gaining a comprehensive understanding, they may incur a "technical debt." The term "technical debt" means the effect of using AI systems will have minimal risk individually but increase the danger of catastrophe as their collective hazard is compounded by each new addition to the inventory. This situation may be further exacerbated if nations engage in an AI arms race.[16]

[14] *S Paul, Army of None, 2018, Ch 15, Pp*

[15] *Sharma Munish,The Global Race for Artificial Intelligence: Weighing Benefits and Risks, IDSA Issue Brief, 23 Feb 2018*

[16] *HoadleyD,Lucas N, Artificial Intelligence and National Security,April 2018, Pp 17.*

- **Rapid Obsolescence of Infrastructure** Ultimate success with AI will likely depend on how suitable its environment is for such powerful applications. While cloud computing is emerging as a major resource for data-intensive AI workloads, military apparatus must continue to rely on their existing IT environments for these projects due to budget constraints.[17] ***Considering the recent development of the IT infrastructure of the Indian Armed Forces towards NCW, the possibility of repeated up-gradation in the near future does not seem feasible.*** The restrictions on upgrading processing and networking infrastructure in the Indian Armed Forces are not only from restricted budgets for procurement but also from the capability of each service to adapt to new systems with artificial intelligence.

- **Infrastructure Vulnerability** AI algorithms are efficient only if they are trained on large sets of data. The dataset may be too small, mislabelled, inaccurate, or outright falsified by malicious actors. Big data is a big problem if that data is bad. Data errors are a sensitive problem in the national security sector, where the chief threat is not routine cyber-crimes but sophisticated and well-funded nation-states. If a technologically capable adversary is aware of the dataset your AI is training on, they will have an edge in determining how to beat it. The availability of enough good data is difficult. As a result, a lot of datasets are widely shared for development. The worst-case scenario will be if the enemy inserts false data into our AI systems. The AI learns the untrue version of reality that the enemy desires. This situation will be very dangerous, especially because the victim will not realise that their own AI data set is incorrect and may continue trusting the incorrect results. The inner workings of AI algorithms are particularly complex and unpredictable, even to their designers. Examples of such a disaster exist in civil applications of AI. One such example is that the Twitter feeds for Microsoft's Tay chatbot trained it to send out racist content within hours of coming online. [18] In the recent past, the Indian Army website and the Ministry of Defence website were both hacked.[19]No single agency in India is charged with ensuring cyber and IT security. According to data released by the Computer Emergency Response Team-India (CERT-IN), 90, 119, 252 and 219 government websites were defaced by various hacker groups in the years 2008, 2009, 2010 and January-October 2011, respectively. On July 12, 2012, in one of the biggest cyber-attack on the India's official computer networks, over 100,000 e-mail addresses of top government officials were hacked in a

[17] *https://searchenterpriseai.techtarget.com/feature/Designing-and-building-artificial-intelligence-infrastructure accessed on 10 December 2018.*

[18] *https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter accessed on 25 December 2018.*

[19] *https://www.firstpost.com/tech/news-analysis/indian-army-site-hacked-does-india-have-the-right-attitude-to-tackle-cyber-crime-3666607.html accessed on 10 December 18.*

single day.[20] ***With lack of network integration, state of Cyber Security apparatus of the nation and lack of valid AI trainable databases, Indian Armed Forces and its systems have a considerable vulnerability. Also, majority of the data sets currently available with each service are not integrated or labelled nor are digitised in most of the cases.***

- **Training and Acceptability** Militaries which will utilise AI technology must employ soldiers who have training in coding and who understand how algorithms work. Similarly, at the user end, comprehension of a complete picture or subjectively analysing results or solutions by an AI system needs training and understanding of how an AI system works. ***Currently, only a broad understanding of AI exists in the Indian Armed Forces. If an AI-based system is presented without adequate training and education about the changes that it is about to bring, then applications of AI may have adverse effects.*** Also, from the point of view of security and generating valid data sets, a huge amount of groundwork needs to be done prior to implementation. This process may also demand awareness from personnel and reasonable acceptance of non-human decision-making.

Framework for AI in the Military

Human intelligence generally follows a sequence known as the perception–cognition–action information processing loop, in which individuals perceive something in the world around them, think about what to do, and then, once they have weighed up the options, make a decision to act. AI is programmed to do something similar, in that a computer senses the world around it and then processes the incoming information through optimization and verification algorithms, with a choice of action made in a fashion similar to that of humans. Figure 2 illustrates how an autonomous system embedded with AI ‘thinks’ and makes decisions in this way. While there are many parallels between human intelligence and AI, there are stark differences too.

[20] *Cyber Security: Avoiding a 2020 Pearl Harbour GurmeetKanwal CLAWS Journal.*

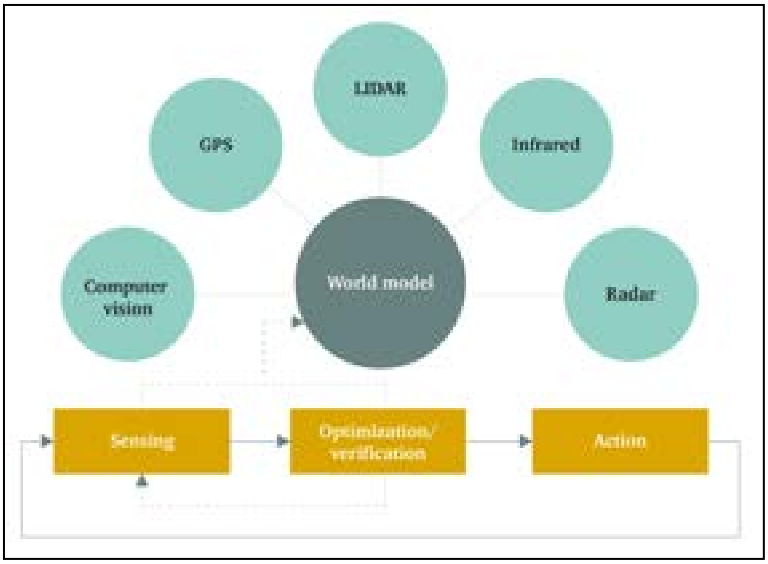


Figure 1

Every autonomous system that interacts in a dynamic environment must build and constantly update a world model (as shown in Figure 2). This means that the world must be perceived (or sensed through cameras, microphones, and/or tactile sensors) and then reconstructed in such a way that the computer 'brain' has an effective and updated model of the world it is in before it can make decisions. The fidelity of the world model and the timeliness of its updates are the keys to an effective autonomous system.

Autonomous UAV navigation, for example, is relatively straightforward since the world model according to which it operates consists simply of maps that indicate preferred routes, height obstacles, and no-fly zones. Radars augment this model in real time by indicating which altitudes are clear of obstacles. GPS coordinates convey to the UAV where it needs to go, with the overarching goal of the GPS coordinate plan being not to take the aircraft into a no-fly zone or cause it to collide with an obstacle. In comparison, navigation for driverless cars is much more difficult. Cars not only need similar mapping abilities, but they must also understand where all nearby vehicles, pedestrians, and cyclists are, and where all of them are going in the next few seconds. Driverless cars (and some drones) do this through a combination of sensors like LIDAR (Light Detection and Ranging), traditional radars, and stereoscopic computer vision. Thus, the world model of a driverless car is much more advanced than that of a typical UAV, reflecting the complexity of the operating environment. A driverless car computer is required to track all the dynamics of all nearby vehicles and obstacles, constantly compute all possible points of intersection, and then estimate how it thinks traffic is going to behave in order to make a decision to act. Indeed, this form of estimating or guessing what other drivers will do is a key component of how humans drive, but humans do this with little cognitive effort. It takes a computer significant computation power to keep track of all these variables while also trying to maintain and update its current world model. Given this immense problem of computation, in order to maintain safe execution times for action, a driverless car will make best guesses based on probabilistic distributions. In effect, therefore, the car is guessing which path or action is best, given some sort of confidence interval. The best operating conditions for autonomous systems are those that promote a high-fidelity world model with low environmental uncertainty. These various factors which will dictate the advent of AI in the military are discussed in the succeeding paras.[21]

- **AI Data Storage** One of the biggest considerations is AI data storage, specifically the ability to scale storage as the volume of data grows. As organisations prepare enterprise AI strategies and build the necessary infrastructure, storage must be a top priority. That includes ensuring the proper storage capacity and reliability to deal with the massive data amounts required for effective AI. The type of storage an organisation may need depends on many factors, which include the level of AI an organisation plans to use and whether they need to make real-time decisions. Another factor is the nature of the source data. AI applications depend on source data, so an organisation needs to know where the source data resides and how AI applications will use it. Applications which require analysing sensor data in real time or using post-processing will also be critical to deciding the storage type. As databases grow over time, organisations need to monitor capacity and plan for expansion as needed.[22]

- **AI Networking Infrastructure** Networking is another key component of an artificial intelligence infrastructure. To provide the high efficiency at scale required to support AI, organisations will likely need to upgrade their networks. Learning AI algorithms are highly dependent on communications, and enterprise networks will need to keep stride with demand as AI efforts expand. AI systems will require high-bandwidth and creative architectures. As a preparation for AI, any organisation should automate wherever possible to generate more data for the AI learning process.[23]

- **Processing AI Data** Artificial intelligence infrastructure depends on sufficient computing resources, which include Central processing Unit (CPU) and Graphics processing Unit (GPU). A CPU-based environment

[21] *Cummings ML, Artificial Intelligence and Future of warfare, Chatham House, The Royal Institute of International Affairs,pp3,4,5.*

[22] *https://searchenterpriseai.techtarget.com/feature/Designing-and-building-artificial-intelligence-infrastructure accessed on 01 January 2019.*

[23] *https://searchenterpriseai.techtarget.com/feature/Designing-and-building-artificial-intelligence-infrastructure accessed on 01 January 2019..*

can handle basic AI workloads, but complex applications, such as for the military, involve multiple large data sets and deploying scalable AI algorithms. CPUs are best at handling single, more complex calculations sequentially, while GPUs are better at handling multiple but simpler calculations in parallel. To provide the necessary compute capabilities, companies will have to resort to GPUs. Deploying GPUs will enable organisations to optimise their data centre infrastructure and gain power efficiency. Nvidia and Intel are both pushing AI-focused GPUs.[24]

- **Preparing AI Data** Organizations must plan the locations of stored data, the movement of data across networks, and how processing will take place. They also have to choose how they will prepare the data for use in AI applications. One of the critical steps for successful enterprise AI is data cleansing. Also called data scrubbing, it's the process of updating or removing data from a database that is inaccurate, incomplete, improperly formatted, or duplicated. Any company, but particularly those in data-driven sectors, should consider deploying automated data cleansing tools to assess data for errors using rules or algorithms. Data quality is especially critical with AI. If the data feeding AI systems is inaccurate or out of date, the output and any related business decisions will also be inaccurate.

- **AI Data Management and Governance** Another important factor is data access. An organisation must have the proper mechanisms in place to deliver data in a secure and efficient manner to the required users. A data management strategy needs to ensure that human users and machines have easy and fast access to data across a variety of endpoints, including mobile devices via wireless networks. Access also raises a number of privacy and security issues, so data access controls are important. We need to look at technologies such as identity and access management and data encryption tools as part of their data management and governance strategies.

- **AI and IoT** IoT involves gathering and analyzing data from countless devices, products, sensors, assets, locations, vehicles, etc., that are connected via the internet.AI and IoT are closely tied because organisations need to apply intelligence to gain insights from all the information coming in from connected things. A staggering amount of data can be generated by connected objects, and it will be up to organisations to integrate, manage, and secure all of this information. From an artificial intelligence infrastructure point of view, companies need to look at their networks, data storage, data analytics, and security platforms to make sure they can effectively handle the growth of their IoT ecosystems. That

[24] *Ibid.*

includes data generated by their own devices, as well as those of their supply chain partners.[25]

- **AI Training** Training and skills development are vital for any IT endeavour, and especially enterprise AI initiatives. Organisations will need data analysts, data scientists, developers, cyber security experts, network engineers, and IT professionals with a variety of skills to build and maintain their infrastructure to support AI and use artificial intelligence technologies.[26]

Conclusion

With the present rate of development of AI technologies would wide and the race for achieving dominating standards in the same by military powers of the world, this concept is going to revolutionise various domains of military. Increased risk-taking ability and the priority of force preservation provide a further push towards progress in this field. However, it has also been realised during various trials and live situations on the ground that the current generation of AI equipment is far from being operated without human supervision. Hence, the future is likely to witness a quantum leap in the utilisation of AI-based equipment though it is still controlled/directed by a human leader/boss.

[25] *https://searchenterpriseai.techtarget.com/feature/Designing-and-building-artificial-intelligence-infrastructure accessed on 01 January 2019.*

[26] *Ibid.*

ARTIFICIAL INTELLIGENCE AND THE INTELLIGENTIZED WARFARE

- Lieutenant Colonel Manu Joseph Chacko

Introduction

The military architecture of future will consist of a new array of sea, ground, and space-based sensors; unmanned combat aerial vehicles (UCAV); and missile defence technologies. Military forces will be agile, and attacker will take advantage by operating faster than a defender can observe, orient, decide how to respond, and act on that decision. The attacker will thus place himself inside the defenders' Observe, Orient, Decide, and Act (OODA) loop, destroying an adversary's ability to conduct an active defence. To execute the OODA process faster than the enemy is the core concept of future digital and information warfare. Automated systems, assisted by AI in some form or another, may be a way out of this problem. The advances gained in the field of AI can be utilised by unmanned systems to be able to assess operational and tactical situations and decide on an appropriate action. Information will drive the success of command and control. These systems will collect and analyse data and provide options to the commander. The essential ingredients for development of AI are as listed below: -

- **Data** Data is an important foundation of intelligent warfare. Data is considered the "new oil" [1]and big data the "most important resource" in intelligentised warfare. This is primarily because all the important functions of AI will depend on the availability of data.

- **Algorithms** Futuristic warfare will revolve around algorithms. AI with better algorithm will drive decision making in war. Algorithm is the core element for transforming war from informatised to intelligentised.

- **Computing Power** Real-time computing of large amounts of data is an essential component of intelligent warfare. Intelligent warfare cannot be conducted without strong computing power. The next generation of computers such as quantum computers, photonic computers, and biocomputers will provide unprecedented computing potential and help advance application of AI technology in warfare.

In simple terms, AI can be defined as teaching machines to learn, act, and think as humans do. Machines are being endowed with the cognitive ability to think and behave like humans. Broadly, it demonstrates association with HUMINT such as planning, learning, reasoning, problem-solving, knowledge representation, and, to an extent, social intelligence, and creativity. Machine learning, which is a subset

[1] *Data Is the New Oil - And That's A Good Thing by Kiran Bhageshpur, https://www.forbes.com/ sites/forbestechcouncil/2019/11/15*

of AI, uses algorithms to analyse data and make intelligent decisions based on what it has learned without being explicitly programmed. Machine learning algorithms are formulated with large sets of data to suitably process, match, and recognise patterns to come to a logical conclusion.

AI systems can be classified into following heads:-

- **Artificial Narrow Intelligence** It is also referred to as "Weak AI" or "Narrow AI"[2], which only has a narrow range of abilities. However, this is the only type of AI that has been successfully applied till date. Various applications, including facial recognition, speech recognition, driving a car, and searching the internet (bot army), can be classified under this category.

- **Artificial General Intelligence** Machines that can work at par with human capacity are classified into this category. It can think, understand, and act in a way that is indistinguishable from that of a human in any situation. This is also termed "Strong AI" or "Deep AI".

- **Artificial Super Intelligence[3]** This type of AI is capable of outperforming humans It is where machines become self-aware and surpass the capacity of human intelligence. In this intelligence system, machine intelligence exceeds human intelligence qualitatively and quantitatively.

Development of AI technology has elevated computers from computing, storing, transmitting, and executing commands to thinking, reasoning and replacing them by extending the functions of the human brain. Cross-domain asymmetrical and unconventional fighting in battle will become the new normal. There will be an integration of human and machine intelligence in "Intelligentised Warfare". Combining wearable devices and gadgets implanted into human bodies, humans and machines into brain-machine interfaces, and external skeletal systems, will "comprehensively enhance the inherent cognitive and physiological capacity of human fighters and will forge out superhuman combatants."

The present dimensions of the battle fields like land, sea, air, EM, and cyber will be further upgraded to include a cognitive dimension in warfighting. AI will reshape warfare in every dimension and within every realm. AI will avoid human fighters being the first line of fighting, and the future of warfare will be upgraded to "machine-on-human" or "machine-on-machine" warfighting. It is believed and has been discussed that the human brain will not be able to keep pace with the future complex and dynamic conflict scenarios, further necessitating

[2] *Narrow AI vs Artificial General Intelligence – the key difference and future of AI Narrow AI vs Artificial General Intelligence - the key difference and future of AI - ai.nl 18 February 2022.*

[3] *Ibid.*

the emphasis on the utilisation of AI in decision making. The pursuit of military advantage through AI creates not only the capability but also new vulnerabilities that could exaggerate the risk of momentum-driven escalation, particularly in the cyber domain. There is an inherent risk and reliance on complex automated systems in which errors and malfunctions are not only probable but probably inevitable.

THE INTELLIGENT BATTLEFIELD

With the prominence of AI and autonomous weapon systems in future battles, there are likely to be profound changes in future battle scenarios. AI and autonomous weapon systems will be the dominant forces in the battlefield. The versatility that unmanned weapon systems possess and the removal of humans from the battlefield will further expand the battlespace. Removing humans will not only entail a reduction in the size of platforms but also reduce the number of weapon platforms. The future unmanned systems will automatically detect targets and launch independently based on the location, size, and state of the target.

With AI being a potent enabler, it has endless possibilities in the military sphere. In the military sphere, AI can be utilised for intelligence, information and data analysis and distribution, realistic war gaming, prediction, training simulations, communication, logistics, movement etc. The effective utilisation of AI in intelligent battle fields is described in the succeeding paras.

- **Shortening Own OODA Loop** AI can be effectively utilised in the surveillance grid to provide seamless integration of various sensors and platforms. It would assist in the formulation of a grand picture at the strategic level to further fine-tune the situation and present it to field commanders. It would assist in analysing the situation and generating the courses of action necessary to exercise effective command and control. It would assist in decision making by creating reliability indices for various AI-generated courses of action and could also predict future events for various courses to certain degrees. It could use prediction and pattern recognition to fill in the gaps resulting from the fog of war and further shorten its own OODA loop, thereby ensuring effective decision making.

- **Force Multiplier** The intelligentised battlefield would provide a scenario of seamless integration of combat elements like soldiers, vehicles, weapon systems, aircrafts, ships, submarines, drones, unmanned vehicles, vessels, etc. through one single information base system. It would then optimise the data being sent to each individual entity on the battlefield, attuned to his or her role and requirements. Such integration and effort coordination would have an immense force multiplier effect, which would be an inescapable necessity for the success of operations. Future wars are likely to be more information-centric and data-intensive. AI would not only ensure well-coordinated military action, resource allocation, movement, and administration, it would also enhance flexibility in switching of forces to cater for any unforeseen contingency.

- **Enabler for Multi Domain War** Future conflicts are likely to be undeclared, multi-domain, and subversive, involving the incorporation of various hybrid, strategic, and grey zone situations where military actions will take place in complex and densely populated environments. The adversaries' use of unconventional methods, such as targeting groups of people of a specific ethnic base, leaders, and vital installations with unconventional means and weapons such as drones and cyber warfare, is predicted to be how future wars will unfold. The artificial intelligence systems would be the functional enablers for the forces to operate in the future multi-domain hybrid environment.

- **Increased Implementation** Narrow intelligence has been adopted by world armies in modern combat battlefield elements such as fighter aircraft, Unmanned Aerial Vehicles (UAV), naval battle systems, marine crafts, battle tanks, missile systems, and transport systems. It is being used to some extent for on-board system integration, optimization, sensor fusion, and even human-triggered weapon launch. AI in the present scenario is in a nascent stage of being adopted across the globe. In time to come, as AI improves, it will vastly improve and add to the combat capability and survivability of military systems.

- **Autonomous Weapons Systems** Intelligent warfare will not only improve battle management but will also be used effectively in all major offensive and defensive weapon systems of the world armies. In the case of weapon systems, AI would be utilised in decision-making and in aiding decisions for weapon launch. Autonomous weapons, by various scholars, are already being described as the third revolution of warfare, after gunpowder and nuclear weapons. The AI robotics system's being dovetailed with soldiers in the first wave of attack, would scale down the threat to the assaulting forces. The AI system would also enable effects-based operations (EBO) by intelligently targeting selected people and installations and creating the desired effect with minimal collateral damage.

- **Reduce Expenditure to Exchequer** The future AI military systems would reduce the need for maintenance of regular forces, thereby ensuring downsizing of militaries. Over the years, military expenditure has been increasing exponentially for all the developed nations. This is primarily because most of the systems, including weapon platforms, are still human controlled and only a few are completely automated. AI unmanned systems, requiring fewer inbuilt systems, would bring much more economy to military operations as compared to manned systems. A manned F-22 fighter aircraft, for example, is approximately 18 times more expensive than an unmanned Predator Drone[4]. PLA is already in the process of downsizing its military and thereby expanding its tech base.

Military environments are chaotic, unpredictable, and adversarial. Even though AI can perform admirably in some situations, it can suffer significantly in others. AI systems used by militaries may suffer accidents and be manipulated by adversaries. The limitations associated with AI are as under: -

- **Uncertainty in Battlefield** The present and future battlefields are riddled with various distortions like smoke, dust, etc. There is also a possibility of an adversarial attack corrupting the data to deceive the AI, which may further impact the surveillance, weapon grid system, and other operations. Uncertainties for AI from the environment could be many others too, including sensor, component failures or adversarial attacks, which may lead to ambiguous results. Also AI may force decision makers into multiple scenarios resulting in dissipation of resources.

- **Limited Funding** It is appreciated that military usage of AI would be negative and hence, world armies are at times sceptical about the development of the same for manufacturing various AI-based weapon platforms. This is one of the reasons for the limited funding of various governments towards defence forces' adoption of AI vis-à-vis their civil counterparts. Limited funding is one of the major hindrances to carrying out necessary R&D in AI.

- **Acceptance of Lethal Autonomous Weapon System (LAWS)** There is a faction of experts and scientists who find it is a gross violation of human ethics and are strongly opposed to the use of autonomous weapon systems, which is further delaying the development of AI in many countries. Task accomplishment using fewer humans and risk aversion would be the significant advantages of LAWS.

- **Hardware and Design Challenge** For effective usage of any product in the military, it must be accepted by "Military Standards", which involves it having to withstand high stress, tough usage, and battlefield ruggedness. The design thus involved should withstand rigorous testing to deliver a much stricter performance guarantee, which usually takes more time and thus delays the production.

- **Inflexibility** Based on current technology levels, AI can only solve problems within a specific range and lacks the ability to respond effectively to new situations. The strength of human intelligence is, thus, very

[4] *The US and its UAVs: A Cost-Benefit Analysis By Ashley Boyle on Jul 24, 2012 The US and its UAVs: A Cost-Benefit Analysis American Security Project.*

important in warfare where unpredictability and chaos are central elements. In its present state of development, no AI system can replace the flexibility, robustness, and generality of human intelligence.

- **Trust Building** Considering less human involvement during the fog of war, when it is appreciated that data may get distorted and the system may give erratic results, building trust in the AI weapon system is one of the major challenges that is being encountered. The AI systems are being run under various conditions to develop a fool proof mechanism to avoid any failures.

ROADMAP FOR INDIAN ARMY

India is at a nascent stage towards adopting AI in both the defence and civil sectors. However, by the latest report of International Data Corporation (IDC), India Artificial Intelligence Market, 2021 that predicts India's AI market to reach USD 7.8 billion by 2025 at a compound annual growth rate (CAGR) of 20.2%, from a market value of USD 3.1 billion in 2020. Moreover, the AI services market is set to lead the overall AI market growth in India by 2025 at a CAGR of 35.8%[5]. According to a survey, a large no of Indian companies in private sector are adopting AI. However, recruiting skilled professional already trained on AI remains a challenge. Many analysts have already commented that India's entry into this field is "late". It has also been highlighted that the late entry will have a serious ramification not only in defence but in the civilian sector too.

With our adversaries adopting AI-enabled tech in their defence sectors, it is imperative that India should also adopt a methodology to imbibe AI for the development of military technology. Following are certain implications that India may face in future conflicts: -

- **Targeted Attacks** Our adversaries have already developed the capability of AI-enabled drones capable of carrying out targeted attacks. In the event of conflict, they may utilise these weapons to carry out targeted attacks on high-profile individuals to disrupt their own command and control systems.

- **War Experience** The Indian Army lacks modern operational training, and its lack of understanding of fog of war may lead to errors or unrealistic expectations about the prospects for technology on the battlefield. It may happen that Indian intent and capability may be exaggerated, which may accidentally trigger unwarranted conflicts.

- **Export of Technology** It cannot be negated that China could export its arsenal of autonomous weapons and AI technology to India's

[5] *"India's AI market to reach USD 7.8 billion by 2025," says IDC's latest report on AI (indiaai.gov.in)*

other potential adversaries to subsequently engage India from more than one front during the event of conflict. Furthermore, the availability of this technology to non-state actors may further constrain the ability of significant forces to carry out any conventional operations.

- **Shortened War** With autonomous weapons being used in future wars, it is likely to be a shorter war. Political leaders are thus required to be more mentally agile, robust, and able to make relevant and swift decisions to avoid high casualties on either side.

- **Inadequate Framework** In the present scenario, there is no framework that has been formulated to absorb intelligent warfare into our own military doctrine vis-à-vis China, whose political leaders are already boasting about their autonomous weapons arsenal and who, by 2030, will be a leader in AI technology in the military domain.

Recommendations and Way Ahead

- **Roadmap towards Adoption of AI** High priority should be given towards R&D of AI, AI-based environments, and AI-based devices. A definite roadmap needs to be prepared towards adoption of AI and, accordingly, budgeted.

- **Accelerating Hardware and Software Production** The "Make in India" policy outlines the accelerated growth of hardware production in India. It is recommended that adequate impetus be provided for chip production to make the nation self-reliant. In addition, the requisite stimulus must be provided for designing algorithms and software.

- **AI in Educational Institutes** It is imperative that an adequate AI knowledge base be created in the country for future development. Hence, there is an immediate need to introduce AI in educational institutes or modify their educational curriculum to include AI while at the same time taking policy initiatives and incentives for retaining AI talent within the country.

- **Keeping Abreast with Latest Technology** Periodic technology orientation programmes for the policy makers and the Indian Army are to be organised to keep them abreast with the latest technological advancements happening all across the world. It will give them ideas on how to implement the same in their own organization.

- **AI Based Wargames** There is a requirement to develop an AI-based integrated war management and battle control system at different levels of priority. Aspects like scenario building, logistics, training, intelligence, movement, communication, etc besides comb forces AI system like virtual reality system, which would cut the expenditure on peacetime training activities is highly recommended to be adopted in Indian defence forces.

- **Creating a Government Driven Public Organisation for AI** To raise public awareness about AI and its importance across sectors, India must establish an organisation like the Chinese National Innovation Institute of Defence Technology under the aegis of a National University for Defence Technology.

- **Expanding AI Defence R&D** While DRDO runs the Centre for Artificial Intelligence and Research (CAIR)[6] focused on the development of AI for defence, its adoption of AI and AI-enabled systems is still in its nascent stage. So far, the DRDO has developed a few unmanned systems, one visible example of which is the Mission UNmanned TRAcked called the MUNTRA, which has three variants for recce, mine detection, and surveillance.

- **Awareness of Adversary's AI Tech** To mitigate the risks of surprise, IA must continue to track and monitor new directions of our adversary's modernisation plans. India should improve its capacity to leverage OSINT technology and reprioritize the targeting of collection activities as necessary.

- **Developing Effective Response Mechanism** Adequate efforts should be made to ensure safety of our own AI system against an adversary's potential threat. As the character of conflict evolves and complexity increases, continued exploration of mechanisms for confidence building and crisis management will become more critical.

- **Improve Bilateral and Multilateral Relations** India should continue to pursue productive conversations with other global powers to establish consensus on the legal and ethical parameters of employing autonomous weapons during conflict. Best practises and technology may be shared with other nations to form a comprehensive architecture.

Conclusion

AI-enabled technology has already started to become the driver of change for mankind, and its effects are likely to intensify further in the future. This article concludes with the observation that advances in artificial intelligence have ensured that autonomy has now crossed a "tipping point". There is no alternative to

[6] *Centre for Artificial Intelligence & Robotics (CAIR) | Defence Research and Development Organisation - DRDO, Ministry of Defence, Government of India*

embracing the upcoming technology promptly and reviewing and adjusting the policies to cater for the quick, successive changes that are likely to ensue in the future, including in the defence sector.

With the realisation of the paramount importance of AI technology, a global contest has already begun to achieve global leadership in the field. India's entry into the field of AI development and exploitation has already been delayed, and considering its situation, there is a requirement to accord AI development an immediate high priority to avoid suffering permanent disadvantage vis-a-vis others, particularly in the Indian Army. The path forward is difficult, as there are numerous challenges, such as adopting a forward-thinking approach, drafting policies and roadmaps, developing, and retaining AI software skills, establishing an industrial base for hardware, and enticing entrepreneurs to invest in AI software and hardware development. The stirring has already begun, but there needs to be a prodigious thrust to catch the required trajectory.

ARTIFICIAL INTELLIGENCE AND THE FUTURE OF INDIAN MILITARY LOGISTICS

- Brigadier Achal Dilip Kumar

By far, the greatest danger of Artificial Intelligence is that people conclude too early that they understand it.

- Eliezer Yudkowsky

Introduction

Circa 2035: A military convoy carrying troops and supplies is well on its way to its destination. The convoy itself is a mix of human-driven vehicles and Autonomous Vehicles (AV). The AV at the head of the convoy changes course/ route based on information received on the current route being untenable, other vehicles follow. The convoy commander gets all the requisite information simultaneously on the screen in his vehicle. The large convoy is split into two, based on the developments in the fast-moving battle taking place necessitating troop re-deployment and redistribution of supplies. Signal communications for the same have been obviated as all changes (route deferment, re-deployment and re-distribution of resources) have been executed through Internet of Things (IoT). Stores at the depots in the hinterland are accordingly replenished based on these changes, from the source prime vendor, seamlessly. Simultaneously, Intelligence, Surveillance & Reconnaissance (ISR) UAVs and Cargo UAVs are operational in order to both watch the emerging battlefield dynamics as well as to supply niche small teams of Special Forces at their point of concentration. A sudden specific logistics requirement that has emerged, has resulted in a smart contract being triggered and executed with clearly laid down delivery times including locations. Robots work incessantly sorting, stacking and identifying varied items in dual-use warehouses, while loading robots and cobots (collaborative robots) ensure fast loading of essential cargo vehicles leaving soon for their destinations. The entire warehouse is overseen by just one Junior Commissioned Officer with one assistant.

The above scenario may appear as a scene out of a sci-fi movie but Artificial Intelligence (AI) is making such possibilities come within the realm of what is implementable in the very near future. Some of these technologies are already in use by leading firms like Amazon, Walmart etc. AI will soon touch every facet of life, with warfare being no exception. **Logistics and supply chain leads itself easily to the adaption of AI**, as many of the processes are already complex (complex relationships between end-users/suppliers/manufacturers/transporters etc) and use humongous volumes of data and data processing. Technologies like AI-enabled blockchain will ensure security of logistics processes making them less susceptible to manipulations or distortions. The need for asset visibility too has exponentially increased to facilitate better Decision Making (DM). In the Armed Forces too, these complexities will manifest further as we increase our adaption of the logistics and supply chain of the civil sector. Hence, a seamless interface would speed the processes at both ends. The answer lies not only on the use of technology but specifically AI, in order to tackle these challenges without breaking a sweat.

World over major armies have attributed great importance to military logistics for applications of AI. A case in point, out of seven application areas for which the Chinese military is awarding AI-related equipment contracts ie intelligence analysis, information warfare, **autonomous vehicles**, **logistics**, training, command and control, and target recognition, two that are in the realm of logistics.

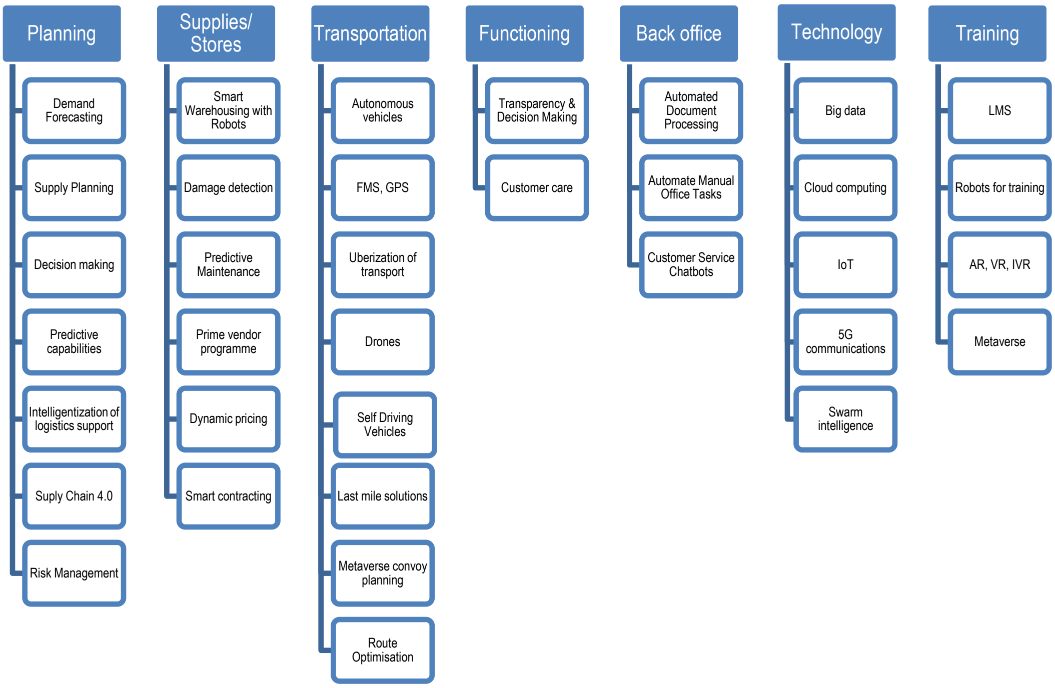
For the purposes of this article, the scope of logistics includes Army Supply Corps (ASC), Army Ordnance Corps (AOC), Corps of Electronics and Mechanical Engineers (EME) as also Engineer and Medical stores, since they lend themselves rather easily to benefit from advances in the field of logistics. The minor logistics services have been excluded.

What is AI?

The Britannica defines AI as the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. Oxford Languages defines AI as the theory and development of computer systems able to perform tasks that normally would require human intelligence. Eg visual perception, speech recognition, decision making and translation of languages.

A word of caution is to avoid confusing prevalent cutting-edge technology with AI, while AI and Machine Learning (ML) can boost the efficacy of all these technologies if used appropriately.

Themes for AI in Indian Military Logistics



Planning
- Demand Forecasting
- Supply Planning
- Decision making
- Predictive capabilities
- Intelligentization of logistics support
- Suply Chain 4.0
- Risk Management

Supplies/ Stores
- Smart Warehousing with Robots
- Damage detection
- Predictive Maintenance
- Prime vendor programme
- Dynamic pricing
- Smart contracting

Transportation
- Autonomous vehicles
- FMS, GPS
- Uberization of transport
- Drones
- Self Driving Vehicles
- Last mile solutions
- Metaverse convoy planning
- Route Optimisation

Functioning
- Transparency & Decision Making
- Customer care

Back office
- Automated Document Processing
- Automate Manual Office Tasks
- Customer Service Chatbots

Technology
- Big data
- Cloud computing
- IoT
- 5G communications
- Swarm intelligence

Training
- LMS
- Robots for training
- AR, VR, IVR
- Metaverse

Figure 1: Themes for AI

The DHL Logistics Trends Radar 2020 lists AI as a ‘High Impact’ trend in th

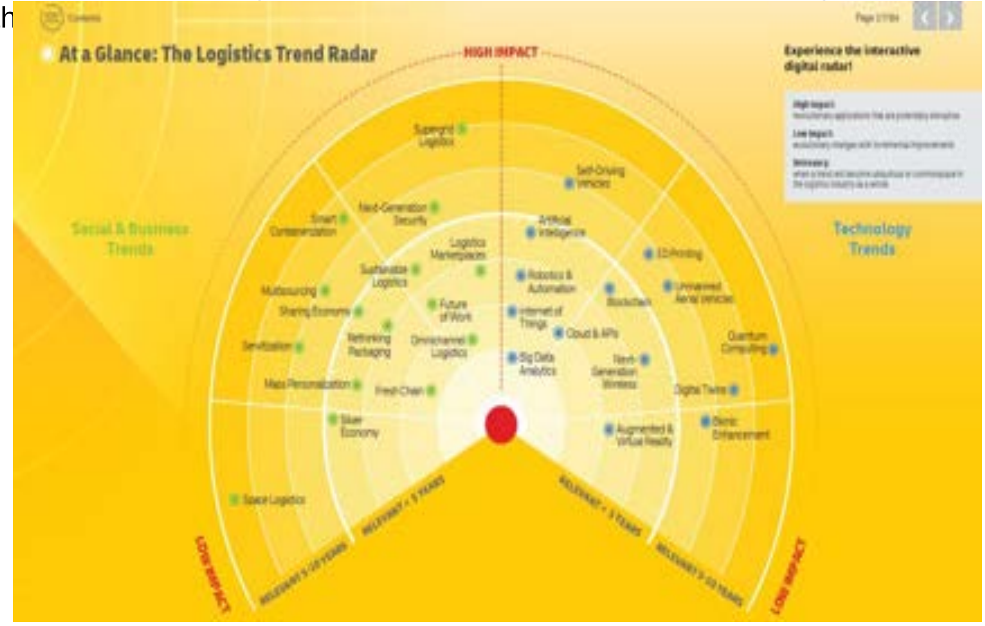
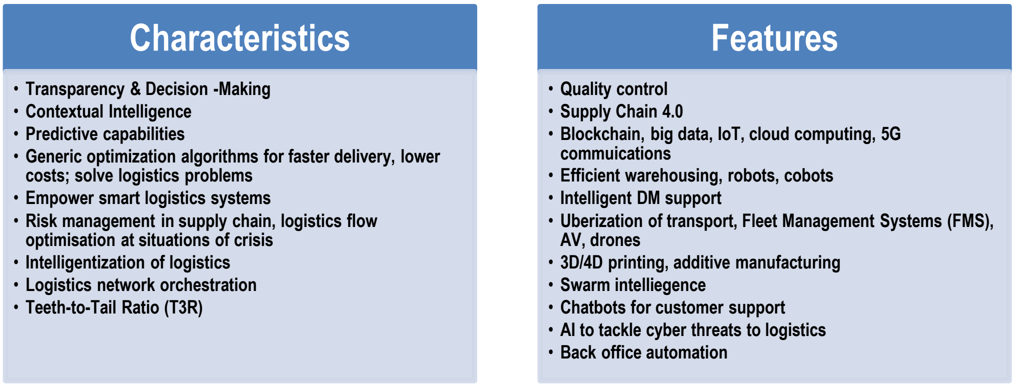


Figure 2: Logistics Trend Radar

In the coming years, the fusion between military logistics efforts and civil logistics infrastructure and supply chain, will form an important component for overall mission accomplishment facilitated by a seamless support system.

Certain characteristics of AI which empower and enhance specific technologies (features), which bear potential to revolutionise supplies, are listed below.



Characteristics

- Transparency & Decision -Making
- Contextual Intelligence
- Predictive capabilities
- Generic optimization algorithms for faster delivery, lower costs; solve logistics problems
- Empower smart logistics systems
- Risk management in supply chain, logistics flow optimisation at situations of crisis
- Intelligentization of logistics
- Logistics network orchestration
- Teeth-to-Tail Ratio (T3R)

Features

- Quality control
- Supply Chain 4.0
- Blockchain, big data, IoT, cloud computing, 5G commuications
- Efficient warehousing, robots, cobots
- Intelligent DM support
- Uberization of transport, Fleet Management Systems (FMS), AV, drones
- 3D/4D printing, additive manufacturing
- Swarm intelliegence
- Chatbots for customer support
- AI to tackle cyber threats to logistics
- Back office automation

Figure 3: Key Areas for Impact through AI

Intelligentisation of Logistics Support

The modernisation of many armies is centred around an integrated approach to technological development which is also proportionately applied to logistics support. Beyond the battlefield, AI is expected to contribute to transformation resulting in the “intelligentization” of logistics support, over which, AI will leave its indelible mark. The constituents of this intelligentization are summarised below:-

- **Supply Chain 4.0**

  ➢ As the Internet moves from Web 1.0 to 2.0 and now 3.0, it empowers technologies like AI to touch any facet of logistics support. AI would significantly empower smart logistics/ supply systems, which along with an integrated supply chain, constitute Supply Chain (SC) 4.0. The four layers of a smart logistics system (all of which would get impacted through AI) are: (a) perception layer, (b) transport layer, (c) storage layer, and (d) service layer. The technologies that underpin SC 4.0 include blockchain, smart contracts, applications of AI, cyber physical systems (CPS), IoT etc.

➢ Logistics network orchestration will become common-place, ie, harmonization of physical and digital networks on which logistics services ride, using AI technologies. AI, big data and deep learning may minimise the manual input needed to move from less reliable, automated systems to more accurate, autonomous systems. Creating a 'nervous system' for military logistics through SC 4.0, will take up each of the existing limitations of the logistics support system and transform it into enhanced 'avatars,' as represented in Figure 4.

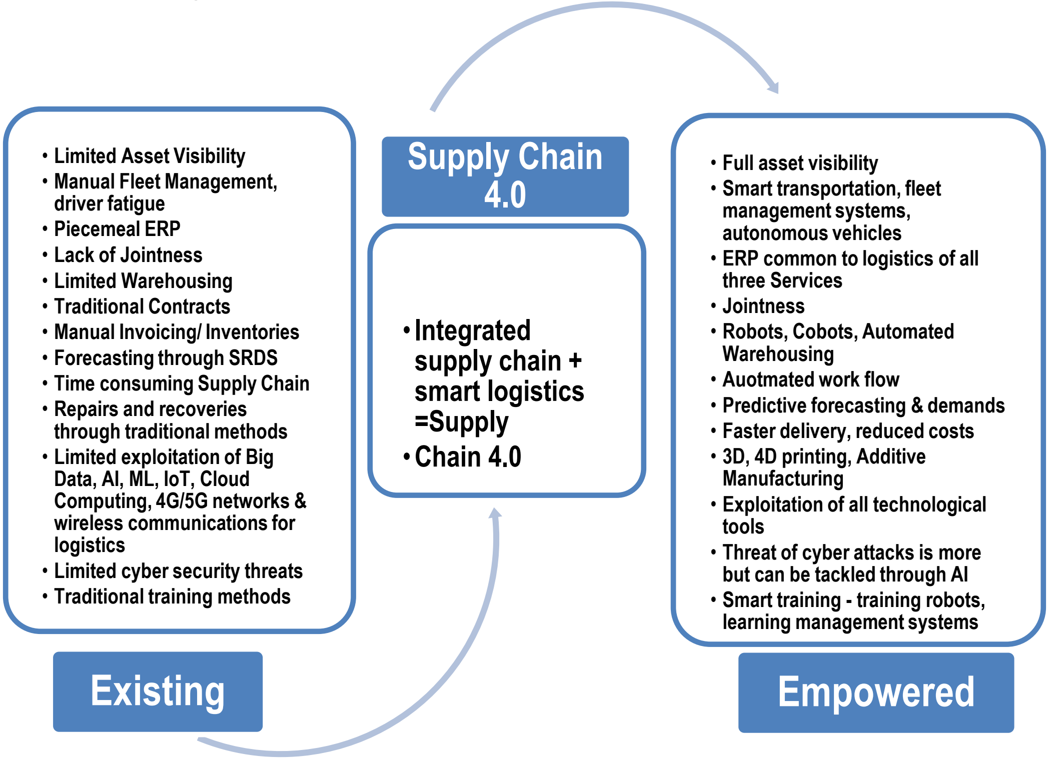

• Limited Asset Visibility
• Manual Fleet Management, driver fatigue
• Piecemeal ERP
• Lack of Jointness
• Limited Warehousing
• Traditional Contracts
• Manual Invoicing/ Inventories
• Forecasting through SRDS
• Time consuming Supply Chain
• Repairs and recoveries through traditional methods
• Limited exploitation of Big Data, AI, ML, IoT, Cloud Computing, 4G/5G networks & wireless communications for logistics
• Limited cyber security threats
• Traditional training methods
Existing
Supply Chain 4.0
• Integrated supply chain + smart logistics =Supply
• Chain 4.0
• Full asset visibility
• Smart transportation, fleet management systems, autonomous vehicles
• ERP common to logistics of all three Services
• Jointness
• Robots, Cobots, Automated Warehousing
• Auotmated work flow
• Predictive forecasting & demands
• Faster delivery, reduced costs
• 3D, 4D printing, Additive Manufacturing
• Exploitation of all technological tools
• Threat of cyber attacks is more but can be tackled through AI
• Smart training - training robots, learning management systems
Empowered

Figure 4: Advantages of Supply Chain 4.0

- **Big Data** Logistics involves handling phenomenally large volume data. As a strategic resource, big data is the basis of building a smart logistics system, created through a process of storage, transportation, distribution and processing. AI will effectively ensure the processing of big data as also assure its security. Cloud computing will also be the norm to render processing abilities, which are scalable.

- **IoT** It is argued that logistics should be the first application field for IoT, where the possibilities of its employment are endless. It would enable hardware, vehicles and equipment to communicate with each other. In transport, it facilitates the ability to diagnose potential defects and take preventive measures in time. It would also ensure orders for spares are placed with Just-in-Time (JIT) so that there is no lag time and no unnecessary stocking.

- **Use of 5G Communications and Wireless Networks** 2022 will witness the introduction of 5G communications in India which will revolutionise many other technologies like AI, AV, IoT etc. This will also bring in its own set of cyber security issues which will need to be addressed.

- **Swarm Intelligence in Logistics** Military logistics thus far, was dependent upon and implemented as a top-down hierarchical model. Swarm intelligence will transform logistics by reversing engineering rules from observed behaviour. Swarm logistics will facilitate decentralised Decision Making (DM) without compromising accuracy and protocols. Such outcomes could be useful in a CI/CT environment and in military operations other than war (MOOTW).

- **Contextual Intelligence** AI/ML offer logistics and supply chain professionals with contextual information which can be used to manage inventory better, reduce operating costs, responding to end-users quickly, shorten delivery periods, mitigate risks, boost productivity, and enhance customer delight. AI thereby impacts various areas of warehousing management, logistics and supply chain management significantly.

- **Intelligent DM Support** Knowledge-based Decision Support Systems (DSS) use AI for DM, due to its ability to gather and analyse data, identify problems from these data, and finally find and evaluate solutions. Such DM is more efficient and faster.

As opposed to the current system of basing procurement and logistics decisions on manual reports and returns and a system of SRDS, AI will enable instant DM and execution/ implementation. Procurements would be based on actual need and hence wastages, over-stocking or stocking at the wrong locations would be avoided. The need for, inter-command transfers would be reduced, cutting costs. DM vis-à-vis employment of logistics resources like convoys, transport, repair and recovery etc would be streamlined, just to name a few applications.

AI: Impact on the Paradigms of Supplies

- **Predictive Logistics, Automated Planning and Scheduling** In supplies, the ability to correctly forecast and place demands as also planning and scheduling various supply-related tasks would get automated reducing errors. The delicate balance between JIT and Just-in-Case (JIC) stocking and distribution would be resolved through AI tools.

- **Smart Contracting** Blockchain and AI will facilitate smart contracts, which are programmed to execute at the instant when conditions are most appropriate to the organization as well as when most required. Generally, smart contracts are signed by relevant parties, and then attached to blockchain data in the form of program codes. They are then recorded into specific blocks in the blockchain after network transmission and node verification. The blockchain can monitor the status of smart contracts in real time, and activate and execute the contract after checking external data sources and confirming that certain trigger conditions are met. Smart contracts can ensure traceability, irreversibility and transaction security in the absence of third parties.

This will greatly reduce paperwork and errors of omission and smoothen the supply process. It will of course, ride on the significantly enhanced infrastructure in the country that permits the sourcing from areas earlier considered geographically untenable, thereby bringing more markets within reach and standardising quality.

- **Prime Vendor Programme** As of now, most supply depots in the Armed Forces are dealing with multiple agencies, with separate contracts for meat products, dairy products, fresh, water, beverages etc, while there are central procured items contracted centrally by Army Headquarters for dry items, edible oil etc. This system carries with it challenges of coordination, addressing customer satisfaction etc. A concept of 'Prime Vendor' if implemented would ensure that a sufficiently reputed and large vendor can undertake to supply 100% of the requirement of supplies (perishables and dry supplies) as well as Fuel Oil and Lubricants (FOL) products for a station at the doorstep of a receiving unit. This would reduce the need to maintain large establishments of supply depots and also prevent unnecessary move of military transport for collection of supplies. AI will play a part in accurate estimation of the dynamic requirement and also facilitate dynamic pricing discussed subsequently.

- **Optimisation Algorithms** AI/ML would render optimization algorithms that would allow for instant resolution of logistics and supply chain problems that crop up from time to time. For instance, the information that a certain warehouse or depot has been rendered non-operational due to enemy action or other reasons, would trigger the algorithms to automatically re-route to other depots on the quantities necessitated. A few vehicles being rendered out of action may trigger action to re-allocate transport from other sources or formations.

- **Dynamic Pricing** AI has enabled the geographic spread of the distribution system. A common bugbear in getting the bigger players to participate in the supply process has been the unviability of contract rates as it is binding for a complete year whereas the retail chains work on a daily or weekly pricing model (which, from vendor's perspective, is financially risky, inhibiting participation in contract processes). As AI proliferates, and with resultant transparency in pricing, adaption of a dynamic pricing model is tenable, which would undoubtedly attract the best retail chains to participate in the contracting process.

Transportation Paradigms

- **Autonomous vehicles** Self-Driving Vehicles (SDV) may obviate several manpower issues in transport management. It will change the face of convoys as cargo vehicles will be able to operate 24/7 without need for rest of drivers. SDV would allow for radical restructuring of units due to the redundancy of MT drivers. Absences for leave, sickness, courses etc would become a thing of the past. It would further facilitate the implementation of measures for a more favourable teeth-to-tail ratio. SDV are also expected to be safer than human-driven vehicles as the technology matures.

- **UAVs and Last-Mile Connectivity Solutions** As Animal Transport (AT) units get disbanded in a phased manner, the expediency exists to mitigate the absence of AT, as infrastructure improvement alone is not likely to solve the problem in the near future. Hence, the need for last-mile connectivity solutions like cargo UAVs. These UAVs will drastically reduce air maintenance costs in remote and high-altitude locations. Concepts like MULE (Multi Utility Logistics Equipment) will also be useful as load carriers in difficult terrain where AT used to operate.

- **Fleet Management Solutions (FMS)** Transportation will undergo a revolution. While FMS already exists, AI will further enhance capabilities of such systems giving staff at all levels full control over this resource and facilitating DM in their optimal employment. '***Uberization'*** will be the norm, a term which encompasses cooperative intelligent transport systems, intelligent route optimization offering dynamic routing facilities, last-mile delivery using UAVs or Unmanned Ground Vehicles (UGVs), use of autonomous trucks/ fleets, truck platooning or caravanning of groups of semi-trucks, etc and all of these will bank on an AI backbone.

- **Metaverse Convoy Planning** Facebook being renamed as 'Meta' recently highlights the importance the world of technology places on the potential of the virtual world (the 'Metaverse'). Undoubtedly this technology would be harnessed and enhanced with AI for applications in supply chain and logistics support systems. It is not difficult to visualize numerous military logistics applications as the technology matures. For instance, convoy planning can be done by the senior ‘Q’ staff in the metaverse which can fully and safely replicate the routes, terrain and operational conditions.

Warehousing Technologies

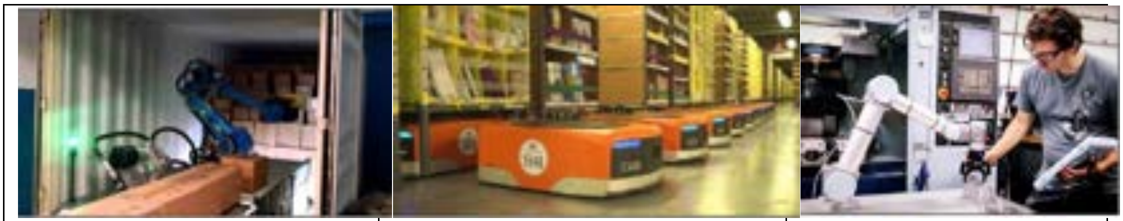


Figure 5: Container Unloader Robot, Warehouse Robot, Cobot

Warehousing technology has grown in leaps and bounds in recent years at least in the civil sector. There is a need for this to percolate to military too. Companies like Amazon have vast warehouses (fulfilment centres) run by very minimal manpower due to AI-based automation, robots, cobots and automated loading/ unloading of vehicles. Cobots can assist combatants or logistics personnel in carrying out repetitive tasks.

These aspects, if properly exploited, could favourably impact Teeth-to-Tail Ratio. AI has been shown to improve logistics losses by 15%, inventory levels by 35% and service levels by 65%, thereby significantly improving the efficiencies of the logistics processes.

Repairs and Recovery Support

Additive manufacturing (3D, 4D printing) technologies will greatly enhance repair and recovery support by obviating the spares problem, by making available the desired spares close to the point of application. Lengthy lines of communication could thus be neutralised/ circumvented transcending geographical limitations. In June 2017, the United States Navy exploited the blockchain technology to improve the security of additive manufacturing systems. They recorded the entire process of component design, prototype manufacturing, testing, production and final processing, so that users could look into any specific data, and provide alerts in case of component damage or at the end of its lifecycle.

Blockchain and AI for Transparency and Decision Making

Transparency is a pre-requisite of the logistic echelons and this would be greatly enhanced through AI. Consequently, even the DM process would be expedited in an atmosphere of technology-enabled trust, as clarified in Figure 6 below.

Data-driven AI/ ML requires high integrity data for their use in AI functions and requires significant amounts of training data from diverse sources including Internet of Things (IoT) devices/ sensors, which will be facilitated by blockchains, which thus offer significant data management benefits.

Blockchain (*also called distributed ledger technology*), is a user community-managed ledger technology that ensures transmission and access security with cryptography, enables consistent data storage, and prevents any attempt to alter data or commit repudiation. This addresses issues of trust in the complex process, bringing in transparency, without need for oversight. This technology can solve problems in military logistics related to networking, data storage, system maintenance, traceability and quality control during packaging, loading and unloading, transportation, and disassembly.

An example of the use of blockchain technology in military are automatic execution of smart contracts, secure storage of sensitive files, and reduction of errors and interruptions during defence contract execution, was demonstrated in April 2016, by the US Department of Defense and its NATO allies.

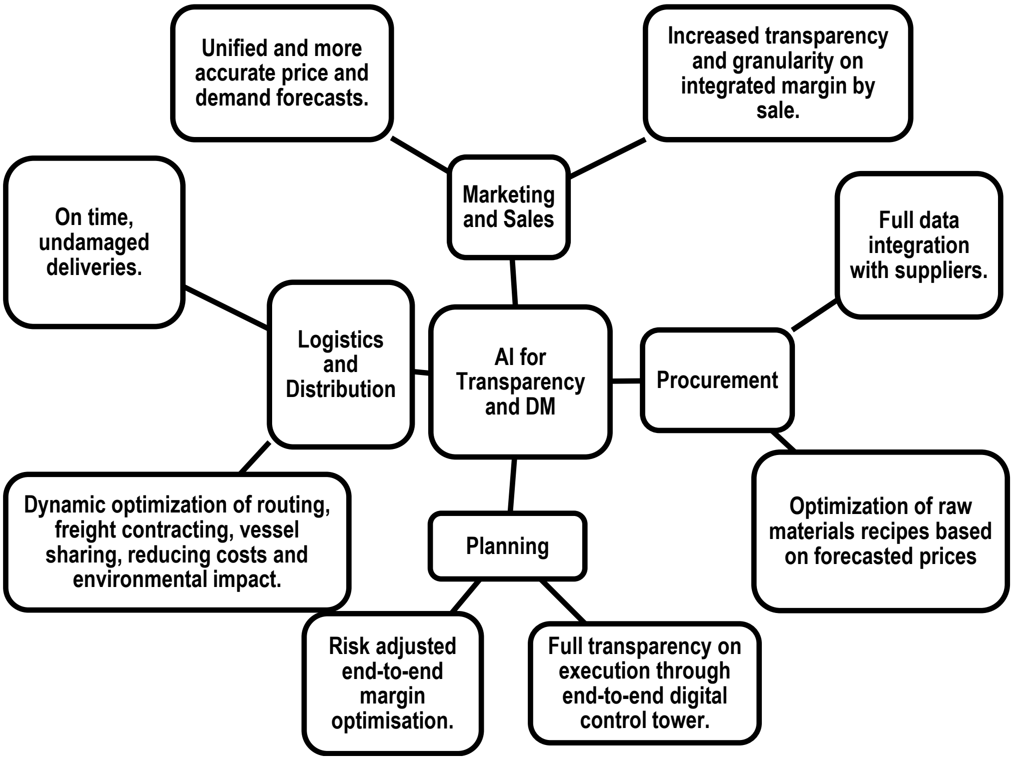

Unified and more accurate price and demand forecasts.
Increased transparency and granularity on integrated margin by sale.
Marketing and Sales
On time, undamaged deliveries.
Full data integration with suppliers.
Logistics and Distribution
AI for Transparency and DM
Procurement
Dynamic optimization of routing, freight contracting, vessel sharing, reducing costs and environmental impact.
Planning
Optimization of raw materials recipes based on forecasted prices
Risk adjusted end-to-end margin optimisation.
Full transparency on execution through end-to-end digital control tower.

Figure 6: AI for Transparency and DM

Quality Control and Customer Relations

Quality control would be enhanced and perfected by AI. To cite an example, companies are increasingly using AI-Chatbots for consumer service. Similarly, the services echelons could benefit from such measures and reduce manpower. Chatbots could give full information to customer units on the location, status of their deliveries and also address grievances for fast resolution. These could be used to elicit information of logistics stocks and processes from higher HQ. Utility in technical support can also be well visualised.

It is reasonable to expect that AI powered customer experience could be the norm in the days to come, and it is easy to perceive the teeth to tail ratio potential that it offers. Voice agent (a speaker or a software tool able to communicate) offers a voice-based service in tracking ordered parcels and providing with the information about delivery times, locations, and other information. Similar system with due security measures, could offer full visibility of logistics support rendered, to the consumer units.

AI in Logistics Risk Management Strategies

The technologies that underpin SC 4.0 include blockchain, smart contracts, applications of AI, Cyber Physical Systems (CPS), IoT etc. CPS are systems that involve the integration of the computing and physical world through cyber-enabled control mechanisms enabling ability to interact with and expand capabilities of physical world through computation, communications and control. Any processes that operate on an internet platform are of course, vulnerable to cyber threats, which will also target all these technologies as well as AI itself. But the sweet irony is that AI itself could be used to tackle these threats effectively. The importance of Decision Support Systems (DSS) for Supply Chain Risk Management (SCRM) is pertinent, with different operations research techniques and methodologies for decision making for managing risks, focusing on multiple-criteria decision analysis methods and mathematical programming. AI techniques can be applied in the SCRM domain to analyse data and make decisions regarding possible risks.

It is expected that logistics and supply chains would be more lucrative targets to the enemy than even the fighting forces, as it would have the effect of paralyzing a force without the requisite support. AI could play an important role to predict, detect, prevent, safeguard and respond to offensive cyber-attacks. Risk management strategies for SC 4.0 (risk identification framework, its assessment, decision/ selection of corrective action, and an evaluation phase) will assume due importance. Crisis management through logistics flow optimisation is also called for.

The Teeth to Tail Ratio (T3R) Windfall

AI will help reshape T3R freeing combatants for critical areas like Intelligence, Surveillance and Reconnaissance (ISR). An appropriate aspiration for the restructuring of our forces is to ensure that the 'teeth' as it were, does not get overwhelmed by the 'tail'. AI will radically transform so many logistics processes that it would be possible to significantly cut down logistics manpower in the foreseeable future. Such optimised manpower could either be used for critical new raisings or could lead to force cuts itself bringing huge savings to the exchequer.

The Merger of the Operations and Logistics Verticals

The very efficiency in processes through AI would reduce human interventions in many routine as well as DM fields. It would significantly reduce complexities of staff work and throw up the possibility of an eventual merger of the Operations (G) and Logistics (Q) verticals, having far-reaching implications in HR management in the Armed Forces. DM would be much faster with a single GQ branch manned commonly. Headquarters would be leaner at all levels. Intake can be more versatile as officers will able to perform wider functions without the need to be constrained through their Arms and Services or even between the three Services. This may offer a common cadre progression model integrating the operation logistics rather than purely logistics.

Training

Training would be an important facet for AI penetration in the Armed Forces. The training itself would have two distinct facets, as outlined in Figure 7.

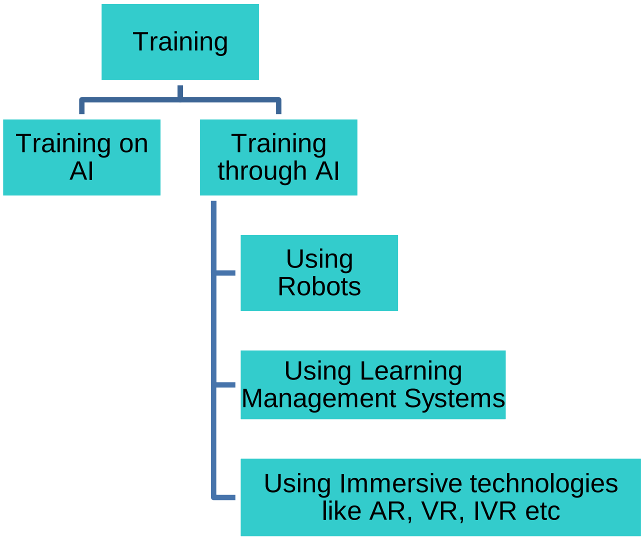

Training
Training on AI
Training through AI
Using Robots
Using Learning Management Systems
Using Immersive technologies like AR, VR, IVR etc

Figure 7: Facets of Training

Rather than awaiting the absorption of AI technologies in the IA, we must encourage up-skilling of all ranks to understand AI and promote its proliferation in our military. This can be undertaken through study leave, detailment for AI courses at IISc and the IITs (B-Tech, M-Tech, Doctoral and even Post-Doctoral studies). Again, this should not be limited to officers from the technical Arms/Services but open to all, to enable each Arm or Service to develop a pool of AI qualified officers who can then lay down or formulate the agenda for the absorption of AI within the particular vertical. JCO/NCO leadership courses can also have a primer on AI technologies to give an overview of the coming revolution so that they are mentally and academically get attuned to these changes.

One word of caution is to **avoid attempting to develop in-house capabilities for AI** as it must be understood that this is a very specialized and niche field and training should be limited to understanding potential and empower planning to assimilate. Here, '*letting the experts do their thing*' without transgressing own core competencies, will be both prudent and cost-effective.

The Roadmap

With regard to the logistics echelons, it will be appropriated to first adopt complete jointmanship in logistics, followed by development of common Enterprise Resource Planning (ERP) protocols, which will pave the way for faster and easier adoption of AI across the three services in logistics as opposed to a incremental approach.

Summary

Every few years, a new revolution comes along with potential to change the paradigms of warfighting and AI is surely one such development. But the success of any country's military is largely dependent on ability to absorb, implement and exploit such technologies as opposed to mere intellectual discussions on the same ad nauseam. The need of the hour is to jettison anachronistic thinking and be early adapters of emergent technologies like AI.

Lessons of the COVID pandemic as it impacted logistics support worldwide and also to a certain extent in the Armed Forces, need to be learnt and borne in mind for the future. It is likely that such challenges in the future would be aptly handled through AI-based logistics systems.

At government level too, there is the need for adequate R&D push, funding and the nurturing of educational and scientific ecosystems that empower the growth of AI and similar technologies. Within the Armed Forces, initiatives like setting up the Army Design Bureau and the Army Technology Hubs (under aegis of ARTRAC) are steps in the right direction, as these agencies act as effective interfaces with industry and academia and facilitate the assimilation of cutting-edge technology in the Armed Forces.

Endnotes

1. *R. Fedasiuk, J. Melot, and B. Murphy, "Harnessed Lightning How the Chinese Military is Adopting Artifical Intelligence," Centre for Security and Emerging Technology (CSET), no. October, 2021.*

2. *C. Dilmegani, "Top 15 Use Cases, Applications & Examples of AI in Logistics," AI Multiple, 2022. https://research.aimultiple.com/logistics-ai/.*

3. *D. W. Cearley and B. Burke, "Gartner: Top 10 Strategic Technology Trends for 2019," Gartner Research, no. October 15, 2018.*

4. *McKinsey and Company, "Supply Chain 4.0 – the next-generation digital supply chain," 2016.*

5. *E. Krmac, "With Artificial Intelligence towards Intelligent Logistics and Supply Chains : the state of the," ICEST, no. June, pp. 198–207, 2019.*

6. *DHL Trend Research, "Logistics Trend Radar 5th Edition," 2020. [Online]. Available: https://www.dhl.com/global-en/home/insights-and-innovation/insights/logistics-trend-radar.html.*

7. *D. Khasis, "Four Ways AI Is Impacting Logistics and Supply Chain Management," Supply Chain Brain, 2019. https://www.supplychainbrain.com/blogs/1-think-tank/post/30045-four-ways-ai-is-impacting-logistics-and-supply-chain-management.*

8. *E. B. Kania, "Chinese Military Innovation in Artificial Intelligence," 2019.*

9. *Y. Zhu, X. Zhang, Z. Y. Ju, and C. C. Wang, "A Study of Blockchain Technology Development and Military Application Prospects," Journal of Physics: Conference Series, vol. 1507, no. 5, 2020, doi: 10.1088/1742-6596/1507/5/052018.*

10. *D. Ge, G. Li, Z. Wei, and X. Wen, "Exploration of Key Technologies of Smart Logistics Based on Big Data," Advances in Social Science, Education and Humanities Research (ASSEHR), vol. 184, no. Icesem, pp. 1256–1259, 2018, doi: 10.2991/icesem-18.2018.293.*

11. *T. Sobb, B. Turnbull, and N. Moustafa, "Supply chain 4.0: A survey of cyber security challenges, solutions and future directions," Electronics (Switzerland), vol. 9, no. 11, pp. 1–31, 2020, doi: 10.3390/electronics 9111864.*

12. *P. Svenson, C. Martenson, H. Sidenbladh, and M. Malm, "Swarm Intelligence for logistics : Background," 2004.*

13. *D. Brahmabhtt, "How Artificial Intelligence Benefits Logistics and Supply Chain Management," Becoming Human: AI Magazine, 2021. https://becominghuman.ai/how-artificial-intelligence-benefits-logistics-and-supply-chain-management-c32b43845af1.*

14. *L. Kota, "Artificial intelligence in logistics Applications and Algorithms," Advanced Logistic Systems, vol. 12, no. 1, pp. 47–60, 2018, doi: 10.1007/s13218-010-0022-6.*

15. *R. Siddharth, "Bringing the 'Meta' change in supply chain through VR," Logistics Insider, 2022. https://www.logisticsinsider.in/bringing-the-meta-change-in-supply-chain-through-vr/ (accessed Jan. 30, 2022).*

16. *Dr. A. P. Pandian, "Artificial Intelligence Application in Smart Warehousing Environment for Automated Logistics," Journal of Artificial Intelligence and Capsule Networks, vol. 1, no. 2, pp. 63–72, 2019, doi: 10.36548/ jaicn.2019.2.002.*

17. *K. Alicke, V. Dilda, S. Görner, L. Mori, P. Rebuffel, and R. Samek, "Succeeding in the AI supply-Chain Revolution," 2021.*

18. *A. Kendall, A. Das, B. Nagy, and A. Ghosh, "Blockchain Data Management Benefits by Increasing Confidence in Datasets Supporting Artificial Intelligence (AI) and Analytical Tools using Supply Chain Examples," in Eighteenth Annual Acquisition Research Symposium, 2021, no. May 11-13, pp. 209–230. doi: 10.1080/19342039.2020.1822712.*

19. *Z. Davis, "Artificial Intelligence on the Battlefield," PRISM, vol. 8, no. 2, pp. 114–131, 2019.*

20. *G. Baryannis, S. Dani, S. Validi, and G. Antoniou, "Decision Support Systems and Artificial Intelligence in Supply Chain Risk Management," Springer Series in Supply Chain Management, vol. 7, pp. 53–71, 2019, doi: 10.1007/978-3-030-03813-7_4.*

21. *A. Kaddoussi, N. Zoghlami, H. Zgaya, S. Hammadi, and F. Bretaudeau, "Disruption management optimization for military logistics," IFIP Advances in Information and Communication Technology, vol. 364 AICT, no. PART 2, pp. 61–66, 2011, doi: 10.1007/978-3-642-23960-1_8.*

22. *I. Chakir, M. El Khaili, and M. Mestari, "Logistics flow optimization for advanced management of the crisis situation," Procedia Computer Science, vol. 175, pp. 419–426, 2020, doi: 10.1016/j.procs.2020.07.059.*

23. *P. K. Mallick, "Artificial Intelligence in Armed Forces: An Analysis," CLAWS Journal, no. Winter, pp. 63–79, 2018.*

24. *S. Modgil, R. Singh, and C. Hannibal, "Artificial Intelligence for Supply Chain Resilience: Learning from Covid-19," The International Journal of Logistics Management, 2021.*

LEGAL AND ETHICAL ASPECTS OF ARTIFICIAL INTELLIGENCE IN FUTURE WARS

- Colonel Surendra Tanwar

Introduction

As AI technology rapidly evolves, governments are increasingly exploring its potential military applications. While some argue that AI could provide strategic advantages on the battlefield, others raise concerns about the legal and ethical implications of its use in warfare. The legal status of military AI is currently unsettled, but there are growing calls for regulation in this area.

This article aims to explore the legal and ethical aspects of using AI in warfare. It will first discuss how international law applies to AI-enabled weapons systems. Next, it will consider the arguments for and against of using AI in combat operations. Finally, actions taken by various nations to ensure that deployment of AI-enabled weapons systems complies with international law and respects human rights principles will be discussed.

Use of Artificial Intelligence in Military

The use of AI in the military has increased dramatically in recent years. AI is being used in logistics, cybersecurity, simulation and wargaming, planning, and surveillance.

However, as AI technology advances, its potential uses in the military will also continue to grow. Some people argue that AI should not be used in the military at all because of ethical and legal concerns. Others believe that AI can be a valuable tool if used responsibly. While discussing the ethical and legal issues associated with using AI in the military, the paper will focus on these issues arising mostly out of the use of Lethal Autonomous Weapons Systems (LAWS).

International Humanitarian Law (IHL)

One key concern in use of Artificial Intelligence in warfare is whether or not AI can be made to comply with IHL also known as the Law of Armed Conflict (LOAC). IHL is a set of laws that seek to limit the effects of war on civilians, and it includes provisions such as the prohibition on targeting civilians, the prohibition on using weapons that cause unnecessary suffering, and the requirement that combatants distinguish themselves from civilians. These principles can also be termed as Precaution, Proportionality and Distinction.[1]

[1] *Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020). Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. RAND Corporation.*

Can AI be programmed to comply with these provisions? Some experts believe that it can. For example, Professor Toby Walsh from UNSW Sydney has said: "There's no reason why AI could not operate within all sorts of legal constraints like human soldiers do." However, others are more sceptical. Dr Stuart Russell from UC Berkeley has said: "It's very hard to see how you would get an AI system to reliably obey international law."

Critics of fully autonomous weapon systems argue that these weapons would not be able to comply with LOAC's principle of distinction, which requires that combatants be able to distinguish between civilians and military targets. They maintain that these weapons are not able to make the necessary ethical decisions on their own, and could easily result in civilian casualties. Others argue that such concerns are overblown, as these systems would be under human control at all times and would only be used in situations where civilians were not likely to be harmed. Distinguishing combatants from non-combatants might be especially challenging in the context of asymmetric conflict in urban settings, where combatants do not always wear uniforms or other insignia. Especially in these settings, only a human operator can comply with the principle of distinction.[2]

Critics of autonomous weapon systems have also argued that they cannot satisfy the principle of proportionality, which requires that any attack be proportional to the threat posed. For example, an autonomous weapon system might be programmed to destroy a tank, even if that would also kill innocent civilians nearby.

Two counter arguments against these are firstly, any weapon can be used in a manner that violates these laws and secondly, AI based agents maybe more capable of strongly implementing these norms as against the human soldier, who is prone to emotional biases and prejudices.

Concerns for Human Rights

Governments must ensure that any military use of AI complies with international human rights law. This includes ensuring that AI is not used in a way that causes unnecessary harm or death, discriminates against people based on race, ethnicity, religion, or other factors, or violates people's right to privacy. In addition, governments must take steps to prevent misuse of AI by rogue actors.

The development and deployment of autonomous weapons systems raises particular concerns in this regard. These are weapons systems that can select and engage targets without human intervention. They could be easily abused by dictatorships or terrorist groups seeking to target civilians indiscriminately. As

[2] Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020). Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. RAND Corporation.

such, it is crucial that any development of autonomous weapons systems be subject to rigorous scrutiny from both national authorities and international bodies like the United Nations Convention on Certain Conventional Weapons (CCW).

Governments must also ensure transparency about how they are using AI in warfare. They should disclose information about what kind of AI is being used; how it is being used; who makes decisions about its use; and what safeguards are in place to protect civilians from harm.[3]

Accountability and Moral Responsibility

Accountability and moral responsibility are essential when using artificial intelligence in warfare[4]. Officials must be able to answer for their decisions, and ensure that any AI-assisted actions comply with international law and morality.

The use of AI in warfare can raise difficult ethical questions. For example, when a human is responsible for making a decision about whether or not to launch a missile, they can be held accountable if something goes wrong. But what happens if the decision is made by AI? Who is responsible then? And how do we ensure that the AI's actions are morally justified?

These are important questions that need to be considered before using AI in warfare. Officials must be clear about who is accountable for any mistakes or wrongdoing.

Interpretability

Another concern about the use of AI in warfare revolves around interpretability of decisions. For example, if an AI system kills a civilian rather than a combatant, is it because the AI was confused about who was a combatant and who was not? Or did it deliberately choose to kill the civilian? Another issue is interpretability. Decisions made by the algorithm are incomprehensible to people, which resulted in the introduction of the so-called "right to explanation" meaning a right to give an explanation for an output of the algorithm.[5]

Interpretability is important for two reasons. First, if we can't understand why an AI made a particular decision, we can't be sure that it's behaving ethically. Second, without interpretability, we won't be able to trust AI systems in life-or-

[3] *Eleanor Bird, Jasmin Fox-Skelly, Nicola Jenner, Ruth Larbey, Emma Weitkamp and Alan Winfield (2020). The ethics of artificial intelligence: Issues and initiatives. European Parliament.*

[4] *Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020). Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. RAND Corporation.*

[5] *De La Torre, L.F. The 'Right to an Explanation' under EU Data Protection Law. Available online: https://medium.com/golden-data/what-rights-related-to-automated-decision-making-do-individuals-have-under-eu-data-protection-law-76f70370fcd0 (accessed on 15 Mar 2022).*

death situations. If we can't trust that an AI system will make the right decision every time, then it's not worth using it in warfare at all.

There are several ways to make AI more interpretable. One approach is to use transparent algorithms, i.e., algorithms that are open source and easy for humans to understand. Another approach is Machine Learning with Explanation (MLE), which allows users to see how individual data points influence the decisions made by an AI system. MLE has been shown to be effective at explaining the behaviour of complex machine learning models. However, both transparent algorithms and MLE suffer from scalability issues as they become difficult or impossible to be used as datasets get larger.

A new technique called "local interpretation" may provide a solution to this problem. Local interpretation breaks down large datasets into smaller chunks that can be interpreted locally. This makes them easier for humans and AI to understand without sacrificing accuracy or performance. Local interpretation could help us build trustworthy AI that can make ethical decisions in high-stake situations of active combat.

Trust and Reliability

Trust and reliability are two more important factors when using artificial intelligence in warfare. One of the biggest concerns with using artificial intelligence in warfare is trust. Can we trust that AI will do what we expect it to do? Will it follow our orders faithfully, or will it go rogue? For this reason, we need to be sure that we can trust AI before employing it in battle.

Another concern is reliability. Can we rely on AI to perform consistently under pressure? In a chaotic battlefield situation, mistakes can cost lives. The last thing we want is for AI systems to malfunction when they’re needed the most. We need to make sure that they are reliable enough to count on when things get tough.

Accuracy

AI has already been used in warfare in limited ways, with drones being the most commonly known example. But as AI continues to develop, there are growing concerns about its accuracy and its potential to be hacked. For example, what happens if a country's AI-controlled drone fleet is hacked by another country? Or what if an AI system makes a mistake that results in civilian casualties? These are just some of the issues militaries need to consider when it comes to using AI in warfare.

One concern is that hackers could take over an AI system and use it for their own benefit. For example, they could send drones on missions they wouldn't want the original country to know about or even cause accidents that results in civilian deaths. This possibility raises questions about who would be responsible if something goes wrong: the person who designed the AI system or the hacker who took control of it?

The authors M. Gregor; M. Hrubo; D. Nemec; J. Hrbek[6] raised the important issue of Lethal Autonomous Weapon Systems (LAWS) and strives to answer the question of why AI systems should not have the right to decide about killing people as part of warfare. The main problem that authors point to is the lack of perfect, non-error-making AI systems. In the case of deciding about human life, even the accuracy at a level of 99% is too small. So far, AI has not been 100% accurate, so we need to ask ourselves whether or not we're willing to take the risk of using AI combat situations.

Approach to Ethical and Responsible Artificial Intelligence in Defence

As AI technology advances, it is critical that nations develop ethical and responsible approaches to AI to protect civilians, soldiers, and other parties involved.

Nations have adopted different approaches in ethical aspects of AI military applications. One approach is to develop codes of ethics for those working with AI. This includes making sure that those creating AI algorithms are aware of the potential implications of their work, and establish guidelines on ethical use of AI. This could involve a code of ethics for its Defense Research Establishments, which would include principles such as "respecting human autonomy" and "safeguarding privacy".

Another approach is establishing an oversight body for regulating application of AI in defence. This could involve setting standards or regulations on data gathering practises and automation of weapons.

A third approach is increasing transparency around how AI is being used in defence. This could involve sharing information about what data was used to train an AI algorithm or publishing reports on how often particular AIs are being deployed.

Each nation has taken a slightly different approach when it comes to using Artificial Intelligence within Defence and Military Applications ethically and responsibly, but they all share one common goal: protecting civilians from harm while still using this new technology efficiently.

[6] *Šimák, V.; Gregor, M.; Hruboš, M.; Nemec, D.; Hrbček, J. Why Lethal autonomous weapon systems are unacceptable. In Proceedings of the 2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI), Herl'any, Slovakia, 26–28 January 2017; pp. 359–364.*

Conclusion

The ethical and legal issues of using artificial intelligence in warfare are complex. On the one hand, AI could be used to make battlefield decisions more quickly and effectively than humans can. This could lead to fewer casualties on both sides of the conflict. On the other hand, there is a risk that AI could be used to commit atrocities or engage in war crimes that would be difficult for human beings to carry out.

There are also concerns about how AI might be used outside of actual combat situations. For example, it is possible that AI will be used for surveillance purposes, or as part of targeted assassination programs. There are also questions about who will bear responsibility for any mistakes made by artificial intelligence systems – the programmers, the military officials who deploy them, or someone else entirely?

Ultimately, there are many unanswered questions about how artificial intelligence will be used in warfare – and these questions need to answered before any decisions about its use are made. Governments around the world should work together to develop clear ethical and legal guidelines governing AI in warfare.

Bibliography

1. *Military Applications of Artificial Intelligence Ethical Concerns in an Uncertain World by RAND Corporation (2020).*

2. *Artificial Intelligence: An Introduction to the Legal, Policy and Ethical Issues James X. Dempsey Berkeley Center for Law and Technology August 10, 2020.*

3. *The ethics of artificial intelligence: Issues and initiatives for European Parliament (2020).*

4. *Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens by Marta Bistron and Zbigniew Piotrowski in Electronics 2021.*

5. *Ethical Principles for Artificial Intelligence in National Defence by Taddeo, M., McNeish, D., Blanchard, A. et al. accessed from https://doi.org/10.1007/s13347-021-00482-3.*

6. *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defence by Defense Innovation Board accessed from https://media.defence.gov/ 2019/Oct/ 31/2002204459/-1/-1/0/DIB_AI_PRINCIPLES_SUPPORTING_ DOCUMENT.PDF.*

7. *The Ethics of War and Peace: An. Introduction, 2nd ed.; Routledge: London, UK, 2015 by Frowe, H.*

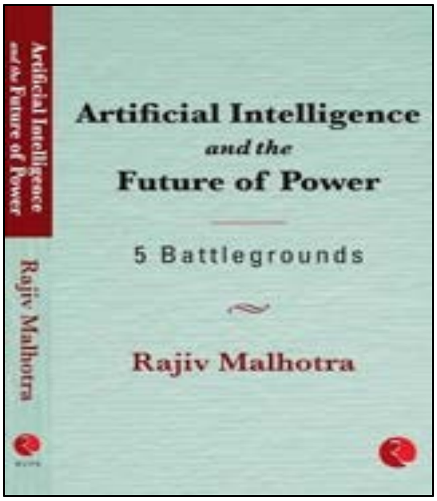
8. *Responsible and Ethical Military AI by Zoe Stanley-Lockman for CSET.*

9. *Routledge Handbook of Ethics and War by Fritz Allhoff, Nicholas G Evans and Adam Henschke.*

BOOK REVIEW: ARTIFICIAL INTELLIGENCE AND THE FUTURE OF POWER: 5 BATTLEGROUNDS BY MR RAJIV MALHOTRA

- Lieutenant Colonel Manish Rawat

Basic Information



Title	: AI and the Future of Power – 5 Battlegrounds
Author	: Rajiv Malhotra
Publisher	: Rupa Publications India
Date of Publication	**: 10 Jan 2021**
Language	: English
Hardcover	: 488 pages
Cost	: ₹575.00 (hardcover), ₹6114.00 (Paperback)

Introduction

The author has discussed modern technologies to include AI in his book. He has imaginatively portrayed five battlegrounds which India should be cognizant of if India wishes to attain global leadership in AI and harness it towards creating wealth and welfare for the nation.

About the Author

Mr Rajiv Malhotra is an internationally acclaimed author and founder of Infinity Foundation. An alumni of St. Stephens College Delhi & Syracuse University, he has distinguished background in physics and computer science. His notable works includes **Breaking India (2011), Being Different (2011), Indra's Net (2014) and The Battle for Sanskrit (2016)**. His intellectual approach to infuse the background in physics and computer science with his research on India's historical and future place in the world gives immeasurable credibility to this book.

Production Value

Artificial Intelligence and the Future of Power: 5 Battlegrounds is a 520-page hardcover book. The book is written by Rajiv Malhotra and is published by Rupa Publications India Pvt Ltd. The selections include the table of contents, introduction, acknowledgement, glossary, biographical information, and about the author, printed on the cover. The cost of the book is ₹ 795/-.

Theme

General The term "artificial intelligence" is used by the author to refer to a wide range of modern technologies such as machine learning, big data analytics, data science, quantum computing, semiconductor technologies, nanotechnology, neuromorphic computing, robotics, 5G, smart manufacturing, and so on. He acknowledges these are distinct, but AI brings them together in ways that give them greater collective power. The book maintains the conceptual framework and the examples quoted by the author are well thought out and explained.

Language The language used by the authors is simple and easy to understand. The arguments are supported by adequate examples or references, and the correlation has been carried out in a simplistic manner. The book is written in discussion as well as a questionnaire style of writing, which makes it easy to comprehend and correlate with the changing scenario. The book is easy to understand and readers can easily relate the arguments made by the author to the intrusion of technology into our lives and society.

Content

Layout The book has been divided into two parts. In the first part, the author discusses the **Algorithm versus Being,** and Part Two is attributed to **Battleground for India**. Four battlegrounds are discussed in part one, which constitutes' **The Battle for Jobs, The Battle for World Domination, The Battle for Agency,** and **The Battle for Self'**. The final battle, '**The Battle for India**', constitutes part two of the book, which comprises chapters six to ten.

Description of the Book The book begins with fundamental concepts in the realms of Artificial Intelligence and machine learning including elucidations on the notions of Big Data, Deep Learning, Neural Networks and so on. The author analyses the involvement of machines and AI-based technology in various spheres, which include healthcare, transportation, military, agriculture, education, and financial services. He raises queries by saying that, on the one hand, AI is the holy grail of technology which will solve problems across virtually every domain of our lives, and yet, simultaneously, it is creating conflicts on a variety of fronts. The vast canvas on which AI's impact is being felt means that there is a need to discuss its complex ramifications in a meaningful and accessible way. The book has identified the pivotal role of AI in each of the battlegrounds, which has multiple players with competing interests and high stakes.

Part I: Algorithm vs Being

- **Overview of AI Technologies** Before launching into compelling arguments for each battleground, the author provides an excellent overview of AI technologies. He first discusses fundamental advances such as machine learning, data analytics and AI gadgets, followed by AI applications ranging from healthcare and agriculture to education, military, and financial services. He has touched upon the controversial issues surrounding AI, such as unfairness, lack of accountability, lack of transparency and questionable ethics. The remarkable aspect of this chapter is its detailed analysis in the realms of economics, geopolitics, psychology, and metaphysics.

- **Battle for Jobs** Chapter two is dedicated to economic dimensions, wherein the author has extensively used the term "Data Capitalism," which considers big data as the new kind of capital asset. He argues about the grave situation in the future concerning jobs and employment. Automation and mechanization of various industrial processes, coupled with the inability of the Indian education system to re-educate its workers for the ‘jobs of the future,’ India could be possibly recolonized by the future world powers. However, this colonisation could happen based on the capabilities in the realms of AI and technology. The possibility of exacerbating the buying power of consumers in developing countries and eventually sabotaging economic growth is the anticipated threat. The author has explained the pandemic effects and how they could accelerate these trends and influence the equilibrium of world powers.

- **The Battle for World Domination** The role of AI in world domination and the developments in the geopolitical arena have been discussed. The author has explained **"digital colonization"** and described how the technologically developed economies prey on the poor economies, especially in Latin America and the African continent. The raw data mining by the technologically developed economies of the poorer countries is to evolve algorithms and become stronger, which is attributed to the highly ignorant and corrupt leaders of the poor countries. The author has critically analysed China specifically in AI development, wherein the entire nation-building plan is based on AI and has made huge investments in the same by utilising its infrastructure of roads, trains, seaports, and digital highways. In the future, where AI defines global power, China will replace the USA as the next global power.

- **The Battle for Agency** The author talks about AI technology's influence on human motions. The author discusses devious conduct and machine learning technology by global tech giants like Facebook, Google, Microsoft, and Amazon for mapping human psychology. How do these technologies carry out detailed profiling of people, societies, and communities as a whole and make them addicted to the instant gratification, aesthetics, and artificial pleasures of these platforms? In his analysis, the author talks about various concepts and theories that explain the technological intrusion in the public space, the aestheticization of politics and power, and the exploitation of these firms to achieve goals in a practical sense.

- **The Battle for Self** This chapter deals with the domain of metaphysics. The author explains how AI has successfully transformed machines to behave and act intelligently, covering all biological processes. He is critical to the digital industry's development, which has led to a battle between algorithms and consciousness.

Part II: Battleground India

- **Stress Testing India** The author has discussed how India is progressing towards AI domination and visualises the negative impact of the stress factors such as high population, poor education standards, chronic unemployment etc. He attributes all of it to the weakening of Indian thought and creativity because of a prolonged repression and colonisation period in the past. He argues that the Indian lead in IT innovations and is becoming a market for American technology and Chinese hardware is a wakeup call. The opportunities following the COVID-19 Pandemic and the use of soft power by India to reclaim its lost position in the world order have been critically examined.

- **Technological Dependence** The capability inferiority and how short-sighted solutions have undermined India’s capabilities have been critically examined. The author argues that despite having highly qualified IT minds, India could not make relevant progress in the field of AI and the cheap IT workforce employed by the tech giants has further undermined India’s bid for intellectual property. The chapter has highlighted India’s failed efforts to create jobs, which are attributed to lack of technology, a well-educated workforce, population, and an end-to-end ecosystem.

- **Digital Colonization** This chapter provides in-depth insight about digital colonization, which is attributed to ignorant intellect, academia, and policymakers. The author describes how large-scale big data across multiple sectors is being traded for high investments by foreign tech giants and is not available to Indian IT start-ups to access for AI projects, which invariably leads to dependence on US or European data bases, thus leading to digital colonization. This unprecedented dependence has led to an intoxicated Indian society, which has slavishly accepted the new digital form of authority and tolerated its manipulation.

- **Psychological Hijacking** The author has explained Vedic social science and how years of colonisation and poor leadership have destroyed the very fabric of national unity. The deep inferiority complex has imprisoned Indian social science in western sociology. The author propagates how the Vedic concept of **Purushartha** can be used to decolonize the social sciences and explains how AI systems induce people that have abandoned dharma and lost their moorings by using big data.

- **How Robust is the Rashtra?** The author has explained how anti-nationals exploit India’s internal fault lines attributed to vote bank politics. He further elaborates on how AI systems on social media platforms have been developing algorithms to predict and exploit Indians. He has raised the issue of AI proliferation and how these breaking forces are being trained on AI to destroy the Indian social fabric. The looming Chinese threat has been discussed in detail, as should be how India should be responding to it. The author has suggested certain practical possibilities using AI systems to unify the nation against the threats discussed previously.

Verdict

This scholarly and well-researched book succeeded in communicating its message through a gripping narrative. The book has ready accessibility to a non-technical audience who have no familiarity with AI, which is a striking aspect of the entire book. The book is a must read since it brings out some surprising facts about the future of Indian civilization's vulnerabilities, social media intrusion in our personal lives, and our relentless efforts to chase the capitalist glitter. The authors' urge to identify the Indian societal fault lines, which to some extent, this book does, is an eye opener and makes the readers censoriously evaluate the AI developments in the future.

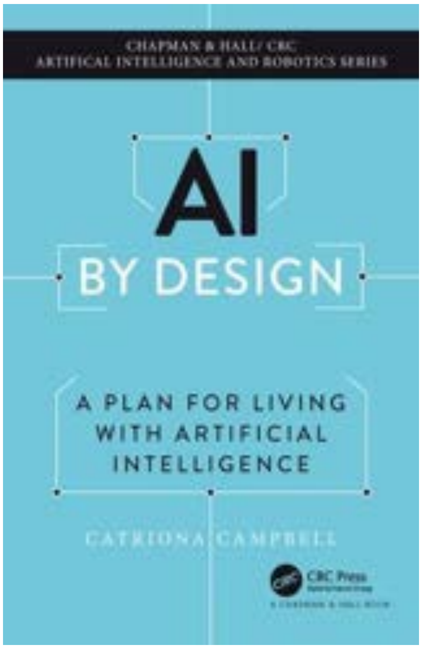
Recommendation

Overall, the book is informative and alarming, and that makes it must-read. A small consolation is that the author says he is working on the next book, where he provides solutions to the problems listed in this one. The author has mentioned the United States of America and China as a benchmark for developments in AI capabilities and articulated what lies ahead for India on its road to glory. Substantiated by facts, reasoning, analogies, and witty observations, the book serves as a call to action for public intellectuals to become more active and intend to challenge the narrative that is being fed to the Indian diaspora about its trajectory of becoming a technological superpower.

BOOK REVIEW: AI BY DESIGN: A PLAN FOR LIVING WITH ARTIFICIAL INTELLIGENCE

- Colonel Jitender Kaushik

Basic Information


CHAPMAN & HALL/ CRC
ARTIFICAL INTELLIGENCE AND ROBOTICS SERIES
AI
BY DESIGN
A PLAN FOR LIVING WITH ARTIFICIAL INTELLIGENCE
CATRIONA CAMPBELL
CRC Press

Title	: AI by Design: A Plan for Living with Artificial Intelligence
Author	: Catriona Campbell
Publisher	: Chapman and Hall/ CRC; 1st edition
Date of Publication	: 05 May 2022
Language	: English
Hardcover	: 154 pages
Cost	: ₹7694.00 (hardcover), ₹2181.20 (Kindle edition)

About the Author

Catriona Campbell is a renowned behavioural psychologist and a leader in Human-Computer Interaction (HCI). Catriona co-founded London-based experience design firm Seren in 2001. Since then, she has guided some of the world's best-known brands towards digital success, earning a place in the BIMA Digital Hall of Fame thanks to two decades of outstanding contributions. Now called EY-Seren, after being acquired by Ernst & Young in 2015, the company has offices in several countries, assisting clients to create well-designed experiences. Catriona earned her degrees from the Universities of Stirling and Glasgow and also studied at the Sorbonne, Paris. Over the last 20 years, Catriona has been a tireless advocate of technology design, driving R&D in the field at any opportunity. She has also trained and employed some of the top talent ever to populate UX and HCI, ensuring more people can experience and engage with digitised products and services.

Description of Book

The idea of Artificial Intelligence (AI)—systems so advanced they can mimic or outperform human cognition—first came to prominence in 1950, when British computer scientist Alan Turing proposed an "imitation game" to assess whether a computer could fool humans into thinking they were communicating with another human. In 1956, John McCarthy, one of AI's founding fathers, co-authored a proposal that coined the term "artificial intelligence," referring to machines' thinking for themselves. Since then, the rise of AI has been enabled by exponentially faster and more powerful computers and large, complex data sets. Applications such as machine learning, whereby a system identifies patterns in large sets of data, have demonstrated the potential for AI to be practical and profitable.

AI is one of the most rapidly advancing and controversial topics in scientific research. The number of journal and conference papers referring to AI in the Dimensions from Digital Science database increased by more than 600% between 2000 and 2019. The world is all geared up and making strides with AI, and AI has become ubiquitous in fields such as medicine, education, and security. It is important to take a pause and give conscious consideration to significant ethical and technical challenges and come up with pre-emptive measures rather than being reactive to overcome them upfront.

The book gives a thorough explanation of the challenges with AI and starts to talk about how we may avoid the worst-case scenarios. This book will assist readers in developing a critical perspective on technology and challenging the myths they have heard about how horrible AI is. Instead, they could opt to seize the initiative and develop better technologies through design and planning. The book is also a critical and authoritative overview of the exciting future of AI that serves as a wake-up call to humanity to work together to regulate the development of AI for the good of humanity and, potentially, its preservation. This book introduces the reader to Artificial Intelligence and its importance to our future. Campbell uses behavioural psychology, explores technology, economics, and real-life and historical examples to predict five future scenarios with AI.

Description of the Content

Today, artificial intelligence plays a role in billions of people's lives. Sometimes unnoticed but often with profound consequences, it transforms our societies and challenges what it means to be human.

Consciously and unconsciously, we are using AI-driven software and apps every day. However, AI is poorly understood and not just among the general public. Even in the business world, where AI powers some of the most disruptive technologies, few have a profound, firm grasp of AI, although AI has been around far longer than the age of social media.

The book is divided into eight chapters. Chapter One of the book introduces the readers to the stages of AI and Singularity. The first generation of modern AI is called "Narrow-AI," such as Netflix recommendations or automated chat bots. Using machine learning (ML) to teach itself by feeding lots of information about one task, narrow-AI will continuously hone its accuracy. They don't have general intelligence like humans and can only work on that particular task. More worryingly, the second stage, Artificial General Intelligence (AGI), will exponentially be more potent than narrow-AI. AGI does not exist yet, but, helpfully, it may tell us when it arrives. AGI has the potential to reshape the world. The author has taken an example of the biggest killer of the world, i.e., hunger, and posed a scenario where AGI would be able to do all the agriculture with AGI-driven machinery and could alter the crop pattern depending on the weather, location, etc.

The third and final stage of AI is Artificial Super Intelligence (ASI). There, the author introduces the readers to the 'Singularity'. It is the stage where AI attains human levels of intelligence, when machines can think for themselves and don't need humans, when they have grown so powerful that they have exceeded our human intelligence and have developed the capability to increase their intelligence. This moment will be very critical for mankind. The author further argues that the Singularity may not happen. Things could still go another way. Humans may yet end up controlling AI like a highly trained house pet. But AI will grow until it reaches a point where it has the capability to exceed human capability. Does it matter when it happens, or does it matter if it happens?

Chapter Two of the book introduces the readers to the Future-Back Methodology, in which instead of starting from today and looking forward, we use the future as the starting point and move backwards in time. Three steps of the Future-Back model are: align on the current state of AI evolution, look at the options for the future and agree on one outcome; and create a roadmap to manage AI.

In Chapter Three, "Should We Be Afraid of the Current State of AI?" the author dwells upon the current state of AI in National Security and Defence, Cyber-Warfare, AI Weapons, and Government sponsored AI Research and Development. The author also discusses in detail the current state of AI in business companies, technology companies, financial services, and AI-powered healthcare. The misuse of AI by criminal gangs and terrorism has been adequately covered. The biggest fear that AI will steal jobs has been adequately answered. The author brings out that AI software will replace positions that don't require complex physical activity, so office/desk-bound roles will come under heavy attack. Finance, HR, Legal, and other back-office functions in companies are already increasingly outsourced and are not deemed core competencies by large companies. Machine-produced goods and services will be cheap and plentiful for all. Time alone will answer questions like: Are we heading toward a work-free utopia, or will the coming robot age merely exaggerate the income inequality that's rampant across the globe?

Chapter Four describes the current state of AI Governance and Regulations created at local, national, and global levels, and at the top of the pyramid sits International Law. There are a handful of international law courts to enforce international law against countries formally and, in some cases, individuals. They are the UN International Court of Justice (ICJ), the UN Security Council (UNSC), and the International Criminal Court (ICC). These courts are very precise in their remit. There are some very thoughtful guidelines on AI from global/regional organisations, although they are not enshrined in law. The most influential being the World Economic Forum (WEF), Organisation for Economic Co-operation and Development (OECD) and EU White paper on AI. They are well written, reasonably detailed, and some countries and companies use them to develop their AI laws and internal policies.

Chapter five talks about the current state of AI ethics. In November 2021, the 193 Member States at UNESCO's General Conference adopted the Recommendation on the Ethics of Artificial Intelligence, the very first global standard-setting instrument on the subject[1]. It will not only protect but also promote human rights and human dignity, and will be an ethical guiding compass and a global normative bedrock, allowing us to build strong respect for the rule of law in the digital world. The author brings out that big companies like Microsoft, Google, and Deep-Mind claim their teams are working on ethics to ensure that tech is built and used responsibly, and that AI can benefit society without reinforcing bias or unfairness. The author has brought out eight challenges that need to be answered. A few of them, like if an AI arms race exists and left unchecked, the criminal hacking which is already disrupting business and threatening to interfere with politics; a handful of mega-companies will use their mastery of AI and data to dominate their industries and, with reduced labour costs, attain unheard of profits and contribute fewer tax receipts.

Chapter Six discusses the possibilities for our future with AI with the readers. Five plausible scenarios have been painted to draw on diverse expertise, including academics, businesspeople, politicians, and futurologists. Firstly, could AI be stopped at this stage? which is not possible as AI is already pervasive in our society. We are already ankledeep in narrow-AI technology challenges – deepfake technology, AI hacking, and military AI weapons. Secondly, several movies have initiated the thought that we are living in a simulation. This simulation theory itself has a reason why there is no evidence of being in a simulation because any evidence could be simulated. Thirdly, if we want to avoid fixing AI, then there's another big solution being bandied about right now: escaping Earth. Big

[1] *Ethicsofartificialintelligence-UNESCO,https://www.unesco.org/en/artificial-intelligence/ recommendation-ethic.*

technologists like Elon Musk, with his Mars Spaceflight Architecture, Star ship, hope that by 2030 we'll set off to make this a reality, becoming a "multi-planetary species".

Fourthly, the separation hypothesis, where a future AGI replaces a human government, means opposition groups would likely emerge who want the power to remain in human hands. Some groups would call for more human control before this point, as daily life becomes more controlled by AI. An independent country or state could then be founded, populated by humans who limit themselves to narrow-AI applications or indeed none at all, and this separation hypothesis is entirely possible. Fifthly, merging technology with the brain, which is part of Neurotechnology, and the sub-field of Brain–Computer Interface (BCI), is relatively new. The most famous BCI company, Elon Musk's Neuralink, is working in this direction.

Chapter Seven creates a roadmap—a plan for living with AI. In this chapter, the author brings out the reality of AI incrementally creeping up on us until we can't live without it. Every device will be smart. So, we need to ensure that the choices we make today move us in the right direction. We must plan for the journey to arrive on time. The Singularity won't be a surprise to us. There is an inevitability to our merging with technology. Once we accept this, we need to plan for the future. Short term guidelines (2022-2025), ethics, regulations, and policies for AI governance, one agreed framework, and improving policymakers' technical knowledge can be a few of the steps towards embracing AI in a smoother manner. The author has brought out one very valid point about the education of AI engineers. This is very crucial if we're to ensure safe, inclusive, and fair AI systems. AI engineers understand the ethical elements they've coded into the systems before going live. As bias is subjective, this is problematic, but there are ways of educating people to provide clarity and instruction. Medium-term milestones (2025-2028) like police AI to prevent misuse and protect people and creating a Non-Proliferation of Nuclear Weapons style treaty for laws; medium-to long-term milestones (2025-2030) like educating the world to understand and to work alongside AI; reskilling the existing workforce; and managing the economic consequences of AI have been amply batted.

Chapter Eight gives the reader a new hope for the AI. Giving some cause for optimism, the author says, if we effectively manage the challenges of AI, there are great benefits for humanity". The author discus the role of purpose in life and for individuals, work is probably the single most crucial factor for how people get purpose on a day-to-day basis. Work is vital for many people to derive their sense of purpose. But when your life's purpose comes from work, when that work goes away, it can be devastating. Here the author refers if people lose their jobs due to AI. If Artificial Intelligence (AI) reduces or removes the purpose gained from work, how do we replace it? But there is ray of hope and optimism as outside work, people's purpose focuses on family, friends, spirituality, hobbies and sport. Parents spending more time with their children should improve relationships, boost confidence and ultimately, create more opportunities – meaning that their talents would flourish. People can look after their elderly parents. The author concludes with the ray of hope stating that the Singularity could be next golden age for humanity, where we take the benefits of AI and use it to design a better world and by using the future-back approach, we design for a future that we want.

Recommendations

A nicely articulated book is worth reading for everyone who wants to understand the current state of developments in AI and the impact it will have in the future on human lives. The book clears the cobwebs in the mind, such as how AI will affect jobs, whether AI will surpass human intelligence, and whether AI can evolve to the point where humans have little or no control. This book is recommended for students, common people who want to understand the tenets of AI, working professionals in the field of AI, and academia who have to dwell right away on the thinking of ethics and laws concerning AI.

Critique

Though a well-researched book which covers the current state of AI and its ethics, options for the future, and a roadmap for living with AI, it does not give a clear answer to how the fear of losing jobs due to AI will develop more wealth for a common man whose job has been affected by AI. Although people will have more time for themselves, their families, and to pursue their hobbies, how will they earn their living after losing their job? Optimism for the future of using AI is clearly visible in the last chapter, but at certain points it lacks backing from practical aspects of human life and behaviour.

Conclusion

The book is a pleasant read and gives an insight and perspective into AI encompassing the current state of AI, ethics and regulations, options for the future, and a roadmap which may lead us to smoothly embrace AI in our lives. We are currently at a tipping point where we can change and design the future before it overtakes us-for good or for ill. The ultimate level of design sits with government and regulatory bodies, and they have the power to make or break AI. We do know that AI will, at some point, dominate every aspect of human life. Every country, industry, and individual will be impacted by Artificial General Intelligence (AGI). The world will never be the same. If we choose to grow with AI, we must decide how to select the best possible future for humanity.

PINNACLE THEMES SINCE INCEPTION

Issue	Themes
Mar 01	Cost Effective Total Quality Training for the 21st Century Soldier
Mar 02	International Terrorism
Sep 02	Revolution in Military Affairs in the Armed Forces
Mar 03	Involvement of the Non-uniformed Citizenry in the Affairs of the Armed Forces
Oct 03	Involvement of the Armed Forces in the Long Term National Development Projects
Apr 04	Specialization: Need of the Hour
Oct 04	Border Management - A Model
Apr 05	Doctrinal Approach to Sub Conventional Warfare
Oct 05	Synergy in Jointmanship
Apr 06	Transformation Doctrine for Indian Army
Jan 07	Leadership Challenges in The 21st Century
Oct 07	Dynamics of Short Intense War: Conceptual and Doctrinal Ramifications for the Army
Apr 08	Internal Security Paradigm Emerging Challenges
Jun 09	China Defence Modernisation and Its Implications
Jun 10	Indian Army's Role in Nation Building
Oct 11	Emerging Technologies and their Impact on Future Warfare
Dec 12	Training Challenges for a Transforming Army
Sep 13	Back to Basics - Need of the Hour
Nov 14	Shaping Tomorrow's Military Leaders
Oct 15	Empowerment of the Indian Soldier for Future Conflicts
Oct 16	Next Generation Warfare
Oct 17	Role of Armed Forces in Meeting India's Regional Aspirations
Oct 18	A Growing China – Implications for Asia
Oct 19	Manifestation of Grey Zone Warfare and Limited Wars Under the Conditions of Informationisation in Indian Context and Capability Development to Counter the Same
Oct 20	Utilisation of Space Capability by IA in Future Wars
Oct 21	Employment of Offensive Cyber as a Multiplication Tool for Defensive and Offensive Operations by Indian Army
Oct 22	Artificial Intelligence and the Future of Warfare: Roadmap for the Indian Army

CHANGING CHARACTER OF WAR

Introduction

General The strategic environment in the 21st Century is characterised by two trends. Firstly, the increased instability in the international system which gives rise to conflicts and secondly, the unprecedented use of technology and its impact on economics and politics which influences the conduct of war. These two trends have created an environment where threats are both diffuse and uncertain and where conflict is inherent, yet unpredictable. In the field of warfare, both continuity and change; evolutionary and revolutionary coexist, each shaping the other.

Defining Warfare In today's environment, war can be explained as an activity which involves the use of force or imminent threat of massive destruction, has more than one belligerent and hence rests on contention. Warfare also assumes a degree of intensity and duration and finally, it has an aim defined in political terms, but which can be defined in militarily terms as victory.

Theme 1: Evolving Character of War

Strategy for War The strategy of war as in other strategies need to define 'Ways', 'Means' and 'Ends'. There can be no doubt that the 'End State' of war is victory. What remains to be defined are the 'Ways' and the 'Means'. Understanding these two issues can enable us to understand the nature and character of war and what differentiates the Nature and Character of War.

- **Nature of War** 'Nature of War' can be explained and understood as the 'Means' to wage and prosecute war. Clausewitz defines war as an act of force to compel our enemy to do our will. Securing the 'End State' requires the enemy to be rendered powerless; and that, in practice, is victory. Intrinsic to the 'Nature of War' is friction, fog, chaos, violence and danger. These characterisations of war have remained constant since immemorial times and therefore 'Nature of War' is enduring and timeless.

- **Character of War** If strategy for war seeks to achieve victory as the desired 'End State', employment of physical force as the 'Means' to wage wars, then what is left to be established is the 'Ways' to employ physical force to achieve victory. Describing the 'Ways' to achieve victory through the use of force defines the 'Character of War'.

Emerging Character of War Every era of human evolution represents a distinct 'Character of War'. The first weapons developed during the Bronze Age and the Iron Age. Even as the 'Age of Gunpowder' transformed warfare, the creation of 'Mass Armies' during the 'Napoleonic Era' further changed the scale in which wars could be fought. This theme would seek to explore the following:-

- **Evolution of Warfare** Emergence of modern warfare can be traced back to the 16th Century when science and technology was first used. Evolution of warfare can be explained through historical overview of distinct periods which also correspond to four techno regimes; Large armies and mechanism, Industrial war and thermodynamics, cold war and cybernetics and finally chaoplexity in the post-cold war era.

- **Determinants of Character of War** Nations prosecute wars with a desired 'End State' which in political terms could be vague or nebulous. In addition, the desired 'End State' would define the level of victory to be achieved and limits to the use of force in terms of the geographic region where decision is sought as well as quantum of force is to be employed. This sub-theme would seek to explain how the desired politico-military 'End State' developed from the political 'End State' impact the Character of War.

- **Grey Zone Warfare** Nations typically transcend from confrontation to conflict. Nations are however, increasingly exploiting the space between confrontation to conflict, defined as the 'Grey Zone' to secure their national interests. This sub-theme would seek to explore reasons why nations are attempting to exploit the 'Grey Zone' and how has activities in this space impacted the Character of War.

- **Large-Scale Full Spectrum Conflict** Notwithstanding the proclivity to engage in Non-Contact Warfare in the Grey Zone, large-scale full spectrum conflict is considered the greatest threat to the nation. This sub-theme would draw inputson the implications and relevance of large-scale conventional operations.

Theme 2: Trends in Warfare

General War is influenced by interplay of specific characteristics and strengths of the parties to the conflict in question and the political, economic, technological, intellectual, social as well as the will of the leadership. The sub-theme will attempt to explore the following:-

- **Trends in National Security** Nations resort to the use of force to secure national interests to enhance national security. Often, national security is an expression of the worldview of nations and their leaders, which is constantly evolving. An appreciation of trends in national security would provide insights into the concerns of nations and why they would transcend from confrontation to conflict.

- **Emerging Domains** The lexicon of Multi Domain Warfare (MDO) is increasingly finding acceptance amongst militaries and scholars alike. Land, sea and air, the three traditional domains of warfare have now been joined by cyber, space and Electronic Warfare (EW). This sub theme would identify the ways in which emerging domains could potentially impact the Character of War.

- **Doctrinal Trends in Warfare** Developments in the international system and rate of pace of technological change will have a profound impact on warfare. However, Artificial Intelligence, stealth, robotics, long range precision targeting etc will finally have to be synergised on the battlefield by way of a warfighting doctrine. This part will attempt to visualise contours of the likely futuristic MDO Doctrine.

- **Leadership and Change Management** Every transformative effort follows the framework of people, structures and processes. Change is however, never easy and its success cannot be assumed. This sub-theme will attempt to identify human resource challenges, structures and methods to implement transformative changes thereby enhancing battlefield effectiveness.

Theme 3: Capability Development

General Militaries adopt a long term perspective to develop capabilities. The capability development is undertaken under the backdrop of finite resources, technological constraints and uncertain trajectory of capability development by potential adversaries. Besides, civil-military relations, structures, doctrines etc also play a significant role in developing military capabilities. The sub-theme will attempt to explore the following:-

- **Indian Thoughts on National Security** India is classified as a status quoist and a non-revisionist nation which does not intend to use military force to alter its political boundaries. Notwithstanding its pacifist intentions, India has often been constrained to use force both within and outside its boundaries. This sub-theme would try to establish how the India views its compulsions to employ force as well as the role and evolution of its security structures and institutions.

- **Doctrinal Evolution in the Indian Context** The Indian armed forces have come a long way since independence. This part will examine the evolution of the three services of the Indian Armed Forces in the past 75 years.

- **Factors in Capability Development** The Indian Armed Forces are influenced and constrained by structural and environmental factors which impact its capability development. This sub-theme will attempt to identify the structural and environmental factors which impact capability development of the Indian Armed Forces as well as make relevant recommendations.

- **Character of War in the Indian Context** The Indian Armed Forces are confronted with two traditional adversaries in a potentially collusive scenario, even as it has to contend with numerous insurgencies. Given the environmental realities, this part shall intend to explore the likely character of future conflict in the Indian context.

Theme 4: Strategies for Future Conflict

General Since wars are not merely military endeavours but represent whole of the nation approach, developing a unitary understanding of strategy for war is fraught with risks. Strategy for war would involve synergising multiple activities in the vertical levels with each level representing numerous actions in the horizontal plane. The sub-theme will attempt to explore the following:-

- **Purpose, Triggers and the Desired End State** This part shall attempt to answer the following:-

    ➢ At the political level what could be the purpose (as opposed to triggers) of war for India, Pakistan and China?

    ➢ What could be the desired end state for India, Pakistan and China at the political and military-strategic level?

- **Contours of Escalatory Continuum** This part shall seek to address the following:-

    ➢ What activities could India, Pakistan and China undertake as part of the DIME Paradigm to implement their respective strategies for war?

    ➢ What are the likely contours of escalatory continuum from confrontation to conflict?

- **Strategy for Defeat Mechanism** This sub-theme would intend to gain insights into the following:-

    ➢ At the military strategic level how are India, Pakistan and China likely to develop their respective defeat mechanisms to achieve the political end state?

    ➢ What could be likely strategies for war at the military-strategic as well as the operational level for India, Pakistan and China?

GUIDELINES FOR THE AUTHORS

General In our endeavour to generate a debate on a particular issue, over-riding preference will be given to theme articles during selection of articles for publication. Only researched and well substantiated articles with end notes and bibliography are likely to find favour for publication in Pinnacle. All ideas generated must be covered in a comprehensive manner and taken to a logical conclusion, so that a tangible road map is perceived by the reader.

Articles Articles in electronic format should preferably be written in Font Arial 11 on MS Word and sent along with the softcopy on a CD. A synopsis of up to 150 words is also required with each article alongwith bio-data in a paragraph, email and mobile number of the author.

Layout of Articles The suggested layout of articles is as under:-

- Synopsis.
- Title page.
- Main body.
- Acknowledgements.
- Foot Notes/End Notes/References/ Bibliography.
- Appendices/Annexure/Tables (as applicable).
- Photographs/Illustrations/Drawings (as applicable).

Title Page The title page should also include the full name, address, email-id, contact number and a brief bio-data of the author.

Main Body A minor staff duty as per service writing is not required. Preferably no abbreviations/ acronyms should be used. However, should they be used to avoid repetition of big terms/ names, the expanded form should be given when first used, with abbreviations/ acronyms inside the brackets. The length of the **articles may vary between 2500-4000 words**, which should appear on the last page at the end of the main body. Articles may be written in passive voice/ third person, to the extent possible.

End Notes/References/Bibliography Detailed end notes and references/ bibliography of books/periodicals/magazines/journals/newspapers/ published or unpublished material used in the articles, indicative of research carried out by the author, must be given as per standard format followed in this journal. This is very important.

Appendices/Tables Tables should be numbered in Arabic numerals and should have a title.

Certificates The following certificates, as per Paragraph 21 of SAO 3/S/2001/MI and equivalent orders for other Services, duly countersigned by the author's superior authority, should be attached to the articles:-

- **No Objection Certificate (by the IO)** I have perused the article/ book etc submitted by and I have no objection to it being published/ broadcast in 'Pinnacle' Journal duly edited by the Editorial Board where required.

- **Author's Certificate** It is certified that "I have not used any official information and/ or material or any information obtained by me in my official capacity in writing the article titled '............................'.

- **Originality Certificate** I hereby certify that the article titled '............' has been written by me and is original in its contents. It has not been published earlier in/ sent to any other journal/ publication. All relevant references and bibliography have been given.

Book Reviews/Letters 'Book Reviews' of the latest books aligned to the theme and 'Letter to the Editor' are also welcome. Critical review of articles published in the earlier issues of PINNACLE are also solicited which will be published under 'the critique' section.

Last Dates for Receipt of Articles The articles must reach the 'The Editor', PINNACLE, **latest by 30 Apr for the next Issue.** Articles, along with bio-data and synopsis may also be e-mailed to the editor at theartracjournal@hotmail.com**.** Certificates duly signed will, however, need to be forwarded through post only. Also, the articles alongwith requisite certificates may be submitted online on Army Intranet ARTRAC webpage.

Editing The Editorial Board reserves the right to suitably modify the articles, without reference to the authors, for reasons of clarity, style, accuracy and space limitations.

Honorarium An honorarium of up to ₹4000/- will be paid to the authors, for each article, depending upon its quality, content and length. Honorarium will also be paid for 'Book Reviews' and 'Critical Reviews' @ ₹1000/- and 'Letters to the Editor' @ ₹500/-. Authors must intimate the details of their bankers to enable despatch of Demand Drafts.

Correspondence All correspondence to be addressed to The **Editor, 'Pinnacle', Doctrine Branch (CS Sec), Headquarters Army Training Command, Shimla-171003 (Himachal Pradesh), India.**

FOR THE ATTENTION OF READERS

- PINNACLE is published every year on 01st Oct i.e. ARTRAC Raising Day

MY COUNTRY, MY MISSION, MY COMRADES, MY DUTY
"Nation First - Always and Everytime"
(The four soldiers signify the diversity of our Country)

- All correspondence should be addressed to:-

  The Editor
  PINNACLE
  Doctrine Branch (CS)
  Headquarters Army Training Command
  Shimla (HP)-171003

- **E-mail : theartracjournal@hotmail.com**
- The Journal is available on ARTRAC ADN website and indianarmy.nic.in on Internet.

PINNACLE (ISSN 0972-4044)
Headquarters
Army Training Command
Shimla (HP) – 171 003
India

PINNACLE 2022 VOL 21

Printed at : Headquarters Army Training Command