USE OF ARTIFICIAL INTELLIGENCE FOR IMPROVING OPERATIONAL EFFICIENCY IN THE ARMED FORCES

PARDEEP BHARDWAJ

INTRODUCTION

Many countries have declared their national Artificial Intelligence (AI) strategies after they recognised its potentials. Most advanced countries are investing in AI Research and Development (R&D). The United States (US) and China stand out as the front-runners in this technological race, each with distinct strategic objectives.[1] The US aims to retain its dominant position in AI, emphasising its leadership in innovation and military applications. China, on the other hand, has articulated an ambitious goal to surpass the US and become the global leader in AI by 2030.[2]

Group Captain **Pardeep Bhardwaj** is in the Aeronautical Engineering branch of the Indian Air Force (IAF). He has been Project Manager for monitoring the network-centric warfare related systems in the IAF. He has worked as Joint Director at Air Headquarters (HQ) and Deputy Project Director at the Centre for Airborne Systems (CABS), Defence Research and Development Organisation (DRDO), as part of Air Force Project Monitoring Team. Presently, he is undergoing the Higher Command Course at the Army War College, Mhow, MP.

1. Gloria Shkurti Osdemir. "Artificial Intelligence Application in the Military: The Case of United States and China: Analysis", SETA, June 20, 2019. https://www.setav.org/en/security/analysis-artificial-intelligence-application-in-the-military-the-case-of-united-states-and-china#:~:text=Gloria%20Shkurti%20%C3%96zdemir-,Artificial%20Intelligence%20Application%20in%20the%20Military%20%7C%20The%20Case%20of%20United,of%20the%20U.S.%20and%20China. Accessed on July 9, 2024.
2. Forrest E. Morgan, Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima, Derek Grossman, "Military Applications of Artificial Intelligence, Ethical

As per the recommendation of the task force, the Defence Artificial Intelligence Council (DAIC) is to guide and provide structural support. Additionally, the Defence AI Project Agency (DAIPA) has been formed to enable AI-based processes in defence organisations.

AI's amalgamation into drone operations and its role in supporting human decision-making in conflicts is indeed changing the dynamics and ethics of warfare. In the context of the ongoing conflict between Russia and Ukraine, AI is being utilised by both sides, with Ukraine particularly leveraging AI to gain an asymmetric advantage.[3]

The Indian government started its ambitious defence task for the incorporation of AI to improve the operational ability of the Indian armed forces to prepare the defence and security forces for next-generation warfare. The task force was set up by the Department of Defence Production (DDP), which was led by the chairman of Tata Sons. The task force also included senior officers from the Indian armed forces, the national cyber security coordinator, Indian Institute of Technology (IIT) and Indian Institute of Science (IISc) professors, and representatives from the Indian Space Research Organisation (ISRO). As per the recommendation of the task force, the Defence Artificial Intelligence Council (DAIC) is to guide and provide structural support. Additionally, the Defence AI Project Agency (DAIPA) has been formed to enable AI-based processes in defence organisations.[4]

Innovations by the Indian defence industry, Defence Public Sector Undertakings (DPSUs) and Defence Research and Development Organisation

Concerns in an Uncertain World", Research Report by RAND Corporation, Published April 28, 2020, p. 78.

3. Callum Fraser, "AI's Baptism by Fire in Ukraine and Gaza Offers Wider Lessons", International Institute for Strategic Studies (IISS), April 22, 2024. https://www.iiss.org/en/online-analysis/military-balance/2024/04/analysis-ais-baptism-by-fire-in-ukraine-and-gaza-offer-wider-lessons/. Accessed on July 7, 2024.
4. Ministry of Defence Press Release, Release ID: 1810442, "TASK FORCE FOR IMPLEMENTATION OF AI," Press Information Bureau (PIB) Delhi, March 28, 2022, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1810442#:~:text=2019%20created%20Defence%20AI%20Council,structural%20support%20for%20AI%20adoption. Accessed on July 6, 2024.

(DRDO) in the field of AI are expected to play a big role in strengthening the *Aatamnirbhar Bharat* programme and to aid in a strong defence sector.

The aim of this paper is to study the different ways in which the Indian defence industry and DRDO can contribute in the field of AI to help the Indian armed forces in improving operational efficiency and to list various challenges in the introduction of AI-based systems in the Indian armed forces as an integral part of the defence Services.

Integration of Artificial Intelligence (AI) and Machine Learning (ML) can further refine surveillance capabilities as an integral part of the command and control systems.

CURRENT SCENARIO AND SCOPE FOR IMPROVEMENTS IN THE ARMED FORCES

The Indian armed forces have made significant strides in integrating modern technology across various operational domains. The deployment of advanced applications on contemporary platforms has enhanced capabilities in surveillance, security, logistics management, and intelligence. However, despite these advancements, there remains substantial potential for further improvement in operational efficiency across the army, navy, and air force by the use of AI. The elaboration in the subsequent paragraphs covers the current progress / achievements in the given fields and the ways efficiency can be improved.

Surveillance

Current Progress*:* The Indian armed forces have leveraged satellite technology, Remotely Piloted Vehicles (RPVs), and advanced radar systems for comprehensive surveillance. These technologies enable real-time monitoring of border areas, maritime zones, and airspace, contributing to enhanced situational awareness.

Intelligence analysis can be improved by the use of AI algorithms that can uncover patterns and insights from the data, enabling more sophisticated analysis and decision-making.

Scope for Improvement: Integration of Artificial Intelligence (AI) and Machine Learning (ML) can further refine surveillance capabilities as an integral part of the command and control systems. AI models can be developed to use predictive analysis for threat evaluation and a model can be developed to prioritise the available weapons, based on various parameters such as cost-benefit analysis, type of threat, etc., and the experience of weapon operators can also be used for improvement in weapon assignment criteria.

Security

Current Progress: All arms of the defence Services have their Information Technology (IT) infrastructure and policies on cyber security for the security of their data/information. Policies to avoid and handle security breaches are also in place. Various measures like user authentication using strong passwords/biometric access/encryptions are used for security.

Scope for Improvement: The armed forces need to upgrade their IT and cyber security infrastructure to keep pace with the emerging security threats. Continuous upgrade on existing systems and training of the personnel for the timely response by users are some mandatory requirements of the day. Future projects and contracts need to include the scope for periodical infrastructure upgrades and training by the Original Equipment Manufacturers(OEMs) or service providers such as DPSUs/DRDO/Indian defence industry. Also, the tri-Services need to stress more on having a common communication infrastructure and security protocol standards for interoperability and improved operational efficiency.

Intelligence

Current Progress: All three Services have their own systems with various types of equipment for different forms of intelligence gathering,

including Electronics Intelligence(ELINT), Signal Intelligence (SIGINT), and Human Intelligence (HUMINT). There is limited sharing of information, with time delays in sharing due to Service protocols and incompatibility of the data being used by the different arms. Within the Services, sharing of intelligence data has been progressed for different echelons for better threat assessment and strategic planning.

AI enabled applications can be used in command and control systems for enhanced situational awareness and neutralisation of threats based on the solutions offered by AI.

Scope for Improvement: Intelligence analysis can be improved by the use of AI algorithms that can uncover patterns and insights from the data, enabling more sophisticated analysis and decision-making. Even a simple tool like power Business Intelligence(BI) can help in generating analysis reports for the decision-makers. The government needs to encourage the Indian defence industry/DPSUs/DRDO for development of indigenous technologies as presently there is a lot of dependence on foreign vendors for intelligence gathering systems.

BENEFITS OF AI IN IMPROVING OPERATIONAL EFFICIENCY

Like in other fields and sectors, the influence of AI has resulted in transformation in the functioning of the armed forces. Inclusion of AI in different fields in the armed forces has many benefits for improving operational efficiency, as listed below:

- Enhanced speed of decision-making.
- Scope of use of big data.
- Improved targeting and vision.
- Decision-making support.
- Improvements in accuracy and precision.
- Reduction in manpower and operational costs in the long run.
- Improvement in Intelligence, Surveillance, and Reconnaissance (ISR).

Advanced image and signal processing algorithms allow AI to identify and track targets more accurately, even in challenging environments or through obstacles.

Enhanced Speed of Decision-Making

AI can be helpful even in critical war-like situations with high stress as it has fast processing and decision-making capability to analyse potential threats. With the human-in-the-loop for the final decision, AI can be of great benefit to offer a fast response in the time when it really matters as time is the most important factor in decision-making during operational missions. AI enabled applications can be used in command and control systems for enhanced situational awareness and neutralisation of threats based on the solutions offered by AI.[5]

Scope of Use of Big Data

In the present day, when current systems with advanced technologies enable enormous data collection by the use of various available sources/ sensors such as radar, Unmanned Aerial Vehicles (UAV), cameras, ELINT/ COMINT (Communication Intelligence), sensors, etc., it is a complex and time-taking process for even hundreds of humans to analyse such large data. However, the big data analytics of AI offers the capability to process large data to draw insights for the actions and decisions support system.[6]

Improved Targeting and Vision

AI enhances the precision of targeting systems, improving the effectiveness of military strikes while minimising collateral damage. Advanced image and signal processing algorithms allow AI to identify and track targets more accurately, even in challenging environments or through obstacles. For example, in smart weapons, AI-guided missiles and bombs can adjust their trajectory in real-time based on changing conditions, ensuring higher accuracy in hitting targets.[7]

5. Morgan, et al., n.2, pp.15-20.
6. Ibid.
7. Ibid.

Decision-Making Support

AI assists military leaders by providing comprehensive analysis and recommendations, enabling informed decision-making. These systems can integrate and interpret data from various sources, simulate potential outcomes, and suggest the best course of action, thereby reducing the cognitive load on human operators.[8]

AI can help in reducing the need of armed forces personnel to physically engage in the activity by involving trained machines / robots for such tasks, reducing manpower requirements and operational costs in the long run.

Improvements in Accuracy and Precision

Accuracy and precision of targets / data is the prime factor in any operational mission for the armed forces. AI plays a prime role for improvement in accuracy and precision. Various techniques such as cleaning and pre-processing data to handle missing and outlier values aids in improved precision and accuracy. Enhanced target identification is one of the examples wherein AI can contribute to the development of systems for identification and targets tracking with improved accuracy even in difficult terrains, complex environments and challenging conditions.[9]

Reduction in Manpower and Operational Costs in the Long Run

Due to high-risk environments, the armed forces operate in difficult terrains and high-risk areas, including handling bombs, search and rescue in areas prone to access by terrorists. The armed forces incur a major expense in the training and deployment of their soldiers, and high risk areas not only endanger the soldiers but also increase operational costs. AI can help in reducing the need of armed forces personnel to physically engage in the activity by involving trained machines / robots for such tasks, reducing manpower requirements and operational costs in the long run.[10]

8. Ibid.
9. Ibid.
10. Ibid.

The defence forces use AI-enabled autonomous systems for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR).

Improvement in Intelligence, Surveillance, and Reconnaissance

Intelligence, Surveillance, and Reconnaissance (ISR) capabilities that utilise AI enable decision-makers to derive insights from vast amounts of data collected by a variety of sensors onboard systems with the ISR functions. With the passage of time and the conduct of various training, and independent as well as joint operational exercises by the armed forces, there is a huge collection of ISR "big data". This big data needs to be processed, exploited, and disseminated to the higher formations and sister Services to draw useful insights and generate comprehensive intelligence reports for improvements in strategic planning. Use of AI improves ISR capabilities and helps end users to gain the maximum advantage from each mission. For example, as part of satellite imagery analysis, AI algorithms can process and analyse satellite images to detect and monitor enemy movements, infrastructure, and other key intelligence data.[11]

APPLICATIONS OF AI IN VARIOUS FIELDS IN THE ARMED FORCES INVOLVEMENT OF INDUSTRY AND DRDO

Major future requirements of the Indian armed forces for using AI include those focussed on data processing and analysis, cyber security, simulation and autonomous systems, particularly drones. Certain areas of work in the armed forces wherein the Indian defence industry, DPSUs and DRDO can contribute include the AI-based mission planning and debrief system, AI-based target identification, game theory for interception solutions, object detection, pattern recognition, Natural Language Processing (NLP) swarming, and up to Level 4 autonomy for unmanned systems.

The defence forces use AI-enabled autonomous systems for Command, Control, Communications, Computers, Intelligence, Surveillance and

11. Ibid.

Reconnaissance (C4ISR). These AI-enabled systems can perform tasks that are recognised as "dull, dirty, dangerous or dear" and provide AI-enabled decision support for combat scenarios. Use of AI in C4ISR systems development provides better feedback, outcome, caution and information, which results in more reliable intelligence analyses.[12]

Another recent major development took place in May 2024 wherein DRDO collaborated with the Indian Institute of Technology (IIT), Bhubaneswar, for AI related projects. IIT, Bhubaneswar has been handed nine sanctioned projects of DRDO and another seven projects are likely to be sanctioned to it by DRDO.

Two major centres of DRDO i.e Centre for Artificial Intelligence and Robotics (CAIR) and DRDO Young Scientist Labs (DYSL) are working in the field of AI. CAIR is involved in Research and Development (R&D) in the areas of AI for development of mission critical systems. The DYSL at DRDO, Hyderabad, stands apart for its path-breaking development of the latest weapon systems like 'swarm drones' which are AI-enabled. These are self-intelligent drones that synchronise with each other to attack the enemy as an army. The DYSL is also working on future-generation weapon systems, including the technology intensive projects 'Gun on Drone', 'Rat Cyborg', etc.[13]

DRDO Chairman Mr. Samir V Kamat recently stated in January 2024 that "India is working with other countries on developing tools as well as fundamental research in improving the algorithm which goes into AI."[14]

12. István Szabadföldi, "Artificial Intelligence in Military Applications: Opportunities and Challenges", sciendo, *Land Forces Academy Review*, vol. XXVI, no. 2(102), June 28, 2021, https://sciendo.com/article/10.2478/raft-2021-0022. Accessed on June 27, 2024, pp. 161-162.
13 ETV Bharat Tech Team , "DRDO Young Scientists Lab Making Progress on 'Swarm Drones' Weapon Systems",*ETV Bharat*, July 3, 2023, English edition, State section, Telangana, Hyderabad, https://www.etvbharat.com/english/state/telangana/hyderabad-drdo-youth-lab-excels-in-future-generation-weapons-development/na20230703094726493493084. Accessed on June 28, 2024.
14. ANI, "India Working with Friendly Nations on Leveraging AI to Enhance Defence Capabilities: DRDO Chief" , *The Economic Times*, January 18, 2024, https://economictimes.indiatimes.com/news/defence/india-working-with-friendly-nations-on-leveraging-ai-to-enhance-defence-capabilities-drdo-chief/articleshow/106964125.cms?utm_source=contentofinterest&utm_

India is teaming up with 'friendly' countries on improving the use of AI for enhancing defence capabilities.

Another recent major development took place in May 2024 wherein DRDO collaborated with the Indian Institute of Technology (IIT), Bhubaneswar, for AI related projects. IIT, Bhubaneswar has been handed nine sanctioned projects of DRDO and another seven projects are likely to be sanctioned to it by DRDO. This collaboration will be helpful in defence applications of electronics warfare, AI-driven command and control systems, power systems, surveillance systems, etc.[15]

AREAS OF ENHANCEMENT IN THE INDIAN ARMED FORCES TO IMPROVE OPERATIONAL EFFICIENCY

Airborne mission systems are critical components in modern military operations, providing enhanced capabilities for surveillance, reconnaissance, communication, electronic warfare, and command and control. These systems, integrated into various types of aircraft such as fixed-wing planes, helicopters, and Remotely Piloted Vehicles (RPVs), play a pivotal role in ensuring mission success and operational efficiency. Enhancements can be planned by DRDO in its projects already developed for enhancement of operational capabilities by including AI-based solutions in various fields, including analysis, decision-making, etc. DRDO has already delivered the Airborne Early Warning and Control (AEW&C) airborne mission system to the Indian Air Force (IAF), which is being operationally exploited by the IAF. Various areas that need to be earmarked and use cases finalised to improve operation efficiency are the systems being developed by DRDO i.e., airborne mission systems, related to ISR, image intelligence and ELINT. Additionally, DRDO can work on AI in the fields of C4ISR, cyber security, and predictive maintenance.

medium=text&utm_campaign=cppst, Business News›News›Defence Section. Accessed on June 28,2024.

15. ANI, "DRDO to Collaborate with IIT Bhubaneswar for AI-driven Surveillance, Other Projects", May 8, 2024", https://telecom.economictimes.indiatimes.com/news/industry/drdo-to-collaborate-with-iit-bhubaneswar-for-ai-driven-surveillance-other-projects/109938773 , News, Industry section. Accessed on 28 June 24.

Enhancements in Airborne Mission Systems

AI use cases can be incorporated in the fields of Software Defined Radio (SDR) integration, mission system software including the following major areas:[3]

- Cognitive Module of Identification, Threat Evaluation: Using activity templating and trend estimation for attack profile prediction, target type prediction, automatic group recognition for package.
- Interception and Surveillance: Game theory-based aircraft interception.
- Voice Identification: To identify own aircraft as friendly and other use cases.
- AI-based multi-sensor fusion of airborne targets.

Enhancements in Operational and Combat Platforms with Multi-intelligence

Multi intelligence is the need of the day with improvements in intelligence gatehring technology. ISR and Intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) is the activity of equipping armed forces' with information and intelligence to assist in combat roles and other operational duties. The main task is to identify the existing limitations in gathering intelligence from various available sources (digital print media and videos, social media platforms, satellite imagery from Indian defence satellites or any commercial satellite imagery, aerial imagery using platforms like aircrafts, RPAS/ UAVs, SAR (Synthetic Aperture Radar Imagery), Electronic Warfare). The major challenge is to use AI progressively to help in informed decision making in the armed forces using this information.[4] The best applications of AI in C4ISR are to:

- Use all types of imagery to undertake time series analysis, change detection, and identification along with rapid correlation with inputs from other sources.
- Be capable of milking out data in latitude - longitude from all types of aerial sources adequately corrected for oblique imagery and remove biases due to human errors by using multiple image sets.

- Identify targets of interest based on interactive inputs.

Cyber Security

Use of AI is envisaged to help in predictive analytics for anomaly detection in the network, enhance the reliability of cyber security threat detection, enhance network security by network traffic analysis, reduce threat response time, eliminate zero-day vulnerabilities, improve human analysis of networks and automate security tasks.[16]

Predictive Maintenance

AI-enabled predictive maintenance is transforming the aviation industry by allowing for tailored maintenance practices that meet the specific needs of individual aircraft. By leveraging advanced data analytics and machine learning techniques, maintenance can be optimised, resulting in improved operational efficiency, cost savings, and enhanced safety. However, successful implementation requires addressing challenges related to data quality, algorithm accuracy, and regulatory compliance. As technology continues to advance, AI's role in predictive maintenance will likely expand, further revolutionising aircraft maintenance practices.[17]

The major challenge in predictive maintenance is the analysis of the large volumes of data to suggest preventive steps to improve the reliability and Mean Time Between Failure (MTBF) of equipment, reduce the Mean Time to Repair (MTTR), optimise servicing schedules and design Built-In Test Equipment (BITE). The challenges faced are the volume of data on maintenance, different platforms in the Services, and availability of data in different formats. Modern air forces are trying AI-enabled programmes for the

16. Srinivas A Vaddadi, Rohith Vallabhaneni and Pawan Whig , "Utilising AI and Machine Learning in Cybersecurity for Sustainable Development through Enhanced Threat Detection and Mitigation" , *IJSDAI (International Journal of Sustainable Development through AI, ML and IoT)* vol. 2, issue 2, 2023, pp. 4-6.
17. Kosmas Alexopoulos, et. al., "Predictive Maintenance Technologies for Production Systems. A Roadmap to Development and Implementation", *Researchgate*, July 2021, https://www.researchgate.net/publication/353196175_Predictive_maintenance_technologies_for_production_systems_A_roadmap_to_development_and_implementation). Accessed on June 29, 2024, pp. 51-64.

formulation of maintenance practices to suit individual aircraft requirements. By predicting failures before they occur, maintenance can be scheduled proactively, reducing unscheduled downtime and improving aircraft availability. Preventing unexpected failures and optimising maintenance schedules can significantly reduce maintenance costs. AI-driven maintenance can also extend the life of components by preventing over-maintenance. Early detection of potential issues ensures that maintenance is performed before a failure occurs, enhancing the overall safety of the aircraft. AI provides data-driven insights, enabling maintenance teams to make informed decisions and prioritise actions based on the actual condition of the aircraft.[18]

Underwater Mine Warfare

Underwater mine warfare involves the strategic placement of explosive devices, known as mines, beneath the surface of the water to disrupt or control the movement of marine vessels. These mines are powerful tools used in both offensive and defensive maritime strategies, aiming to channel or deny passage through crucial waterways and to protect strategic assets or territories. To mitigate the threat posed by underwater mines, Mine Counter-Measure (MCM) operations are conducted. These operations aim to locate, identify, and neutralise mines to ensure safe passage for vessels. Advances in technology have led to the development of sophisticated detection methods, including the use of sonar systems.[19]

Recent advancements in technology have significantly enhanced MCM capabilities, particularly through the use of Autonomous Underwater Vehicles (AUVs) equipped with Synthetic Aperture Sonar (SAS). Given the large volumes of SAS imagery collected by AUVs, automatic target classification has become crucial. This process involves the use of algorithms to automatically differentiate between mines and non-threatening objects. The advent of Deep Neural Networks (DNNs) has revolutionised this field.

18. Ibid.
19. Dr Peter Svenmarck, Dr Linus Luotsinen, Dr Mattias Nilsson, Dr Johan Schubert, "Possibilities and Challenges for Artificial Intelligence in Military Applications", *NATO STO*, May 2018, https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-160/MP-IST-160-S1-5.pdf. Accessed on June 30, 2024.

Using AI to automatically analyse imagery and signals from reconnaissance assets to identify and classify targets, are benefits of increased accuracy in target identification, reduced workload for analysts, and faster targeting processes.

Underwater mine warfare remains a significant challenge in maritime security. The integration of advanced technologies such as AUVs, SAS, and DNNs has dramatically improved the effectiveness of mine counter-measures. These innovations provide precise, efficient, and safe methods for detecting and neutralising underwater mines, ensuring the safe passage of marine vessels through strategic waterways. As technology continues to evolve, the use of AI in applications for underwater mine warfare MCM operation holds the promise of even greater advancements and enhanced maritime safety.[20]

PATH FORWARD FOR USE OF AI AND USE CASES TO IMPROVE OPERATIONAL EFFICIENCY

AI has the potential to revolutionise C4ISR and cyber security by improving efficiency, speed, and accuracy. However, maintaining human responsibility for key decisions ensures that ethical, legal, and equitable considerations are appropriately managed. Certain use cases for C4ISR[21] and cyber security[22] which can be helpful in improving the operational efficiency in the armed forces are given below.

C4ISR

- **Enhanced Situational Awareness**
  Real-Time Data Fusion: Utilising AI algorithms to fuse data from various sources, such as satellites, UAVs, ground sensors, and human intelligence, to create a comprehensive and real-time operational picture.

20. Ibid.
21. Szabadföldi, n. 12, pp. 161-162.
22. SDi, AI "THE MOST USEFUL MILITARY APPLICATIONS OF AI IN 2024 AND BEYOND" Sentient Digital, Inc., https://sdi.ai/blog/the-most-useful-military-applications-of-ai/, Accessed on July 4, 2024.

This will improve decision-making, and enable faster response times and enhanced situational awareness for commanders.

- **Predictive Analysis and Decision Support**
  Predictive Analytics for Threat Assessment: Implementing machine learning models to analyse historical and real-time data to predict potential threats and enemy movements. This gives the added advantage of proactive threat mitigation, optimised resource allocation, and enhanced strategic planning.
- **Automated Target Recognition**
  AI-Powered Image and Signal Processing: Using AI to automatically analyse imagery and signals from reconnaissance assets to identify and classify targets. There are benefits of increased accuracy in target identification, reduced workload for analysts, and faster targeting processes.
- **Network-Centric Warfare**
  Integrated Communication Systems: Developing a unified communication network that integrates all the branches of the armed forces, ensuring seamless and secure communication. Enhanced coordination and interoperability, real-time information sharing, and improved operational efficiency will be the added advantages.
- **Autonomous Systems**
  Autonomous UAV Swarms for ISR Missions: Deploying swarms of autonomous UAVs for continuous surveillance and reconnaissance missions, coordinated through AI. This will benefit the armed forces in terms of persistent surveillance capabilities, reduced risk to human operators, and efficient coverage of large areas.

Cyber Security

- **Threat Detection and Response**
  AI-Driven Intrusion Detection Systems: Implementing AI-based systems to detect anomalies and potential cyber threats in real-time, using

Utilising SOAR platforms to automate the investigation and response to cyber incidents, guided by predefined playbooks and AI-driven insights will provide benefits.

behavioural analysis and pattern recognition. There will be faster identification of threats, reduced false positives, and improved response times.

- **Automated Incident Response**
  Security Orchestration, Automation, and Response (SOAR): Utilising SOAR platforms to automate the investigation and response to cyber incidents, guided by predefined playbooks and AI-driven insights will provide benefits. Some additional benefits will be reduced response time, consistent and efficient incident handling, and enhanced resilience against cyber attacks.
- **Vulnerability Management**
  AI-Powered Vulnerability Scanning: Employing AI to continuously scan and assess the network for vulnerabilities, prioritise them based on risk, and recommend remediation actions. Proactive vulnerability management, reduced risk of exploitation, and improved overall security posture are the additional benefits of using AI.
- **Secure Communication**
  Quantum Cryptography for Secure Communications: Implementing quantum cryptography techniques to ensure secure and tamper-proof communication channels. This way, unbreakable encryption, protection against quantum computing threats, and enhanced security for sensitive information can be achieved.
- **Cyber Training and Simulation**
  AI-Driven Cyber Range Platforms: Developing cyber range platforms powered by AI to simulate realistic cyber attack scenarios for training purposes. Improved preparedness, hands-on experience for cyber defence teams, and enhanced skills in threat detection and response are the added advantages of using AI for training and simulation.

UNIQUE CHALLENGES OF USING AI IN THE INDIAN ARMED FORCES

The armed forces personnel must trust the reliability of the systems they use. However, the use of AI and ML data technologies also introduces certain complexities. One major challenge is that AI often operates as a "black box," making it difficult for even trained individuals to fully comprehend its inner working. The unique challenges that will be faced while using AI in the systems being developed for the Indian armed forces are:

Quality of Data

Where data is stored, how it is classified (data quantity/quality/labelling/security), etc. are questions that need to be considered while collecting data as existing systems and technologies have inherent compatibility issues with the way the data is captured and processed. AI does not have its own conscience of making independent choices but learns from the views of others, which brings in bias. Biased AI-based systems can perform in a manner that is not warranted and may lead to incorrect assessment of the situation, resulting in an incorrect outcome.[23]

Developers Need Access to Data

A major issue for the best utilisation of AI is the availability of data in the correct form. However, due to the chances of leakage of important operational missions / exercise data, the armed forces are either reluctant, or not in position, to share the labelled /identified data as it is classified or of a secret nature. To give a few examples: location and classification of friendly and enemy vital locations like sensors, batteries, weapon systems of tactical / strategic importance during their operational movements in war-time exercises. The dilemma is that if such details (in some form) are not shared with the developers for purification or preprocessing, then this

23. Svenmarck, et. al., n. 19.

Although hacking an adversary's AI system is difficult, one way to attack the system is to compromise the training data that the adversary uses or alter the AI model itself by changing the parameters.

data set cannot be used that effectively even with the use of AI.[24]

Systems are Vulnerable to Become Large and Slow

AI systems often rely on large data sets to learn and make predictions, which raises concerns about the collection, processing, and storage of such data. To quote an example, in ISR data sets, the amount of data stored in the form of videos, high definition images and classified data sets requires huge storage and enormous compute power for processing the data sets to draw inferences.[25]

AI Needs Training and Training Cycles

A variety of research issues need to be overcome to facilitate the inclusion of AI in operationally significant military systems. To ensure rapid reaction times and the ability to function in real-time, more rapid and adaptive machine learning techniques must be developed. To be effective in operational settings, AI must be able to learn continuously, unlike today's batch training approaches. An additional challenge that must be overcome is ensuring that we can rely on the decisions made by the AI systems. Finally, the AI systems need to be able to explain their decision-making rationale to the users, given the stakes involved in many military decisions.[26]

Black Box Problem for Critical Decision-Making System

The black box phenomenon has critical problems such as ill informed decision-making, or a lack of overall trust in AI systems, as the logic behind how a decision has been arrived at cannot be determined. In many AI-based tools, the processing part to refine data and results is not transparent in terms

24. Ibid.
25. Ibid.
26. Ibid.

of exact input and output. End users often have no insight into how complex AI systems work. It may not be possible to truly understand how a trained AI programme is arriving at its decisions or predictions. This poses an immediate threat to intent and causation tests that are legal questions, especially in high risk systems.[27]

Incorporating humans into the AI loop is essential for ensuring compliance with laws, rules of engagement in the stages of war/ peace, maintaining ethical standards, and providing clear accountability.

Functioning in Contested, Uncontrolled Domains

International studies indicate that adversarial attacks can deceive AI systems, causing them to make incorrect or unintended decisions. Although hacking an adversary's AI system is difficult, one way to attack the system is to compromise the training data that the adversary uses or alter the AI model itself by changing the parameters. Training data can be manipulated, or poisoned, in the hope that the adversary will use it. One can poison images used for training so that incorrect decisions are arrived at.[28]

Human Resources

Employment of AI in the defence forces, requires the higher defence organisation to have a proper understanding of contemporary AI technologies, their applications, and restrictions. The availability of a pool of AI experts and good data scientists who will know how to apply the technology to an aerial scenario requires enhancement. The DRDO, defence forces and related industries in India are struggling to attract top talent and may not be in a position to build an indigenous team for AI implementation. Outsourcing a team is an option but has multiple constraints.[29]

27. Ibid.
28. Ibid.
29. Ibid.

HUMAN ROLE IN AI

Accountability in AI is a multifaceted issue that impacts customer trust, legal liability, and ethical behaviour. As AI systems become more prevalent, especially in mission-critical applications, clear accountability structures are important. These structures not only guard the systems from operational risks and legal issues but also ensure that AI technologies are used ethically and responsibly. Moreover, the collaboration between human decision-makers and AI systems is vital for achieving the best outcomes, leveraging the strengths of both to drive productivity, and minimise errors. Humans will still be necessary as they possess the abilities of empathy, solving problems creatively, and ethical design, which cannot be achieved through AI. Incorporating humans into the AI loop is essential for ensuring compliance with laws, rules of engagement in the stages of war/peace, maintaining ethical standards, and providing clear accountability. The human-in-the-loop aims to leverage the strengths of both human intelligence and machine learning to create models that are more accurate and cost-effective. By continuously integrating human insights and feedback, the models can adapt and improve over time which is depicted in Fig. 1 below.[30]

Fig 1: Human-in the-Loop

Source: Author's creation.

RECOMMENDATIONS

The influence of AI has benefitted the civil world in different fields. Similar advantages can be leveraged in the armed forces by the use of AI which will have advantages of the fast decision-making process,

30. Morgan, et. al., n. 2, pp. 41-42.

increased speed, accuracy, and efficiency in military operations. Certain steps need to be taken by the armed forces, DPSUs and DRDO to fast track the use of AI in the armed forces. The recommendations are as follows:

Technical Cooperation and Policy Alignment

The Indian armed forces should work to promote shared understanding and the development of compatible policies with the industry partners, DPSUs and DRDO. Ultimately, the defence Services need to develop a framework for compatible rules of engagement and collaboration that would facilitate smooth operations for AI usage.

Organisation and Human Resource Aspects

Integrated efforts for enhancing the speed of embracing AI-beyond inter-departmental and inter-Services domain issues, to optimise resource and data sharing with the other defence Services and organisations working in the development process

Talent mapping and dedicated AI courses with specialisation to build up in-house expertise in young scientists.

Big Data Framework

Preparation of a roadmap for digitisation and to identify well in time fields where AI is to be used.

Organisation of collection and digitisation of data, including security and labelling of data. Data warehousing to have a repository of structured big data across the IAF and the Services for cross-utilisation and enabling AI-based algorithms.

Development of the Model

Standard formats of development, wherever possible, to exploit convergencies. Outsourcing of AI developing models while utilising the

in-house expertise of Centres of Excellence towards project monitoring and management.

Human Must in the AI's Decision Loop

The integration of AI in mission critical applications for the Indian armed forces necessitates the presence of a "man-in-the-loop" due to several critical factors. Despite advancements, AI systems are not yet reliable enough to operate autonomously in high-stakes environments like warfare, where the penalties of errors can be disastrous. The human element in AI operations ensures that key decisions, particularly those involving the use of lethal force, are made with the necessary oversight.

Encourage Defence R&D in Industry and Academia

Promoting a collaborative environment among the DPSUs, DRDO, and AI industries will lead to substantial advancements in defence technology and national security. Collaborations with experienced agencies like DRDO and IIT, Bhuhaneswar and other countries in developmental projects must be built up for long-term gains. This development will contribute to the emerging Research and Development (R&D) need of defence and make a stronger eco-system in India for development with self-reliance. These collaborations will benefit in nation-building, with inherent advantages such as innovation and advanced technology intake, speed and efficiency, resource optimisation, enhanced capabilities, economic growth.

CONCLUSION

The Indian defence industry, DPSUs and DRDO can significantly contribute to the development of AI applications for the Indian armed forces. Leveraging AI for applications in C4ISR, cyber security, predictive maintenance, and the upgrade of existing systems can enhance the capabilities of the armed forces. However, there are several challenges that will be faced in these endeavours. By addressing these challenges through strategic planning and

implementation of the recommended actions, the developmental agency can successfully harness the potential of AI to enhance the capabilities of the Indian armed forces. Focussed efforts on securing AI systems, managing costs, developing skills, ensuring data quality, and addressing ethical concerns will be crucial for the successful deployment of AI in defence applications.