**Artificial intelligence IN Defence**

Lets Discuss a brief about (ETAI) which is Evaluating Trustworthy artificial Intelligence in this we are just measuring some spectrum of AI in Defence sector .

**Artificial intelligence (AI)** refers to the simulation of human intelligence in machines that are programmed to think, learn, and problem-solve like humans. AI involves the creation of algorithms and systems that can process information, recognize patterns, make decisions, and improve over time through experience.

There are different types of AI, ranging from narrow AI (or weak AI), which is designed to perform a specific task (like voice assistants or recommendation systems), to general AI (or strong AI), which would have the ability to perform any intellectual task a human can do. AI is used in various fields, such as healthcare, finance, transportation, and entertainment, to improve efficiency, automate processes, and enhance decision-making.

About Evaluating Trustworthy Artificial Intelligence (ETAI) Framework

It is the risk-based assessment framework designed to ensure integration of reliable emerging technology into critical defence operations. It defines comprehensive set of criteria for evaluating trustworthy AI and ETAI Guidelines provide specific measures to implement these criteria.

**About AI and defence**

AI in defence refers to the integration of artificial intelligence technologies into military systems, operations, and decision-making processes to enhance effectiveness, speed, and precision. The application of AI in defence spans a wide range of capabilities, including autonomous systems, cyber security, intelligence analysis, logistics, and battlefield management. Here are some key aspects of AI in defence:

1. Autonomous Weapons and Systems

Drones and UAVs (Unmanned Aerial Vehicles): AI allows drones to perform reconnaissance, surveillance, and even attack missions autonomously. These systems can identify targets, make decisions, and execute tasks with minimal human intervention. Autonomous Ground Vehicles: AI-powered ground robots or vehicles can be deployed for reconnaissance, logistics, or combat operations without direct human control, reducing risks to personnel.

2. Cyber security and Defence

Threat Detection: AI can be used to detect cyber threats, predict attacks, and respond in real-time, making military networks and systems more secure against cyber-attacks. Automated Defence: Machine learning algorithms can monitor defence networks, identify vulnerabilities, and take proactive actions to safeguard critical infrastructure.

3. Intelligence Analysis

Data Processing: AI can rapidly process and analyze large volumes of intelligence data from various sources (e.g., satellite imagery, communications, sensor data) to identify patterns, threats, and actionable insights. Predictive Analytics: AI models can be used to predict enemy movements, identify emerging threats, and help strategize military actions by simulating different scenarios.

4. Decision-Making Support

Battlefield Management: AI can assist commanders in making more informed decisions by analyzing vast amounts of data from the battlefield, logistics, and intelligence, providing real-time situational awareness. AI in Command and Control (C2): AI systems can enhance communication, coordination, and execution of military operations by providing recommendations based on current and historical data.

5. Training and Simulation

Virtual Training: AI-driven simulations and virtual environments can be used to train soldiers in complex scenarios, from combat situations to strategic decision-making, improving preparedness and reducing training costs. Autonomous Simulation: AI can simulate realistic enemy behaviour, providing soldiers with more challenging and dynamic training exercises.

6. Logistics and Supply Chain

Optimized Logistics: AI can optimize supply chains, predict maintenance needs for military equipment, and ensure that critical supplies are delivered on time, helping to maintain military readiness. Resource Allocation: AI systems can manage resources more efficiently, optimizing the deployment of troops, equipment, and supplies based on real-time needs.

7. Ethical and Legal Concerns

Autonomy and Accountability: One of the primary ethical concerns with AI in defence is the accountability of autonomous systems, especially in life-or-death situations like warfare.

International Laws: The use of AI in defence raises questions about compliance with international humanitarian law, especially when it comes to lethal autonomous weapons systems (LAWS) and their potential to act without human oversight.

8. AI in Space Defence

AI is also playing a critical role in space defence, where it can help in detecting and tracking potential threats in space, such as hostile satellites or debris, and even in autonomously controlling space-based defence systems. In summary, AI has the potential to revolutionize the defence industry by enhancing operational effectiveness, decision-making, and security. However, it also raises significant ethical, legal, and strategic challenges that must be addressed as these technologies evolve.

**Significance of using AI in various aspects of Defence & Security**

Autonomous Weapons and Loitering Weapon Systems: It autonomously searches targets, identifies them and engages; allowing faster and more precise strikes. E.g. Israeli Harpy and Harop drones.

Enhanced Target Recognition and Precision: To identify and engage specific military targets like missile systems avoiding civilian infrastructure if desired.

E.g. The Iranian made Shahed-136 Al drones in the Russia-Ukraine war.

Real-Time Data Analysis: To process huge data from surveillance systems in real-time, providing critical intelligence for battlefield decision-making. For example, Project Maven, a U.S. initiative to analyse large quantities of surveillance data. Combat Simulation and Training: Generative Al can improve military training and educational programs by creating new training materials. Eg. Training modules for Sukhoi 30 MKI aircraft. Prediction of Crimes and Criminal Tracking: Using Command, Control, Communications, Computer and Intelligence, Surveillance and Reconnaissance (C4ISR) Systems.

For example, BEL developed the Adversary Network Analysis Tool (ANANT) for the predictions of attacks.

Protect Cyber attacks: AI can detect potential threats and use predictive analytics to help predict future attacks using data analytics.

Do you know ?

Article 36 of Additional Protocol I of the 1949 Geneva Conventions requires states to conduct legal reviews of all new weapons, means and methods of warfare in order to datarmine whether their use is prohibited by international

\* For example, Project Seeker, developed and deployed by the Indian Army for surveillarice, garrison security and population monitoring.

**Issues in using AI in Defence**

The integration of AI in defence presents several challenges and difficulties that must be addressed to ensure its effective and ethical use. These challenges span technical, ethical, legal, strategic, and operational dimensions. Here are some of the key difficulties:

1. Ethical Concerns

Autonomy in Lethal Decision-Making: One of the biggest ethical concerns is the use of autonomous AI systems in combat, particularly lethal autonomous weapons systems (LAWS). These systems, if allowed to make life-and-death decisions without human intervention, raise questions about accountability, the potential for unintended consequences, and the lack of empathy in decisions. Discrimination and Proportionality: AI systems may struggle to differentiate between combatants and non-combatants, particularly in complex environments. Ensuring that AI systems adhere to international humanitarian law (e.g., the Geneva Conventions) and principles like discrimination (targeting combatants, not civilians) and proportionality (avoiding excessive force) is difficult to guarantee in highly dynamic, unpredictable battlefields.

2. Accountability and Transparency

Lack of Human Oversight: Autonomous systems making independent decisions can complicate accountability in military operations. When AI makes mistakes, it may be unclear who is responsible—whether it's the developers, the operators, or the AI system itself.

Black-Box Nature of AI: Many AI algorithms, especially deep learning systems, are considered "black boxes" because it is difficult to understand exactly how they reach their decisions. This lack of transparency complicates oversight, audit ability, and trust in AI systems, especially in critical defence applications.

3. Reliability and Trustworthiness

Unpredictability in Complex Environments: AI systems are not infallible and may behave unpredictably in complex and dynamic environments like warfare. While they can process large amounts of data rapidly, they may still struggle with ambiguous or novel situations that deviate from their training data. Vulnerabilities to Adversarial Attacks: AI systems, particularly those based on machine learning, can be susceptible to adversarial attacks, where small manipulations to input data (such as images or sensor readings) can cause the system to malfunction or make wrong decisions. In a military context, this could be catastrophic if an adversary exploits these vulnerabilities.

4. Cyber security Risks

Hacking and Manipulation: AI systems used in defence are attractive targets for cyber attacks. Malicious actors could attempt to manipulate or corrupt AI systems, potentially leading to misguidance of autonomous weapons, falsification of intelligence, or disruption of strategic decision-making processes.

5. Legal and Regulatory Issues

International Law Compliance: The use of AI in defence raises questions about how current international laws and treaties apply to autonomous systems, especially when it comes to the use of force, self-defence, and targeting decisions. Many existing legal frameworks do not fully account for AI’s potential capabilities or limitations.

Regulation and Control: There's a lack of global consensus on how to regulate AI in defence. The proliferation of AI-powered weapons and systems could lead to an arms race, with countries competing to develop increasingly sophisticated autonomous technologies without clear rules of engagement or safety standards.

6. Operational Integration and Training:

Integration with Existing Systems: Many military forces rely on legacy systems, and integrating AI into these systems can be complex, requiring significant infrastructure changes, interoperability efforts, and time for adaptation. AI solutions also need to work in tandem with human personnel, which requires effective coordination.

Training and Expertise: The adoption of AI in defence requires skilled personnel who can develop, maintain.

**Indian Initiatives in adopting AI In defence**

Strategic Implementation of AI for National Security and Defence Task force: Chaired by C. Chandrasekaran, with a view to strengthening Al-based weapon systems.

Based on its recommendations, Defence AI Council (DAIC) and a Defence AI Project Agency (DAIPA) were set up in 2019 Launched 75 newly developed Al technologies: Indian Defence Minister launched Al technologies during the first-over 'AI In Defence' (AlDef) symposium in July 2024.

**Steps taken Internationally to regulate AI in defence**

A Group of Governmental Experts, on the UN Convention on Certain Conventional Weapons (CCW), was established in 2016 to discuss issues related to technologies in the area of lethal autonomous weapons systems including Al.

First Committee of UN Approved New Resolution on Lethal Autonomous Weapons in 2023, and suggested an algorithm must not be in full control of decisions involving killing regarding.

UNIDIR Guidelines for the development of national strategies on Al in security and defence in October 2024. International Committee of the Red Cross (ICRC): Advocating for a comprehensive, and binding, set of norms and rules for development and use of autonomous weapon systems of AL.

**In The Future**

* For national security: Intelligence Surveillance and Reconnaissance (ISR): The Indian military needs to build working relationships with the private technology sector in India working in the Al space like the US and China.
* Develop both offensive and defensive cyber-war capabilities: As cyber warfare becomes faster, more sophisticated, it becomes necessary to both protect and counterattack.
* For International regulation

Need of International law: To limit the types of targets, the geographical scope, and the context in which they would be employed.

* Arms control regime on AI: States and regional organisations can bring Al weapon systems and industry under arms control regime.
* Identify principles for responsible military use of Al: Codify such principles in official documents through collaborative multilateral processes.

SHUBHANGI PANDEY 

(Columnist)