INDIAN ARMY AI ROADMAP 2026-27 – DEFENCE

NEWS: The Indian Army is fast-tracking AI integration following lessons from Operation Sindoor (May 2025), a cross-border operation targeting terror infrastructure in Pakistan and PoK. A detailed roadmap for deploying **AI, ML, and Big Data Analytics by 2026-27** has been outlined.

WHAT'S IN THE NEWS?

Indian Army's AI Roadmap 2025–27

- **Purpose**: To integrate Artificial Intelligence (AI) into the Indian Army's operations to enhance combat readiness, efficiency, and strategic decision-making.
- **Timeline**: 2025–27, aligning with India's broader National AI Strategy and Atmanirbhar Bharat (Self-Reliant India) initiative.
- **Vision**: Transform the Indian Army into a technologically advanced, AI-driven force capable of addressing modern warfare challenges.

Key Objectives of the AI Roadmap

- **Operational Enhancement**: Deploy AI for real-time intelligence, surveillance, and reconnaissance (ISR).
    - Enhance situational awareness through AI-based predictive analytics.
- **Autonomous Systems**: Develop and deploy AI-enabled unmanned systems (drones, robots, vehicles) for combat and non-combat roles.
    - Focus on swarm intelligence for coordinated operations.
- **Cyber and Electronic Warfare**: Strengthen AI-driven cybersecurity to counter advanced cyber threats.
    - Use AI for electronic warfare, including signal jamming and threat detection.
- **Logistics and Maintenance**: Optimize supply chains and logistics using AI for predictive analytics.
    - Implement AI for predictive maintenance of critical assets like tanks, aircraft, and weapons.
- **Training and Capacity Building**: Establish AI-focused training programs for personnel across ranks.
    - Use **AI-based simulations for war-gaming** and tactical training.

Key Defence AI Projects

- **Combat Information Decision Support System (CIDSS):** A **command and control tool** under development by the Indian Army.
    - Integrates various battlefield inputs for: **Situational awareness, Tactical planning, AI-based threat prediction.**
    - **Core aim:** Enable commanders to make **data-driven decisions in near-real-time**.

- **Operational Data Fusion Project:** Seeks to **consolidate sensor inputs** from ground, aerial, and satellite sources.
    - Utilises **AI-based fusion algorithms** to reduce information overload and improve clarity in high-pressure situations.
    - Particularly relevant for **multi-domain operations**.
- **AI for Surveillance and Image Analysis:** Projects under **DRDO and BEL (Bharat Electronics Limited)**:
    - Use of **computer vision** for UAV/drone footage interpretation.
    - **Object recognition**, **target classification**, and **automated movement tracking**.
    - Supports border security and internal counter-insurgency missions.
- **AI-based Logistics Management System:**
    - **AI tools to optimise: Troop movement, Ammunition & fuel supply chains, Predictive maintenance** for vehicles and aircraft
    - Aimed at reducing dependency on manual updates and delays.
- **Cyber Defence AI Projects: CERT-IN & NTRO** (National Technical Research Organisation) involved in building:
    - AI-driven **intrusion detection systems**
    - Threat modelling and attack prediction tools
    - Deep packet inspection for encrypted threat detection
- **Speech and Natural Language Processing (NLP) Applications for Military Use:** AI-based **speech-to-text** and **multilingual translation** tools under trial.
    - Built to assist:
        - Field operations in linguistically diverse regions.
        - Interoperability among defence forces and intelligence units.
- **Autonomous Combat Drones (in R&D phase):** AI-led drone development by DRDO and private defence startups.
    - Targets include **Autonomous navigation, Target recognition and engagement, Swarm coordination** (inspired by US/Israeli doctrines)
    - **AI Capability in Swarm Drones:** Provides an aerial manoeuvre capability during offensive as well as defensive tasks.
    - **Project Storm Drone:** AI-enabled automated room intervention drone systems with lethal and non-lethal payload are used to carry out building clearance and urban surveillance in GPS denied areas.

- **AI Tools for Operational Efficiency: LLM-based text summarizers** for intelligence reports.
    - **Chatbots, facial recognition, voice-to-text systems** for operational support.
- **Simulation and Wargaming Platforms:** Use of AI to simulate battlefield conditions for training.

Applications of AI in Defence

- **Intelligence, Surveillance, and Reconnaissance (ISR)**
    - **Real-Time Data Analysis**: AI processes satellite imagery, drone feeds, and signals intelligence for real-time threat detection and situational awareness.
        - Example: AI-based analysis of border surveillance data to identify potential threats along India's borders.
    - **Predictive Analytics**: Uses machine learning to predict enemy movements, assess threats, and enhance situational awareness.
        - Example: Indian Army's AI-driven ISR systems under the C4ISR framework for real-time battlefield intelligence.
    - **Automated Target Recognition**: AI algorithms identify and classify targets from visual or sensor data, reducing human error.
        - **Example**: Integration in drone surveillance systems like **DRDO's Netra UAV.**
- **Autonomous Systems**
    - **Unmanned Aerial Vehicles (UAVs)**: AI-powered drones for reconnaissance, surveillance, and targeted operations.
    - **Unmanned Ground Vehicles (UGVs) and Naval Systems**: AI-driven robotic vehicles for logistics, mine detection, and combat support in hazardous areas.
        - Example: **Jaguar robot, a semi-autonomous unmanned ground vehicle (UGV)**, is primarily used by the **Israel** Defense Forces (IDF) for border patrol missions along the Gaza Strip border.
    - **Swarm Intelligence**: Coordinated operations of multiple autonomous units using AI for tasks like area domination or attack.
        - **Swarm drones have proven successful in conflicts such as the Russian-Ukraine conflict.**
- **Cybersecurity**
    - **Intrusion Detection and Response**: AI systems detect and neutralize cyber threats, including malware and hacking attempts, in real time.
        - **Example:** Indian Army's **"Cyber Shield"** initiative to protect military networks from AI-driven cyberattacks.

    - **Countering Adversarial AI**: AI tools to identify and mitigate enemy cyberattacks that leverage AI technologies.
    - **Electronic Warfare**: AI for signal jamming, interception, and countering enemy electronic systems.
- **Logistics and Supply Chain Management**
    - **Supply Chain Optimization**: AI optimizes resource allocation, inventory management, and supply chain logistics for efficient operations.
        - Example: Smart logistics systems under the Indian Army's AI Roadmap for real-time supply tracking.
    - **Predictive Maintenance**: AI predicts equipment failures (e.g., tanks, aircraft) to reduce downtime and maintenance costs.
        - **Example**: US Air Force's Condition-Based Maintenance Plus (CBM+) program to optimize fleet maintenance, increase aircraft availability, and minimize downtime.
    - **Resource Allocation**: AI-driven systems ensure optimal distribution of resources in combat and non-combat scenarios.
- **Decision Support Systems**
    - **Real-Time Decision-Making**: AI provides commanders with actionable insights for rapid decision-making in dynamic combat environments.
        - Example: AI-based C4ISR systems for real-time battlefield strategy formulation.
    - **Risk Assessment and Modeling**: AI models simulate scenarios to assess risks and plan strategies.
    - **Command and Control Enhancement**: AI integrates data from multiple sources to support centralized command and control.
- **Training and Simulation**
    - **Immersive Training**: AI-powered virtual reality (VR) and augmented reality (AR) for realistic training environments.
    - **War-Gaming Simulations**: AI creates complex scenarios for strategic and tactical training, improving preparedness.
    - **Personalized Training**: AI tailors training programs based on individual soldier performance and skill gaps.
- **Health Monitoring and Medical Support**
    - **Soldier Health Monitoring**: AI-driven systems monitor soldiers' health in real time, especially in remote or combat zones.

        - Example: Project **BHISHM and BHISHM 2.0** for AI-based health diagnostics and monitoring.
    - **Medical Decision Support**: AI assists in diagnosing injuries and recommending treatments in field hospitals.
        - AI tools for triage and medical logistics in high-intensity conflict zones.

Challenges in Defence AI Deployment

- **Lack of Defence-Specific Data Ecosystem:** AI systems require large, clean, and mission-oriented datasets, but military data in India is fragmented, often classified, and lacks standardisation.
    - This limits AI training for object recognition, threat prediction, or battlefield simulations, especially in Indian terrain and conflict conditions.
- **Integration Challenges with Legacy Platforms:** Most Indian defence platforms were not built with AI in mind, making retrofitting complex and costly.
    - Legacy systems like tanks, aircraft, and artillery face challenges in embedding AI modules for predictive maintenance or sensor fusion.
- **Ethical and Legal Ambiguity in Battlefield Use:** There are no clear legal frameworks or accountability norms for autonomous systems using lethal force.
    - Use of AI for targeting raises concerns under international humanitarian law, especially if non-combatants are misidentified or collateral damage occurs.
- **Lack of Transparency and Explainability:** Many AI systems, especially deep learning models, lack explainability and transparency in decision-making.
    - This creates hesitation among commanders to rely on AI during critical operations where human judgment and traceability are essential.
- **Vulnerabilities to Cyber and Adversarial Attacks:** AI can be manipulated through spoofing, data poisoning, and adversarial inputs, compromising its reliability.
    - Drones or surveillance systems may be misled by altered visual inputs or hacked to misclassify threats or misfire targeting protocols.
- **Shortage of Skilled AI-Ready Defence Workforce:** There is a critical gap in personnel trained to develop, interpret, or deploy AI tools in military settings.
    - Operational commanders often lack familiarity with algorithms, reducing effective deployment and oversight of AI-enabled systems.
- **Dependence on Foreign Hardware and Software:** India relies heavily on imported AI chips, processors, and proprietary algorithms, risking strategic vulnerabilities.
    - In scenarios of geopolitical tension, access to key AI infrastructure may be restricted or compromised by supply chain disruptions or embedded malware.

Government Support and Initiatives for AI in Defence

- **Innovations for Defence Excellence (iDEX 2018)**: A flagship initiative under the **Ministry of Defence** to foster innovation in defence by engaging startups, MSMEs, and innovators.
    - **Role in AI**:
        - Supports development of AI-based defence solutions, including autonomous systems, cybersecurity, and ISR technologies.
        - Provides funding, mentorship, and market access to startups working on AI projects.
- **Defence AI Council (2019)**: An **advisory body** established by the **Ministry of Defence** to guide the adoption of AI in defence operations.
    - **Functions**:
        - Formulates policies for AI integration in military applications.
        - Coordinates between the Indian Army, DRDO, and private sector for roadmap implementation.
- **AI Task Force (2018)**: Formed by the Government of India to recommend strategies for AI adoption in defence and national security.
    - **Key Recommendations**:
        - Integration of AI in ISR, cybersecurity, and autonomous systems.
        - Establishment of AI research centers and training programs for defence personnel.
        - Promotion of public-private collaborations for AI innovation.
- **Defence AI Project Agency (DAIPA 2019):** DAIPA was established to provide the necessary guidance and implementation framework for AI adoption in defense organizations.
    - It serves as the central execution body for AI projects and initiatives across the Indian military.
- **AI Research and Development in DRDO:**
    - **Centre for Artificial Intelligence and Robotics (CAIR), Bengaluru (1986):** Conducts workshops to train DRDO scientists in AI for defense systems and supports start-ups by nurturing innovation and collaboration.
    - **DRDO Young Scientist Laboratories (DYSL):**
        - DYSL-AI: Focused on AI-related research and applications.
        - DYSL-CT (Cognitive Technology): Concentrates on cognitive technology advancements for defense.
    - **Defence Institute of Advanced Technology (DIAT):** Offers certified courses in AI and machine learning.

Global Use of AI in Military and Defence

- **United States: AI for Autonomous Systems & Decision Dominance**
    - The US Department of Defense (DoD) is spearheading AI integration via its **Joint Artificial Intelligence Center (JAIC)** and **Project Maven**.
    - AI is used for drone surveillance (e.g., in Afghanistan), battlefield data fusion, autonomous naval vessels, and predictive logistics.
    - DARPA's OFFSET program enables drone swarming for urban warfare simulations.
- **China: Military–Civil Fusion & AI-Driven Strategic Ambitions**
    - China's 2017 AI Strategy aims to make it the **global AI leader by 2030**, including military superiority through **intelligentised warfare**.
    - PLA uses AI for facial recognition, satellite tracking, cyber operations, and decision-making tools.
    - Collaborations with tech giants like **Baidu and Alibaba aid military-grade** AI applications under **"military–civil fusion"** doctrine.

UN Convention on Certain Conventional Weapons (CCW) – Group of Governmental Experts (GGE) on **LAWS** (Lethal Autonomous Weapons Systems):

- Established in **2016.**
- **Mandate:** To discuss issues related to lethal autonomous weapons systems, including those involving AI.

International humanitarian law (IHL) is a set of rules that seeks, for **humanitarian reasons,** to limit the effects of **armed conflict**.

- **Russia: AI in Electronic Warfare & Unmanned Systems**
    - Russia uses AI for electronic countermeasures, battlefield simulations, and autonomous ground vehicles like **Uran-9**.
    - AI is embedded in cyber operations, disinformation campaigns, and hypersonic weapons decision-support systems.
    - Russia also tests AI-based command-and-control in joint exercises.
- **Israel: AI-Integrated Precision Warfare**
    - Israel leads in battlefield AI, notably through its use in the Iron Dome and **Harpy autonomous loitering munitions**.
    - AI is used in image processing, surveillance drones, and predictive border monitoring.
    - In **Operation Guardian of the Walls (2021)**, Israel reportedly deployed AI to generate rapid targeting databases.
- **United Kingdom: AI in Strategic Command and ISR**

- The UK's Strategic Command is experimenting with AI to enhance **Intelligence, Surveillance and Reconnaissance (ISR)** and threat assessment.
- AI-driven cyber defence systems are being tested for use in NATO environments.
- The UK is also investing in ethical frameworks for AI in lethal systems.

Way Forwards

- **Develop Clear Legal Frameworks**: Formulate national and international regulations for AI-driven defence systems, defining accountability for autonomous actions.
    - Advocate for binding agreements in UNCCW (Convention on Certain Conventional Weapons) discussions to regulate Lethal Autonomous Weapons Systems (LAWS), ensuring compliance with International Humanitarian Law.
- **Enhance AI Explainability**: Invest in **explainable AI (XAI)** to make decision-making processes transparent, increasing commander trust and accountability.
    - DRDO's **Centre for Artificial Intelligence and Robotics (CAIR)** to prioritize XAI research for systems like Command Information and Decision Support System (CIDSS) and surveillance tools.
- **Mitigate Algorithmic Bias**: Use diverse, standardized datasets for AI training, incorporating India-specific terrains and conflict scenarios.
    - Develop a centralized defence data ecosystem under the Operational Data Fusion Project to ensure high-quality, unbiased data.
- **Strengthen IHL Compliance**: Embed IHL principles into AI algorithms, ensuring systems prioritize distinction, proportionality, and necessity.
    - Align AI projects (e.g., autonomous drones, C4ISR) with IHL through mandatory human-in-the-loop protocols.
- **Promote Human Oversight**: Mandate **human-in-the-loop mechanisms** for all AI-driven lethal systems to ensure ethical decision-making.
    - Incorporate human oversight protocols in projects like **Project Storm Drone** and swarm drones.
- **Secure Data Privacy**: Build secure data lakes and implement strict access controls for AI-processed military data.
    - Strengthen the **Operational Data Fusion Project** with cybersecurity measures to protect sensitive data (e.g., ISR, logistics).
- **Capacity Building for Ethical AI**: Train personnel on ethical AI use and legal implications to bridge skill gaps and build trust.
    - Leverage **AI Centers of Excellence and Defence Institute of Advanced Technology (DIAT)** for ethical AI training programs.

- **Global Collaboration and Advocacy**: Engage in international forums like **UN CCAC** to shape ethical AI norms and prevent an AI arms race.
    - Propose human-centric AI guidelines, reinforcing India's commitment to responsible AI in defence.

Conclusion

Artificial Intelligence is transforming defence by enabling faster decision-making, autonomous operations, and enhanced situational awareness. India's 2025–27 AI roadmap positions it to leverage cutting-edge technologies while addressing ethical, infrastructural, and strategic challenges. Its success hinges on indigenisation, interoperability, and capacity-building.

Source: https://indianexpress.com/article/india/fast-tracked-after-operation-sindoor-drone-swarming-to-smarter-war-rooms-armys-ai-roadmap-for-ops-by-2026-27-10138891/