International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct- 2026, PP 01-08

Artificial Intelligence in Defence Systems: A Review of Applications, Enabling Infrastructure and Responsible Adoption in The Indian Context

Sayyad Mohd Zeeshaan Mohd Isaq[1] Prof. S. R. Borhade[2] Prof. M. C. Kolse[3] Prof. S. K. Said[4]
Department Of Artificial Intelligence And Data Science Jaihind College Of Engineering Pune,

Abstract—Artificial intelligence is reshaping modern defence by strengthening situational awareness, decision-making and operational readiness. This paper develops an integrated review of AI adoption across defence operations, with attention to the Indian context. It examines how machine learning, deep learning, computer vision, natural language processing and big data analytics support intelligence, surveillance and reconnaissance through analysis of satellite, radar and drone imagery; command and control through data fusion and decision support; cyber defence through intrusion detection; logistics and predictive maintenance of equipment; simulation-based training; and autonomous and unmanned platforms. The paper discusses the organizational and infrastructural foundations required for successful implementation, including reliable data, secure interoperable networks, computing facilities, skilled personnel and collaboration among the armed forces, research organizations and industry. It also reviews risks such as adversarial manipulation of AI models, brittleness in unfamiliar conditions, accountability for autonomous functions and international debates on meaningful human control, together with published ethical principles. A five-layer defence AI architecture is proposed with research gaps, objectives, a comparison of applications and challenges. The review concludes that AI should augment, not replace, human judgement in defence.

Index Terms—Artificial intelligence, defence, ISR, command and control, cyber defence, predictive maintenance, autonomous systems, human control

I. Introduction

1. Motivation

Modern armed forces collect far more data than human analysts can examine: hours of drone video, thousands of satellite images and continuous streams of radar, signals and cyber logs. Artificial intelligence can filter and fuse this information so that commanders see relevant threats faster.

Horowitz [1] argued that AI is a general-purpose technology that may shift the balance of military power, and Sayler [2] summarized its applications in intelligence, logistics, cyber operations, command and control and autonomous vehicles. India has begun to build capacity in this area, for example through the AI in Defence symposium and exhibition of 2022, which showcased AI products developed by the services, defence public sector units and industry [3].

This paper reviews defence AI applications, the infrastructure they require and the risks of adoption, and proposes a layered architecture with human control.

2. Objectives of the Review

- 1. To review AI applications across defence domains.
- 2. To examine data, network, computing and skill foundations for adoption.
- 3. To discuss risks, adversarial threats and ethical principles.

- 4. To propose a five-layer defence AI architecture with human control.
- 5. To identify challenges and future directions for India.

3. Overview of Key Concepts

Defence AI Application Domains

Fig. 1 groups defence AI into intelligence and surveillance, command and decision support, cyber defence, logistics and maintenance, training and simulation, and autonomous platforms.

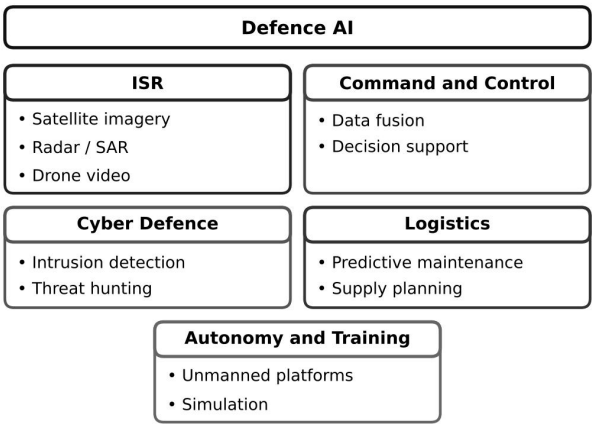


Fig. 1. Application domains of AI in defence systems.

4. Human Control

Scharre [4] distinguished systems where a human is in the loop (approves each action), on the loop (supervises and can intervene) or out of the loop. The degree of autonomy appropriate for a task depends on its risk and legal implications.

II. Review of Existing Work

Surveillance and recognition. Chen *et al.* [5] applied deep convolutional networks to target classification in synthetic aperture radar images and achieved high accuracy on a public benchmark. Lam *et al.* [6] released xView, a large overhead-imagery dataset for object detection, and real-time detectors such as YOLO [7] enable onboard analysis. Bondi *et al.* [8] demonstrated near-real-time detection from thermal drone video, a technique relevant to border monitoring.

Cyber defence. Buczak and Guven [9] surveyed machine learning methods for intrusion detection, which are central to protecting military networks.

Maintenance and logistics. Jardine *et al.* [10] reviewed condition-based maintenance that, applied to vehicles and aircraft, increases availability.

Risks and governance. Eykholt *et al.* [11] showed that small physical perturbations can cause vision models to misclassify objects, a serious concern for adversarial environments. The U.S. Department of Defense adopted principles requiring AI to be responsible, equitable, traceable, reliable and governable [12]. Table I summarizes these works.**TABLE I Summary of Literature Survey**

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct- 2026, PP 01-08

Ref.	Method	Key Findings	Limitations
[10]	Condition-based maintenance	Prognostics framework	Industrial context
[5]	CNN for SAR targets	High SAR classification accuracy	Benchmark conditions
[9]	ML for intrusion detection	Survey of cyber ML methods	Dated datasets
[1]	AI and balance of power	Strategic implications	Policy analysis
[11]	Physical adversarial attacks	Vision models can be fooled	Road signs studied
[6]	xView overhead dataset	Large detection benchmark	Optical imagery only
[8]	Thermal drone detection	Near-real-time detection	Conservation setting
[2]	AI and national security	Survey of applications	U.S. focused

III. Identified Research Gaps

- **G1:** Training data are classified, scarce and often not shareable across services.
- **G2:** Models may fail under deception, camouflage or new terrain.
- **G3:** Interoperability between legacy platforms and AI systems is limited.
- **G4:** Testing and certification methods for military AI are immature.
- **G5:** Doctrine for human control and accountability is still evolving.

IV. System Architecture

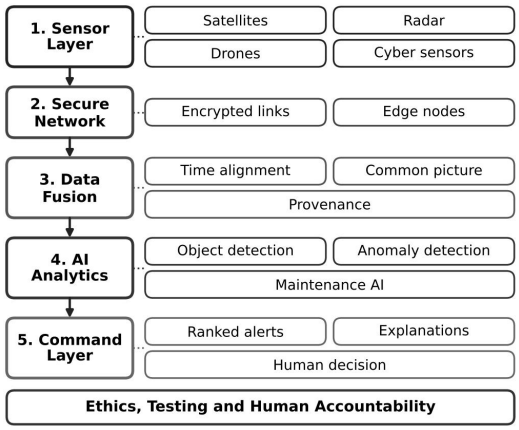


Fig. 2 shows the proposed architecture.

Fig. 2. Proposed five-layer defence AI architecture with human control.

- ### Sensor Layer
- Satellites, radars, drones, ground sensors and cyber sensors collect raw data.
- ### Secure Network Layer
- Encrypted, resilient tactical networks with edge computing move data from sensors to processing nodes.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct- 2026, PP 01-08

- **Data Fusion Layer**
- Data are cleaned, time-aligned and fused into a common operating picture, with provenance tracked.
- **AI Analytics Layer**
- Models perform object detection, anomaly detection, threat assessment, predictive maintenance and course-of-action support.
- **Command Layer**
- Commanders receive ranked alerts and recommendations with confidence and explanations; decisions with lethal or strategic implications remain with humans.

V. Implementation Methodology

Fig. 3 describes the decision-support workflow. A fused threat score combines evidence from several sensors,

$$S = \Sigma_i \, w_i \cdot c_i \cdot p_i \quad (1)$$

where p_i is a detection probability from sensor i, c_i its reliability and w_i its weight. Alerts above a threshold are passed to an operator together with supporting imagery and data.

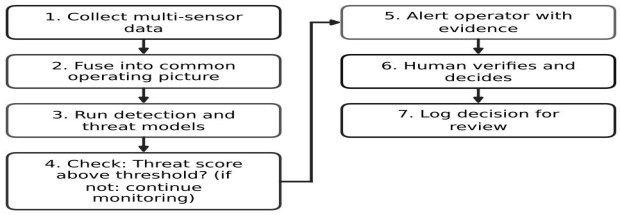


Fig. 3. AI-assisted threat assessment workflow.

VI. Performance Comparison

Table II compares applications by maturity and risk. Maintenance and logistics are lower risk and easier to adopt, while autonomous weapons involve the highest ethical and legal concerns.

TABLE II Comparison of Defence AI Applications

Application	Maturity	Risk Level	Human Role
Predictive maintenance	High	Low	Approves work
Imagery analysis	High	Medium	Verifies detections
Cyber defence	Medium–High	Medium	Supervises response
Decision support	Medium	High	Decides
Autonomous platforms	Emerging	Very high	In / on the loop

6.1 Open Issues and Future Directions

Table III summarizes challenges. Future directions include indigenous AI chips and models, test ranges for AI certification, joint data standards across services and international norms on autonomy.

TABLE III Challenges and Mitigation

Challenge	Mitigation
Classified, scarce data	Secure data sharing; synthetic data
Adversarial deception	Robust training; red-teaming
Legacy interoperability	Open standards; middleware
Testing and certification	Dedicated AI test ranges
Accountability	Clear doctrine; human control

VII. Conclusion

AI can strengthen defence by accelerating intelligence analysis, protecting networks and improving equipment availability. The reviewed literature shows mature techniques in recognition and anomaly detection but also vulnerability to deception and gaps in testing and governance. For India, investment in data, secure networks, computing, skills and partnerships, combined with clear principles of human control, will determine how effectively AI serves national security.

7.1 Acknowledgment

The authors express their sincere gratitude to the Department of Artificial Intelligence and Data Science, Jaihind College of Engineering, Pune, for providing the facilities, guidance and encouragement needed to carry out this work. The authors also thank the faculty members and colleagues whose valuable suggestions helped improve the quality of this review.

References

1. M. C. Horowitz, “Artificial intelligence, international competition, and the balance of power,” Texas Nat. Secur. Rev., vol. 1, no. 3, pp. 36–57, 2018.
2. K. M. Sayler, “Artificial intelligence and national security,” Congressional Research Service, Washington, DC, USA, Rep. R45178, 2020.
3. Ministry of Defence, Government of India, “Artificial Intelligence in Defence (AIDef) symposium and exhibition,” New Delhi, India, Jul. 2022.
4. P. Scharre, Army of None: Autonomous Weapons and the Future of War. New York, NY, USA: W. W. Norton, 2018.
5. S. Chen, H. Wang, F. Xu, and Y.-Q. Jin, “Target classification using the deep convolutional networks for SAR images,” IEEE Trans. Geosci. Remote Sens., vol. 54, no. 8, pp. 4806–4817, 2016.
6. D. Lam et al., “xView: Objects in context in overhead imagery,” arXiv:1802.07856, 2018.
7. J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, “You only look once: Unified, real-time object detection,” in Proc. IEEE CVPR, 2016, pp. 779–788.
8. E. Bondi et al., “SPOT poachers in action: Augmenting conservation drones with automatic detection in near real time,” in Proc. AAAI Conf. Artif. Intell. (IAAI), 2018.

9. A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2016.
10. A. K. S. Jardine, D. Lin, and D. Banjevic, “A review on machinery diagnostics and prognostics implementing condition-based maintenance,” Mech. Syst. Signal Process., vol. 20, no. 7, pp. 1483–1510, 2006.
11. K. Eykholt et al., “Robust physical-world attacks on deep learning visual classification,” in Proc. IEEE/CVF CVPR, 2018, pp. 1625–1634.
12. U.S. Department of Defense, “DOD adopts ethical principles for artificial intelligence,” Washington, DC, USA, Feb. 2020.