Indian Defence Artificial Intelligence Governance: Challenges and Strategic Imperatives

R. Gowri

INTRODUCTION

Artificial Intelligence (AI) has the power to translate the Indian defence environment with its applications. It has the potential to enable disruptive growth by horizontal penetration across verticals for innovative and economic progress. According to the McKinsey Report on "The State of AI in 2025", "most organizations are still in the experimentation or piloting phase" of AI adoption.[1] This indicates that it is high time to establish a clear and critical framework for each phase of the AI applications of the software development life cycle to enable a trustworthy environment.

Generative AI (GenAI) systems are a set of AI powered systems capable of producing innovative and creative content including text, audio, imagery and even software codes. GenAI applications

R. Gowri is a Research Associate at the Centre for Aerospace Power and Strategic Studies.

1. McKinsey Report, *The State of AI in 2025: Agents, Innovation, and Transformation* (2025), p. 8.

have the capability to operate across military functions, from analysis of intelligence, strategic planning, real time operational support, resource and asset allocation, providing training through simulation, and more. This transformative capability has encouraged governments to establish AI governance frameworks that balance innovation imperatives against existential security risks.

Regulators face challenges to navigate through the competing objectives in the defence AI landscape. Those include fostering innovation to maintain strategic advantage while ensuring the security and trustworthiness in the system with national security implications and establishing transparency, accountability, and standardising interoperability among the defence forces without compromising information security. This paper focusses on the Indian AI governance frameworks and initiatives in the defence sector and proposes strategic imperatives for India to establish comprehensive regulatory mechanisms capable of supporting AI deployment in defence operations.

INDIAN DEFENCE AI FOUNDATIONAL ARCHITECTURE AND INITIATIVES

India has established institutional foundations for defence AI governance other than general AI regulations. The Ministry of Defence (MoD) has established the Defence AI Council (DAIC) and Defence AI Project Agency (DAIPA), to provide strategic guidance and implementation support for AI adoption across the armed forces (Indian Army, Air Force, Navy). [2] The Evaluating Trustworthy Artificial Intelligence (ETAI) framework was launched on October 17, 2024, by Chief of Defence Staff

2. Press Information Bureau, "Transformation of India's Defence and Internal Security Posture," August 20, 2025, https://www.pib.gov.in/PressNoteDetails.aspx?ModuleId=3&NoteId=155066&id=155066. Accessed on October 23, 2025.

General Anil Chauhan and Defence Research and Development Organisation (DRDO) Chairman Dr. Samir V. Kamat. [3] The ETAI framework provides five foundational principles specifically for defence AI which are reliability and robustness, safety and security, transparency, fairness, and privacy. This framework provides structured criteria for evaluating trustworthiness throughout the AI development life cycle.

The Indian armed forces standardise all their requirements through the Directorate of Standardisation which is under the Directorate of Defence Production (DDP), MoD. To establish the common standards throughout the India, the Indian government has instituted the Bureau of Indian Standards (BIS). The defence standardisation programme of the Directorate of Standardisation also adopts Indian Standards (IS) issued by BIS, so that products can be dual-use, among both civil and defence applications. For standardisation of AI, BIS is a participating member in ISO/IEC JTC 1/SC 42, which is the international standards sub-committee responsible for AI. This participation enables India to influence emerging international standards while ensuring that domestic frameworks align with globally recognised best practices.

The Defence Acquisition Procedure (DAP), revised in April 2024, explicitly recognises the acquisition procedure for software-intensive Information and Coommunication Technology (ICT) programmes, including AI solutions in Chapter-VIII, running in commercial hardware, modified commercial hardware, and military-grade infrastructure, including, "artificial intelligence projects that has AI output as the main deliverable." The Integrated Defence Staff (IDS), in collaboration with DRDO, industry partners, and academia, has formulated the Technology Perspective and

3. India AI, "Trustworthy AI Framework Launched for Critical Defence Operations," October 21, 2024, https://indiaai.gov.in/news/trustworthy-ai-framework-launched-for-critical-defence-operations. Accessed on November 30, 2025.

Capability Roadmap (TPCR), 2025, which provides a strategic blueprint for military modernisation over the next 15 years. [4] This document comprehensively provides the various projects with use cases for defence AI applications. The scheme for Innovations for Defence Excellence (iDEX) has been established by the Department of Defence Production (DDP) under the Defence Innovation Organisation (DIO).[5] As per operational requirement specifications mentioned by the armed forces, iDEX provides linkage among the armed forces, Defence Public Service Units (DPSUs), research institutions, academia, start-ups, Micro, Small, and Medium Enterprises (MSMEs), industries and innovators to develop technical innovative solutions. The Development of Innovative Technologies with iDEX (ADITI) has been established under iDEX for additional funding and promoting innovations in critical and strategic defence technologies, including AI solutions.

To focus on empowering the military with cutting-edge defence technologies to achieve self-reliance, DRDO, the Research and Development (R&D) wing of the MoD of the Government of India partners with academia, research institutions and industry to work in the field of critical technologies, including AI, to boost defence related applications. It undertakes these efforts through focussed programmes such as the DRDO Young Scientist Laboratory (DYSL)—Artificial Intelligence, DYSL – Cognitive Technologies, Centre for Artificial Intelligence and Robotics (CAIR), and Directorate of Futuristic Technology Management (DFTM).[6] The year 2025 has been observed as the

4. HQ IDS, Technology Perspective Capability Roadmap, 2025, https://mod.gov.in/dod/sites/default/files/FINAL-TPCR-2025_0.pdf. Accessed on October 23, 2025.
5. "IDEX - Innovation for Defence Excellence," https://idex.gov.in/indus_x. Accessed on October 30, 2025.
6. "HOME Defence Research and Development Organisation - DRDO, Ministry of Defence, Government of India," https://www.drdo.gov.in/drdo/. Accessed on October 23, 2025.

'Year of Technology Absorption' rightfully by the Indian Army (IA), to adapt and integrate futuristic and emerging technologies to strengthen the defence technology ecosystem.[7]

DAIC and DAIPA provide institutional coordination to enable integrated strategic planning across the military Services. The operational requirements and security constraints are acknowledged with defence-specific principles. Despite the establishment of an institutional architecture, the defence AI governance of India lacks explicit, enforceable regulatory mechanisms. The current implementation relies on internal organisational practices rather than formal legislation, with enforcement capacity. The limited enforcement capacity in India allows non-compliance to boost AI infrastructure without any consequences. The absence of explicit rules and regulations and statutory penalties reduces the deterrent effects of non-compliance. Also, there are limited financial and skilled human resources compared to other countries, which is a challenge for the development of AI defence applications.

Security Architectures for Military AI Applications

Effective multi-agency AI deployment requires strong and secure data sharing mechanisms that protect the AI infrastructure. It is important to share sensitive data securely without compromising privacy, national security or data integrity. The implementation of the security architecture has to be viewed not as an obstacle to interoperability, but as an enabling foundation. It is vital to implement the best practices throughout the phases of analysis, design, processing of data, coding, implementation, and testing. The cryptographically signed database, usage of checksums,

7. "Theme of the Year 2025 - The Official Home Page of the Indian Army," https://indianarmy.nic.in/about/about-us-site-main/theme-of-the-year-2025-about-us-site-main. Accessed on October 30, 2025.

implementation of cryptographic hashes to detect unauthorised changes, and use of digital signatures have to be implemented to operationalise the secured data. The end-to-end encryption model has to be applied, while data is stored in the system (data at rest), in transmission (data in transit), and during processing (data in use). The Advanced Encryption Standard (AES) provides symmetric encryption for stored data, the Transport Layer Security (TLS 1.3) protects secured transmission of data, and the Trusted Execution Environments (TEEs) protect processing environments from unauthorised access. The unidirectional communication channels can be achieved through data diodes for preventing unauthorised reverse-direction data flow. The hardware-based diodes provide air gap isolation for critical systems and software data diodes can be implemented to enable controlled data sharing within Virtual Private Network (VPN) environments. The implementation of data diodes can be established as per the inter- and intra-agency security requirements to carry out the data sharing mechanism with the zero-trust architecture. The zero-trust architecture requires explicit authentication and verification of authorisation for all data, irrespective of the system's network location.

In India, the Joint Cipher Bureau (JCB) which works under the DRDO, is responsible for maintaining the cryptographic security across all defence and intelligence establishments. The collaborative relationship between the defence organisations and JCB helps to establish the cryptographic security and guidelines for solving the dilemma of data sharing. The common data exchange standards across defence organisations enable Application Programming Interface (API)-driven information sharing on these standardised schemas. The standardised data exchange formats with the cryptographic authentication help to enable the interoperable AI infrastructure while maintaining organisational security parameters.

Military AI Applications for Decision Support

AI applications have the capacity to reduce the human decision-making time across multiple defence domains through their distinctive capability contributions. AI has the capability to enable realistic scenario development through dynamic simulations that incorporate geopolitical variables, asset allocation options, system-of-systems interactions, and multi-level strategic, operational, and tactical perspectives. It can identify patterns in the historical datasets and analyse the behaviour of adversaries for real world scenarios that exceed human cognitive capacity for pattern recognition.

The integration of AI with digital twin technology can help to reproduce the operational infrastructure to provide enhanced situational understanding and training among the forces. Moreover, this also allows higher level decision-makers to test multiple possibilities, evaluate potential outcomes and learn actionable insights, which can be implemented in the real world scenario.

AI-enabled applications in instrumentation support real-time predictive maintenance by continuously monitoring critical systems such as aircraft components, to detect anomalies at an early stage. This helps prevent equipment failures, and facilitates timely corrective action, which significantly enhances operational reliability and safety.

The defence intelligence analysis is the process of analysing multi-dimensional classified data across image, audio and video, human intelligence and open-source information. The data analysis and processing of large volumes of multi-dimensional data can be implemented with the help of AI to extract the thematic insights, and to enable complex analytical reasoning which are beyond human processing capacity. The integration of data across the defence forces helps to provide intelligence to the higher defence leadership and reduce the decision time cycle. The predictive

capabilities of AI support evidence-based foresight, estimation of uncertainty, and objective decision support for planning forward looking and threat appreciation.

AI has the capacity to provide content clarity as per the stakeholder'a specific needs and has the capability to improve visualisation of information by providing clear, understandable and attractive presentations. AI systems can provide near real-time decision support, enabling rapid planning, resource allocation, and execution based on real-time live intelligence. Together, these capabilities strengthen situational awareness, accelerate operational responsiveness, and enhance strategic advantage in defence and security environments.

DEFENCE AI ADOPTION STRATEGIES

The adoption of AI applications typically follows a staged implementation process that progresses from assisted decision support towards increasing levels of autonomy. In the initial phase, the Human-in-the-Loop (HITL) approach is essential, wherein human operators actively contribute throughout the system's life cycle by supplying training data, validating model outputs, and providing continuous feedback to support reinforcement learning. As system maturity and model accuracy improve, this transitions to the Human-on-the-Loop (HOTL) framework, wherein humans supervise system decisions, and intervene only when necessary, thus, enhancing reliability and responsiveness. Ultimately, with sufficient confidence in system performance and safety, the operations can move towards a Human-out-of-the-Loop (HOOTL) stage, enabling full automation with minimal human intervention.[8] This progressive

8. Donald Farmer, "Human Oversight Enables Automated Data Governance | TechTarget," *TechTarget*, December 27, 2024, https://www.techtarget.com/searchdatamanagement/opinion/Human-oversight-enables-automated-data-governance. Accessed on November 30, 2025.

transition ensures responsible AI deployment, operational safety, and trust in autonomous systems.

AI can automate non-critical workloads such as data collation, processing, and routine analysis, enabling human operators to focus on higher-level decision-making as systems gradually evolve from assisted decision support to partial and eventually full autonomy. The iterative assessment framework for military AI proposed by the Asser Institute, Centre for International and European Law, proposes two complementary mechanisms: Iterative Review and Iterative Assessment in Deployment. This framework is based on the principles of international humanitarian law, by emphasising the importance of updating missed unknown real-time scenarios in the dataset iteratively after post-deployment of AI applications.

Edge AI agents, deployed at operational locations, interact with edge users to provide information in that area and help to take decisions. This edge AI architecture helps to reduce edge device computational requirements, enables implementation in air-gapped architecture, processes sensitive data locally and maintains data sovereignty.

STRATEGIC IMPERATIVES FOR DEFENCE AI

The following challenges that need be converted into potential opportunities are strategic imperatives for deployment of defence AI applications in operations.

1. **Procurement of Hardware for AI in Terms of Graphic Processing Unit (GPU):** The delay in the delivery of products leads to the procurement of products that are outdated at the time of delivery. The projects should be implemented as per the timelines and should have the capability or flexibility to upscale features as per the technological maturity available in the market.

2. **Common AI Infrastructure**: The interoperability and harmonised operational capabilities can be achieved by establishing a common AI infrastructure across defence organisations. The integrated ecosystem would help to facilitate secure data sharing and standardised AI development frameworks. The shared infrastructure would help to reduce the duplication of AI solutions development, resource expenditure, as also increase the joint situational awareness, and collaborative threat assessment.
3. **Integration and Sharing of Information**: Currently, all the defence and intelligence organisations are implementing their AI solutions in silos. The integration and secure sharing of information across defence organisations is important for building a robust AI infrastructure. Effective data interoperability enables comprehensive situational awareness, accelerates analytical processes, and enhances mission planning and execution capabilities.
4. **Common Standardisation for Data Exchange:** There is a need for common standardisation frameworks for data exchange among defence organisations. To facilitate seamless communication, and reduce system fragmentation, there is a need for the establishment of uniform protocols, and data governance policies.
5. **Sovereign Model and Infrastructure:** The sovereign Large Language Models (LLMs) have to be built to support India's AI architecture. India uses open source LLMs deployed over Western cloud architecture. Therefore, there is need to develop a fully independent national cloud architecture to develop sovereign AI models and supporting infrastructure. This is not merely a necessity but a strategic imperative to ensure data sovereignty, security, and long-term self-reliance in defence AI capabilities.

CONCLUSION

AI governance in other countries provides multiple frameworks. Especially the European Union (EU) Act implemented in August 2024, applies its rules and regulations even to non-EU companies. The United Kingdom has set up "regulatory sandboxes," to provide an AI test environment as per real-world settings. Brazil has made independent algorithmic impact assessments mandatory for high-risk systems. The approach of China is far more restrictive, with its interim administrative measures tightly governing GenAI through content moderation, data protection, and alignment with state directives. While these are not directly related to military AI, they can be suitably applied to all types of AI development. The existing defence AI framework needs clear rules and regulations to maintain a balance between innovation and control.

The challenges during the procurement and integration of AI infrastructure, sharing of data, standardisation of data exchange protocols, and sovereign AI models and cloud architectures, need to be converted into potential opportunities in the AI ecosystem. Security of information during the development and implementation of defence AI applications needs to comply with existing protocols. There is a requirement to progress in a graduated manner keeping the human in the loop initially before obtaining autonomy. The HOTL configuration for controlled intervention of humans for the updating of policies and regulations should be well suited with rigorous iterative assessment mechanisms to capture post-deployment anomalies and system vulnerabilities. By addressing the existing gaps, Indian defence AI capabilities can leapfrog to strengthen national security.