CENTRE FOR AEROSPACE POWER AND STRATEGIC STUDIES

In Focus

New Delhi

CAPSS In Focus: 48/2026

18 November 2026

India's Military AI Preparedness amidst Strategic Competition for AI Sovereignty in the Contemporary Technology Control Regime

Ms Gowri R
Research Associate, Centre for Aerospace Power and Strategic Studies



Source: Created using ChatGPT AI

Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Aerospace Power and Strategic Studies [CAPSS]

This work is licensed under Creative Commons Attribution – Non-Commercial – No Derivatives 4.0 International License.

Keywords: AI Sovereignty, Global AI Restraints, AI Readiness, Agentic AI

Introduction

On October 16, 2026, China's Ministry of Commerce and Ministry of Science and Technology proposed restrictions and prohibitions on the export of 40 technologies, including 23 related to Artificial Intelligence (AI) and specific to large-scale models, intelligent agents, computing clusters, and information-processing technologies, through its Announcement No. 48. These restraints have been introduced due to the state's concerns about national security and in response to prevent misuse. Since AI has proven its potential for both defensive and offensive use, strategic competition amongst nations is expanding as they seek to balance this technological asymmetry. This has not only driven the sovereign development of AI and related enabling technologies, but also the control of crucial AI technologies to preserve national security and strategic interests. Therefore, AI now serves as an important means of statecraft and an effective geopolitical instrument across the various pillars of national power.

For countries that rely on externally controlled AI technologies, contemporary developments raise critical questions about AI adoption and operational autonomy. As India expands AI adoption in strategic applications, including defence and security sectors, dependence on foreign-origin AI technologies assumes special relevance. The future of capability development and deployment of AI depends on unhindered access to advanced models, computing infrastructure, and related technologies. This article emphasises that AI sovereignty should beat the core of India's military AI development strategy. It further examines the implications of foreign AI restraints against Indian Military preparedness to evaluate the adequacy of current policy, institutional, and structural defences in light of the emerging governance challenges associated with agentic AI systems.

Global AI Restraints and Evolving Technology Control Regime

AI technology-producing countries beyond China also leverage their technological prowess in protecting their strategic interests. While AI technology is still maturing, global technology control is being exercised in terms of restricting the sharing of AI models and AI-Native systems, including their training parameters, datasets, and orchestration architectures, that impact their performance, adoption and absorption across critical use cases. The United States (US) Department of Commerce introduced the Framework for Artificial Intelligence Diffusion in January 2025, alongside advanced-chip restrictions, which regulates certain highly advanced closed-weight AI models and their underlying trained parameters. In May 2025, the US Department of Commerce announced it would not enforce the new compliance requirements of the AI Diffusion rules issued earlier. Despite

this relaxation, regulatory restraints on advanced AI technologies persist because of national security concerns. These control measures have also been extended to private industry. Notably, in June 2026, the US government directed Anthropic to stop providing foreign nationals access to the Fable 5 and Mythos 5 models quoting national security reasons. Earlier in 2023, the Netherlands had imposed controls on exports of specified advanced semiconductor manufacturing equipment under US pressure to restrict access to China. Further, these controls were expanded on April 01, 2025, introducing clearance requirements for exports of certain semiconductor-manufacturing equipment and related technologies to countries outside the European Union.

These developments indicate that growing restrictions on advanced AI technologies are being imposed or expanded with minimal or no notice, causing uncertainty for countries that are dependent on externally controlled AI technologies and infrastructure. Therefore, it is essential to ensure that critical AI-enabled systems, especially in defence forces, remain safe, secure, reliable, and operational even if access to externally developed technologies, models, or services is restricted or denied. While open models of foreign origin provide valuable capabilities, their suitability for sensitive applications depends on the availability of infrastructure, safeguards, and viable alternatives to address degradation or denial of services at the source. As India advances its military AI capabilities and ambitions in AI sovereignty, considerations of design, development, and deployment should be incorporated from the beginning, rather than addressing them as an afterthought once technological dependencies are established.

From Policy Foundations to Implementation

Recognising this overarching strategic significance of AI technologies, India has progressively established policy, institutional and governance frameworks to support development and use across civilian and defence domains. Such initiatives reinforce AI's role as a key enabler of future national capabilities. However, the effectiveness of these measures ultimately depends on their actual and implied operational outcomes.

At the national level, the Government of India, through NITI Aayog, has provided an initial roadmap for AI development and adoption through the National Strategy for Artificial Intelligence published in June 2018. This strategy was later supplemented by AI governance guidelines to promote secure, responsible, and trustworthy AI systems. In the defence sector, dedicated institutional arrangements have been established to facilitate AI adoption. In February 2019, the Ministry of Defence, Department of Defence Production (DDP), created the Defence AI Council (DAIC) and Defence AI Project Agency (DAIPA) to provide strategic leadership and implementation support for AI integration across the defence forces. Additionally, the Defence Research and

Development Organisation (DRDO) launched the Evaluating Trustworthy Artificial Intelligence (ETAI) framework on October 17, 2024, to address trust in AI for defence operations and applications. Thus, the ETAI framework represents a significant step towards promoting trustworthy AI within the defence ecosystem.

In summary, these policy frameworks, institutions, and evaluation mechanisms in India have established a foundation for military AI governance. However, assessing the implementation framework and effectiveness of such arrangements is difficult to fathom due to limitations of publicly available information on their deployment. The primary challenge in the defence context is translating policy objectives into operational outcomes. Clarity in accountability, attribution, periodic evaluation, and institutional coordination are tenets for translating strategic objectives into concrete, measurable operational competencies. As Military AI systems become more autonomous, these requirements gain greater importance due to their ramifications and outcomes. Emerging technologies, such as agentic AI, bring new opportunities and challenges related to security, accountability, and operational control, necessitating adaptive governance mechanisms.

Agentic AI Risks: Responsibility and Inter-Service Coordination

On October 15, 2026, the Indian Computer Emergency Response Team (CERT-In) issued a critical advisory (CIAD-2026-0049) over concerns of unauthorised access by AI agents that are undergoing research and evaluation. It aimed to address deliberate misuse of open-source agentic AI tools against Indian Information and Communication Technology (ICT) assets. While this advisory does not identify any particular AI models, agentic frameworks, providers, or affected organisations, it describes exploits of conventional security weaknesses and recommends safeguards for AI model developers, research laboratories, evaluation agencies, organisations, and service providers.

From a military perspective, CERT-In's advisory highlights potential threats and vulnerabilities posed by increasing adoption of autonomous AI systems in defence. As AI-enabled applications are integrated into an array of defence functions including cyber operations, intelligence analysis, logistics, and decision support, their adoption signals the non-negotiable necessity of resilient governance, accountable oversight, and inter-services coordination. As the level of autonomy in defence systems increases, the risks related to agentic AI, including unauthorised actions, cybersecurity vulnerabilities, and loss of operational control, will require effective governance and coordination mechanisms. However, an adequate balance is to be maintained between promotion and control to ensure positive, scalable development in AI for defence applications. Implementing existing and essential institutional arrangements will be critical in shaping India's long-term military AI readiness, operational autonomy, and AI sovereignty.

Conclusion

The increasing trend of technology control regimes such as AI export controls, access restrictions, and technology-denial measures by major AI-producing states indicates that access to critical AI technologies is now being shaped primarily by geopolitical and national security considerations. For India, these developments underscore the necessity and importance of AI sovereignty to preserve preserving military AI readiness and retain operational autonomy in domains of choice. India has established policy systems, institutional mechanisms, and evaluation initiatives to support AI adoption in defence. The effectiveness of these arrangements will depend on their implementation and their capacity to address challenges arising from increasingly autonomous AI systems.

Although restrictions on advanced AI technologies tend to incentivise domestic capability development, effective technological substitution requires access to computing infrastructure, data, expertise, financing, and sustained demand to drive progressive indigenous design, development and deployment. Therefore, India's response must integrate selective international adoption with appropriate safeguards and targeted domestic investment. The goal of sustaining essential military functions amidst the evolving variables of technology controls and geopolitical conditions shall remain the focus. This requires concentrated efforts to evaluate the effectiveness of existing arrangements, identify limitations in current procedures, and tailor policy measures to address specific dependencies for stated military outcomes. Ultimately, AI sovereignty should be measured by resilience and graceful degradation, along with effective management of critical capabilities that shape India's strategic direction.