ARTICLES

Open-Source AI and the Democratization of Lethal Capability: Security Implications for India

Author: Shubhi Malhotra • **Published:** June 24, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

Open-source AI is no longer just a tool for innovation. It is also becoming a force multiplier for non-state actors, terror networks, insurgent groups, and hostile information operations. As autonomous drones, synthetic propaganda, AI-assisted planning, and dual-use technical knowledge become easier to access, India faces a new security challenge where lethal capability is no longer limited by cost, infrastructure, or expertise.

Introduction

For most of the modern history, the capacity to inflict mass violence was exclusively monopolized by cost, expertise, and infrastructure. Building a missile required a state, synthesizing a nerve agent required a laboratory, designing an improvised explosive device required battlefield experience, transferred through networks over years. Capability was scarce, and scarcity was a form of security.

Artificial intelligence, specifically the open-source ecosystem of large language models, computer vision systems, and autonomous planning frameworks, is dismantling that monopoly. In 2024 and 2025, models with reasoning capabilities comparable to GPT-4 were released under permissive open licenses, downloadable by anyone with a computer and an

internet connection. By early 2026, various advanced models introduced in the market, which are capable of interpreting sensor feeds, generating technical schematics, and coordinating multiple tasks step by step, and were freely available on repositories like Hugging Face and GitHub. The implications of this advancement can be seen across the countries globally. For India, a country navigating active insurgencies, cross-border terrorism, and an increasingly hostile neighbourhood, they are of urgent concern.

How Open-Source AI Empowers Non State Actors

The central danger is not that open-source AI creates capabilities that did not previously exist. The real danger lies in the fact that it brings down the skill gap existing between professional militaries and non-state actors at a negligible level, not even a fraction of what it once was.

Autonomous drone guidance is the most immediate concern. Commercial drones have been weaponized by groups from ISIS in Syria to Naxal-linked actors in India's Red Corridor. Until recently, effective autonomous targeting (the ability for a drone to identify and pursue a target without a human operator) required sophisticated military level expertise. Open-source computer vision models, fine-tuned on freely available image datasets and deployable on edge hardware costing under $200, now make primitive autonomous guidance possible. India's security forces have already encountered crude drone-borne IEDs along the Line of Control in Jammu and Kashmir. The trajectory toward autonomy is not hypothetical, it is ongoing and ever increasing.

Synthesis route generation presents a second dimension of risk. Large Language Models (LLMs), particularly those released without safety checks and balances, can walk a chemically literate person through procedures required for acquisition, reaction conditions, and stabilization methods for energetic materials and toxic agents. While the most dangerous information requires genuine domain knowledge to operationalization, AI dramatically reduces the research burden. A group with one trained chemist and access to an uncensored model can now accomplish what previously required a specialised, expensive team. For a country like India, that shares borders with so many countries, this is a concrete threat.

Operational planning and counterintelligence evasion represents another equally serious risk. Modern AI assistants can analyse terrain, model patrol patterns, identify infrastructure vulnerabilities from satellite imagery, and generate deception strategies. Organizations like Lashkar-e-Taiba and Jaish-e-Mohammed have historically demonstrated sophisticated planning capabilities. To them, AI provides an analytical multiplier that does not require additional human capital, is invisible in transit, and leaves no procurement footprint. Encrypted AI inference operated locally on a laptop produces no signals that can be detected or intercepted.

Finally, the influence and radicalization operations are being transformed. Generative AI enables the mass production of highly personalized propaganda, deepfake videos, and synthetic audio in regional languages, including Hindi, Urdu, Punjabi, Tamil, etc. All these are languages in which moderation infrastructure remains thin. The targeting of youth from marginalized and economically backward communities can be achieved easily in good numbers, and that too at a low cost, in ways that could not have matched earlier.

A Landscape Without Fences: Regulatory Gap

India's current regulatory architecture was not designed for this threat. All the Acts introduced or amended by the Government, whether the Information Technology Act of 2000 that was amended in 2008, or the Digital Personal Data Protection Act of 2023, mentions about cyber privacy and offence, but contains no specific provisions for AI-enabled harm or its dual-use. The Ministry of Electronics and Information Technology's draft AI governance frameworks, introduced in 2023 and 2024, focus primarily on accountability for commercial AI applications, rather than security

dimensions related to it.

The gap is not merely domestic. Open-source AI is globally distributed. For example, a random file uploaded to a server in Russia or France is accessible in any place, including India, Pakistan, or Rwanda. India has no bilateral or multilateral framework that gives it leverage over the decisions taken by the developers of AI outside India, neither any equivalent of export control regimes that govern hardware or conventional weapons. The Wassenaar Arrangement, which coordinates export controls on dual-use technologies among its forty-two member states, has not been updated to meaningfully address AI related issues, partly because defining "sufficiently dangerous" capability in a domain of rapid, nonlinear progress is technically and diplomatically a complex task.

Domestically, the gaps are large. Law enforcement agencies lack the technical capacity and capability to assess AI-enabled threats, conduct forensic analysis of AI-assisted attack plannings, or even recognize when and where AI has been used in an operational chain. The National Investigation Agency (NIA), which handles terrorism cases, has begun developing cyber capabilities, which is a good start, but definitely not enough. The developments, rather than focusing on advanced features still remains structurally dedicated towards conventional digital forensics, eventually pushing back the development we aim for. There is no dedicated unit with the mandate and expertise to monitor the open-source AI threat landscape continuously. On the other hand, advanced countries have taken a leap in this direction, making it a matter of urgent concern for India.

At the conceptual level, Indian strategic doctrine has not yet internalized AI-enabled non-state threats as a distinct category requiring distinct responses. The dominant frame remains conventional military deterrence and intelligence-led counter-terrorism. Both are necessary, but insufficient, when a group in a denied area can autonomously plan, communicate, and execute operations using locally run AI with no discoverable supply chain.

Balancing Innovation and Security: A Path Forward

The solution is not to restrict open-source AI development, which would be neither effective nor wise. India's own technology ecosystem, its startups, research institutions, and defence R&D, is a significant beneficiary of open-source AI. IIT labs, DRDO projects, and the emerging Indian AI industry depend on the same AI models and frameworks that pose dual-use risks. A regime that restricts or blocks open-source access, would impose asymmetric costs for its usage, eventually hampering India's legitimate innovators in this field while doing little to stop determined adversaries who pass these restrictions illegally.

What India needs is a differentiated, layered strategy built on four pillars:

First, capability-specific risk assessment. Not all open-source AI poses equal risk. A classification system should distinguish between models with general usage which is not harmful and the ones with significantly dangerous capabilities, like those that meaningfully assist weapons synthesis, autonomous weapons guidance, or large-scale manipulation operations. The government, working with technical experts from TIFR, IITs, and the private sector, should develop clear criteria for this classification. This enables proportionate regulatory responses without blunt restrictions.

Second, security community capacity building. India should invest substantially in AI-threat assessment. This means employing AI specialists in the NIA and the Intelligence Bureau, establishing a dedicated AI Security Threat cell under the National Security Council Secretariat, and conducting exercises that simulate AI-assisted attack planning. The goal is not to outpace adversaries in AI development but to develop the analytical acumen and institutional power to understand what adversaries are doing with AI in real time.

Third, international norm-building with initiative. India is both a major open-source AI consumer and a country with a big and direct market of AI-relevant terrorist threats. This gives it a unique position to lead in multilateral forums. India

should push for AI safety dimensions to be incorporated into the Financial Action Task Force frameworks for terrorist financing (extending scrutiny to AI tool acquisition), into the Wassenaar Arrangement's dual-use technology discussions, and into bilateral security dialogues with the United States, Israel, Japan, and France, all of which have advanced capabilities in AI-threat assessment. This will create a double impact, serving the security interests as well as giving a push to India's broader ambition for having a leading influence in emerging technology governance globally.

Fourth, domestic legal architecture for AI-enabled threats. India needs a strong legal provision that criminalizes the use of AI to facilitate violent offences, not AI development or deployment generally. It should focus exclusively on the specific application of AI tools in terrorist activities or insurgent contexts. This enables prosecution even when the AI tool used was legally obtained, and sends a deterrent signal to adversaries, while leaving the innovation ecosystem intact. Equally important is updating evidence law to address AI-generated content in criminal proceedings. This is important to address a gap that will grow, with deepfakes becoming an emergent concern and threat.

Conclusion

India has historically managed security threats through a combination of intelligence penetration, security force capacity, and episodic legal reform. This model succeeded in contexts where threat actors had capability limitations. Open-source AI removes those limitations faster than any alert government can curb the new ones.

The choice India faces is not between security and innovation. It is between deliberate, proactive strategy, focusing on building state capacity, shaping international norms, and developing proportionate legal instruments, and the default of institutional lag, in which the security community perpetually responds to the last attack rather than anticipating the architecture of the next one.

The democratization of lethal capability is not a future threat. It is a present condition. India's security architecture must be redesigned accordingly.

Bibliography

1. Brockmann, K. "Regulating Transfers of AI Algorithms, Training Data and Models: The Potential and Limitations of Export Controls." SIPRI. https://www.sipri.org/commentary/topical-backgrounder/2026/regulating-transfers-ai-algorithms-training-data-and-models-potential-and-limitations-export.
2. Cdr Verma, R. "AI, Drones & The New No War No Peace." Indian Aerospace and Defence Bulletin - News for Aerospace and Defence in India. https://www.iadb.in/2025/05/31/ai-drones-the-new-no-war-no-peace/.
3. Dr. Littich, R., and J. Dr. Swienty-Busch. "Using Synthesis And Route Design Technology To Approach API Complexity." Drug Discovery Online. https://www.drugdiscoveryonline.com/doc/using-synthesis-and-route-design-technology-to-approach-api-complexity-0001.
4. Dunsin, D., M. C. Ghanem, et al. "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response." ScienceDirect. Accessed June 9, 2026. https://www.sciencedirect.com/science/article/pii/S2666281723001944.
5. Eiras, F., et al. "Risks and Opportunities of Open-Source Generative AI." ArXiv.org. https://arxiv.org/abs/2405.08597.
6. Ezeh, N., A. Widgery, and C. Canada. "Artificial Intelligence and Law Enforcement: The Federal and State Landscape." National Conference of State Legislatures. https://www.ncsl.org/civil-and-criminal-justice/artificial-intelligence-and-law-enforcement-the-federal-and-state-landscape.

7. Joshi, Y. "Drones of Terror Expose India's Defences." Institute of South Asian Studies. https://www.isas.nus.edu.sg/wp-content/uploads/2019/10/ISAS-Briefs-No.-704.pdf.
8. Kreps, S. "Democratizing Harm: Artificial Intelligence in the Hands of Nonstate Actors." Brookings - Quality. Independence. Impact. https://www.brookings.edu/wp-content/uploads/2021/11/FP_20211122_ai_nonstate_actors_kreps.pdf.
9. Ojha, A. "AI Governance in India: A Case Study." NeGD – National E-Governance Division. https://negd.gov.in/wp-content/uploads/2026/02/Astha-Ojha-AI-Governance-in-India-Final-4.pdf.
10. Prof. Sood, A. K. "India AI - Governance Guidelines." Press Information Bureau. https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf.
11. Singh, R. "Drones a clear, present threat, says army chief." PressReader.com - Digital Newspaper & Magazine Subscriptions. https://www.pressreader.com/india/hindustan-times-bathinda/20210702/281505049200818.
12. United Nations Office. "Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System." United Nations Office on Drugs and Crime. https://www.unodc.org/documents/justice-and-prison-reform/Child-Victims/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of

??The views expressed are those of the authors and do not represent the views of CNAWS.