The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 4 | Issue 3 | March 2026
ISSN: 2583-973X (Online), SJIF IF: 5.6
Website: www.theacademic.in

Ethical Applications of Artificial Intelligence in National Security

Shriya Wadhwa[1], Khushi Gupta[2], Shweta Sinha[3]

[*1] Scholar, Dept. of Computer Science, National P.G. College, University of Lucknow, iamshriyaw11@gmail.com

[2] Scholar, Dept. of Computer Science, National P.G. College, University of Lucknow, khushigupta29@gmail.com

[3]Assistant Professor, Dept. of Computer Science, National P.G. College, University of Lucknow, sinha.shweta020776@gmail.com

DOI : https://doi.org/10.5281/zenodo.19386038

ARTICLE DETAILS

Research Paper

Accepted: 17-03-2026

Published: 10-04-2026

Keywords:

Artificial Intelligence, National Security, Ethical AI, Cyber Defence.

ABSTRACT

Artificial intelligence is transforming defence and national security with the sophistication of surveillance, it is able to spot threats quickly and make better operational decisions. Its increasing popularity, however, poses ethical risks such as breach of privacy, accountability, transparency, and its possible misuse. In this paper, the theoretical background of AI in national security is offered, critical ethical issues are identified, and the necessity to regulate it responsibly is supported by examples at an international level. It ends up by drawing out the future directions and plans of ethical use of AI in defence.

I. Introduction

The Artificial Intelligence integration has been a major factor that transformed the approaches to national security across the globe. The AI systems are currently used to analyse vast amounts of data, border monitoring, and cyberattack prediction, as well as help in making strategic decisions. With the rise in the use of AI, the ethical concern of privacy invading and the use of biased results and transparency have become a major concern. The real-life world events such as erroneous facial recognition, misinformation via deepfakes, and discriminatory surveillance presentations depict these threats. The use of AI in defence directly affects the lives of people, sovereignty, and stability in the international system compared to the civilian industries. An error or prejudice in AI systems related to the military or security

can result in erroneous surveillance, the escalation of the conflict, or the murder of innocent individuals, and thus the problem of ethics cannot be overestimated. The expanded use of systems that fall under the jurisdiction of the algorithms raises dire concern about the privacy and accountability, transparency, and human control of data. The introduction of the AI-related security solution is an inevitable trend since India has to address multifaceted issues on the land border, maritime, domestic security and cyber space. In such a way, not only is it a technological requirement to develop the ethical standards concerning AI, but it is also a strategic one to safeguard democracy, human rights, and national integrity.

II. AI in National Security

2.1 Surveillance and Monitoring

The Company has adopted surveillance and monitoring as an activity of the security personnel. With AI-enhanced surveillance, it is possible to detect deviant behaviour due to the fact that it detects abnormalities rapidly, threats are detected sooner and the analysis of trends is done more efficiently, as compared to humans. Such systems may assist the security agencies to deploy the resources more efficiently, especially in case of large masses of people and other events which are deemed to be risky. With the rising number of smart cities, surveillance cameras, traffic sensors and command centres operated by AI are being connected to defence and internal security databases. It is in this respect that they can share information more quickly in the event of an emergency, though it also worries them about the concomitant over-centralisation of the information.

Case Study: According to The UK Metropolitan Police Trial (2019), AI-facilitated facial recognition systems were often mistakenly used to identify civilians.

2.2 Border Security

The AI-guided drones, heat sensors, and automated trackers are observed to scout complicated and risky areas.The AI-based services in the border security are gaining additional capabilities when it comes to landscape and threat recognition. Artificial intelligence (AI) devices may also be applied in arid regions such as Rajasthan to track movement when patrol is barely possible in harsh climatic conditions due to the heat. AI-enhanced satellite surveillance and thermal sensors are utilized to supplement the Line of Actual Control (LAC) mountainous and high-altitude zones in order to track the weather conditions in the case of poor visibility. Such relevance was increased further after the 26/11 Mumbai attacks which highlighted the fact that there is need to be cautious with regards to technology. The application of AI weather prediction tools can also enhance the safety of the patrols as it predicts the avalanche, storms,

and severe weather conditions such that the patrols could make a more suitable plan to do businesses in the border**.**

Case Study: Israel uses AI-enhanced border surveillance on the territories of conflict zones (Israel Border Surveillance Report, 2020).

2.3 Cybersecurity

AI will assist in identifying malware code, phishing, and suspicious cyber behaviour. Emerging cyber threats are increasingly automatized in nature and the bad actors are in the process of automating their intrusions to render them faster, dynamic, and massive. As a result, AI must be applied to defence mechanisms to win against AI-oriented cyber warfare as well. This is extremely significant in the activities of finding the zero-day vulnerabilities, which are historical undiscovered software vulnerabilities. AI can detect suspicious behaviour as there is no formal threat signature through system behaviour analysis. Some of the most essential national infrastructures that are overly relying on AI-based cybersecurity tools include the power grid, the railway network, communication infrastructure, and the defence sector units of the population. These assets have to be preserved such that they do not create mass disruption and instability in the country.

Case Study: It was pointed out by experts that the 2021 SolarWinds breach was not always known before, which could have been identified with the powerful anomaly-detection AI tools.

2.4 Decision Support Systems

Artificial intelligence-based decision support systems find wide use in military wargames and other strategic games that required commanders to be able to consider different scenarios and their effects and take action in the real world. The logistics management involves the use of AI to streamline troop movement, fuel provision, medical assistance and ammunition distribution. The defence forces can use AI to process patterns and begin the required relief and plan the military support of the civil providers. Case Study: Some of the countries utilized prediction tools based on AI during the COVID-19 pandemic when mapping hotspots and predicting the direction to contain the outbreak. 2.5 Intelligence and Threat Analysis and Prediction. Online behaviours are analysed using AI to inquire of any likely threats based on online communication patterns and trails. AI will be very critical in improving the intelligence gathering through Open-Source Intelligence (OSINT) that utilizes the examination of open-source content of social media, news outlets, satellite photos, and internet forums. By the patterns of behaviour

and communication, AI systems will be able to identify the initial threat indicators of radicalisation, organised crime or even security threats before it has been a big event.

Case Study: Intelligence agencies of the US tested AI-driven pattern recognition before the major cyberattacks.

2.5 Threat Prediction and Intelligence Analysis

AI studies the online behaviour and communication patterns in order to forecast possible threats. AI is crucial in improving intelligence gathering using Open-Source Intelligence (OSINT) that encompasses the evaluation of publicly accessible data of social media, news sources, satellite images, and online forums. By identifying the patterns of behaviour, communication trends, AI systems can identify the initial signs of radicalisation, organised crime or even security threats earlier on before it has become a significant occurrence.

Case Study: The pattern recognition based on AI was tested by the US intelligence agencies prior to significant cyberattacks.

III. Ethical Concerns in AI-Driven National Security

3.1 Privacy Violations

There is the option of AI-based mass surveillance of citizens without their approval.

Case Study: The widespread AI-based surveillance technology in China has become an issue of worldwide privacy.

3.2 Intransparency (Black Box Problem)

AI algorithms tend to give a result without justification on how decisions were made. Case in point: Crime prediction AI tools in the US were accused of having obscure scoring systems

3.3 Bias and Discrimination

The use of AI models trained on biased datasets can be discriminating to some populations.

Case Study: There were multiple studies that reported a larger error rate in darker-skinned people in a system of facial recognition.

3.4 Accountability Issues

Once AI systems develop malfunction or are wrong in their choices, it is hard to hold anyone accountable.

Case Study: Vehicles on autopilot and accident cases have cast doubt on the issue of liability.

3.5 Misuse and Weaponisation

AI may fall in the wrong hands of other hostile countries, criminals, or extremist factions. Illustration: There has already been misinformation, in the political arena, in several countries, through deepfake video.

IV. Need for Ethical Frameworks

4.1 Mandatory Human Oversight

Human approval should be given to all the high risk operational decisions. Illustration: The US military adheres to a human-in-loop AI-driven weapons.

4.2 Strong Governance Policies and Regulations

Data collection, limits of surveillance and use of AI in defence and policing should be clearly stipulated by legislative guidelines.

4.3 Transparency and Auditing of AI Systems

Regular audits and internal checks are necessary to identify and reduce hidden biases and prevent misuse.

4.4 Autonomous Weapon Controls and Restrictions

The lethal weapons with full autonomy should be censored or limited. Examples: The United Nations is still debating the restrictions on the independent lethal AI weapon systems.

V. Problems in Implementing Ethical AI

5.1 Shortage of Skilled Professionals

Ethical AI requires expertise from law, psychology, data science, cybersecurity, and defence strategy, creating a high demand for multidisciplinary professionals.

5.2 Rapid Technological Change

AI advancements often outpace regulatory frameworks, leaving gaps in responsible governance.

5.3 Limited Infrastructure and Funding

Ethical AI requires advanced infrastructure, secure servers, and strong cybersecurity systems, which may be costly.

Ethical Domain	Core Concerns
Human Rights	Privacy protection, limits on surveillance, civilian safety
Accountability	Clear responsibility and legal–ethical oversight
Bias & Fairness	Eliminate discrimination in security and intelligence
Transparency	Explainable and auditable AI decisions
Safety & Reliability	Prevent errors and unintended escalation
Strategic Stability	Control escalation and military AI spread
Cyber Security	Protect AI from hacking and data manipulation

Table: Ethical Dimensions of AI in National Security.

VI. Benefits of Ethical AI

6.1 Increased Public Trust

Citizens feel more secure when AI tools are responsibly regulated.

6.2 Fair and Accurate Decisions

Ethically governed AI reduces false alarms and misidentifications.

6.3 Safer Defence Operations

Real-time AI intelligence helps reduce risk to human personnel.

6.4 Stronger International Partnerships

Countries with ethical AI policies gain greater international trust and cooperation in defence matters.

VII. Future Scope

7.1 Institutionalisation of Explainable and Auditable AI

Future defence-grade AI systems will move beyond black-box models toward explainable and auditable architectures, enabling military decision-makers to trace, verify, and justify AI-driven outcomes. This will enhance operational trust, legal accountability, and compliance with democratic oversight mechanisms in national security operations.

7.2 Human-Centric Human–AI Decision Frameworks

The future of national security lies in human-in-command AI, where artificial intelligence augments- rather than replaces- military judgment. By fusing satellite intelligence, HUMINT, cyber intelligence, and real-time data analytics, AI will assist officers in complex threat assessment while actively mitigating cognitive, cultural, and algorithmic biases.

7.3 Ethically Governed Autonomous Defence Capabilities

Next-generation autonomous systems- such as surveillance drones, border patrol robots, and unmanned combat platforms- will be designed with embedded ethical constraints, mandatory human override controls, and strict adherence to international humanitarian law. This evolution will ensure operational efficiency without compromising moral responsibility or civilian protection.

7.4 India-Specific AI Governance and Defence Ethics Architecture

India’s national security framework is expected to evolve through the creation of dedicated defence AI ethics bodies, integrating military leadership, technologists, legal experts, and policymakers. Such establishments will develop principles of optimal surveillance, cyber deterrence, data sovereignty, and the creation of AI-based indigenous defence systems in accordance with national values and constitutional principles.

7.5 Proactive and Predictive Cyber Defence Ecosystems

Future AI systems will shift cybersecurity from reactive response to predictive threat intelligence, enabling early detection of cyber intrusions, disinformation campaigns, and hybrid warfare tactics. Such anticipatory defence mechanisms will significantly strengthen national digital resilience and critical infrastructure protection.

7.6 Transformation of Military Education and Officer Training

The military academies will be further introduced to AI literacy, ethics, cybersecurity policy, and governance of autonomous systems in their curriculum. This change will equip the officers of the future to lead the AI-enabled forces in a responsible manner, and guarantee leadership informed in the battlefield guided by technology.

7.7 International Norm-Building and Strategic Leadership

Ethical applications of AI in national security will open avenues for global norm-setting and defence diplomacy, positioning responsible states as leaders in shaping international standards for military AI. This will reduce escalation risks, promote transparency, and encourage cooperative security frameworks in an increasingly AI-driven world.

VIII. Conclusion

Artificial Intelligence has become an essential component of modern national security. Its use in surveillance, cyber security and predictive analysis has enhanced speed with regard to operation efficiency and strategic decision-making. However, ethical challenges such as privacy violations, accountability gaps, and risks of misuse highlight the need for strong regulatory frameworks. Real-life global cases demonstrate that unethical AI practices lead to public mistrust, discrimination, and national vulnerability. Therefore, AI systems must be deployed transparently, responsibly, and under strict oversight. Ethical AI will allow countries like India to maintain national security while upholding human rights, public trust, and international credibility.

References:

- S Yu, F Carroll: Implications of AI in national security: understanding the security issues and ethical challenges.

URL: https://link.springer.com/chapter/10.1007/978-3-030-88040-8_6

- FE Morgan, B Boudreaux, AJ Lohn: Military applications of artificial intelligence: ethical concerns in an uncertain world
  URL: https://apps.dtic.mil/sti/html/tr/AD1097313/
- M Taddeo, D McNeish, A Blanchard: Ethical principles for artificial intelligence in national defence
  URL: https://link.springer.com/chapter/10.1007/978-3-031-09846-8_16
- M Ivey - Geo. J.: The ethical midfield in artificial intelligence: Practical reflections for national security lawyers Legal Ethics, 2020
  URL: https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3545307
- JR Shook, T Solymosi, J Giordano: Ethical constraints and contexts of artificial intelligent systems in national security, intelligence, and defense/military operations
  URL:https://www.emerald.com/books/editedvolume/13148/chapterabstract/83612139/Ethical-Constraints-and-Contexts-of-Artificial?redirectedFrom=fulltex