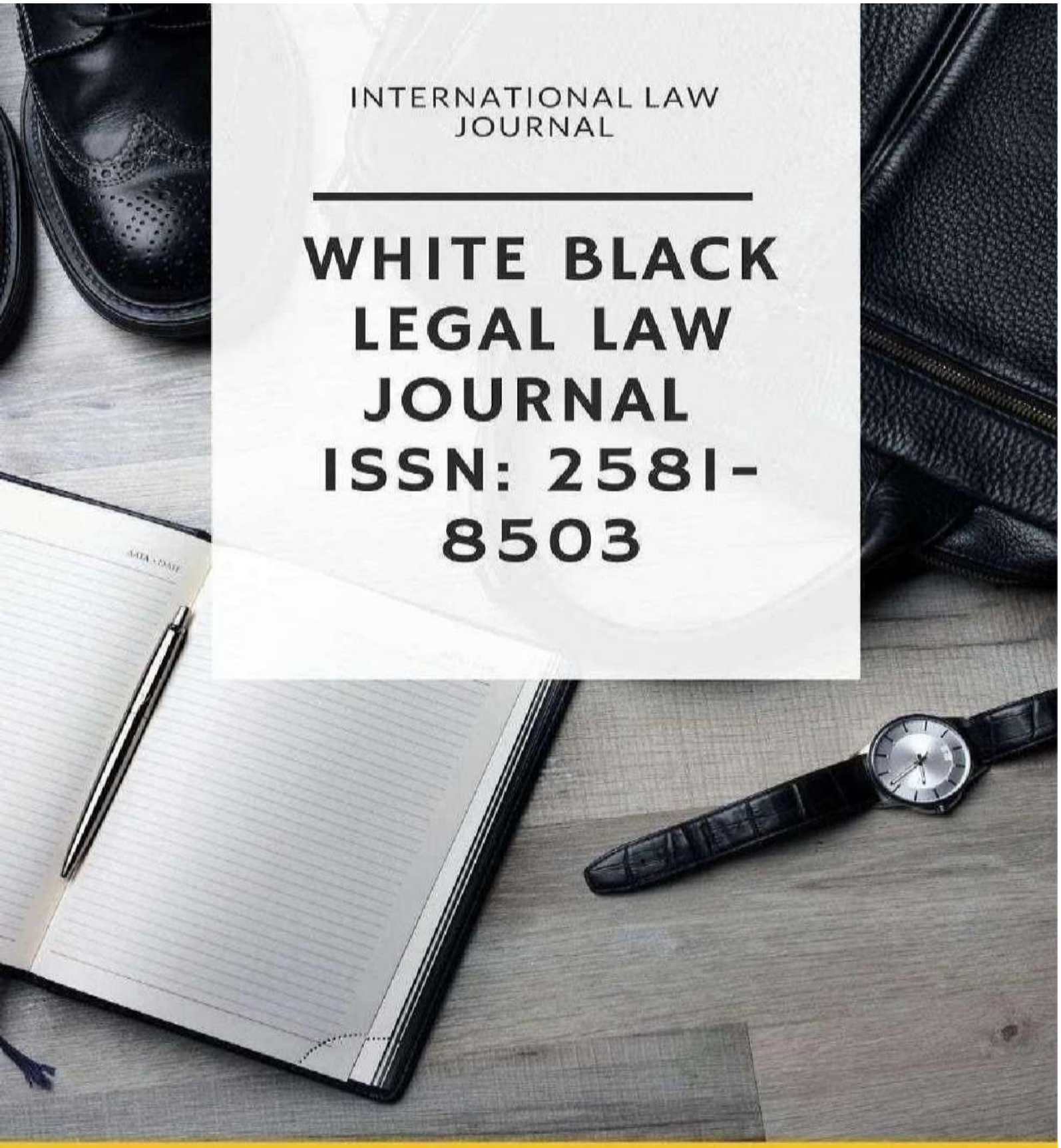

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

ARTIFICIAL INTELLIGENCE'S CONTRIBUTION TO COMBATTING TERRORISM AND SAFEGUARDING NATIONAL SECURITY

AUTHORED BY - DR. DIVYA, MUSHKAN & BHARTI
Anangpuria School of Law

Abstract

In the twenty-first century, national security policies and counterterrorism plans have been drastically altered by artificial intelligence (AI). AI's unparalleled capacity to analyse vast amounts of data, spot threat trends, and facilitate real-time decision-making has made it an essential tool in the war on terrorism. This article explores the various applications of artificial intelligence in cybersecurity, military operations, intelligence gathering, and surveillance, with a particular focus on India's evolving national security framework. It highlights the shortcomings of current governance structures and looks into the moral, legal, and policy concerns brought up by the use of AI. The report, which draws inspiration from case studies and contemporary discourse, advocates for a measured strategy that capitalises on artificial intelligence's potential while upholding democratic values and constitutional rights.

Keywords: National Security, Artificial Intelligence, Counterterrorism, Surveillance, Cybersecurity, Predictive Policing.

INTRODUCTION AND BACKGROUND

The global threat of terrorism is still dynamic and requires states to always be creative in security and defence. Characterised by its asymmetry and unpredictability, terrorism uses technological innovations for fatal purposes. Artificial intelligence has been progressively embraced as a revolutionary agent by the counter-terrorism field. AI is a necessary tool for spotting and reducing risks since it can scan large amounts of data, recognise trends, and learn from past performance.

Among the several technologies that make up artificial intelligence are robotics, computer vision, natural language processing, and machine learning. Within the field of counter-

terrorism, each of them has different purposes. For instance, while computer vision technology can increase surveillance efficiency in highly populated public areas, machine learning algorithms can detect aberrant behaviour in banking transactions suggestive of terrorist financing. Therefore, artificial intelligence improves the capacity of security experts to predict, recognise, and handle risks with more accuracy and speed rather than replacing human judgement.

Including artificial intelligence into national security systems marks not only a technical change but also a basic change in policy, ethics, and governance. This study aims to examine the pragmatic benefits of artificial intelligence together with the fundamental factors guiding its application in democratic nations.

The Evolution of Terrorism in the Digital Age: An Indian Viewpoint

In India, terrorism has historically shown up as left-wing insurgencies, religious fanaticism, and ethno-nationalist movements, among other things. Organisations including Lashkar-e-Taiba (LeT), Jaish-e-Mohammed (JeM), Indian Mujahideen, and several Naxalite factions have carried out acts of terrorism motivated by different ideological reasons over the decades. Though their approaches have changed in the digital era, the roots of many movements are in historical and geopolitical complexity.

The basic framework of terrorism has changed under the digital revolution. Affordable cellphones, fast internet, and encrypted communication apps like Signal and Telegram, along with the rise of social media sites like Facebook, X (previously Twitter), and YouTube, have made terrorist acts increasingly scattered, anonymous, and technologically sophisticated. Today's terrorist groups are not just operating in the physical sphere; they are also using cyberspace to attract young people, spread extreme ideas, raise money via cryptocurrencies, and painstakingly plan attacks.

India has suffered from both domestic extremism and cross-border terrorism, with digital tools progressively guiding terrorist network operations. Though not entirely digital, the 2008 Mumbai attacks showed how Voice over Internet Protocol (VoIP) and GPS-enabled tools might be used for real-time coordination. Recent digital data shows that by means of Telegram chats and other encrypted platforms, companies like ISIS have sought to radicalise Indian youth.

Moreover, India's growing dependence on digital infrastructure makes it vulnerable to cyberterrorism, which consists of data leaks, ransomware attacks, and targeting of vital infrastructure including financial networks, transportation systems, and power grids. Because of their anonymous and international traits, Indian agencies have struggled to monitor these attacks. The 2016 Uri attack, the 2019 Pulwama bombing, and the Kudankulam Nuclear Power Plant malware incident highlight the complicated nature of terrorism in the digital age—physical and digital dimensions combined.

This development calls for a paradigm change in India's counter-terrorism strategy whereby advanced technological capacities—especially artificial intelligence (AI)—enhance conventional law enforcement techniques (Aayog, 2018).

The ascent of artificial intelligence in national security: global patterns and India's development

In national security and counter-terrorism campaigns, artificial intelligence is now a major tool. From many angles of their intelligence and defence systems, nations including the United States, China, Israel, and the United Kingdom have included artificial intelligence. Using artificial intelligence technologies—including predictive analytics, pattern recognition, facial recognition, natural language processing, autonomous drones, and automated surveillance systems—threats are found, behavioural patterns are analysed, communications are monitored, and security risks are real-time mitigated.

India is in an early but quickly advancing stage of using artificial intelligence for national security. Acknowledging the strategic possibilities of artificial intelligence in 2018, the NITI Aayog produced the policy paper "National Strategy for Artificial Intelligence", giving national security top priority. To oversee and coordinate the inclusion of artificial intelligence into the Indian Armed Forces, the Ministry of Defence established the Defence AI Council (DAIC) and the Defence AI Project Agency (DAIPA) in 2020.

Several Indian agencies are now first using AI tools in limited capacities. Alleged to be using AI-enhanced data mining methods for counterintelligence and surveillance are the Intelligence Bureau (IB) and the Research and Analysis Wing (RAW). Using AI-driven algorithms, the National Technical Research Organisation (NTRO) investigates satellite images and signal intelligence. Two examples of artificial intelligence applied in crime pattern analysis—which

can also be used to identify terrorist threats—are the Crime Mapping Analytics and Predictive System (CMAPS) of the Delhi Police and the NIRBHAY AI system of the Mumbai Police.

Private-sector Indian companies and research facilities are developing AI technologies for cybersecurity, sentiment identification, behavioural analysis, and surveillance. Working together among DRDO (Defence Research and Development Organisation), ISRO, and academic institutions including the Indian Institutes of Technology (IITs), indigenous AI tools fit for counter-terrorism uses are being developed.

Attributed to a lack of coherent strategy, inadequate data-sharing protocols, privacy and civil rights concerns, and the absence of thorough legal frameworks controlling the use of AI in national security, India continues to lag behind worldwide leaders in AI-driven counter-terrorism.

Artificial Intelligence Needs for Indian Counterterrorism Efforts

India's unique political, geographic, and socio-cultural setting makes it especially vulnerable to terrorism. Unstable frontiers marked by repeated cross-border incursions and state-sponsored terrorism surround the country. India argues with left-wing radicalism in central India, separatist movements in Jammu & Kashmir, and communal tensions easily sparked by social media. Conventional techniques of intelligence gathering, physical observation, and manual analysis have shown their shortcomings in this complex terrain of danger.

From mobile information, internet activity logs, and social media feeds to CCTV footage—the enormous volume of data Indian security authorities must evaluate daily is daunting. Often resulting in agencies ignoring important warning signals, the manual review of this data is labour-intensive and wasteful. By real-time data analysis, anomaly detection, and predictive modelling, artificial intelligence helps to automate these processes.

Predictive policing represents a major use of artificial intelligence in Indian counter-terrorism. By means of historical data, artificial intelligence can be taught to spot behavioural patterns that precede terrorist activities, such as unusual bank transactions, travel habits, or dubious communications. These projections allow quick interventions and help to prevent assaults.

High-risk settings, including airports, metro stations, and public demonstrations, increasingly

use artificial intelligence-driven facial recognition and gait analysis systems. Initiated by the National Crime Records Bureau (NCRB), the National Automated Facial Recognition System (AFRS) is being built to instantly correlate criminal records with surveillance footage. Especially in the lack of a data protection law, this technology raises serious concerns about surveillance overreach, privacy invasions, and possible usage; yet, it also has great potential for identifying terror suspects.

India faces growing threats in cyberspace, where artificial intelligence can take centre stage. Instantaneously detecting and mitigating phishing attacks, malware, and ransomware, AI-driven cybersecurity solutions can also spot network traffic anomalies and stop breaches that might compromise infrastructure or important defence systems.

Moreover, efforts against radicalisation can benefit much from artificial intelligence. Natural Language Processing (NLP) systems can assess online conversation for extremist material in many Indian languages. Radicalising stories before they become violent can be found by sentiment analysis. This is particularly important in India, where radicalisation usually results from popular content on websites including WhatsApp, Telegram, and YouTube in local languages (NTRO, 2023).

In terms of border security, image recognition technologies, terrestrial sensors, and AI-powered drones can help track attempts at invasion all around India's large land boundaries. Artificial intelligence can improve the performance of the Indian Army in maintaining territorial integrity and the Border Security Force (BSF) when combined with satellite imagery analysis.

Notwithstanding these opportunities, including artificial intelligence in India's counter-terrorism strategy calls for a careful approach. Currently, the legislative framework controlling artificial intelligence use in national security is insufficient. There is not a strong legislative framework controlling how intelligence and law enforcement agencies use artificial intelligence. Originally in Parliament for several years, the Personal Data Protection Bill has been replaced by the Digital Personal Data Protection Act, 2023, which has not yet been fully adopted and does not particularly target state monitoring use artificial intelligence.

Using artificial intelligence also raises constitutional questions, particularly with regard to Article 21 of the Indian Constitution, which guarantees personal liberty and the right to life.

Requiring protections against intrusive surveillance technologies, the Supreme Court's key decision in Justice *K.S. Puttaswamy v. Union of India*, 2017 confirmed the right to privacy as a fundamental one. Therefore, an equilibrium has to be created between the basic rights of people and the justified goals of national security.

MAIN USES OF ARTIFICIAL INTELLIGENCE FOR COUNTER-TERRORISM

In modern counter-terrorism policies, artificial intelligence (AI) has grown to be a major factor improving effectiveness. From cross-border intrusion to domestic radicalisation, the Indian environment is marked by a diversified and dynamic threat landscape that AI helps to promptly gather, process, and interpret large data sets. Its uses cover cybersecurity, intelligence gathering, and surveillance, so arming law enforcement and intelligence agencies with advanced tools to recognise, track, and neutralise threats. Still, every one of these applications presents ethical, legal, and pragmatic issues that call for careful review.

Artificial Intelligence for Intelligence Development

Intelligence collecting—especially through Natural Language Processing (NLP)—is a major use of artificial intelligence in counter-terrorism. Natural language processing (NLP) makes machines able to understand and generate human language, which is therefore indispensable for the study of digital communications connected to terrorism. AI-driven natural language processing is crucial for spotting radicalising trends and covert messaging that might otherwise go unnoticed in multilingual countries like India, where extremist discourse may be spread in Hindi, Urdu, Bengali, Tamil, and several regional languages. These techniques are used by agencies including the Intelligence Bureau (IB) and National Technical Research Organisation (NTRO) to select content for sites including Facebook, WhatsApp, and Twitter. By means of analysis of terrorist manifestos, propaganda, and online dialogue, artificial intelligence systems can spot fresh hazards in real time. These advances, however, have to fit constitutional protections, including the right to privacy recognised by the Supreme Court in K.S. Puttaswamy v. Union of India 2017. Although India lacks a whole framework for AI-driven linguistic surveillance, the Information Technology Act of 2000 and the Indian Telegraph Act of 1885 allow particular forms of monitoring. Though it ignores major flaws in surveillance control, the Digital Personal Data Protection Act, 2023, marks a commendable improvement.

Open-source intelligence (OSINT) is a vital domain in which artificial intelligence speeds data

aggregation and analysis from publicly available sources, including social media, blogs, and news websites. Using artificial intelligence to extract data from many sources, Indian intelligence agencies—including the National Cyber Coordination Centre (NCC) and the National Investigation Agency (NIA)—monitor terrorist recruiting, propaganda, and networks. Algorithms can find terms, geotags, or behaviour connected to radical groups like ISIS or Lashkar-e-Taiga. OSINT operates under a vague legal framework where publicly available information often lacks privacy protections, yet the growing personalisation of social media material calls for more attention. Together with the 2023 Data Protection Act, Article 21 of the Indian Constitution states that even publicly available data must be handled ethically and properly, especially when used for national security aims (NIA, 2022).

Integrating ordered and unstructured data sources calls for artificial intelligence. Traditionally, intelligence gathering has consisted of compartmentalised information—military records, financial activities, surveillance video, and intercepted communications. Artificial intelligence helps different databases to be merged, generating comprehensive risk profiles using machine learning models that find relationships among apparently unrelated data elements. Gradually integrating biometric, geographic, and behavioural data using AI-driven fusion systems, the NTRO and the Indian Army are exposing hidden networks of terrorism. Still, data fusion aggravates privacy problems, particularly in the absence of clear permission systems and defensive actions. Although the Information Technology Act and Indian Evidence Act let particular data processing techniques; nevertheless, the unchecked use of artificial intelligence to gather personal data raises constitutional issues and data exploitation risks (Singh, 2021).

Artificial Intelligence-Enhanced Monitoring

With facial recognition a main tool, artificial intelligence is revolutionising Indian surveillance systems. Major cities, including Delhi and Mumbai, as well as especially at important sites like airports, railway stations, and large public gatherings, face facial recognition technologies that are extensively applied. These systems combine databases of found offenders or suspects with facial images taken by cameras. In counter-terrorism scenarios—such as keeping border areas under security or tracking radicals during demonstrations—face recognition helps law enforcement act quickly. Still, the use of this technology has drawn criticism because of its biases and errors, especially in heterogeneous populations free from traditional control. Although monitoring is generally allowed under the Information Technology Act for public safety reasons, the lack of a specific control controlling facial recognition aggravates the

situation. In this context, the problems underlined in the Puttaswamy ruling on proportionality and the legal basis of surveillance especially apply (NCRB, 2023).

In public safety, behavioural analytics marks yet another AI-driven invention. Using video analytics, this system detects anomalies in crowd behaviour—such as lingering, sudden gatherings or erratic movements—that might point to reconnaissance or an approaching attack. Using this technology in high-risk areas, including Indira Gandhi International Airport in New Delhi and CST Station in Mumbai, Indian law enforcement agencies have found These systems offer preventive actions and proactive surveillance. Real-time assessment of personal behaviour raises moral and constitutional issues. The current legal systems, such as the Indian Telegraph Act, lack the required clarity to control complex and extensive surveillance, allowing possible abuse or profiling.

One significant area of artificial intelligence-augmented surveillance is drones and automated monitoring systems. Equipped with high-resolution cameras and artificial intelligence algorithms, drones patrol border activity in regions including Kashmir and Punjab, sending real-time intelligence to ground forces. These drones monitor insurgent movements, help to identify smuggling paths, and protect important infrastructure. The Unmanned Aircraft Systems (UAS) Rules, 2021, set Indian drone operations' legal environment. Still, the quick adoption of drones without careful legal, ethical, and privacy policies continues to highlight governance concerns.

Cybersecurity's Uses

One important field where artificial intelligence is applied for counterterrorism initiatives is cybersecurity. Cyberterrorism is now a major threat since terrorist groups are using digital media more and more. Finding cyberattacks—including phishing, ransomware, and denial-of-service operations targeted at essential infrastructure—also depends on artificial intelligence algorithms. AI tools have been used by the Indian Computer Emergency Response Team (CERT-In) and the Ministry of Home Affairs to find traffic anomalies, spot trends in breaches, and carry out preventative counteractions. By quickly spotting unusual network activity and isolating compromised systems, AI-driven intrusion detection systems can help to minimise interruption. Nevertheless, even if the Information Technology Act, 2000, creates the legal framework to combat cybercrime, India lacks a particular legislative instrument meant to target cyberterrorism. Though it does not cover the technological complexities of AI-assisted

cyberwarfare, the Unlawful Activities (Prevention) Act, 1967 (UAPA) creates a framework for punishing crimes related to terrorism.

Despite its undeniable urgency, India is still in the early stages of the legal discussion surrounding the use of AI in counterterrorism. There is currently a significant gap between technological capabilities and legal accountability due to the lack of explicit regulation governing AI uses in national security. The growing use of AI systems that can autonomously identify, flag, or act upon humans without obvious supervision makes this discrepancy all the more worrisome. In an era of automated governance, a robust legal framework is both a constitutional and regulatory necessity to safeguard civil liberties. India needs comprehensive legislation that outlines the permissible uses of AI in security contexts, protects against algorithmic bias or inaccurate profiling, requires transparency and auditability of AI decisions, and creates judicial or parliamentary oversight frameworks. The absence of such a framework puts the public's trust in governmental institutions at risk as well as operational overreach by intelligence services. When AI-driven systems are used for targeted operations, detentions, or surveillance, it can be challenging to hold people accountable for misuse or technical malfunctions due to the legal void.

With artificial intelligence technologies being used increasingly to monitor encrypted and anonymous communication networks, the dark web remains a haven for illegal terrorist activities. Indian agencies like the NIA work with foreign agencies like INTERPOL to probe dark websites for evidence of terror financing, arms trafficking, or the dissemination of extremist materials. Artificial intelligence helps to find links between pseudonymous people and physical hazards; still, the covert features of these systems create legal difficulties. The IT Act controls digital activities in India; nevertheless, surveillance operations targeted on the dark web have to follow legal permission, proportionality, and need. Legislative accuracy on AI-driven covert operations is desperately needed, especially as terrorist groups get more technologically sophisticated.

CASE STUDIES AND USEFUL APPLICATIONS

1. United States

Leading worldwide in the application of artificial intelligence technologies for homeland security projects and counter-terrorism is the United States. AI has been included in national security, surveillance, intelligence gathering, and counterterrorism initiatives by several U.S.

government departments, including the Department of Homeland Security (DHS), National Security Agency (NSA), and Department of Defence (DoD).

Homeland Security Department (DHS)

AI systems meant to enhance border security, intelligence gathering, and cybersecurity have been developed and put in use by the DHS. One prominent example is the AI-based screening systems used at American borders to check goods and passengers. By means of X-ray images and cargo manifests, these systems use machine learning algorithms to detect hidden explosives, weapons, and drugs. Daily evaluation of thousands of shipments by the AI system allows it to spot suspicious behaviour requiring human inspection, so improving the effectiveness of security staff.

Furthermore, at airports and other important infrastructure locations, the DHS's AI-augmented systems provide real-time facial recognition technology. Facial recognition technologies match travellers' faces to databases of people linked to criminal or terrorist activity and terrorist watch lists (DHS, 2022).

NSA, The National Security Agency

To improve intelligence collecting and cybersecurity, the NSA uses artificial intelligence technologies. To find terrorist activity, threats, and communications in real time, NSA AI-driven algorithms can examine enormous volumes of digital communication data, including emails, social media content, and internet traffic. One well-known project is the NSA's use of machine learning techniques to monitor foreign communications networks and identify possible threats connected to terrorism. These tools monitor encrypted messages that terrorist groups are progressively using to hide from discovery. Furthermore essential for decryption programs and threat assessment are NSA's AI-powered tools, which help the American government to obtain vital intelligence from intercepted data and prevent cyberterrorism attacks before they start (NSA, 2021).

Defence Department of Policy (DoD)

For reconnaissance and combat operations in terrorism-prone areas—including the Middle East—the Department of Defence makes use of AI-driven drones and other autonomous systems. Using real-time intelligence, the AI-operated drones could monitor terrorist activity, conduct reconnaissance, and carry out focused strikes.

Using artificial intelligence, the U.S. military improves predictive analytics for counter-

terrorism missions. To project possible future attack sites, machine learning methods look at past terrorist assaults, meteorological conditions, and sociopolitical factors. These prediction models let the United States proactively reduce terrorist threats and more wisely allocate its resources.

2. Israel

Israel's advanced defence and counter-terrorism technological successes are well known. Securing the country's borders and stopping terrorist activity depend on its AI-driven defence systems.

Iron Dome System

Israel developed the artificial intelligence-driven missile defence system known as the Iron Dome in order to guard against short-range rocket attacks. It uses advanced radar and artificial intelligence techniques to track approaching rockets, calculate their paths, and evaluate whether they might endanger civilian areas. The system uses an intercept missile to neutralise the approaching rocket before impact with its target upon identification of a threat. Among the most effective missile defence systems available worldwide is thought to be the Iron Dome (IDF, 2021).

The Iron Dome's ability to separate real rockets that pose a threat from benign missiles, such as artillery shells or flares, depends on artificial intelligence and machine learning. The system instantly analyses millions of data points to produce these essential conclusions.

AI Systems for Border Control

Along its borders with Palestine, Syria, and Lebanon, Israel uses artificial intelligence for security and border control. Driven by artificial intelligence, surveillance drones across borders track and identify intruders, so preventing terrorist events before they start. Equipped with machine vision technologies able to perform real-time image analysis, these drones can identify individuals or groups approaching border areas lacking sufficient identification.

Monitoring underground tunnels used by terrorists to enter Israel is being done using artificial intelligence systems. Along the border, AI-driven seismic sensors are installed to detect tunnelling activity, enabling security officials to react quickly to prevent assaults or smuggling. Using AI systems to synchronise data from military surveillance, border patrol, and intelligence agencies to create a complete risk assessment, the Israeli approach is notably coherent among many agencies (Bloomb, 2020).

3. India

Artificial intelligence has been increasingly applied in India into intelligent police and surveillance systems to counter terrorism, boost law enforcement, and improve public safety. India's use of artificial intelligence technologies in counter-terrorism is crucial given its several sociopolitical concerns, including regional insurgencies and cross-border terrorism.

Artificial intelligence surveillance and intelligent law enforcement

Under the Smart Cities Mission, Indian cities—including Mumbai, Hyderabad, and Delhi—notably have established AI-driven surveillance systems. These systems track people in real-time and spot dubious behaviour using predictive analytics, AI-driven facial recognition, and CCTV cameras. Established in several cities, the Integrated Command and Control Centres (ICCC) offer real-time monitoring of public areas, thoroughfares, and vital infrastructure (Mehta, 2022).

Using behaviour analytics and facial recognition technology, the AI-driven surveillance system seen in Delhi tracks people in high-risk areas, including religious sites, bus terminals, and metro stations. The technology can alert police enforcement in real time and spot unusual movements, including loitering or abandoned baggage.

Using artificial intelligence in border security and Naxalism

AI-driven drones and surveillance systems are used to monitor far-off areas affected by insurgency, including Chhattisgarh and areas impacted by Maoist activity, so preventing access by terrorists or insurgents. These artificial intelligence systems monitor international weapon and explosive trafficking and help to identify movement patterns.

Where terrorism and cross-border intrusion remain constant concerns, AI capabilities support the Indian Army and Border Security Force (BSF) in surveilling vast, difficult borders with Pakistan and China. AI-powered surveillance systems track militants' or traffickers' movements, so enabling quick responses.

4. European Union

Through Europol, the EU's law enforcement agency, and its affiliate, Eurojust, the EU has used artificial intelligence for counter-terrorism projects. Among EU members, Europol has put AI-driven systems for intelligence distribution, criminal investigations, and transnational security cooperation into use.

Artificial Intelligence Tools for Terrorism Mitigation Tools from Europol

Artificial intelligence is used by Europol to examine vast databases on terrorist networks, financing sources, and international communications. Driven by artificial intelligence, i-ARMS (Integrated Arms Monitoring System) looks at trends in arms trafficking and projects likely sources of illegal weapon sales used by terrorist groups. Artificial intelligence helps Europol track gun distribution among member states and spot terrorist activity connected to weapon trafficking.

Using public surveillance cameras, Europol has included artificial intelligence-driven facial recognition and video analytics to identify people linked with terrorist activity. By means of data analysis from many sources—including social media, public databases, and surveillance footage—machine learning algorithms offer real-time risk assessment.

Worldwide Artificial Intelligence for Counterterrorism

Cross-border data-sharing systems using artificial intelligence help European intelligence agencies to coordinate better. Artificial intelligence is being used to augment the European Arrest Warrant (EAW) system and the Schengen Information System (SIS II) to predict terrorist movements and track persons linked with cross-border criminal activity. These systems combine many data points—including criminal histories, biometric information, and transnational travel patterns—so enabling law enforcement agencies to react more quickly and precisely. These case studies provide important new angles on the present application of artificial intelligence in global counter-terrorism projects. While these initiatives show great success in enhancing security, they also raise important legal, ethical, and privacy concerns that demand attention, particularly with relation to the balance between national security and personal liberties.

ETHICAL, LEGAL, AND HUMAN RIGHTS CONSIDERATIONS FOR COUNTER- TERRORISM ENABLED BY ARTIFICIAL INTELLIGENCE

Important ethical, legal, and human rights questions arise as India and other nations include artificial intelligence in counter-terrorism policies. This covers the limitations of surveillance, the equity of artificial intelligence algorithms, legal responsibility, and the growing relevance of international humanitarian and human rights legislation in guiding the application of developing technology in security operations.

Especially in democratic countries like India, the use of artificial intelligence in mass surveillance raises serious privacy and civil liberties questions. Facial recognition, biometric tracking, video analytics, and real-time social media monitoring are among AI technologies that enable governments to monitor vast populations with low human involvement. Particularly in metropolitan areas as part of the Smart Cities Mission, India has quickly adopted artificial intelligence surveillance technologies. Initiatives with limited public transparency include Automated Facial Recognition Systems (AFRS) and Integrated Command and Control Centres (ICCCs) at Delhi, Hyderabad, and Lucknow. While these steps seek to lower crime rates and guarantee national security, such monitoring could easily violate constitutionally guaranteed fundamental rights. Under Article 21 of the Indian Constitution, privacy is a basic right, as ruled in Justice K.S. Puttaswamy v. Union of India (2017). Any governmental intervention, the Supreme Court decided, must meet the threefold standards of legality, need, and proportionality. Still, India lacks a comprehensive surveillance law and efficient monitoring systems. Mass surveillance driven by artificial intelligence compromises free expression and peaceful assembly, so violating Articles 19(1)(a) and 19(1)(b) of the Constitution. Lack of judicial or parliamentary control on surveillance technologies aggravates these concerns and motivates important ethical questions on the determination of surveillance targets, the consent for data collecting, and the safe and lawful storage of such data (mission, 2022).

Counterterrorism AI systems often make use of databases containing institutional, sociological, or historical biases. Should these databases disproportionately reflect particular groups in terrorism-related arrests or threats, artificial intelligence could mistakenly profile people based on geography, religion, or ethnicity. One well-documented issue is the profiling of religious or regional minorities—especially Muslims and those from Kashmir or northeastern areas—in counter-terrorism operations in India. Artificial intelligence systems that learn from erroneous past data could reinforce and magnify already ingrained prejudices. Facial recognition methods applied at events like the 2019–20 anti-CAA demonstrations drew criticism for only identifying minority groups. Likewise, predictive police systems driven by artificial intelligence could disproportionately identify members of particular communities, leading to a cyclical pattern of prosecution and prejudice. Under Article 14, which guarantees equality before the law, this has important legal and constitutional consequences; under Article 15, which forbids discrimination based on religion or place of birth, Furthermore, violating international human rights norms set by treaties, including the International Covenant on Civil and Political Rights (ICCPR, 1966) and the International Convention on the Elimination of All Forms of Racial

Discrimination (ICERD), is algorithmic prejudice. Autonomous algorithms, open data use, diverse training sets, and easily available grievance redressal systems for those unfairly targeted are immediately needed to address these issues (watch, 2020).

Since they are AI-driven technologies that can independently identify, choose, and interact with targets without direct human control, lethal autonomous weapons systems (LAWS) mark a new territory of concern. Investments from the Army Design Bureau in autonomous vehicles, drones, and combat robots show that although not now operational in India's active combat zones, these technologies are becoming more and more of interest. These developments call for a quick ethical and legal review, especially regarding responsibility in cases when an artificial intelligence system mistakenly results in civilian casualties and computer dependability in separating combatants from non-combatants. These problems directly relate to Article 21 of the Indian Constitution, so guaranteeing the right to life and liberty. International humanitarian law requires that all behaviour in conflict follow the guidelines of distinction, proportionality, and military necessity; autonomous weapons unable of consistently making these distinctions may be intrinsically illegal. International criminal law states that state responsibility may apply for war crimes—that is, illegal killings carried out by sovereign nations. Unlike countries like the United States, China, and Russia, who have taken more firm positions, India has not yet developed a national policy on lethal autonomous weapon systems (LAWS) and has refrained from supporting worldwide campaigning projects like the Campaign to Stop Killer Robots.

Especially with international humanitarian law (IHL) and international human rights law (IHRL), the use of artificial intelligence in targeted killings and drone strikes questions the moral and legal foundation. When artificial intelligence is involved in life-or-death decisions—such as determining whether a suspected terrorist merits a precision strike—these concerns get more intense. International examples, especially U.S. drone operations in Yemen and Pakistan, where AI-enhanced surveillance has sometimes informed targeting decisions, have faced criticism for violating sovereignty and resulting in civilian lives lost. These events relate to India, which faces continuous cross-border terrorism concerns and might consider AI-enhanced precision operations in regions including Pakistan-occupied Kashmir going forward. Article 2(4) of the UN Charter mandates that any such action cannot violate the sovereignty of another state. Moreover, Article 6 of the ICCPR and Article 21 of the Indian Constitution, together with concepts of international humanitarian law—including necessity, proportionality,

and distinction—demand due process even in circumstances of armed conflict. If India uses AI-assisted targeting methods, its dedication to non-intervention and sovereignty in its foreign policy has to be kept. India participates in the UN Group of Governmental Experts (GGE) on LAWS; it has not stated a clear stance regarding their legitimacy or control, though.

In conclusion, even if artificial intelligence has great potential to improve India's counter-terrorism efforts, their application has to be carefully assessed under ethical, legal, and constitutional angles. Mass surveillance cannot violate anyone's rights to peace, freedom of expression, privacy, or peaceful assembly. Algorithmic fairness is absolutely essential to prevent systematic prejudice towards underprivileged groups. Both national and international legal systems must clearly specify the responsibility structure for negative artificial intelligence uses. India has to simultaneously improve statutory protections, support judicial and parliamentary monitoring, and include openness in the design and execution of AI systems as it advances the integration of artificial intelligence in security operations. The aim should be to reach equilibrium between the democratic values supporting the Indian Republic and the needs of national security. Ensuring that India's counter-terrorism strategy is both fair and effective depends on legal reform, public consultation, and the evolution of ethical artificial intelligence policy (watch, 2020).

CHALLENGES AND CONSTRAINTS OF ARTIFICIAL INTELLIGENCE IN COUNTER-TERRORISM

Even if artificial intelligence has great revolutionary potential for counter-terrorism, its application faces significant strategic, ethical, legal, and practical difficulties. In underdeveloped countries like India, these problems are exacerbated by political, socioeconomic, and infrastructure constraints as well as economic ones. The precision and dependability of AI models define a major limitation of artificial intelligence in counter-terrorism. False positives—erroneously labelling an innocent person as a threat—and false negatives—failure to identify an actual threat—can both have disastrous results, including violations of basic rights and death in cases of undetectable hazards. Counterterrorism operations in India often take place in highly populated, high-risk areas, including Kashmir, Central India (Maoist regions), and metropolitan metropolises where mistakes in facial recognition systems or predictive policing algorithms might lead to erroneous arrests, minority community profiling, or even extrajudicial action (Police, 2023). With reports showing

accuracy rates below 80%, Delhi Police's facial recognition technology used during demonstrations has come under fire for its errors, especially with relation to gender, skin tone, and age. Many of the flagged people might be totally innocent, yet they still go under observation or interrogation. Trained on inadequate data—such as criminal records resulting from biased policing—AI algorithms merely copy and magnify the current prejudices in law enforcement. Thus, the dependability of AI tools becomes not only a technological but also a constitutional and human rights issue. Whereas false negatives may allow real threats to evade detection, culminating in terrorist attacks, exemplified by the 2008 Mumbai attacks, where intelligence failures were central, false positives can lead to unlawful detentions, harassment, and breaches of Article 21 (Right to Life and Liberty).

Artificial intelligence models depend on the quality of the data used for their training. The lack of systematic, verified, and ethically based data in India seriously impedes the development of effective counter-terrorism tools driven by artificial intelligence. Different data systems are used by law enforcement agencies around Indian states, and many police stations still rely mostly on paper records with little digitising. Given India does not now have a complete data protection law, privacy issues are particularly relevant. Although a progressive measure, the Digital Personal Data Protection Act, 2023, gives the government wide exemptions for national security, so enabling possibly uncontrolled data collecting. Mass surveillance under the pretence of national security is sparked by surveillance projects, including NATGRid, CMS, and Aadhaar integration, not requiring individual consent. In Justice K.S. Puttaswamy (2017), the Supreme Court recognised a basic right—privacy—as such. Still, the state's reliance on broad data policy exclusions reduces the significance of this decision. When this data is applied in artificial intelligence models for counter-terrorism goals, the absence of data minimisation, purpose limitation, and user control in data-collecting processes poses a major risk. Poor or morally dubious data produces erroneous, biased, or maybe dangerous AI outputs, compromising national security and civil liberties.

Particularly in India, a growing global concern is the deliberate use of artificial intelligence by terrorist groups, who are progressively using contemporary technologies for destructive goals. Deepfake movies created by artificial intelligence and voice changes can cause public upheavals, copy military or political leaders, or spread false attack reports. Given India's communal sensitivities, this might cause diplomatic tensions, mass fear, or mob violence. Made-up films shared on WhatsApp and Twitter were later found to be AI-manipulated

material during the 2020 Delhi riots. Repurposed as cheap tools of terror, autonomous drones linked with facial recognition technology and AI-driven navigation could be used. This poses a real threat given the drone smuggling events in Punjab and the infiltration along the Line of Control. AI technologies could be used by terrorist groups to carry out automated cyberattacks on key infrastructure, including financial markets, air traffic control systems, or nuclear plants. Indiaas in the past seen events like the 2020 Mumbai power system outage, thought to be involving foreign cyber agents. India does not yet have a thorough national cybersecurity law, a legal definition of AI-enabled terrorism, or a clear process for attribution and response to AI-generated cyberattacks or information warfare, complicating prosecution, responsibility, and deterrence (CERT-In, 2023).

Deploying AI systems for counter-terrorism is resource-intensive; thus, advanced infrastructure, skilled personnel, and continuous research and development investments—challenges more marked in developing nations like India—are needed. Predictive analytics systems, machine learning frameworks, and AI drones—among other advanced artificial intelligence technologies—demand large investments. Although India's defence budget is rather large, it also has to stress border logistics, personnel pay, and conventional warfare. There are few artificial intelligence researchers, data scientists, and cybersecurity experts working for the public sector. For top expertise, the government regularly deals with private technology companies. Often operating independently are India's intelligence and law enforcement agencies: the Intelligence Bureau (IB), Research and Analysis Wing (RAW), National Investigation Agency (NIA), and state police. AI systems require coordinated data-sharing, which presents technological and administrative difficulties. India also mostly depends on foreign technologies and alliances with private-sector companies, especially those from Israel and the United States, which causes concerns about data sovereignty, espionage risks, and supply chain flaws in necessary artificial intelligence infrastructure (CERT-In, 2023).

While artificial intelligence presents transforming tools for counter-terrorism, India has great challenges to ensure that these technologies are constitutional, ethical, and successful. This covers ensuring algorithmic accuracy and equity, protecting data privacy and personal rights, stopping hostile uses of artificial intelligence, and supporting local AI capacity and interagency cooperation. Legislative changes, calculated investments, and the creation of AI governance structures fit for India's constitutional values and international obligations help to overcome these constraints.

The uses of artificial intelligence in counter-terrorism are expected to get more complex, ethical, and worldwide coordinated as it develops. Future developments aim to solve different ethical, legal, and dependability problems related to present implementations while also increasing operational efficiency. Explainable artificial intelligence (XAI) is a significant development since it denotes AI systems marked by transparent, interpretable, and comprehensible decision-making mechanisms for humans. Explainability is crucial for responsibility, public confidence, and court review in counter-terrorism when AI-driven decisions could lead to surveillance, arrests, or targeted assassinations. Conventional "black-box" artificial intelligence models—especially deep learning algorithms—often lack the capacity to explain the reasoning behind designating someone as a threat. Legally speaking, this lack of openness may go against the ideas of natural justice, which include the rights to a fair trial and to be informed of the reasons for an accusation. XAI will be especially important in India, where counter-terrorism activities may draw on constitutional rights under Articles 14, 21, and 22. When artificial intelligence is used to predict radicalisation or prioritise suspects in an investigation, for example, law enforcement has to explain the reasoning behind the profiling of a particular person and the indicators or risk factors supporting that classification. Consent-driven, transparent data exchange finds a basic foundation in the Data Empowerment and Protection Architecture (DEPA) paradigm promoted by NITI Aayog. Explainable artificial intelligence (XAI) will probably be required of future Indian AI laws as a compliance criterion for high-risk uses, including national security.

Another frontier technology with great promise to change encryption and massive data analytics is quantum computing. Deciphering terrorist communications and improving AI-driven threat prediction models by quantum machine learning constitute the most possible applications for counter-terrorism. To evade monitoring, terrorist groups are increasingly turning to end-to-end encrypted apps like Signal or Telegram. Because of their computational ability, quantum computers could possibly destroy traditional encryption systems like RSA or ECC in a few seconds—an effort that classical computers would need years to complete. Apparently investing in quantum technologies are India's rivals, including state-sponsored companies. India must quickly develop quantum-resilient algorithms and quantum key distribution systems for safe communications among its military divisions and intelligence agencies to avoid a strategic disadvantage. Accelerated simulations of social behaviour, movement patterns, and complex terror networks will be made possible by quantum computers, so allowing real-time modelling of assault probability, crowd dynamics, and cross-border

infiltration likelihood. Starting in 2020 with a budget of ₹8000 crore, the National Mission on Quantum Technologies & Applications (NMQTA) aims to improve India's quantum research capacity. Working together, DRDO and top institutes including IISc and IITs are developing native quantum encryption and communication systems (NMQTA, 2023).

Real-time, multi-modal systems—platforms combining data from many sources, including text, video, audio, satellite, biometric, and social media—to provide a coherent operational overview for decision-makers—will define artificial intelligence in counter-terrorism. Real-time data integration from CCTV, drones, radar, mobile surveillance, and social media; consolidated threat dashboards that simultaneously inform intelligence agencies, law enforcement, and military units; and AI-enhanced command centres with predictive alerts and automated resource allocation recommendations will all be included in these systems. Currently developing C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) systems to combine intelligence from several agencies—including RAW, IB, NIA, and state police forces—is India. Forerunners of these multifarious systems are the integrated command and control centres set up under the Smart Cities Mission.

These systems should be extended from cities to important borders, ports, airports, and religious sites. With privacy, ethical, and constitutional protections to prevent use, challenges include inter-agency collaboration and interoperability, modernisation of legacy systems, and standardisation of protocols. In a possible future scenario, an artificial intelligence (AI) detects someone arriving in India, links this information with voice messages taken on social media, matches their facial data with a worldwide watchlist, and alerts border authorities—all in real time (GPAI, 2023).

Since terrorism is a global threat, its effective prevention calls for international cooperation, especially in the digital sphere where limits are flexible. In counter-terrorism, artificial intelligence's future will be shaped by growing worldwide cooperation and international organisation standard setting. Member states use Interpol's AI-enhanced database systems—I-Checkit and I-24/7—to track terrorists, stolen documents, and cross-border travel activity. India participates actively and has arrested fugitives abroad using INTERPOL warnings. Through a human rights-orientated perspective and ethical application of artificial intelligence in counter-terrorism, the UN Counter-Terrorism Centre (UNCCT) supports AI technologies for monitoring terrorist finance and radicalisation, especially through cryptocurrencies and

dark web platforms (INTERPOL, 2022). India might cooperate on AI standards through bilateral technological diplomacy and the Global Partnership on AI even though it is not a NATO member. Through memoranda of understanding and cooperative research projects, EUROPOL's Innovation Lab helps AI technologies be advanced for India's combat of cybercrime and terrorism. India has to improve its diplomatic and strategic alliances to enable real-time AI-driven terror intelligence exchange, build interoperable AI systems with shared threat lexicons and protocols, and stop AI technological colonisation by safeguarding technological sovereignty while under international cooperation (Europol, 2021).

Ultimately, the future of artificial intelligence in counter-terrorism is complex and rather bright. The detection, study, and neutralising of terrorism will be transformed by innovations including explainable AI, quantum-enhanced decryption, real-time multi-modal threat detection, and global AI collaboration. Still, these developments must be anchored in ethical values, constitutional protections, and international cooperation to ensure they increase security without endangering democracy or human rights. India must ensure inclusivity, openness, and sovereignty while simultaneously modernising its artificial intelligence ecosystem for national security (ICRC, 2021).

ADVICE FOR POLICY AND GOVERNANCE

India must create a strong governance structure that harmonises technological development with constitutional protections, ethical responsibility, and geopolitical readiness as it incorporates artificial intelligence (AI) into its national security and counter-terrorism policies. This part outlines necessary institutional changes and policy paths India and the world community have to follow to ensure the ethical and effective use of artificial intelligence in counter-terrorism (UNCCT, 2023).

Ethical standards for the use of artificial intelligence in military and counterterrorism must be established absolutely. AI applied in important settings—such as predictive policing, autonomous drones, or surveillance systems—must follow standards ensuring responsibility, openness, and proportionality. Being a democratic country with a constitutional framework, India has to fit its AI military strategies within Article 21 of the Constitution, which guarantees personal liberty and the right to life. Ethical government has to include the concept of proportionality set by the Supreme Court in the Puttaswamy privacy ruling, so stressing that state actions using artificial intelligence monitoring or profiling must be legal, required, and

the least intrusive means available. Regarding AI-assisted military uses, India should set up a national ethical council on lethal autonomous weapons systems (LAWS) to work with defence agencies assessing new technologies before they are put into use on the ground. This will ensure respect of both national human rights obligations and international humanitarian law.

A basic feature of responsible artificial intelligence governance is the formulation of a national AI security policy. India does not now have a comprehensive statement defining its national artificial intelligence vision for internal security and defence. The legal, technical, and operational elements of AI application in intelligence, law enforcement, cybersecurity, and military sectors must all be covered in a well-written national AI security policy. Along with explicit guidelines for data acquisition, algorithmic responsibility, and civilian supervision, it must include legislative frameworks to monitor and evaluate AI systems used by state and federal law enforcement agencies. Especially in conflict-sensitive regions like Jammu & Kashmir or the Northeast, this policy must clearly state the auditing processes for artificial intelligence systems to reduce bias, misidentification, and misuse. The institutional obligations of several agencies—including the Ministry of Home Affairs, Ministry of Defence, National Security Council Secretariat, and National Cyber Security Coordinator—in running and supervising AI-driven activities will be discussed in this paper. It also has to follow changing global norms for the responsible use of artificial intelligence in security environments (Chakraborty, 2023).

The management of AI-driven counter-terrorism systems depends much on international cooperation. Because of the transnational nature of terrorism and cyber threats, artificial intelligence surveillance systems have to be standardised globally by bilateral agreements, multilateral platforms, and participation in world standard-setting bodies. To create interoperable standards for algorithmic transparency, data-sharing protocols, and AI auditability in transnational investigations, India should aggressively cooperate with organisations including the United Nations Office of Counter-terrorism, INTERPOL, the Global Partnership on Artificial Intelligence (GPAI, 2020)and regional alliances such as the Quad and BRICS. Moreover, India should lead the effort for a worldwide non-proliferation treaty concerning autonomous weaponry and surveillance technology, similar to present agreements on chemical and nuclear armaments. This will show India's commitment to moral leadership in AI governance as well as guard against the non-state entities' or authoritarian governments' abuse of artificial intelligence technologies.

Promoted as a basic approach for improving AI innovation in the security industry are public-private partnerships (PPPs). In disciplines including computer vision, language modelling, biometric systems, and predictive analytics, the Indian private sector—especially start-ups and AI labs in Bengaluru, Hyderabad, Pune, and Delhi NCR—has shown great promise. The government should make use of this technical capacity by means of structured public-private cooperation models that support private innovation under preservation of public accountability. Working with DRDO, CDAC, and private companies could help indigenous AI-driven surveillance drones, real-time data fusion systems, or threat prediction engines catered to Indian environments and threat profiles come to be developed. Under strict ethical and legal oversight controlled by standard agreements requiring data protection, fairness assessments, and intellectual property distribution for national security uses, these collaborations must operate (DRDO, 2022).

All things considered, India's constitutional obligation as well as a technological need is the development of a thorough and morally decent AI policy framework for counter-terrorism. Formalising ethical standards, creating a national AI security framework, engaging in international standardising, and advancing industry-wide cooperative innovation with business leaders will define the road forward. These actions will help India to maintain democratic values and human rights underlining its constitutional framework while using the revolutionary possibilities of artificial intelligence in counter-terrorism.

CONCLUSION

The development of artificial intelligence (AI) has started a new phase in the global fight against terrorism. AI is drastically changing how governments evaluate vast intelligence data quickly and use predictive threat modelling to see, stop, and react to terrorist attacks. Examining the several uses of artificial intelligence in counter-terrorism, this chapter has covered intelligence gathering, surveillance, cybersecurity, military operations, and international cooperation. These developments are fundamentally revolutionary, allowing governments to move from reactive counter-terrorism to proactive threat neutralising, not only augmenting already in-use systems. Artificial intelligence has evolved in India into a strategic tool able to address the complex, multifarious problems posed by transnational terrorism and domestic insurgents. Recent investments in intelligent surveillance networks, facial recognition technologies, and predictive police strategies by India show a growing institutional will to include artificial intelligence in national security systems (Sharma).

Using artificial intelligence in counter-terrorism raises important moral and legal conundrums deserving of thought. Especially the rights to privacy, liberty, and non-discrimination, the application of artificial intelligence for mass surveillance, risk assessment, and autonomous decision-making routinely compromises the fundamental liberties embodied in the Indian Constitution. In a diverse society marked by high sociopolitical tensions, instances of algorithmic bias, misidentification, and illegal profiling create serious problems. The Supreme Court's landmark decision in Justice K.S. Puttaswamy v. Union of India confirmed that governmental monitoring has to follow legality, need, and proportionality. For artificial intelligence systems used in security contexts, constitutional protections have to be strictly followed to stop the deterioration of the democratic framework of the country under the pretext of national security. India's strategic challenge thus is not only the acceptance of AI technologies but also their application inside a framework that upholds rights, guarantees legal responsibility, and guarantees openness, so respecting their integrity.

India and the world community have to cooperatively create a strategic vision that gives ethical AI governance top priority inside international counter-terrorism projects. This covers the development of auditable and explainable artificial intelligence systems as well as international norms controlling AI use in surveillance and military operations. India's leadership in platforms including the Global Partnership on AI (GPAI), BRICS, and the Quad has unique power to shape world opinion on these issues. Moreover, a safe AI-driven order can only be reached by strong public-private cooperation, international intelligence sharing, and significant institutional capacity building. India has to create a thorough National AI Security Strategy, raise data security standards, and set control systems to guarantee technological performance and respect of constitutional values.

The use of artificial intelligence in counter-terrorism perfectly embodies the main difficulty of the digital era: balancing the use of transformational technology for society's benefit with the preservation of the values defining an open, fair, and democratic society. India is at a turning point in this effort: it has the technological know-how and geopolitical might to lead, but it is also limited by the need to lead sensibly. Algorithms and codes will not be the only factors determining the course of counter-terrorism; ethical and legal frameworks controlling their use will also shape it. The balance between national security needs and civil liberty obligations helps one to see and realise a safe, AI-driven global order.