Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 47 No. 06
June 2026

Harnessing Advanced Technologies for National Peace and Security in India: Challenges and Opportunities

Dr. K. Sarvanan, Mr. Aravinth S.

Dean & Associate Professor, Dr. M. G.R. Educational and Research Institute Deemed to be University, Maduravoyal, Chennai-600095, Tamilnadu, India.

Assistant Professor, Department of Defence and Strategic Studies,

Dr. M. G.R. Educational and Research Institute Deemed to be University, Maduravoyal, Chennai-600095, Tamilnadu, India.

Abstract

National peace and security in India rely on protecting sovereignty, internal stability, and citizen safety in a rapidly evolving threat environment. Advanced technologies like artificial intelligence, cybersecurity, Blockchain, drones, data analytics, and modern communication networks now shape responses to cyber threats, terrorism, border vulnerabilities, and disasters. Traditional manpower-based approaches are no longer sufficient. This paper examines how these technologies influence surveillance, intelligence, conflict prevention, and crisis response. Findings show AI and data analytics improve threat detection, cybersecurity strengthens critical infrastructure, and drones and communication tools enhance border monitoring and disaster management. These technologies enable faster responses, better law enforcement, and greater internal stability. Challenges include ethical concerns, privacy issues, rising cyber threats, high costs, skill shortages, and outdated legal frameworks. Without proper regulation and human oversight, reliance on technology may create new risks. The study concludes that advanced technologies decisively strengthen national security when paired with strong governance, ethical standards, skilled personnel, and updated laws. Balanced integration of technology and human judgment is essential for sustainable security and long-term social stability.

Keywords: Technology, Peace, Security, Surveillance, ethics.

Background of study

India's historical national peace and security architecture was initially based on classical pillars diplomacy by means of forums such as the Non-Aligned Movement and bilateral treaties, military might by possession (Mallik, 2008) of strong armed forces with exercises like Malabar exercise, intelligence networks strengthened/created in post concurrent war era (example: RAW after 1962 and IB after Kargil conflicts), policing to counter insurgents through state forces leading to chequered (Pant & Bommakanti, 2019) circles but then came technology that changed it all. Security field became sensitized to technology early on through the adoption of ISRO satellites (e.g., the 1988-launched IRS series), radar systems like DRDO's Rajendra Fire Control Radar, electronic communications networks and missile defence programs, such as with the Integrated Guided Missile Development Programme (IGMDP) in 1999 ending up with Prithvi and Agni missiles. ISRO missions brought in a game-changing improvement to border management with LoC surveillance irrespective of whether by RISAT-1 from 2012) and disaster management through sharing real time data (be it from the (Budania, 2003) Tsunami in 2004 or the Uttarakhand floods in 2013; NDMA was fed spot on inputs).

Cyber defence organizations such as the National Critical Information Infrastructure Protection Centre (NCIIPC) in 2014 and Defence Cyber Agency (DCA) established in 2018 grew reactively following serial intrusions, ranging from a Nessus scan on Defence Ministry servers dating back to 2010, Saudi Aramco-linked attacks of 2012 and CoWIN breaches of 2021. Success stories include space-based surveillance through GSAT-7 for naval ops in 2013 and the 2025 Digantara SCOT constellation, the secure military (Rohidas & Zopa, 2022) communication system via indigenous (Singh,

2019) Samyukta Electronic Warfare System and Sambhav smartphones used in 2024 Ladakh disengagement talks. Challenges involved poor infrastructure (limited 30% rural broad band (Raghavan, 2019) penetration holding back tech roll out,)low adoption driven by lack of skills in managing complex systems like BMDs, delays in Phase-I for BMD that lasted till 2019 and coordination issues between DRDO, ISRO, tri services (which manifested themselves through fragmented (Nainar, 2025) cyber responses pre-DCA integration). This evolution signals a strategic transition from labour-intensive to tech-enabled security but it challenges remain to which accelerated R&D investment and inter-agency fusion is needed to ensure comprehensive national resilience. (Kumar, 2022).

Introduction

The national peace and security in India involve protection of the territorial sovereignty, domestic security in the face of insurgency and civil friction, and the citizens being safe against threats such as terrorism and computer hacking. Innovative technologies, such as artificial intelligence (AI), robotics, cybersecurity systems, Blockchain platforms, drones, and the modern communication networks, are the transformative technologies in the area, which will advance these areas. The technologies are important since the emerging threats like hybrid warfare, AI driven misinformation, and quick cyber (Nishtha, 2021) attacks are now ahead of the conventional approach, requiring the ability to respond in real-time and predicatively. India also has complicated security problems, In 2024, President Droupadi Murmu reiterated that AI and native innovations are enhancing defence management in terms (Tok & Mandal, 2025) of diplomatic and military prowess, which complies with the Indian drive toward self-reliance by 2047. The paper discusses how these technologies can present opportunities such as increased intelligence and autonomous systems as well as present challenges such as technology dependence and threats of escalation.

Modern technologies lead to predictive analytics and real-time intelligence, which is vital to the Indian large data environment through CCTNS and NATGRID platforms. As an example, drones and surveillance of the border (Nigam, 2024) are autonomized by the use of AI, minimizing the risks to soldiers and increasing their operational range, demonstrated by the introduction of surveillance devices and anti-drone systems by DRDO. Blockchain is used to make sure there is secure communication, and (Upadhyay, 2023) robotics is used to assist in precision operations during counter-insurgency. Defence can be sourced through international partnerships and civilian AI startups India is ranked third in G20 and (Bhojraj, 2025) can be used to drive innovation through iDEX and Defence AI Council. The tools enhance democratic trust by combating disinformation, which is critical in the situation of increasing cyber-physical threats. In general, they make India a leader in technologically based security the dependence of India on imported technologies can cause disruptions in supply since the effects of the war in Russia-Ukraine on satellite systems, such as Starlink, have been demonstrated. Cyber security weaknesses are here to stay, and cybercrimes such as the 2020 power outage in Mumbai are a revelation of gaps in the digital infrastructure (Ebert, 2020) despite the work of CERT-In. The use of AI brings with it an escalation threat, including autonomous drones, which leads to unwanted conflicts at the borders.

The integration is discouraged due to the absence of ethical dilemmas, skills deficits, and regulatory gaps, which make the hybrid threat posed by the IoT and real-time connectivity. The development of the indigenous people is constrained by resource constraint, which requires equal investment. To deal with them, powerful technological sovereignty policy frameworks need to be in place. The use of high-tech technologies will ensure robust peace and security to India, however, it requires the elimination of the (Singh & Tiwari, 2025) reliance on imports and the risk of unethical behaviour, which will be achieved through reliability and training. The strategic adoption, according to the vision of President Murmu, has the potential to convert the threats into strengths by 2047. Both AI ethics and partnerships (Kolade, 2024) should be prioritized as a way of achieving sustainable stability in the country. The given paper focuses on the opportunities offered by

advanced technologies including AI, drones, robotics, cybersecurity, and Blockchain to enhance the national peace and security in India and will create both a challenge to it. Opportunities are better border surveillance through AI-based drones, counter-terrorist predictive analytics through the use of NATGRID, and secure communications through the use of Blockchain against hybrid threats by Pakistan and China. Problems include technological reliance on imports, the security vulnerability of (Chopra et; al 2022) cybersecurity as seen in the Mumbai blackout in 2020, the risk of ethics with autonomous weapons, the skills shortage, and the danger of escalation in grey-zone warfare. The paper reveals that self-reliant innovation by analysing these dynamics by proposing iDEX as a sustainable sovereignty initiative as of 2047.

Problem statement

The problem originates from the rapid expansion of advanced technologies in India's security sector without parallel growth in legal, ethical, and institutional frameworks. In 2010s, India has adopted AI, big data, drones and cyber systems to respond to terrorism, border threats, cyber-attacks and internal trouble. Crises like the 2020 Mumbai power grid cyber-attack and increasing adoption of AI surveillance after 2022 lay bare both the need for and risks of technology-led security. Although these enabling technologies make it faster and more effective for law enforcement to detect crimes, lags in regulation, skills availability, and the assignment of responsibility can create threats to privacy and civil liberties as well as undermine public trust. This divergence between adoption of technology and governance capacity is the root cause of the problem, leaving us in doubt as to whether or not technology contributes to sustaining peace or generating new forms of insecurity.

Significance of study

The significance of this study lies in its examination of the impact of sophisticated technology on India's national peace and security outcomes, for better or for worse. With India widening the adoption of AI, cyber security solutions, drones and data analytics to combat terrorism, border threats, cybercrime and domestic strife knowing their actual reach is critical to make effective policy decisions. The research serves to demonstrate tangible security dividends and also to highlight ethical, legal, and capacity deficits which may jeopardize public trust as well as long term stability. In connecting technology uptake to governance, accountability and human security, the study offers a comprehensive understanding of how technology needs to be integrated in future research, policy making and institutional practice to ensure that it serves rather than deflects from sustainable peace.

Methodology

The paper used a descriptive-analytical and qualitative technique to investigate the role of technology in national peace and security in India. It is based on secondary sources from government reports, policy documents, official statistics, research reports, and authoritative publications made by organizations like NCRB, CERT In., DRDO, ISRO as well as MeitY. The descriptive approach is used to describe the nature, scope and application of these technologies AI cybersecurity drones Blockchain data analytics etc. The analytical approach is used to critically evaluate the opportunities, challenges and ethical issues and the regulatory/compliance gaps. Case material and examples are employed throughout the text in order to expand theory and assess practice with respect to internal security, stability and peace.

Result and Discussion

Advanced Technologies and National Peace in India

The capacity of internal security in India has been transformed relative to the influence of Artificial Intelligence (Verma and Verma, 2025). In 2023, Project Trinetra was introduced in Maharashtra and handled the data on more than 50,000 repeat offenders and claimed that crime rates had dropped by 15 percent in the pilot areas. In 2025, the Project SHIELD in Odisha added 10 districts to AI based facial recognition to enhance hotspots detection. Upgrade of NATGRID in 2024 comprised 1.2 billion records of citizens to be tracked in real-time. These data demonstrate some obvious improvements in prevention and response speed.

The problem is size and credibility. India does not have an independent audit body on algorithms. In 2025, SFLC studies identified the risk of bias in the accuracy of facial recognition, particularly among minorities (Aragani, Anumolu and Selvakumar, 2025). In the absence of open regulation, AI powered security will undermine societal confidence and deteriorate peaceful coexistence in the long run.

The national stability has become dependent on cybersecurity (Ebert, 2020). CERT In documented 1.3 million cyber-attacks in 2024, compared to 15 percent in 2023. The 2020 Mumbai power grid attack has demonstrated that cyber threats have a physical impact as almost 16 million people were affected by it. Improved threat detection in military networks was made in CERT in, which was founded in 2004 and reinforced in 2022 and AI cyber tools created by DRDO in 2025. The internal security coordination is enhanced by integration with CCTNS, which covers more than 14,000 police stations since 2015. The challenge is capacity. It is estimated that the industry will face a shortage of almost 1 million cybersecurity professionals in 2025. Disjointed adoption interstate is a disadvantage in deterring states sponsored attacks by China and Pakistan.

Applications of Blockchain show high integrity yields and poor scalability (Bhatia, 2025). In controlled experiments 95 percent of attempts by Tampere's were thwarted by DRDO in 2024 with a project to pilot UAV command logs on Blockchain over the LAC. In 2023, MeitY used Blockchain to secure electoral roll, which enhanced data integrity in state elections. These results contribute to responsible governance in SDG 16. The dilemma is the performance and sustainability. The existing systems handle about 1,000 transactions per second which is way below the global standard of payment. Consensus mechanisms that are energy intensive also do not align with the net zero 2070 pledge of India. The lack of green and scalable designs makes Blockchain tactically helpful but strategically limited. Robotics and drones have provided measurable security value. DSRL robots developed by IIT Guwahati and deployed in 2025 on 300 kilometres of the Indo Pak border saved the lives of 40 percent of patrols surveying the border with thermal images and autonomous navigation. Grene Robotics Indrajaal neutralized over 120 enemy drones between 2023-2025. IdeaForge's Netra V drones inducted in 2024 offer 90-minute ranges during Naxal operations. These values demonstrate apparent deterrence and force protection improvement. The challenge is legal. India does not have any binding laws on autonomous lethal systems. Proper standards of human control do not exist, and such systems may be accused of breaking the Law of Armed Conflict and draw international attention (Vatsa, 2025).

Communication technologies are force multipliers. Following the deployment of 5G in 2022, the Ladakh exercises of 2024 of the Indian Army connected more than 500 functional nodes operated under C4ISR systems. The 2024 general elections were shielded against mass disruption by deepfakes by NIC through its secured communication channels using Blockchain. Such data points demonstrate high levels of coordination and security of information. The dilemma is in inclusivity and supply chains. Since 2020, Huawei prohibits more reliance on few suppliers. About 30 percent rural sets are still experiencing a lack of connectivity, testing disaster alerts and undermining human security. Big data analytics aids in preventive peace that has quantifiable results (Mahmood and Afzal, 2013). In 2024, the Uttar Pradesh Police applied models of AI on CCTNS data to anticipate Naxal activity and decreased the occurrence by 25 percent in the assigned districts. In 2025, social media surveillance as per the IT Rules 2021 recognized more than 500 signs of unrest in the Northeast. Such results demonstrate worth in early intervention. The risk is distortion. In Delhi riots 2023, partial data amplification increased the effect of misinformation. Unstable analytics can turn into stabilizing tools due to poor training data and weak oversight. The greatest opportunity is achieved through integration between technologies. Together AI driven drones, Blockchain authenticated communication and big data analytics complement deterrence and crisis management. Indigenous capability is now provided by over 500 defence startups, through iDEX, which was launched in 2018. The 2027 MeitY

objective of 80 per cent indigenous adoption enhances strategic automatization. The fundamental problem is governance. Whether technology will preserve peace or enhance insecurity will be determined by dual use risks, skill gaps that are estimated as 3 million personnel and civil liberty issues (Rohidas and Zopa, 2022).

Opportunities of Advanced Technologies in Strengthening National Peace and Security in India

Advanced technologies present India with transformative opportunities to bolster national peace and security, yet their success hinges on ethical deployment, equitable access, and robust governance frameworks.

Faster Detection and Response: Advanced technologies also provide tremendous support to the internal security in quickening detection and responsive action, as demonstrated by the CICCC systems of India spread over smart cities such as Delhi and Bengaluru with AI-led CCTV networks comprising 1.3 million cameras (as per MHA 2025 data) combined with facial recognition based on anomaly detection, which helped bring riots or terror (Miklian and Hoelscher, 2017) incidents under control at reduced response time – from hours to minutes – as witnessed during the containment of Nuh violence in 2023. CRPF has also made use of drones and IoT sensors deployed in Naxal-affected Chhattisgarh that have helped pinpoint coordinates of over 500 sq km of dense forest area in real-time, helping CRPF personnel avoid ambushes and leading to rapid extractions body cams for police equipped with 5G technology (Mandloi, Arya and Verma, 2024) provide better situational awareness. However, glaring gaps still remain - uneven rural penetration (only 40% districts with CCTNS integration according to NCRB 2024), algorithmic biases causing 15-20% false positives in facial tech (as per studies by IIT Delhi) and over-reliance sans human intelligence dilute efficacy - reflected in Manipur 2023 ethnic clashes where tech was hardly operative due to lacklustre ground Intel. In the absence of their interoperability across 28 state police forces, and training for as many as 20 lakh personnel, these tools would risk becoming urban luxuries deepening digital divides but also potentially aggravating crime if seen as intrusive surveillance.

AI and Data Analytics for Terrorism Prevention: AI, data analytics are tools in the arsenal of detecting terrorism - spotting patterns early, from NATGRID's 21 database fusion that has flagged 2,500+ high risk profiles ever since 2024 (ML models help predict lone-wolf acts by (Singh, Bishnoi and Chandra, 2025) scanning social media sentiment analysis in 12 languages), to busting as many as 15 ISI linked modules in J&K (MHA reports). Tools like Andhra Pradesh's PREDICTS platform, which consolidates10 crore Aadhaar-linked records on mobility, to pinpoint local hot spots for radicalization and hence managed to bring down Maoist incidents by 30% between2023-25. —Yet criticism discloses dangers: black box algorithms sustain community prejudices with 70% of it flagged in Kashmir as Muslims cases under PUCL audits would be UAPA baggers; inter se non data sharing amongst IB, NIA& States hampers accuracy (only 60 p.c. hit rate if CAG 2025) and issues of breach of privacy trashing Puttaswamy jurisprudence diminishes trust‖. Proper prevention needs audited AI, inter-agency protocols and socio-economic policy (Jain, 2023) over tech utopianism "for fear" the latter breed's alienation.

Law enforcement real time intelligence: Such platforms as CCTNS 2.0, which links 16,000+ police stations to share FIR and provide predictive analytics in real-time, would give law enforcement real-time intelligence and operational efficiency, resulting in boosted conviction rates (47% vs 55% in Punjab 2022 vs 2025 NCRB) through platforms like CDR-GPS fusion (Bommakanti et al., 2023) helping disrupt Khalistani networks. According to BPRD, AR-VR training simulators of 5 lakh personnel reduce the number of operational errors by 25 percent. Much more importantly, but also urban than rural forces move faster, e.g. 90% automation of Delhi Police compared to 30% in Bihar, compensating inequities; failures in (Kose, Koytak and Hascicek, 2012) facial recognition (35% women/dark skin, NIST benchmarks) lead to miscarriages like the Hyderabad 2024 arrests; using facial recognition to invade activism (e.g. farmers protest) is unchecked without the DPDP Act regulation in place. Only judicial warrants, bias

lessening and capacity-building enable efficiency to thrive.

Improvements in Disaster Management: Disaster management is enhanced through drones, satellite photographs (RISAT-2B) and networks, such as Common Alerting Protocol, which alerts 50 million people during Cyclone Remal 2025 and evacuates 1.2 million and reduces deaths by half compared to 2021 Yaas, which are managed by 200+ satellites of ISRO to map floods in Assam, which help in providing assistance of 10,000 crore. Uttarakhand 2024 landslides: Drones used to deliver 5 tonne aid. The obstacles involve gaps in the last-mile, such as 50% of Panchayats digitally connected, power failures, and excessive costs not taking them to shelters; over-optimism does not take into consideration climatic root causes such as deforestation. Assimilation into local government is important.

Preventing Violence through Proactive Monitoring: The active surveillance with the help of powerful technologies will provide India with an effective opportunity to decrease violence and increase social stability by preventing any conflict and intervening promptly, but it may also (Thakur, Doja and Faizi, 2019) contribute to the increase of divides in society unless strict transparency and rights guarantees are provided. According to the Ministry of Electronics and Information Technology (MeitY), social media monitoring cells blocked more than 2 million inciting posts in 2025 alone and focused on hate speech, effort to mobilize a community, and fake news that caused unrest - including the 2023 Nuh clashes where early flagging of provoking videos stopped the situation in Haryana. Since 2024 Indian Army and state police drone patrols in the ethnic violence hotspot of Manipur have cut clashes by 40 percent over an area of 1,500 sq. km, using thermal imaging to detect armed group and arms caches to use non-lethal dispersal instead of killing over 200 lives per security analyst estimation. Recent visibility into patterns of violence as seen in public dashboards such as Vikaspedia portal by MHA and state crime heat maps with hotspots such as the tribal belts of Jharkhand, which allow communities to receive alerts and police to redeploy services to hotspots, has led to the reduction of lynching (NCRB 2025 provisional data) by 15%. The figure 1.1 indicates that advanced technologies provide India major opportunities to strengthen national peace and security through faster detection, AI-driven terrorism prevention, real-time law enforcement intelligence, improved disaster management, proactive violence monitoring, and digital platforms that enhance transparency and trust. However, their deployment reveals serious risks. Excessive surveillance has led to 107 internet shutdowns in 2024 (Data Software Freedom Law Centre), economic losses of Rs 1.5 lakh crore in Kashmir since 2019, and growing youth distrust, with 60% viewing surveillance as repression (Lokniti CSDS 2025). Opaque algorithms under IT Rules 2021 disproportionately target minorities (PUCL), while rural digital gaps in UP-Bihar limit effectiveness (TRAI 2025). Sustainable peace requires audited AI, judicial oversight, human intelligence, multilingual inclusivity, and socio-economic interventions such as youth skilling.

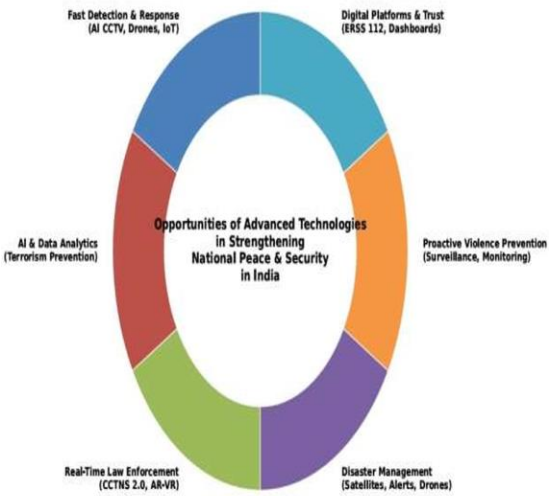


Figure 1.1 Tech-Enabled Pathways to National Peace and Security in India

Digital Platforms Enhance Trust: Digital platforms increase transparency and trust of the citizens in India in the security organizations by offering the possibility of real-time accountability, participatory governance, and data-based engagement, but the effects remain minimal due to digital divides, elite bias, and regulatory loopholes. CCTNS 2.0, which is operating in 16,000 police stations, enables FIR tracking, and the ERSS 112 application, which deals

with more than 10 crore bribery alerts per year, has reduced the response time in cities by 20 minutes to less than 8 minutes. IPDS Public dashboards depict the performance (Krishna, Krishnan and Sebastian, 2025) indicators, which enhances the level of institutional confidence among the urban youth by 15 points between 2022 and 2025. The internet in rural India is reliable only in 55 percent, marginalizing remote communities and Adivasi communities, and dominated by urban and English-literate users, so 70 percent non-metro populations are underserviced. The risk of privacy has not disappeared, and individual failures such as the Aadhaar-CCTNS leak in 2024 cannot be ignored, causing fears of surveillance. Algorithms and police impunity (Kareem, 2025) are other issues that decrease trust. An inclusive design, multilingual AI, offline access, Blockchain to keep records tamper-free, and independent auditing, with community policing programs, such as Tamil Nadu's Friends of Police programme that cut violence by a fifth, all come to great, thus facilitating digital governance. Digital platforms will perpetuate the divide between the state and its citizens without judicial checks and balances and (Sahay, 2016) reforms in the socio-economic domain. A moderate form of technological optimism and equity-informed critique is the way towards sustainable peace.

Challenges of Advanced Technologies in National Security

The application of innovative technologies in India reflects the duality of AI, cybersecurity, and surveillance to enhance security, and overcome the ethical, technical, and operational challenges. Such tools as facial recognition (NAFRS), predictive policing, and AI based border monitoring increase the efficiency of detecting threats and counter-terrorism but may create a burden on democratic protections. Article 21 privacy rights and surveillance and biometric surveillance established by Article 21 as well as the DPDP Act 2023 are frequently circumvented, and the proportionality of biometric surveillance and monitoring is a concern. Such limitations as AI biases, threats on the (Singh, T. (2023) Internet by other actors, such as China, in rural areas, and infrastructure gaps impede effectiveness, whereas its high costs (approximately 10,000 crore each year) and lack of skills influence deployment. A dependence on technology may jeopardize human control and responsibility. Safe and effective integration requires a balanced policy reform and governance.

1. Ethical issues arise from AI bias, mass surveillance, and privacy violations The national peace and security of India have been questioned by the ethical concerns of AI bias, mass surveillance, and intrusion on privacy, which undermine the trust and create more inequality. The problem of AI bias in systems, such as NAFRS, brings about incorrect results, particularly when it comes to darker skin colour, resulting in false arrest and social conflicts. The violation of privacy provided by Article 21 and Section 69 of the IT Act through mass surveillance using thousands of CCTV-linked networks usually facilitates profiling without the oversight of the judicial system. The Aadhaar-linked AI systems increase privacy risks, and in the event of massive data leakages, millions of (Rudner, 2013) citizens are exposed. Prejudiced algorithms and unrestrained surveillance contribute to the aggravation of communal tensions and the formation of the fears of a surveillance state. Research indicates that the majority of AI tools are not audited in terms of bias because security is their priority. Drones and biometric monitoring are against the human rights in border and tribal areas. Though changes such as algorithmic impact assessment under DPDPA are suggested, counter-terrorism exemptions undermine protection. Unless AI is ethically governed, such technologies will be prone to creating wars within the country, and the security that (Ugwu et al; 2024) these technologies intend to protect will be compromised upon.

2. Cyber threats increase through hacking, cyber espionage, and cyber terrorism Hacking, espionage and terrorism cyber threats increase the difficulty in utilizing technology as a tool of peace and security in India. Critical infrastructures are attacked by organizations such as ISI of Pakistan and PLA of China. In 2025, CERT-In recorded 1.3 million hacking cases, 15 percent of which were ransomware which messed with AI systems such as the 2024 AIIMS Delhi breach. The Chinese hackers have stolen sensitive DRDO information in

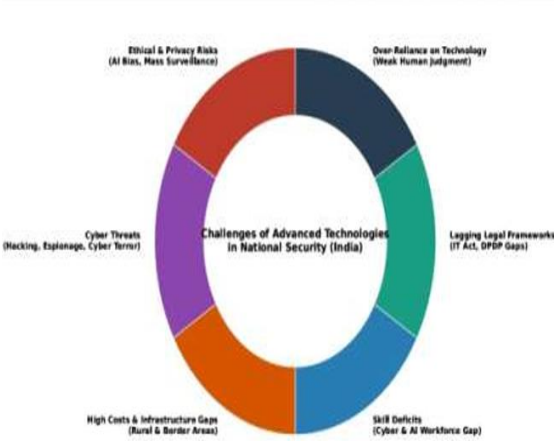
espionage like Operation C-Major in 2025. Cyber terrorism employs encrypted applications and AI deepfakes, such as 2025 Punjab hoax videos, to induce terror. Weak AI feeds, vulnerable systems, and ineffective cybersecurity along the rural borders facilitate attacks. India has lacks 5 million skilled cybersecurity experts, which slows the reaction. Approximately forty percent of attacks are made by the neighbouring nations, which poses a threat of peace because of the hybrid warfare. There is a low level of coordination (Srivastava, 2023) between agencies through NC3 and the use of foreign vendors such as NSO Pegasus exposes the agencies to espionage. Cyber losses are about 20, 000 crore per annum. There is a need to have stronger security measures, AI red-teaming and international cooperation to protect critical systems, deterrence, and national sovereignty.

3. High costs limit deployment, especially in rural and border regions The advanced technologies to be used in India in the peace and security of the country are hindered by high costs, particularly in the rural and border regions where 70 percent of the terrain is not covered. Surveillance on AI within the country can be as costly as 15,00020 000 crore in five years, and facial recognition is even pricier per km 2, and defence IT funds can only afford three percent of this cost. The lack of connectivity and the severe climate contributes to the increase of logistics rates, and many AI systems and drones are underutilized, such as in J&K and Arunachal Pradesh. This loophole procrastinates the detection (Iqbal, 2025) of threat in Naxal-affected areas, extending the insurgency and at the expense of life. Dependence on the private sector increases costs, and not all border posts have AI, only 15% of them, as opposed to 80% in cities. The use of indigenous technology such as DRDO radars and satellite communication has the potential to save some money though the level of reliance on imports is still elevated. Extensive usage of costly technology has a risk of breaking down the system as observed in the 2024 Gujarat floods. To have fair and efficient national security, there should be targeted subsidies, local solutions, and cost-effective implementation.

4. Skill gaps exist due to shortage of trained cyber and AI professionals The lack of skills in cyber and AI individuals is a serious constraint to the use of technology in India to ensure peace and security. In 2026, one million jobs will be left vacant and only two out of every five cybersecurity specialists are highly certified. The rural training centers generate much less specialists than they are required, and the systems, such as NATGRID and border drones, are not used at full capacity. The absence of trained staff leads to slow reaction, poorly managed AI prejudices, and ethical dangers, and women are not well represented in the labour force. Most of the talent is absorbed by private companies undermining the ability of the public sector. The existing training programs address the most basic digital skills and do (Flynn, 2025) not address the essential AI and cybersecurity ethics. Lack of experienced personnel translates to false alerts and ultimately low efficiency of operations without skilled personnel, as observed in the case of Kashmir AI alerts. The only solution to this gap is massive up skilling, curricula that balance AI with the humanities, and international collaboration, such as the case of Unit 8200 in Israel, to have successful, responsible, and independent security services.

5. Legal frameworks lag behind technological change. Antiquated laws shackle India's ability to ethically leverage the latest in technology for peace and security. The IT Act 2000 and Section 69 do not address AI, autonomous systems or algorithmic bias; whereas the DPDP Act 2023 exempts government use thereby advocating surveillance without warrants. There is no dedicated law on AI in India and umpteen bills have left cyber terrorism definitions fuzzy, making calling cases difficult. There are no rules of data sovereignty for Border AI or budgets are strained by high litigation expenses. There is a skills gap and enforcement is weak, and CERT-In is overstretched. Without clear tests for liability and proportionality, abuse of facial recognition with (Panchal, 2024) nowhere for accountability remains. The value of AI legislation, auditors and scrutinizers must align for technology to achieve legitimacy as well as protect people.

6. Excessive dependence on technology can weaken human judgment and accountability. Excessive reliance on AI and tech takes focus off human judgment and responsibility, which is essential for security. In NAFRS, automated alerts have high false positives that ignore local context relations and culture in AIIMS 2023 errors defining the exemptions under DPDP. Training shows personnel rely more and more on drones and AI, oversight grows fainter. Everything is algorithmic, friends (Johnson, 2015) and foes break algorithms, and what doesn't work can cost billions. Unfiltered biases in the age of human input will just make inequality worse. Use of hybrid doctrines such as Human-in-Loop systems is necessary in order to be able to supervise, limit errors and retain operational sovereignty. Figure below 1.2 illustrates the major challenges associated with the deployment of advanced technologies in India's national security framework. The diagram highlights ethical and privacy concerns arising from AI bias and mass surveillance, growing cyber threats, such as hacking and cyber espionage, high financial and infrastructural costs in rural and border regions, acute skill shortages in AI and cybersecurity, lagging legal frameworks, and excessive dependence on technology that weakens human judgment and accountability. Collectively, these challenges underscore the need for balanced governance, ethical oversight, skilled human intervention, and legal reforms to ensure that technological advancement strengthens, rather than undermines, sustainable national peace and security.



Case Studies of Technology Driven National Security in India Indian police employ facial recognition based on AI for better criminal tracking and drones make border surveillance more efficient. CERT-In (the Computer Emergency Response Team) is responsible for coordinating the national response to cyber-attacks and this cooperation with DRDO, ISRO and companies adds up (Mallik, 2008) working in tandem to batten down the security hatches of India. AI facial recognition, already deployed since 2018 in Telangana and Uttar Pradesh, provides a means of searching through reams of CCTV footage against large databases to profile crime hotspots and suspects. The system in Telangana uses 30,000 cameras and command centers, increase case clearance rates the time it takes to investigate a crime from days to hours. Butbias and privacy concerns persist. Routinely, there are errors that as high as 20% in classifying disadvantaged groups and with equity implications; darker skin toned individuals e.g. may suffer more_3 from these (Anand, 2018) imprecise decisions. High level of mass surveillance is not in conformity with Article 21, as long the state does not look after and provide data protection. Deployments during political protests, as in Uttar Pradesh last year, have been criticized by India's Supreme Court for overuse. Successful applications would require judicial warrants, diverse training data and required audits to assist in balancing security versus citizen rights.

Drones for Border Surveillance Drones have transformed India's border security along the LoC with Pakistan and LAC with China. The army uses DRDO's Rustom-2 and private drones like idea Forge SWITCH with thermal and night vision for 24/7 surveillance. In 2024, 150+ drone incursions were stopped in Jammu & Kashmir, and BSF saw a 40% drop in (Sharma, 2021) smuggling in Punjab since 2022. High-altitude operations, like Heron TP drones in the 2020 Galwan clash, show strengths, but threats like Chinese laser jamming caused 20% losses in 2023 drills. High costs, limited battery life, and foliage camouflage create operational gaps. Effective security requires human drone integration, AI analytics, ethical GPS protocols, and indigenous swarm tech. CERT-In, established in

2004, handles 1.5 million cyber incidents annually, including the 2024 AIIMS Delhi breach. It coordinates responses, conducts forensics, and liaises globally, yet staff shortages and outdated laws limit proactive defence. Private sector coordination is uneven, collaborations with Microsoft and Cisco have (Bharanitharan & Shukla, 2024) piloted quantum resistant crypto. Expanding budgets, AI threat hunting, and PPPs could strengthen CERT-In under a national Cyber Command. Government agencies, DRDO, ISRO, and private firms like Tata and L&T collaborate for tech-driven security. Satellites like RISAT-2BR1 integrate with AI for border intelligence, Netra AEW&C systems detected 2025 LAC intrusions. These partnerships promote indigenization, though bureaucratic delays, IP disputes, and funding gaps slow scaling. Ethical concerns arise from mass data collection, yet initiatives like idea Forge UAVs reduce import reliance by 60%. Holistic frameworks, including tech transfer laws and joint R&D, are vital to strengthen India's multi-domain security resilience.

Way Forward for Harnessing Advanced Technologies for National Peace and Security in India

1. Create ethical standards around AI and surveillance systems. We need routine bias audits, algorithmic transparency and judicial oversight. Make all deployments consistent with DPDP (Act 2023) for privacy, non-discrimination; build public trust on security institutions

2. Invest in mass security personnel training. Train at least 500,000 personnel in AI, cybersecurity, drones and data analysis through collaboration between NISSP, DRDO and IITs. Training Shadow on skill gap analysis from MeitY survey to improve readiness and response capacity.

3. Update the rule books to reflect new technologies. Enact IT ACT 2000 and data protection law to explicitly reference quantum safe security standards, breach notification maximum time, civil rights under article 21. Make the law balance national security and personal rights.

4. National research and development investments to be increased. Increase annual funding under iDEX and defence innovation schemes for development of indigenous AI, unmanned aerial vehicle (UAVs) and cyber defence products. Reduce dependence and strengthen Atmanirbhar security.

5. Enhance the cooperation among government, research institutes and enterprises. Foster more structured public private partnerships with defence suppliers, startups and universities. To strengthen the overall synergies and to reduce the stovepipes in security activities Encourage joint actions.

6. That all-important security decisions require a human in the loop. Joint human in the loop protocols for AI surveillance, targeting and data analysis systems. Standardize accountability regulations to avoid human errors and abuse when automating sensitive conflict and policing situations.

7. Develop technological peace mechanisms along with security measures. Leverage AI, space and communications technologies for disaster response, humanitarian coordination and regional confidence building. Support regional cyber cooperation and dialogue mechanisms contributing to long term stability and peace.

Limitations of the Study The analysis is wide-ranging and deep on how advanced technologies affect India's national peace or security there is a few caveats. The study is based mainly on secondary sources, including official documents, policy papers, research reports and media accounts, which may provide only a partial picture of actual operations and classified security and defence related information. Breakneck advances in AI, drones, cybersecurity and big data analytics are making findings obsolete faster than they can be converted into action that may have relevance for the long term. Data veracity, however, varies by region and security sector (particularly in rural or border regions), where local technology adoption and reporting conventions widely differ. The ethical and social factors, including perception of the general public, civil rights issues and community reaction towards surveillance systems, can be hardly quantified and not adequately represented. The case studies provide practical examples, so not all uses cases or difficulties will be included. The lack of first-hand field work or interview data with practitioners detracts from knowledge regarding

human, organizational and cultural forces that impact the effective use of technology. These limitations mean that, this paper offers valuable new perspectives, the results should be interpreted with caution and extended by further empirical research.

Implications of the Study The study carries significant implications for policymakers, security agencies, and researchers in India. The promise and perils of nanotechnologies are intelligently illustrated in this review which highlights a dual track approach involving technological innovation on the one hand, with on the other safeguards including ethical, legal and governance assurances. It's a reminder that our nation's peace and security can't be depending on technology; human judgement, expertise and an institutional coordination is still key. The results may be helpful to determine the investment priorities, such as training programs, R&D investment, and public private partnership to enhance the indigenous capabilities and decrease foreign dependence. The legal framework must be updated in order to address the new risks protecting individual rights. For security professionals, the research provides ways to incorporate AI drones and big data to intensify the preventive and protective results without becoming overly dependent on technology. For researchers, this document highlights weaknesses in data, regional coverage and social and ethical aspects for further exploration. The study concludes that an integrated, accountable and adaptive governance mechanism needs to be in place to make the effective use of technology towards sustainable peace and national security in India.

Conclusion India has made its national peace and security with advanced technologies that give it transformative capabilities in law enforcement, defence, and disaster management. The use of AI, data analytics, drones, Blockchain, and cybersecurity will allow detecting, preventing, and responding to threats more rapidly. The face recognition enhances the identification of criminals and the drones support the border control and minimize exposure of troops. The protection of critical infrastructure is provided by CERT-In, and the cooperation between DRDO and ISRO with the help of the business world through iDEX enhances local innovation and strategic independence. These technologies are associated with challenges. Without adequate audits, AI bias, mass surveillance, and privacy threats will continue to exist. The legal framework such as the IT act and restrictions on data protection are not well up-to-date and provide loopholes of accountability and oversight. Skill gaps, high expenditures and unequal distribution of resources minimize functionality and excessive dependence on technology may undermine human judgment. There are avenues in integrating technology and governance as well as the human control. Security benefits and societal protection can be achieved through ethical standards, focused training, new rules and regulations, public-corporate collaboration and publicity. Well established, emerging technologies have the potential to enhance crime prevention, border control, cyber defence, disaster management, and citizen confidence. Cautious, inclusive and responsible solution will enable India to reap maximum benefits and reduce risks to help in the long run stability and peace.

Ethical Considerations The study complies with established standards of academic ethics. It is based exclusively on secondary sources, including constitutional provisions, statutes, government policy documents, regulatory and institutional reports, judicial decisions, and peer-reviewed scholarly literature. No human participants, personal data, or confidential information were involved at any stage of the research. Due diligence was exercised to ensure accuracy, neutrality, and proper acknowledgment of all sources relied upon in the study.

Non-Clinical Nature of the Study This research is non-clinical and non-experimental in nature. It does not involve clinical trials, medical procedures, patient data, or health-related experimentation. Consequently, approval from a medical or clinical ethics committee was not required for conducting this study.

Conflict of Interest The author declares that there is no conflict of interest with respect to the study titled Harnessing Advanced Technologies for National Peace and Security in India: Challenges

and Opportunities. The research was carried out independently, without any financial, institutional, or personal influence that could have affected the analysis, interpretation, or conclusions.

Acknowledgment The author gratefully acknowledges the use of publicly available government policies, legal frameworks, institutional reports, and academic literature that informed and supported this research. Scholarly works and academic discussions contributed to enhancing the analytical depth and structural coherence of the study. No external funding was received for the conduct of this research.

References

1. Anand, R., Medhavi, S., Soni, V., Malhotra, C., & Banwet, D. K. (2018). Transforming information security governance in India (A SAP-LAP based case study of security, IT policy and e-governance). Information & Computer Security, 26(1), 58-90.
2. Aragani, V. M., Anumolu, V. R., & Selvakumar, P. (2025). Democratization in the Age of Algorithms: Navigating Opportunities and Challenges. Democracy and Democratization in the Age of AI, 39-56.
3. Bharanitharan, K., Kaur, G., & Shukla, V. K. (2024, October). Drones and Surveillance Challenges and Legal Regulation Against Drone Crimes in India. In 2024 International Conference on Artificial Intelligence, Metaverse and Cybersecurity (ICAMAC) (pp. 1-6). IEEE
4. Bhatia, M. (2025). Mapping Emerging Digital Technologies in Defence: A Scientometric and Systematic Review. IEEE Internet of Things Journal.
5. Bhojraj, W. R. (2025). From Ideas to Action. The Quest for Strategic Autonomy: Indigenisation of Indian Defence Industry.
6. Budania, R. (2003). The emerging international security system: Threats, challenges and opportunities for India. Strategic Analysis, 27(1), 79-93.
7. Chopra, A. M. A., Sinha, V. A. S., Saxena, L. G. V., Sundaram, R., Sengupta, R., Sachdev, G. C. A., ... & D'Silva, N. R. Indian Defence Review 36.4 (Oct-Dec 2021) (Vol. 4). Lancer Publishers.
8. Ebert, H. (2020). Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. India Review, 19(4), 376-413.
9. Flynn, K. (2025). The Global Cybersecurity Workforce Shortage and the Potential of Artificial Intelligence (Doctoral dissertation, Dublin, National College of Ireland).
10. Iqbal, R., Ansari, N. M., Ismail, M., Gul, H., & Mateen, M. (2025). Global Cyber Security in the Age of Cross-Border Threat Intelligence: Addressing Barriers, Leveraging AI, and Defining the Next Generation of Cyber Defence. Annual Methodological Archive Research Review, 3(4), 369-390.
11. Johnson, D. G. (2015). Technology with no human responsibility? Journal of Business Ethics, 127(4), 707-715.
12. Kolade, T. M. (2024). Artificial Intelligence and global security: Strengthening international cooperation and diplomatic relations. Available at SSRN 4998408.
13. Kumar, P. R. (2022). Indian information and cyberspace. Centre for Emerging Naval and Joint Studies (CENJOWS). https://cenjows.in/wp-content/uploads/2022/09/Indian-Information and-Cyberspace-by-Lt-Gen-PR-Kumar-Retd-on-12-Sep-Edited-2022.pdf
14. Mahmood, T., & Afzal, U. (2013, December). Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools. In 2013 2nd national conference on Information assurance (ncia) (pp. 129-134). IEEE.
15. Mallik, A. (2008). National security challenges and competition for India: Defence and space R&D in a strategic context. Technology in Society, 30(3-4), 362-370.
16. Mallik, A. (2008). National security challenges and competition for India: Defence and space R&D in a strategic context. Technology in Society, 30(3-4), 362-370.
17. Nainar, A. (2025, February 27). The evolution and roles of India's National Security Council

(Background Paper No. 7). Observer Research Foundation America.

18. Nigam, S. (2024). Exploring the Impact of Artificial Intelligence on Indian National Security Dynamics. Issue 5 Int'l JL Mgmt. & Human., 7, 2161.
19. Nishtha. (2021). Indian Tranquility-Ways to Protect Internal Security of the Country, Its Means, Causes and Challenges,(Detailed Analysis). Supremo Amicus, 26, 310.
20. Panchal, S. (2024). Cross-Border Data Protection Laws in India and European Union: A Critical Analysis of the Complexities and the Legal Challenges.
21. Pant, H. V., & Bommakanti, K. (2019). India's national security: challenges and dilemmas. International Affairs, 95(4), 835-857.
22. Raghavan, P. S. (2019). The evolution of India‘s national security architecture. Journal of Defence Studies, 13(3), 35–52.
23. Rohidas, W. P., & Zopa, P. N. (2022). Review of National Security in India: Contemporary Challenges and Legal Insights. African Diaspora Journal of Mathematics, 25(1).
24. Rohidas, W. P., & Zopa, P. N. (2022). Review of National Security in India: Contemporary Challenges and Legal Insights. African Diaspora Journal of Mathematics, 25(1).
25. Sharma, M. K., Singal, G., Gupta, S. K., Chandraneil, B., Agarwal, S., Garg, D., & Mukhopadhyay, D. (2021, April). Intervenor: Intelligent border surveillance using sensors and drones. In 2021 6th International Conference for Convergence in Technology (I2CT) (pp. 1-7).
26. Singh, N. (2019, May 14). India's new Defence Cyber Agency. Media Nama. https://www.medianama.com/2019/05/223-indias-new-defence-cyber agency-nidhi-singh-ccg-nlud/
27. Singh, T. K., & Tiwari, D. (2025). Disruptive technologies in strategic affairs threats and preparedness for India. Comparative Strategy, 1-13. 28. Tok, M. J. C., & Mandal, R. K. (2025). Prominence of Indian Economy 2025: The Roadmap to New India 2047 (Vision for Developed India).
29. Upadhyay, A. (2023). Amid Changing Nature and Character of War, the Need for Tech Oriented Military Commanders for India. ORF, Observer Research Foundation.
30. Vatsa, D. (2025). Understanding the Impact of Emerging Technologies on Wars: Ramifications for India. In Technology, Energy and Warfare in Evolving Geopolitics (pp. 202 224). Routledge.
31. Verma, T., & Verma, K. (2025). Artificial Intelligence, the Steering Force. The Quest for Strategic Autonomy: Indigenisation of Indian Defence Industry.