ARTIFICAL INTELLIGENCE, BIGDATA AND NATIONAL SECURITY IN INIDA

Sofia Saini[1] and Dr. Ajaz Afzal Lone[2]

Student/ Assistant Professor

UILS, Chandigarh University, India

Abstract

"The nation that leads in Artificial Intelligence will be the ruler of the world."

-Vladimir Putin

Big Data analytics and artificial intelligence (AI) are modernizing cybersecurity management, intelligence collection, and defence operations, which in turn is changing India's national security framework. Real-time surveillance, automation, and AI-driven predictive analysis are enhancing India's defence and security institutions' ability to combat both established and new threats. Big Data improves intelligence capabilities by making it possible to process data quickly and recognize patterns that are crucial for public safety and national defence. But these technical developments also bring with them serious problems regarding accountability, privacy, data security, and ethical governance. The possibility of abuse, excessive surveillance, and violations of citizens' rights rises in the lack of thorough legal frameworks and regulatory procedures. This essay looks at India's defence modernization plans, policy measures, and changing legal frameworks to strike a balance between democratic protections and technical advancement. It concludes that ethical regulation, AI-driven innovation, and India's quest for digital sovereignty and strategic autonomy must all be carefully aligned for sustained national security.

Keywords: Big Data, cybersecurity, data analytics, artificial intelligence, defence technology, India, and national security.

1. Introduction

The emergence of Artificial Intelligence (AI) and Big Data have turned out to be a game-changer in the modern Indian context of national security, altering generic strategies, operations structures, and policies. Their combination will help in more predictive operations, threat surveillance, and more responsive actions to the emerging security threats and is therefore necessary in protecting the sovereignty and security of the nation.

Artificial intelligence (AI) and big data have emerged as key elements of national security, defence, and governance in the modern period. Machines that can learn, reason, and make decisions—tasks that normally require human intelligence—are referred to as artificial intelligence (AI). Digital platforms,

[1] Author is the LLM Student at Chandigarh University, India
[2] Co-Author is an Assistant Professor at Chandigarh University, India

sensors, and communication networks generate large amounts of complicated information every second, which is referred to as big data. Governments can make choices about security and defence activities more quickly and accurately when these technologies are combined.

Traditional paradigms of intelligence and warfare have changed because of the ongoing Fourth Industrial Revolution (Industry 4.0). This revolution, which is typified by automation, networking, and real-time data processing, has extended conflict into digital and cyberspace in addition to traditional battlefields. AI is being utilized in cybersecurity operations, autonomous drones, predictive analysis, and surveillance, giving countries the ability to identify and neutralize threats with never-before-seen accuracy.

Countries including the US, China, and Russia are making significant investments in AI-powered defence systems worldwide to strengthen their strategic edge. Aware of this worldwide trend, India has already started using AI into its national security framework. To advance AI research for defence modernization, organizations such as the Defence AI Project Agency (DAIPA) and the Defence Artificial Intelligence Council (DAIC) have been established. AI-powered satellite imagery, facial recognition, and surveillance are being used in counterterrorism and border management activities.

But the quick uptake of new technologies also emphasizes how important it is to have a strong national security framework that guarantees responsibility, safety, and transparency. India's defence systems are confronted with new threats like cyberattacks, digital espionage, data manipulation, and privacy violations as they become increasingly dependent on data. Therefore, technological readiness as well as military might are key to the future of national security. India must create a legal and institutional framework that can effectively regulate AI and Big Data to preserve its sovereignty and autonomy.

The vision of AI for All in India is inclusive and responsible use of technology, where India is focused on making the country global in artificial intelligence. It informs policy and governance through insightful pieces of information that can guide the policymakers to establish balanced frameworks that encourage innovation and also lead to transparent and ethical AI oversight. It provides defense modernization by implementing AI and Big Data to improve data-driven defense planning by enhancing intelligence collection, threat determination, and strategic decision-making. It also can also close the policy and security gap as well by aligning technological progress and national security goals and enhancing digital sovereignty. There is also the focus of the vision on the development of the indigenous environment, which proposes the promotion of the development of the local AI and cybersecurity systems to minimize reliance on external technologies.

2. Literature Review

The existing literature investigates the use of AI and Big Data in the security and defence domains and its problems. The integration of AI into predictive policing, cyber defence and cross-agency intelligence sharing is highlighted as among the numerous policy documents of Indian interest, institutional reports as well as recent research, and there are also continued concerns of interoperability, data privacy, ethical governance and technological self-reliance.

2.1 Conceptual Framework

This research is organized with the convergence of the technological developments with the national security demands. It uses cybersecurity, protection of critical infrastructure, digital sovereignty, and public policy theories to conceptualize AI and Big Data as strategic resources and as the reasons behind novel vulnerabilities in the Indian security ecosystem.

2.1.1 Artificial Intelligence

National security is only one of the many areas where artificial intelligence[3] (AI) is being used as a game-changing technology. Its incorporation into India's security and defence frameworks is changing tactics, intelligence collection, and defence operations in general. This study examines AI's applications, advantages, difficulties, and global environment to determine how technology might improve India's strategic and defensive capabilities.

Artificial intelligence (AI) is the term used to describe computer programs that can reason, learning, and solving problems—tasks that call for human-like intellect. Neural networks, deep learning, robotics, machine learning (ML), and natural language processing (NLP) are important areas of artificial intelligence.

Systems may learn from data and make decisions on their own thanks to machine learning. Neural networks handle complicated issues by simulating the human brain. Multi-layered networks are used in deep learning to analyse data in a sophisticated way. While robotics and computer vision analyse images and videos for real-time intelligence, natural language processing (NLP) enhances human-computer communication. AI helps with strategic decision-making, cybersecurity, surveillance, and predictive analytics in national security. It can identify dangers, strengthen defences, and increase operational effectiveness.

The ability of machines to carry out tasks that often call for human intelligence is known as artificial intelligence (AI). It makes it possible for systems to grow from mistakes, adjust to novel circumstances, and resolve challenging issues on their own. AI analyses data, finds patterns, and produces answers using datasets, algorithms, and huge language models. As they gain experience, these systems become more capable of reasoning, decision-making, and communication like people.[4]

AI has several advantages, including enhanced decision-making, safer transportation, better healthcare, and effective governance. But it also results in employment displacement, prejudice in algorithms, privacy issues, and ethical dilemmas. To handle this, one needs to be well-versed in mathematics, statistics, Python programming, and practical machine learning skills to guarantee safe AI use.

[3] SURYANSH NIGAM AND DR. VIDUSHI SRIVASTAVA, "Exploring the Impact of Artificial Intelligence on Indian National Security Dynamics", INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES [ISSN 2581-5369] Volume 7 | Issue 5 2024

[4] Transforming India with AI, available on https://www.pib.gov.in/PressReleasePage.aspx?PRID=2178092 (last visited October 17,2025)

Through programs like the AI in military Symposium and the Indian Navy's "AI for Future Fleet" workshop, the country's military industry is aggressively embracing AI. India's dedication to using AI for strategic benefit is demonstrated by the employment of AI in intelligent weapons, autonomous vehicles, swarm drones, and border monitoring systems. International cooperation, ethical use, and data security continue to present difficulties. India needs to create strong laws that guarantee accountability, openness, and conformity to international standards if it hopes to reap the full benefits of AI.

2.1.2 Big Data

Big data is well defined by Farboodi and Veldkamp, albeit they do so from a business standpoint: "Big data is the term for vast amounts of data, frequently from several suppliers, as well as the capacity to collect, store, and interpret them to provide novel types of measures, observations, and forecasts for specific clients"[5].

When "customers" are substituted with "actors," national security concerns surface. Big data is made up of structured data sets (databases) that can be analysed by individuals with access using methods (algorithms) that reveal meaningful patterns and provide helpful forecasts. Originally employed to assist with insurance underwriting, the technique dates at least to the seventeenth century and the establishment of actuarial science[6]. The value and significance of big data have significantly increased due to recent developments in data collecting, management, and analysis. An exclamation point is provided by the current enthusiasm some could even say overzeal about Al tools.

Divergent opinions exist on the respective contributions of the three elements of contemporary data mining collection, organization, and interrogation to big data functionality. Since algorithm design is the most intelligent and inventive of the elements, many people whose careers depend on their capacity to produce and disseminate knowledge place a high value on it. However, other experts contend that developments in organization and algorithmic techniques the product of astute programmers tend to spread rather swiftly[7]. Data collecting is clumsier and depends more on sweat than creativity. However, these experts contend that the most crucial factors influencing the value of data mining and the opportunities for innovation are the volume and Caliber of the data gathered, not the creation of better software for organization and analysis[8].

An important realization emerges from a closer examination of big data as the foundation of the new analytical and predictive technologies. Big data operates like a system that emerges. When an entity

[5] Maryam Farboodi & Laura Veldkamp, Data and Markets, 15 ANN. REv. ECON. 23, 24 (2023).

[6] James Hickman, History of Actuarial Profession, in ENCYCLOPEDIA OF ACTUARIAL SCIENCE 838, 839 (Jozef L. Teugels & Bjorn Sundt eds., 2004); Edmond Halley, An Estimate of the Degrees of Mortality of Mankind, drawn from curious Tables of the Births and Funerals at the City of Breslaw; with an attempt to ascertain the Price of Annuities upon Lives, 17 PHIL. TRANS. ROYAL SOC'Y 596 (1693).

[7] PAUL B. STEPHAN, THE WORLD CRISIS AND INTERNATIONAL LAW: THE KNOWLEDGE ECONOMY AND THE BATTLE FOR THE FUTURE 276-77 (2023).

[8] KAI-FU LEE, Al SUPERPOWERS: CHINA, SILICON VALLEY, AND THE NEW WORLD ORDER 14, 104-12 (2018); VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 6-7 (2014).

(system) has characteristics that are attributed to the whole rather than its constituent parts, it is said to exhibit emergence[9]. In physics, observers can monitor and control a gas's properties without having to take into consideration the positions and behaviours of the individual molecules that comprise it, let alone the conditions of the particles within the atoms that comprise the molecules[10]. In economics, a market generates observable and practical data without the need to separate or identify the numerous transactions that make up the market[11].

On the other hand, the risks and advantages of a given big data system rely on the database's quality, the capabilities of the algorithms it is connected to, and the intended uses. Regulators must recognize the distinction and avoid conflating control over the outputs made possible by big data with safeguarding the security of data within a data set. Although they are mostly independent, each goal is significant. Any cost-benefit analysis of building a specific big data system must take into consideration the system's capabilities, both positive and negative, in addition to the hazards of releasing specific data without authorization.

2.1.3 National Security

All initiatives, regulations, and plans aimed at safeguarding India's borders, sovereignty, and people are included in the country's national security[12]. To maintain peace, stability, and independence, it prioritizes intelligence collection, economic and cyber security, internal security, and military defence. Maintaining national strength through economic stability, defence readiness, and technology is the aim.

Defence and Military Security: The primary tenet of national security in India is the military. Having a robust and modern military is crucial because of the border tensions with China and Pakistan along the LoC and LAC. Artificial intelligence (AI) is increasingly a part of modernization efforts to enhance logistics, monitoring, decision-making, and precision targeting. Given India's large and varied terrain, an army that is both well-equipped and adaptable is essential.

Internal Security: In territories like Jammu & Kashmir and left-wing extremist strongholds, India is particularly vulnerable to internal threats including terrorism, insurgency, and communal conflict. Effective law enforcement, intelligence, and public collaboration are necessary to maintain internal peace. AI helps to anticipate and mitigate security threats by enhancing data-based policing, surveillance, and crisis management.

Cybersecurity and Economic Security: Stability and national defence are bolstered by a robust economy. Economic safety is threatened by things like supply chain hazards, espionage, and cyberattacks.

---

[9] Claus Emmeche, Simo Koppe & Frederik Stjernfelt, Explaining Emergence: Towards an Ontology of Levels, 28 J. GEN. PHIL. SC1. 83 (1997); PETER CHECKLAND, SYSTEMS THINKING, SYSTEMS PRACTICE 3 (1981) ('The central concept 'system' embodies the idea of a set of elements connected together which form a whole, this showing properties which are properties of the whole, rather than properties of its component parts.").

[10] SEAN CARROLL, THE BIG PICTURE: ON THE ORIGINS OF LIFE, MEANING, AND THE UNIVERSE ITSELF 94-104 (2016).

[11] THOMAS C. SCHELLING, MICROMOTIVES AND MACROBEHAVIOR 47-51 (1978).

[12] SURYANSH NIGAM AND DR. VIDUSHI SRIVASTAVA, "Exploring the Impact of Artificial Intelligence on Indian National Security Dynamics", INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES [ISSN 2581-5369] Volume 7 | Issue 5 2024

With Digital India and Aadhaar, India is moving toward digital systems, making infrastructure and data protection essential. Here, artificial intelligence (AI) is crucial because it can identify cyberthreats instantly and bolster defences against hackers and data breaches.

Modernization and National Security Strategy: India is still relying on imports and international alliances, but it is also modernizing its defence sector. It has been stressed that to align military, scientific, and economic goals, a comprehensive National Security Strategy (NSS) is necessary. India wants to guarantee strategic autonomy, technical advancement, and international cooperation, even though previous proposals (from 2007 and 2018) were not formally adopted.

AI in National Security: One significant step toward modernization is the incorporation of AI into security systems. AI acts as a force multiplier in complicated scenarios by improving threat identification, surveillance, predictive analytics, and decision-making. To guarantee openness, responsibility, and adherence to international norms, its application must be constrained by moral and legal principles.

2.2 Indian Perspective

The AI ecosystem in India[13] is growing quickly. About 89% of the 1.8 lakh startups that were operating in 2024–2025 used AI. 87% of companies currently use AI solutions, and the nation is home to more than 1,800 Global Capability Center, 500 of which are dedicated to AI. With 26% of Indian enterprises reaching AI maturity, India ranks among the top four countries in the world for AI capabilities, scoring 2.45/4 on the NASSCOM AI Adoption Index. Industrial automation, consumer goods, healthcare, and finance are all significant drivers of AI growth.

2.2.1 The India AI Mission: The ₹10,371.92 crore IndiaAI Mission was introduced by MeitY in March 2024 with the goal of "Making AI in India and Making AI Work for India "by means of seven pillars":

- Compute: ₹65/hour for over 38,000 GPUs.
- Application Development: more than 30 AI initiatives in government, agriculture, health, and climate.
- AIKosh: A repository of 243 AI models and more than 3,000 datasets from 20 different industries.
- Foundation Models: AI models with an Indian focus are being developed by startups such as Sarvam AI, Soket AI, and Gnani AI.
- FutureSkills: 500 PhDs, 5,000 postgraduates, and 8,000 undergraduates supported by laboratories and fellowships in Tier 2–3 cities.
- Startup Financing: IndiaAI Startups Global provides funding and international visibility for Indian AI companies.
- AI that is safe and trustworthy should prioritize explainability, ethics, privacy, and bias reduction.

[13] Transforming India with AI, available on https://www.pib.gov.in/PressReleasePage.aspx?PRID=2178092 (last visited October 17,2025)

2.2.2 Initiatives that Complement Each Other: Through Centres of Excellence (Coes) in smart cities, agriculture, and health, government initiatives fund AI research. Policymakers are trained by the AI Competency Framework, and entrepreneurs can develop internationally with the aid of the Global Acceleration Program. Inclusive innovation is demonstrated by initiatives like Sarvam AI (enhancing Aadhaar by generative AI) and Bhashini (multilingual AI for 20 Indian languages). Bhashini and CRIS teamed up in June 2025 to introduce multilingual AI to railway systems.

2.2.3 AI Impact Summit 2026: The summit, which is slated for February 2026, would highlight India's leadership in AI worldwide through a Research Symposium, Global Innovation Challenges, and AI Pitch Fest (UDAAN). more than 30 countries and more than 300 exhibitors. creation of eight new foundation model projects and thirty new AI Data Labs (for a total of 570). the addition of 13,500 scholars to the India Fellowship Program.

2.2.4 AI and Jobs: AI is generating jobs in data science, analytics, and AI engineering, while automation is increasing job concerns. The number of AI specialists will increase from 6.5 lakh to 12.5 lakh by 2027. Future Skills has trained more than 3.37 lakh pupils.

2.2.5 AI in Everyday Life

- Healthcare: Rural patients can obtain telemedicine, imaging, and early diagnosis.
- Agriculture: Kisan e-Mitra and other programs help farmers with weather predictions and pest control.
- Education: Programs like YUVAi assist students in developing AI-based solutions under NEP 2020.
- Governance & Justice: AI is used by the e-Courts Project for scheduling, documentation, and translation.
- Climate & Weather: Mausam GPT assists with cyclone tracking, weather forecasting, and climate change monitoring.

2.3 Global Perspective

Artificial Intelligence (AI) is one of the hallmarks of the twenty-first century, revolutionizing economies, government, and national security globally[14]. Countries have implemented national AI policies in recognition of its transformative potential in an effort to improve public services, increase productivity, and preserve their position as the world's leading technology. Comprehensive AI strategies describing their visions, goals, and implementation frameworks have been released by countries like the United States, China, Japan, the United Kingdom, and France.

Automation, data analytics, and intelligent decision-making are all powered by artificial intelligence (AI), a fundamental component of the Fourth Industrial Revolution. Today, nations vie to use AI to advance

[14] NITI Aayog, National Strategy for Artificial Intelligence, Government of India (June 2018)

their economies, welfare, and national security. For example, the U.K. forecasts that AI will contribute 10% of GDP by 2030, whereas China anticipates that it will contribute 26%.

2.3.1 Landscape of Global Policy: Countries are creating AI plans at a rapid pace to boost growth in important industries. In 2016, the United States launched its first policy, which was later adopted by China, Japan, France, and the United Kingdom. These tactics highlight:

- In creating demand in industries like mobility, healthcare, education, and defence.
- To bolstering supply via infrastructure, data hubs, and research.
- In enabling systems such as public-private partnerships, finance, and governance.

With USD 2.4 billion spent in 2017, the United States makes significant investments in AI for defence and homeland security. Through partnerships with Baidu, Alibaba, and Tencent, China incorporates AI into healthcare, education, and urban planning. While France and the United Kingdom support AI in healthcare, agriculture, the environment, and defence, Japan's "Society 5.0" strives for a data-driven, AI-driven society.

2.3.2 Constructing an AI Infrastructure: To encourage the development of AI, governments are updating their digital infrastructure. The United Kingdom has spent GBP 1 billion on data trusts and 5G to ensure secure data sharing. China is working on supercomputers, semiconductors, and 5G networks, Japan provides tax breaks for AI research and development, and France has established "innovation sandboxes." To improve accessibility, the United States supports open-source AI tools such as Weka Toolkit and Open NLP.

2.3.3 Investing money in Talent and Research: The development of AI depends on human capital. Countries are increasing research collaborations, R&D, and AI education. By 2027, the UK intends to increase R&D spending to 2.7% of GDP, establishing more than 1,000 PhD positions and Turing Fellowships. France is increasing international mobility and researcher pay. China's "AI+X" initiative will establish 50 AI institutions and teach 5,000 students. The United States invests $200 million in computer science education and, in partnership with corporate behemoths, supports AI research at Stanford, MIT, and Carnegie Mellon.

2.3.4 Frameworks for Finance and Governance: The U.S. National Science and Technology Council, Japan's Strategic Council for AI Technologies, and the U.K. AI Council are just a few examples of the organized AI governance organizations that nations are forming. Additionally, funding is growing China and France have invested billions in AI projects, the United Kingdom has a GBP 2.5 billion startup fund, and Japan intends to increase its scientific budget by JPY 900 billion. One of the biggest donors worldwide is still the U.S. Department of Defence. Major AI systems like TensorFlow, Alexa, and Aliyun have been developed by private corporations like Google, Amazon, Alibaba, and others, incorporating AI into cloud services, robots, and smart technology.

2.3.5 Cooperation and Global Alliances: Government, academic, and industrial cooperation speeds up the development of AI. While the U.K.'s Tech Nation promotes innovation through regional R&D partnerships, Japan and Israel collaborate with the U.S. on AI technologies. Strong state-industry cooperation is demonstrated by China's national AI team, which consists of Baidu, Tencent, and Alibaba.

2.3.6 Data protection and ethical governance: Data privacy and ethical governance have emerged as global issues as AI develops. A standard for responsible AI use is established by the EU's GDPR, which places a strong emphasis on accountability, transparency, and permission. Similar data protection laws are being adopted by other countries to protect residents' privacy and encourage innovation.

3. Discussion and Analysis

According to the analysis, the use of AI and Big Data in India is slowly transforming the internal architecture of security in India. Predictive analytics, real-time surveillance and artificial intelligence-based intelligence fusion are enhancing more efficient threat detection and response, although the implementation is still uneven among states, and traditional problems like institutional silos and regulatory fragmentation still exist.

3.1 Role of AI and Big data in National security

India's defence, surveillance, and intelligence capabilities have changed because of the incorporation of artificial intelligence (AI) and big data analytics into the national security framework. Modern warfare, intelligence analysis, and decision-making procedures are being transformed by AI-driven technologies, which are also improving the effectiveness, speed, and accuracy of national security operations. The main areas where AI and Big Data are transforming India's security environment are methodically described in the sections that follow.

3.1.1 Monitoring and Information Collection: India's border and internal security measures are greatly improved by AI-enabled surveillance and reconnaissance technologies.

- **The role of AI and big data:** AI algorithms automatically identify suspicious activity by analysing real-time video feeds from CCTV networks, satellites, and drones. To find new threats and patterns of behaviour, Natural Language Processing (NLP) systems analyse large amounts of intelligence data, such as social media, open-source information, and intercepted communications.

- **Applications:** Drone-based surveillance and Automated Facial Recognition Systems (AFRS) are enhancing urban security management and border vigilance. In high-risk areas, where prompt detection and action might avert possible attacks, these technologies are especially essential.

- For instance, the Delhi Police utilize an AI-based facial recognition system to monitor public meetings, manage crowds, and identify criminals. Similar to this, the military uses AI-powered drones and reconnaissance devices to monitor incursions along delicate borders.

3.1.2 Threat detection and cybersecurity: AI and big data are essential for protecting India's digital borders in an era of growing cyberwarfare.

- **AI and Big Data Role:** To identify irregularities and anticipate possible cyberattacks, machine learning systems examine enormous amounts of network data. Finding malware signatures and estimating the scope of cyberthreats are made easier with the use of big data analytics.
- **Applications:** By responding to and eliminating cyberthreats on their own, AI-powered cybersecurity systems can reduce response times and possible harm. By stopping assaults before they happen, predictive algorithms also improve cyber resilience.
- For instance, the Indian Computer Emergency Response Team (CERT-In) uses automated analysis and AI-based threat monitoring to identify, categorize, and lessen cyber events. These technologies are essential for preserving the accuracy of government databases and important infrastructure.

3.1.3 Modernization of Defence: India's military and defence capabilities are being modernized with AI at the forefront.

- **AI and Big Data Role:** The Indian Armed Forces and the Defence Research and Development Organization (DRDO) are integrating AI into robotics, logistics, autonomous weaponry, and battlefield management. By analysing real-time data from many sources for tactical advantages, artificial intelligence (AI) improves decision-making.
- **Applications:** AI is used in robotic ground troops, autonomous submarines, and unmanned aerial vehicles (UAVs) for military operations, surveillance, and reconnaissance. Additionally, AI-based systems are enhancing target recognition, missile defence, and military equipment predictive maintenance.
- For instance, Key innovations include DRDO's AI-enabled robotics and autonomous drone systems, An AI-powered weapon sighting system called Project "Smash 2000 Plus" improves Indian soldiers' target accuracy, Mine detection and field reconnaissance are aided by the Sapper Scout, an unmanned ground vehicle driven by artificial intelligence.

3.1.4 Internal Security and Border Management: AI-powered solutions are essential for preserving internal stability and safeguarding India's borders.

- The **role of AI and big data** is to facilitate intelligent alarm production, movement tracking, and predictive modelling of infiltration tendencies. With automated sensors and Big Data integration, smart fencing enables real-time border zone surveillance.
- **Applications**: AI-based anomaly detection systems keep an eye on border activity and send out notifications when there are suspicious movements or unauthorized crossings. Security agencies can coordinate their responses with the help of predictive algorithms.
- For instance, the Comprehensive Integrated Border Management System (CIBMS) uses integrated command systems like "Sarvatra Pehchaan," AI-driven analytics, and smart fence to detect intrusions and coordinate real-time responses.

3.1.5 Response to Disasters and Crises: Big Data and AI also improve India's capacity to respond to and manage both man-made and natural calamities.

- **AI and Big Data Role:** By analysing satellite and meteorological data, predictive analytics models predict natural disasters including earthquakes, floods, and cyclones. AI supports rescue efforts, resource allocation, and emergency response during emergencies.
- **Applications:** High-risk reconnaissance operations, logistics, and casualty evacuation all make use of AI-driven command systems and robots. Big Data systems help civil authorities, disaster management, and defence agencies coordinate during crises.
- For instance, India's early warning systems have been enhanced by AI-based disaster prediction technologies, which assist agencies in organizing quick evacuations and resource allocation. Autonomous vehicles with AI capabilities are also being tested by the military to offer aid in remote locations.

3.1.6 Using AI in Intelligence Analysis: AI greatly enhances the gathering, processing, and analysis of intelligence.

- Data processing and Natural Language Processing (NLP): AI tools, particularly NLP algorithms, can analyse large datasets from social media, open-source platforms, and communication intercepts to identify behaviour patterns and possible threats.
- Predictive intelligence gives intelligence organizations a strategic edge in national defence by enabling them to foresee and eliminate threats before they become real.
- Operational Efficiency: Security agencies' situational awareness is improved, and prompt decision-making is supported by the quick processing of vast amounts of data.

3.1.7 Using AI to Make Strategic Decisions: AI plays a major role in crisis management and military planning.

- Predictive analytics: AI systems model strategic situations and assess possible outcomes for different approaches.
- Decision Support Systems: These systems improve strategic planning, logistics, and crisis response by giving military and policy leaders data-driven insights.
- Result: AI optimizes resource allocation and operational success by ensuring that decisions are prompt, evidence-based, and strategically sound.

3.2 Comparison Perspective

India, China, and the United States are key players in the use of AI for defense, each with distinct strategies. The US leads with a private-sector-driven innovation model, emphasizing advanced military AI applications and strong technological infrastructure. China follows a state-led approach, investing

heavily in AI to integrate civilian and military data for advanced warfare capabilities. India adopts a socially inclusive AI strategy, focusing on scalable defense applications but still faces challenges in foundational research and technological independence. This comparison[15] highlights differing priorities and levels of advancement in AI defense use among these nations

3.2.1 India's Defence Strategy for AI: With a focus on sectors like intelligence, surveillance, autonomous vehicles, and predictive maintenance, India is aggressively incorporating artificial intelligence (AI) into its national defence policy. In contrast to China, India has made less headway in implementing AI for defence. The comparatively low investment in research and development (R&D)—India devotes just around 0.7% of its GDP to R&D, compared to 2.1% in China—is one of the main causes of this gap. India also has issues with workforce skills, interoperability, ethical and legal issues, and data quality. Despite these challenges, India is dedicated to overcoming these obstacles by creating strategic alliances and advancing its own AI capabilities. Crucially, India avoids the more prevalent Chinese practice of combining military and civilian AI applications, instead emphasizing ethical considerations in its approach to AI in defence.

3.2.2 China's Defence Strategy for AI: China views artificial intelligence (AI) as a vital technology for improving both its national security and worldwide competitiveness. To combine AI capabilities across several domains, such as space, cyberspace, information warfare, and psychological operations, the nation formed the Strategic Support Force (SSF). China makes significant investments in AI R&D, concentrating on target identification, swarm drones, autonomous systems, and predictive maintenance. The "military-civil fusion" doctrine, which uses the commercial tech industry for military applications to speed up research and deployment, is a noteworthy component of China's AI strategy. China's strategy, on the other hand, puts national security and stability ahead of personal privacy and frequently uses AI-enabled monitoring for social control.

3.2.3 The US Method: On the other hand, unlike China, the United States lacks a centralized national AI policy. The US, on the other hand, has a more decentralized approach to AI governance, which is marked by large investments in AI research and development but slower advancements in the creation of legislative and regulatory frameworks. There have been worries that the US may lag China in the arms race for artificial intelligence, especially in fields like military applications and autonomous weaponry. Notwithstanding these difficulties, the US places a strong emphasis on the development of ethical AI and the necessity of tackling hazards related to AI, such as privacy issues and election meddling.

4. Result and Insights

The study concludes that, even though India has come a long way in implementing AI and Big Data to support national security, it is necessary to invest in it on a regular basis, have an ethical framework, and coherence in policies to ensure the benefits are maximized and risks are minimized. The future of the

[15] SURYANSH NIGAM AND DR. VIDUSHI SRIVASTAVA, "Exploring the Impact of Artificial Intelligence on Indian National Security Dynamics", INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES [ISSN 2581-5369] Volume 7 | Issue 5 2024

security paradigm in India is to be able to strike a balance between its technological ambition and its governance, capacity building and collaboration in the government and the non-government sectors.

4.1 Benefits of AI and Big Data

Artificial intelligence (AI) has the potential to significantly[16] advance national security because of its capacity to process vast volumes of data and mimic some aspects of the human brain. AI may enhance decision-making and bolster security operations in a few ways when given the proper resources.

4.1.1 Boosting Real-Time Intelligence: AI's ability to efficiently handle and analyse massive datasets makes it very helpful in intelligence. Artificial intelligence (AI) can produce actionable intelligence that speeds up security agencies' response times by fusing structured data with powerful computation. To find anomalies or possible security risks, AI, for instance, can transform unstructured data like financial records into insightful knowledge.

4.1.2 Developing Autonomous and Semi-Autonomous Systems: Without endangering human life, autonomous systems expand the military's operational area. To improve operational effectiveness and border security, these technologies can be integrated into large military vehicles such as fighter planes, drones, ground vehicles, and naval ships.

4.1.3 Lethal Autonomous Weapon Systems (LAWS): are unique weapons that can autonomously locate and engage targets using sensors and computer algorithms. They can function without human oversight, lowering soldier risk and enabling quick and accurate action in combat scenarios.

4.1.4 Enhancing Logistical Capability: AI has the potential to be a significant factor in military logistics. To guarantee operational readiness, it may intelligently recommend maintenance and repairs and continuously monitor border infrastructure.

To improve military cyber operations in both offensive and defensive roles, artificial intelligence is essential. AI can spot irregularities in network traffic, providing a dynamic and all-encompassing defence against cyberattacks, in contrast to traditional cybersecurity solutions that simply identify known dangers.

Humans Being Replaced in "Dull, Dangerous, or Dirty" Work: By taking over monotonous, dangerous, or hazardous jobs, autonomous systems can free up humans to work on more intricate and important projects. To lessen human exposure to risk, artificial intelligence (AI) can help with long-term intelligence gathering, analysis, or remediation of chemical weapons-contaminated areas.

4.2 Limitation of AI and Big Data

Even though AI has several advantages for national security, India still faces a few obstacles[17] to its widespread use:

[16] Artificial Intelligence and National Security, available on https://cdn.visionias.in/value_added_material/Artificial-Intelligence-and-National-Security (last visited October 16, 2025)
[17] Artificial Intelligence and National Security, available on https://cdn.visionias.in/value_added_material/Artificial-Intelligence-and-National-Security (last visited October 16, 2025)

4.2.1 Clarity Deficit in Policymakers: Decision-makers don't fully comprehend artificial intelligence (AI) or how it should be applied to national security. Important questions like "what kind of AI do we need?" are yet unsolved. How much autonomy should robots have on the battlefield? Should we use fully autonomous drones for aerial combat or autonomous patrol cars at borders? Particularly for a middle-income nation like India, which cannot make significant investments in AI at the expense of overall development, a clear vision for the AI program is crucial.

4.2.2 Absence of Critical Infrastructure: Artificial intelligence depends on intricate algorithms and vast amounts of data. To support both civilian and military AI applications, the nation needs strong hardware, computer infrastructure, and secure data banks. One of the main obstacles to India's adoption of AI is the lack of such vital infrastructure.

4.2.3 Creation of Ethical Standards: Using AI in defence presents several ethical issues, such as who is responsible if AI fails to deliver on its promises., How can artificial intelligence be incorporated into the military's current procedures? How much can we trust AI to protect our country? The safe and responsible implementation of AI in national security requires the establishment of unambiguous ethical criteria.

4.2.4 Enhanced Cyberattack Vulnerability: As AI systems are used, more "hackable" platforms—such as moving cars and other kinetic systems—are available. This may enable attackers to take advantage of systems, which could have fatal consequences. Additionally, it can lead to a rise in ransomware assaults like WannaCry, data theft, and cyber-espionage. One of the biggest challenges is making sure that data is available for AI systems while protecting people's and organizations' privacy.

4.2.5 Theft Vulnerability: Because AI systems are primarily software-based, they are susceptible to theft. Numerous AI technologies created for non-commercial purposes are openly accessible on unclassified online sites. Other countries or non-state actors may be able to exploit these tools if they are modified for military purposes.

4.2.6 Difficulties Technology Control: AI has the potential to boost military operations' scope and pace. The destructive potential of AI systems may increase in the event of system breakdowns if processes surpass human comprehension or control. Internal flaws in AI systems include unexpected failures, such as subpar picture processing in specific contexts, which renders them unreliable. bias in algorithms brought on by a lack of training data. Military deployment may encounter difficulties due to domain adaptation, or the inability to transition between several operational contexts.

4.2.7 Limited Private Sector Role in Defence: AI necessitates large capital expenditures and highly qualified staff. Effective AI development requires a supporting ecosystem that permits the unrestricted flow of capital and talent. The limited and peripheral involvement of the private sector in defence AI now limits innovation and accessibility.

4.3 Recommendation

India's national security environment, encompassing cybersecurity, intelligence operations, and defence capabilities, could be revolutionized by artificial intelligence (AI). The following policy and strategic considerations are put out to properly use AI:

4.3.1 Create Sturdy Legal and Ethical Frameworks: India needs to create precise legal and moral standards for the use of AI in intelligence and defence. The significance of accountability, openness, and conformity to international human rights standards is emphasized in NITI Aayog's 2018 National Strategy for AI. These regulations ought to cover moral issues and guarantee that AI is used responsibly in national security operations.

4.3.2 Integrate AI-Driven Technologies into Defence and Intelligence: Defence and intelligence operations should aggressively include AI technologies including autonomous systems, predictive analytics, and real-time threat identification. To maintain India's military's technological competitiveness, policymakers ought to encourage AI research and development. Prioritizing advanced surveillance technologies is necessary to support strategic defence planning, increase autonomous weapon regulation, and improve situational awareness.

4.3.3 Boost Cybersecurity: To defend sensitive information and vital infrastructure against online attacks, AI-powered threat detection and response systems are crucial. Investing in cybersecurity frameworks powered by AI can increase resistance to changing cyberattacks. To exchange best practices and bolster group cybersecurity defence, collaboration between public and private sector entities as well as foreign partners should be encouraged.

4.3.4 Address Ethical and Human Rights Considerations: To handle ethical concerns of AI, such as data privacy, security, and autonomous weaponry, proactive legislation is required. Applications of AI must pass a stringent ethical evaluation process and adhere to human rights norms. The public's confidence in national security systems will be preserved through moral leadership and the prudent application of AI.

4.3.5 Encourage International Cooperation: To influence global AI governance standards, India should take an active position in international conferences. Collaboration with technologically advanced nations can encourage knowledge sharing and make AI advances more accessible. To guarantee the safe and responsible deployment of AI, agreements on the ethical use of AI and autonomous weapon systems should be promoted.

4.3.6 Encourage Future Research: Understanding the long-term effects of AI on domestic and international security dynamics should be the main goal of future research. Research ought to cover sociopolitical ramifications, ethical issues, and methods for reducing unforeseen outcomes. Strategic planning and adaptable policy creation for AI in national security will be guided by research findings that are supported by evidence.

5. Conclusion

With revolutionary potential to improve cybersecurity, intelligence operations, and defence readiness, the intersection of artificial intelligence (AI) and big data is changing India's national security landscape. With predictive capabilities, real-time surveillance, and autonomous decision-making, AI-driven technology and data analytics enable India's security apparatus to respond to new threats more quickly and accurately. By processing enormous volumes of data from many sources, big data improves these capabilities and makes it possible to conduct thorough threat analyses and make well-informed strategic plans.

But there are also a lot of operational, ethical, and legal issues with this technical advancement. Strong governance frameworks and regulatory interventions are required to address issues including data privacy, algorithmic bias, accountability, and the dual-use nature of AI. India is actively working to ensure that innovation is balanced with moral responsibility and the interests of the country through programs like the Responsible AI Framework and the National Strategy on AI.

India must keep funding its own AI infrastructure, training, and international partnerships going forward to guarantee technological independence and strategic adaptability. Big Data and AI integration into national security must continue to be governed by human oversight, accountability, and openness. When used properly, these technologies have the potential to not only protect India's sovereignty but also establish the nation as a leader in the safe and wise application of cutting-edge technology for peace and stability on a worldwide scale.

6. Bibliography

1. Farboodi, M., & Veldkamp, L. (Year unavailable). Big Data concepts and analytics in business and security contexts.

2. National Institute of Standards and Technology (NIST). Various reports on AI governance and ethical AI.

3. Reports and white papers from the Indian Ministry of Electronics and Information Technology (MeitY).

4. Publications by NITI Aayog related to National AI Strategy and responsible AI frameworks.

5. National Strategy for Artificial Intelligence by NITI Aayog, Government of India.

6. Defence AI Project Agency (DAIPA) and Defence Artificial Intelligence Council (DAIC) reports.

7. Digital India initiatives and other government reports on AI applications.

8. Research papers from the Observer Research Foundation (ORF) and Institute for Defence Studies and Analyses (IDSA).

9. Scholarly articles on AI ethics, cybersecurity, and big data analytics in defense published in reputed journals.

10. Comparative analyses of AI in defence from global perspectives, including countries like US and China.

11. European Union General Data Protection Regulation (GDPR) for data privacy standards.

12. Frameworks and guidelines on ethical AI by the United Nations and other international bodies.

13. Articles from KPMG, Hindustan Times, and other credible news sources on India's AI defence strategies.

14. Reports on AI infrastructure and private-public collaboration in AI from industry analysis firms like NASSCOM and Gartner.