International Journal of Global Research Innovations & Technology (IJGRIT)
ISSN : 2583-8717, Impact Factor: 6.382, Volume 02, No. 03, July-September, 2024, pp 59-64

SECURING TOMORROW: ARTIFICIAL INTELLIGENCE AND THE FUTURE OF INTERNAL SECURITY IN INDIA

Dr. Meghna Meena[*]

ABSTRACT

Artificial Intelligence has the potential to change the course of internal security, bringing about opportunities that were never like before and posing numerous challenges. This research paper looks into developing AI landscapes in Indian scenarios, their impacts on security strategies, ethical issues and regulatory frameworks. India's socio-economic landscape is diverse and dynamic and has been at the forefront in adopting AI driven solutions for internal security boosting. Urban centres as well as other sensitive areas could be more effectively monitored through a system of artificial intelligence surveillance thus making it easier to detect threats proactively. Crime forecasting using predictive analytic algorithms can facilitate resource optimization, smarter policing and improved crime mapping. On the other hand, there are also ethical concerns and regulatory complexities associated with employing AI in internal security systems. Massive amounts of personal data are collected and involved in Artificial intelligence and this makes privacy an issue which should be addressed by setting up rigid measures against unauthorized entry into such information. Furthermore, discriminatory results caused by biasness imbedded within AI algorithms can either foster social inequality or undermine public trust towards safety establishments. Mitigating these risks and gearing them towards responsible utilization of AI is therefore dependent on effective governance frameworks. The regulatory framework in India is evolving with initiatives such as the National Strategy for AI that mainly insists on ethics, transparency and accountability in AI deployment. Policymakers, technologists, and civil society must come together to create a policy making system that both respects constitutional values and employs AI in improving security. In this research paper we will try to explore how AI technology would be able to contribute to India's national security. This research paper explores the current landscape of internal security challenges in India, identifies the role of AI in addressing these challenges and examines the initiatives undertaken by the Indian government and private sector.

Keywords: *Artificial Intelligence, Internal Security, Technology, Information.*

Introduction

Artificial Intelligence (AI) is an emerging technology which enables computers and machines to simulate human intelligence and problem-solving capabilities. It enables creating models and algorithms that let computers carry out operations like learning, reasoning, solving problems, perception, and making decisions that ordinarily demand for human intelligence. Artificial Intelligence is becoming more common in fields, such as robots, computer vision, decision support systems and natural language processing. As AI technology develops, it has the potential to completely transform a wide range of sectors and aspects of our daily lives, but it also raises significant ethical questions about how best to develop and apply it responsibly. It appears that the Age of Information is giving way to the Age of Artificial Intelligence in the global order. The Age of Information mandated that people must be well-informed to succeed in any field since making decisions based on knowledge was essential to that achievement. Given the circumstances, the information is definable as data or facts that distinguishes "between a decision and a guess." Since intelligence is the knowledge of "what lies ahead," it can be regarded as the cornerstone of successful "action" in any field, including security. The crucial point is that the relationship between intelligence, decision-making, and response has gained renewed importance in the modern day.

[*] Assistant Professor, Government Dungar College, Bikaner, Rajasthan, India.

Artificial Intelligence is transforming global economies and presents a unique opportunity for India. Globally, in the U.S., industry leaders like Microsoft and Google are catalyzing economic growth by driving AI innovations with substantial private investments. Similarly, China is aggressively funding AI, with plans to establish a $150 billion AI industry by 2030, showcasing how strategic state support can accelerate technological development. In Europe, the EU's investment of €700 million in AI research emphasizes the role of public-private partnerships in enhancing competitiveness.

For India, AI offers significant economic and social development prospects. According to Accenture, AI could boost India's annual growth rate by 1.3 percentage points by 2035. The potential includes increasing healthcare access, enhancing agricultural productivity, and improving education and infrastructure through intelligent solutions tailored to India's unique challenges. This integration across sectors positions India to not only advance its economy but also serve as a crucial AI hub for other developing nations, embodying the role of an "AI Garage" for 40% of the world.

AI is a constellation of technologies that enable machines to act with higher levels of intelligence and emulate the human capabilities of sense, comprehend and act. Thus, computer vision and audio processing can actively perceive the world around them by acquiring and processing images, sound and speech. The natural language processing and inference engines can enable AI systems to analyse and understand the information collected. An AI system can also take action through technologies such as expert systems and inference engines or undertake actions in the physical world. These human capabilities are augmented by the ability to learn from experience and keep adapting over time. AI systems are finding ever-wider application to supplement these capabilities across enterprises as they grow in sophistication.

Brief History of Artificial Intelligence

- **1950s: Birth of the modern AI field**

  John McCarthy first used the phrase "Artificial Intelligence," whereas Alan Turing proposed the term "Turing Test" to assess computer intelligence.

- **1960s-1970s: Early symbolic AI systems and expert systems**
  - Based on hard-coded rules
  - Examples: MYCIN (medical diagnosis), DENDRAL (chemical analysis)
- **1980s: Shift to machine learning**
  - Algorithms like neural networks and decision trees
  - Instead of using hard-coded rules, systems learn from data.
- **1990s-2000s: Neural networks and deep learning**
  - Inspired by the structure and operation of the human brain
  - Excelled in natural language processing and computer vision
- **21st century: Revival of AI**
  - Driven by large datasets (ImageNet), computing power (GPUs)
  - Algorithmic advances such as deep learning
  - Major tech companies heavily invested in AI research
- **2010s-present: Significant breakthroughs**
  - Natural language processing (example ChatGPT by OpenAI)
  - Reinforcement learning (example AlphaGo by DeepMind)
  - Computer vision (example object detection by DeepMind)
  - Widespread adoption of AI technologies across industries

Elements of Artificial Intelligence

- **Machine learning:** A subfield of artificial intelligence called machine learning enables systems to learn on their own and gradually acquire greater intelligence without the need for explicit programming. One such example is email clients' spam filtering, which uses data patterns to identify spam emails.

- **Deep learning:** It is a branch of machine learning that learns hierarchical data representations by means of multi-layered artificial neural networks. An illustration would be facial recognition software used to unlock smartphones or tag individuals in pictures.
- **Natural language processing (NLP):** The field of artificial intelligence known as "natural language processing," or NLP, focus on enabling the computers to comprehend, interpret, and produce human language. One example would be voice-activated virtual assistants, such as Alexa or Siri.
- **Computer vision:** A multidisciplinary area of artificial intelligence called "computer vision" enables computers to recognize and analyze digital photos or videos in order to represent the visual world. An illustration would be self driving vehicles that are able to identify and detect objects, people, and traffic lights.
- **Neural networks:** Inspired by the neural connections found in the human brain, neural networks are a type of machine learning models. They are made up of networked neurons or nodes that evaluate incoming data, identify patterns, and then use that knowledge to make judgments or predictions. An illustration would be the recommendation system that streaming services like Netflix employ to make movie and television suggestions based on customer tastes.

How does AI Work

- AI system gather information, analyze it, and extract pertinent characteristics.
- In order to identify patterns in the data, suitable algorithms—such as machine learning, deep learning, or rules—are selected and trained.
- In order to generate predictions or choices based on fresh input data, the trained models are assessed, optimized and put into use.
- Artificial Intelligence, imitates human intelligence through the use of technology such as computer vision, natural language processing, and reasoning.
- It becomes better and learns all the time by being exposed to additional data and criticism.

India & Artificial Intelligence

Various organizations and the government have implemented multiple initiatives to support and encourage the growth and implementation of artificial intelligence within the nation. Below are a few important initiatives:

- **National Strategy for AI (2018):** It defines the vision, objectives, and a thorough strategy to leverage artificial intelligence for boosting economic prosperity and enhancing societal progress.
- **Sector-specific AI initiatives**
  - AI for All: To support the advancement of AI education and research.
  - Responsible AI for Social Empowerment (RAISE): focuses on creating AI solutions for the betterment of society.
  - AI for Agriculture: Enhancing agricultural efficiency and supporting farmers' well-being.
  - - Responsible AI for Youth: Responsible AI for Youth so that youth can be well equip with the necessary skills and mindset for AI readiness.
- **AI Centers of Excellence:** To encourage AI research and development, the government established AI Centers of Excellence at a number of institutions and colleges, including IITs.
- **FutureSkills PRIME**: Future Skills PRIME is a collaborative effort between NASSCOM and MeitY that aims to bridge the talent gap by reskilling and upskilling IT professionals in cutting-edge fields like artificial intelligence.
- **INDIAai:** The National AI Portal of India is called INDIAai, and it acts as an ecosystem-building project, a research organization, and a knowledge portal.

Due to recent advancements such as free access to AI tools, limitless processing power, drastically reduced data storage costs, and an explosion of digital and structured data, the integration of AI into our system has increased dramatically.

Nevertheless, the field of national security has also seen upheavals as a result of the growing usage of AI. In the following context, it is no longer possible to disregard these disruptions:

- **Changing nature of security**: Technology advancements are causing the traditional components of security to grow quickly, creating new, AI-dependent issues.
  - Growing Incidence of Hybrid conflict: As a result of technology being used by both state and non-state actors, there are now more aspects to conflict. For instance, the latest data theft by the China-backed company Zhenhua may pose a threat to the internal security of a country targeting only key individuals.
  - Rise in frequency and cost of cybersecurity threats: Reports suggest that there was a 37% increase in cyberattacks in Q1 of 2020 in India. This increase in frequency is accompanied by rising strength of malware and ransomware which proportionately increases the losses associated with cyberattacks. Some reports suggest that cyberattacks could globally cost more than $5 trillion per year by 2024. AI enabled tools have the potential to increase the defensive capabilities of security systems.
  - Security is growing more complex: Growth of continuous real-time connectivity, mobile platforms and Internet of Things (loTs) in conjunction with Cyber-Physical systems has made the security landscape more complex. Al's integration into the security architecture can assist in identifying internal threats and weaknesses as well as preventing them.
- **Increased availability of tools based on AI:** In the past, most tools and technologies with security implications (such as nuclear technology) were largely shielded. This made sure that access to these technology was restricted to specific actors. However, this is not the case for AI due to the following:
  - The dual-use nature of AI applications: Many AI applications are dual-use, meaning they have uses in both the military and the civilian sector. Because of this, it is very challenging to manage the flow of such technologies.
- **Lack of international alliances for AI-based instruments Tools on lines of Wassenaar Arrangement or Missile Technology Control Regime (MTCR)**: All parties, including non-state actors and rogue nations, participate in the unrestricted cross-border movement of these instruments. This could make it possible for non-state actors to design operations that have disproportionately big effects, for instance, tampering with air traffic control systems.
- **Unavoidable presence of AI:** Artificial intelligence is currently affecting both the social and economic spheres of human existence. AI, for instance, is a crucial component of the technology employed by social media sites and can be helpful in countering concerns to national security on these platforms, such as radicalization and hate speech. Its presence is further bolstered by the following:
  - AI may be integrated into a wide range of applications, hence enhancing the "Internet of Things". For instance, AI may be included system controlling hazardous chemicals which can create a potential threat.

The incorporation of AI into a product may not be immediately apparent, meaning that the physical structure of the system may not be changed, but the system's overall functionality may be altered. For instance, it would be exceedingly challenging to determine whether a drone is being operated remotely or by an AI-based system.

In 2018, the Indian government established a task force led by Natarajan Chandrasekharan, which included members from several sectors including as government, academia, industry, services, professionals and startups to create an AI road map for national security purpose. The majority of its proposals were adopted by the government in 2019, establishing an institutional framework for the use of AI in national security. **Following can be cited as key recommendation of this framework:**

- **Defense AI Council (DAIC):**A high-level DAIC has been created under the chairmanship of Defense Minister with following responsibilities:
  - Provide strategic direction towards AI driven transformation in Defense.
  - Provide guidance and addressing issues related to data sharing.
  - Provide guidance in building strategic partnership with industry.
  - Review recommendations concerning acquisition of technology and startups.
  - Review the ethical, safe, secure and privacy assured usage of AI in defense.
    - Set policies in partnership with government institutions and industries to create deterrent for social and technology misuse.

- **Defense AI Project Agency (DAIPA):** It also envisages to establish a DAIPA with Secretary (Defense Production) as its ex-officio Chairman. The key responsibilities of DAIPA will be to-
  - Evolve and adopt a preferred technology stack within Defense establishments for development of AI Use Cases.
  - Evolve and adopt standards for development of technology and delivery process for AI projects.
  - Formulate policy for Intellectual Property Rights (IPR).
  - Enable and review the delivery of AI projects.
  - Incentivize the use of AI in existing systems and processes that demonstrate operating benefits.
  - Formulate policy for selection of, and contractual engagement with strategic industry partners.
- **Integration of AI into India's Defense Strategy:** All organizations in Ministry of Defense have been asked to integrate and embed AI, in an appropriate manner, in their strategies. These include the three Services, the Coast Guard, DRDO and DPSUs among others.
- **Capacity Building within Defense through:** Training courte in ple deense trande tonteresap a crstates: AI training of defense personnel in order to develop a critical mass of in-house data analysts, data scientists and AI specialists.

The potential challenges in adoption of AI for National Security

- **Absence of clarity on 'what is AI' and 'what we intend to do':** There is lack of understanding of some key questions like is it necessary to use completely autonomous drones to engage enemy aircraft in dogfights or can we use autonomous vehicles to patrol the boundaries and complete the task at hand? To what extent should the machines in the combat be allowed autonomy? etc.
  For a middle-income nation like India, a clear vision for the AI Programme is essential because we cannot afford to invest extensively in this area at the expense of development.
- **Lack of critical infrastructure:** Lack of essential infrastructure is one of the main things preventing AI from being used in India, both for military and civilian purposes. It is crucial to have reliable hardware and functional data banks in the nation since AI processes a large amount of data using three intricate algorithms.
- **Creation of Ethical Standards:** There are a lot of ethical concerns that come with using AI in defense. For example, who is responsible if AI doesn't perform as expected? In what way can AI be included into the military' existing protocols? To what extent can one trust AI to safeguard the nation? Adoption of AI for National Security is contingent upon the development of certain ethical principles.
- **Increased vulnerability to cyberattacks:** It can also lead to increased instances of crimes like cyber-espionage, data theft and proliferation of ransomwares like WannaCry. Also, ensuring that data is available without compromising the privacy of the entities or individuals would be a challenge.
- **Theft vulnerability:** AI systems are particularly vulnerable to theft by virtue of being almost entirely software based. For example, a large number of AI tools that have been made for civilian use have been shared widely on unclassified internet sites. Some of these tools can be adapted for use as weapon systems thus making them accessible to major military powers and non-state actors.
- **Technology cannot be controlled completely:** Using AI systems can significantly increase the scale and speed at which military operations are conducted. If the pace of operations exceeds human intelligence to understand and control events, that can increase destructive potential of the system in the event of a loss of system control. Also, it has some internal weaknesses:
  - AI systems can fail in unexpected ways, for example image processing results in certain cases are extremely poor. Thus making them unreliable.
  - AI systems may be subject to algorithmic bias as a result of their training data.
  - "Domain adaptability," or the ability of AI systems to adjust between two disparate environments, may also present challenges for militaries.

- **Limited role of private sector in defense:** AI demands high-skills and capital as innovations need an ecosystem supporting the free flow of both money and skill Thus, the role of the private sector will be pivotal in making the AI accessible and efficient. However, as of now the participation of private sector in defense is both limited and peripheral.

What can be done to Overcome these Challenges

- **Vision document on AI:** India should envisage a clear strategic vision regarding the AI. Having a Vision document provides clarity to policymakers as well as the defence establishments regarding capital envisaged outcomes.
- **Enhancing Ethical Frameworks:** Develop universal ethical guidelines for AI, inspired by the GDPR, through collaborations between bodies like the United Nations and the International Telecommunication Union. These should cover fairness, transparency, and accountability. Additionally, implement AI impact assessments before installing new systems, especially in sensitive areas like policing and healthcare. Ex: Montreal Declaration calls for responsible development of AI.
- **Creation of a supportive ecosystem:** Along with a clear policy, there is a dire need to invest in critical infrastructure so that the data servers lie within the territory. It would not only guarantee strategic independence but also take care of data privacy issues.
- **International cooperation:** To ensure that India is at par with other countries with regard to adoption of AI in National Security, various efforts like joint development, technology sharing, encouraging development of global policy and standardization could be done. For instance, India and Japan have finalized the text on cybersecurity agreement that will promote cooperation in key areas such as 5G network and Artificial Intelligence.
- **Tapping the civilian innovation ecosystem:** The AI-market for civilian purposes in the country is on the rise. For instance, India ranks third in G20 countries in AI-based startups. Policymakers could tap this potential for the defense sector. For example, marrying the flagships initiatives of the current government. Make in India in Defense and Digital India - to bring a technological revolution in the defense industry.
- **Balancing adoption and innovation:** Since India is a late entrant in the field vis-à-vis powers like China and US, it could capitalize on the late-movers advantage, i.e., learning from the existing AI technologies, to fulfil its basic security needs (like border patrols and intel-gathering) alongside innovating over and above the existing technologies.
- **Investing in AI Literacy and Public Engagement:** Enhance AI education at all levels and facilitate public dialogues on AI’s societal impacts through platforms like citizen assemblies.

Artificial intelligence has the capacity to outsmart human intelligence and can complete any given work considerably more precisely and effectively. Without a question, AI has enormous potential, which contributes to making the world a better place to live. But excess of everything is bad, and nothing compares to the human brain in terms of functionality. Thus, excessive use of AI is not recommended since it can lead to a highly dangerous environment for both present humankind and future generations who rely too heavily on computers and automation. India's internal security is a dynamic area that calls for continuous efforts from the the government, security forces, and citizens.. Maintaining social peace, progress, and safety all at the same time is still quite difficult.

References

1. https://www.iqraias.com/basics-of-ai-challenges-and-the-future-for-india/
2. https://www.drishtiias.com/to-the-points/paper3/artificial-intelligence-16
3. https://d19k0hz679a7ts.cloudfront.net/value_added_material/Artificial-Intelligence-and-National-Security.pdf
4. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
5. https://forumias.com/blog/threats-posed-by-artificial-intelligence/
6. https://byjus.com/free-ias-prep/artificial-intelligence-upsc-notes/
7. https://vajiramandravi.com/quest-upsc-notes/artificial-intelligence/.