RESEARCH JOURNAL OF ENGLISH (RJOE)
www.rjoe.org.in | **Oray's Publications** | ISSN: **2456-2696**
An International Approved Peer-Reviewed and Refereed English Journal
Impact Factor: *8.373 (SJIF)* | **Vol. 10, Issue 3 (July, August& September;2025)**

Impact of Artificial Intelligence and Cyber Terrorism in Bharat: Challenges and Solutions

Samiksha Dixit
M J P Rohilkhand University, Bareilly, Uttar Pradesh

Paper Received on 12-08-2025, Accepted on 17-09-2025
Published on 18-09-25; DOI:10.36993/RJOE.2025.10.3.705

Abstract
Artificial Intelligence (AI) and cyber terrorism are increasingly prominent concerns in the paradigm of digital age all across, and more particularly for nations like India has a goal to achieve the vision of "Viksit Bharat". This paper explores the intersection of AI and cyber terrorism, scrutinizing the legal frameworks and intricate policy implications which are prevalent in Bharat regarding Cyberspace. As of, the integration of AI technology into various sectors has revolutionized industries, governance, and security across all the borders. However, the dual-use nature of AI poses significant risks, particularly in the realms of cyber terrorism. As Bharat aspires to attain its "Vision for Viksit Bharat" by establishing itself as a developed and secure nation, In present scenario the legal and policy frameworks governing AI and its integrated tools and cybersecurity require to bring changes for AI-driven solutions to cyber terrorism, ultimately contributing to the development of Viksit Bharat.

Keywords: Artificial Intelligence, Cyber Terrorism, Cybersecurity, Legal Frameworks, Viksit Bharat

Introduction

Artificial Intelligence (AI) has rapidly transformed from a futuristic concept into an integral part of our daily lives, influencing industries, governments, and societies at large. This technology has engulfed today almost every sector and in the upcoming years it will become strong further more with the launch of numerous futuristic tools like Q star, SORA AI etc. It is just simply a tool it can be used positively as well as negatively, intrigued the psyche of man typically. For some it is creating widespread opportunities but at the same time others feel threatened that in the long run it will wipe out many creative jobs due to its huge impact. In the past, the focus of Bharat on technology was rooted in building a digital infrastructure, aiming to bridge the digital divide (The difference between rural and urban population in terms of the usage of technology) and enhance economic growth. As we moved into the present, AI's capabilities expanded, bringing both opportunities and challenges at the same time. Among these challenges, the rise of cyber terrorism has become a critical concern for the entire nation, where AI is increasingly being hold by malicious actors to exploit vulnerabilities in cyberspace. Because of this it has become very difficult today to track what is "Real" and what is "Computer Generated", only by the use of keyboard it has become possible for anyone to create any hypothetical world. With its advent many Industries are facing upside down including the most creative ones like Animators, Video Game designers, Graphic designers' etc. In the upcoming time platforms like Stock video and Stock photo will be completely destroyed. The day is no far when it almost become impossible for a human eye to differentiate between these, in such a case it would become much easy for propagandists to spread fake news and for exploiters to exploit but then a technological solution can also be created for these recurring problems currently emerging in the society with a rapid growth.

In contemporary time period, Bharat stands at a crossroads, grappling at large with the legal and policy implications of AI in the context of cybersecurity. The need for vigorous legal frameworks and policies to battle cyber threats is essential than ever due to the rapid increment in the cases related with cyber space. The nation's legal system is being tested by the complexities introduced by AI-driven cyber threats, requiring swift and effective responses from the cyber security. In Bharat the legal frameworks related with cyberspace primarily regulated by Information Technology Act (2000), though with the passage of time or specifically with the enhancement in technology the then government till now has brought many amendments. Looking towards the future, as Bharat aspires to achieve the vision of Viksit Bharat, the role of AI in both questioning the strength and securing the nation becomes even more critical as well as crucial. The challenge lies in crafting a legal and policy landscape that not only addresses the current threats but also anticipates and mitigates future risks associated with AI in cyber terrorism. Ensuring that Bharat is well-prepared for these challenges, which is essential for realizing the vision of a secure and prosperous Viksit Bharat.

The aim of "Viksit Bharat" envisions a nation characterized by technological advancement, economic prosperity, and powerful security, above all a positive realm with the implication of advanced technology. However, the rise of cyber terrorism can pose some significant challenges to this vision. Cyber terrorists increasingly exploit AI to conduct sophisticated attacks on critical infrastructure, financial systems, and government institutions. This paper examines the legal and policy implications of AI in the context of cyber terrorism, exploring how Bharat can tackle AI related complexities for cybersecurity while addressing the associated risks. Undoubtedly the advent of AI has transformed the digital landscape, offering unprecedented opportunities for innovation and efficiency. As Bharat embarks on its journey towards becoming a developed nation by 2047, under the "Viksit Bharat" vision, the need to address the legal and policy challenges associated with AI and cyber terrorism become imperative.

Objectives

1. To explore how artificial intelligence (AI) can be used to enhance national security, particularly in detecting and preventing cyber terrorism, within the context of Bharat aim for attaining the vision for Viksit Bharat.
2. To analyze the current legal frameworks governing AI and cybersecurity in Bharat, identifying gaps and challenges in addressing AI-driven cyber terrorism, and assessing the ethical implications of AI deployment in national security.
3. To develop recommendations for AI-specific legislation and regulatory frameworks that align with the vision of Viksit Bharat, ensuring that AI technologies are used responsibly and effectively to fight cyber threats.
4. To advocate an active participation of Bharat in international efforts to establish global standards for AI and cybersecurity, facilitating cooperation and alignment with global best practices.
5. To emphasize the importance of safeguarding individual rights and civil liberties while integrating AI into national security measures, ensuring that legal frameworks include ethical guidelines and oversight mechanisms.

Literature Review

The literature on the intersection of law, artificial intelligence (AI), and cyber terrorism reveals a rapidly evolving landscape that presents both significant challenges and opportunities in the sphere of Cyber space. AI role in national security has garnered considerable attention, particularly for its potential to enhance the detection and response to cyber threats. The Indian Ministry of Electronics and Information Technology emphasizes AI transformative impact on cybersecurity, highlighting its ability to process large datasets and predict attacks. However, the dual-use nature of AI, where the same technology can be harnessed for both defense and offensive purposes, raises substantial concerns in front of everyone. This dual-use dilemma instigates the development of sophisticated legal frameworks capable of managing these risks. Here the gap lies in addressing the complexities introduced by AI in the legal diameter. The rapid pace of AI development frequently outstrips the ability of laws to keep up with it and thus creating regulatory gaps perpetually. Certainly the evolving nature of AI technology challenges the existing legal structures all across the borders. Along with this the ethical concerns also permeate the discourse on AI in national security. AI positioning for surveillance and data analysis raises significant privacy and human rights issues. The European Union's General Data Protection Regulation (GDPR) serves as a model for balancing AI use with the protection of individual rights, as discussed by Floridi (2019). In the context of Bharat, the Personal Data Protection Bill (2019), is a step towards addressing these concerns, but its effectiveness in regulating AI remains to be seen. The NITI Aayog's National Strategy for Artificial Intelligence (2018) advocates for using AI to enhance governance and national security, but this vision requires the establishment of legal frameworks that are both adaptive and resilient in nature.

Research Methodology

In this research paper, a primarily qualitative and analytical research methodology is used, combined with a policy analysis implementation by the government of India.

Artificial Intelligence in Cybersecurity

In this technological advancement era, Artificial intelligence (AI) is playing a dominant role in revolutionizing cybersecurity by providing advanced tools for detecting, preventing, and responding to cyber threats. Through machine learning and data analysis, AI enhances the ability to monitor network activity in real-time, identifying anomalies that could indicate potential security breaches. In cybersecurity, it can analyze vast amounts of data, detect patterns, and predict potential threats. AI-driven tools are used for real-time monitoring, threat detection, and incident response, making them invaluable in defending against cyber-attacks. It aids in threat detection by recognizing patterns that might be missed by conventional methods, allowing for quicker and more accurate identification of malware, phishing attempts, and other cyberattacks. AI also enables automated responses to incidents, reducing the time it takes to diminish threats and minimizing damage. Predictive analytics powered by AI can foresee future vulnerabilities, helping organizations proactively strengthen their defenses. Additionally, AI plays a crucial role in protecting sensitive data by optimizing encryption techniques and enforcing access controls based on user behavior. However, as AI becomes more integrated into cybersecurity, it also brings challenges, such as the potential for conflicting attacks where AI systems are manipulated by cybercriminals commonly refer as hackers. Undoubtedly AI has now become a significant part not just in one domain but in all, advances the chance for opportunists as well as for exploiters to exploit in new ways. Despite these challenges, AI continues to be a critical asset in the ongoing battle against cyber threats, significantly improving the effectiveness and efficiency of cybersecurity measures.

Cyber Terrorism Defined

Cyber terrorism involves the use of digital technology to carry out attacks that cause disruption, damage, or fear, particularly targeting critical infrastructure or government systems by the propagandists, in recent years many such serious cases have aligned. Unlike traditional cybercrime, cyber terrorism is politically or ideologically motivated, using technology to achieve political or ideological goals aiming to undermine national security and public safety. In a nutshell, it involves using computers and the internet to cause harm or threaten others, often to spread fear or disrupt in the society. Cross border cybercrimes also have a perplexed dimension via this to detect it, also come out as a tough task for cyberbranch. Most of the time, offensive organizations used this technology in an indirect way, for instance in manipulation or radicalization of common people. Some cyberthreats listed below are:-

1.Stuxnet (2010): A computer worm that targeted Iran's nuclear facilities, disrupting its uranium enrichment process. While its origins are unclear, it's widely believed to have been a cyberattack orchestrated by a nation-state.

2. Sony Pictures Hack (2014): A group called "Guardians of Peace" hacked Sony Pictures, leaking confidential data and threatening attacks if the company released the movie "The Interview," which depicted the assassination of North Korea's leader.

3. Ukraine Power Grid Attack (2015): Hackers took down part of Ukraine's power grid, causing a blackout for hundreds of thousands of people. This attack demonstrated how cyber terrorism could directly impact critical infrastructure.

The Role of AI in Cyber Terrorism

Artificial Intelligence (AI) plays a dual role in the realm of cyber terrorism, both as a tool for defense and a potential weapon for attackers as well. On the defensive side, AI is employed to enhance cybersecurity measures by detecting threats in real-time, analyzing patterns of network traffic, and automating responses to potential data breaches. AI-driven systems can identify unusual behavior, predict potential cyber-attacks, and neutralize them before they cause significant damage. However, AI also poses a significant threat when hold by cyber terrorists. For instance, it can be used to create sophisticated phishing attacks that adapt to a target's behavior, making them harder to detect and prevent. Moreover, AI can automate large-scale attacks, such as Distributed Denial of Service (DDoS) attacks, which can cripple critical infrastructure by overwhelming systems with traffic. Additionally, AI-generated deepfakes can be used to spread disinformation or blackmail individuals, amplifying the psychological impact of cyber terrorism. The evolving capabilities of AI thus present both a formidable defense mechanism and a potent tool for cyber terrorists, highlighting the importance of ongoing advancements in cybersecurity to stay ahead of these threats. So typically, it is playing the role like a double-edged sword in this paradigm. Currently lot of terrorists' organizations are using this technology to automate and amplify their attacks and in the upcoming time with the advancement of technology, it will become even easier for them to regulate terrorists' misdeeds more. For instance, AI-driven malware, phishing attacks, and autonomous hacking tools can be more effective and harder to detect, posing new challenges for law enforcement and cybersecurity professionals. So it is required for the government to also advance themselves in the sphere of legal frameworks with the emerging technology in order to detect such kind of crimes which proclaim some dangerous threat to humanity and society at large.

The Current Legal Framework in Bharat

The Legal framework of Bharat for addressing cyber terrorism and cybersecurity is continuously evolving with the passage of time. However, it faces several challenges in keeping pace with the rapid advancements in AI and the growing threat of cyber terrorism.

Information Technology Act, 2000

The primary legislation governing cybersecurity in Bharat launched with the Information Technology Act, 2000, along with its amendments. The Act addresses various cybercrimes, including unauthorized access to computer systems, data breaches, and cyber terrorism. However, the Act was not designed with AI in mind back then, due to this its provisions may be inadequate in contemporary era to address the complex nature of AI-driven cyber threats.

National Cyber Security Policy, 2013

The National Cyber Security Policy, 2013, outlines approach of Bharat to protecting its digital infrastructure. The policy emphasizes the need for a secure and resilient cyberspace, highlighting the importance of public-private partnerships and the development of cybersecurity skills.

Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019, aims to protect personal data and ensure privacy in the digital age. This bill typically addressing the data protection rather than cybersecurity or cyber terrorism. The increasing use of AI in processing and analyzing personal data, there is a need to consider the implications of AI in the context of both data protection and cybersecurity to strengthen it.

Updating the Legal Framework

At present legal framework of Bharat must be updated to address the challenges posed by AI in the context of cyber terrorism with the emerging technology. This includes revising the Information Technology Act, 2000, to incorporate provisions specifically targeting AI-driven cyber threats. Because of this, with the shouting technology lot of amendments have been made to ensure the protection from cyberthreats. Additionally, new legislation may be required to regulate the development and use of AI in cybersecurity, ensuring that AI systems are used responsibly and ethically across all the sectors.

Developing a National AI Strategy for Cybersecurity

Bharat should develop a comprehensive national AI strategy that includes specific measures for cybersecurity. This strategy should focus on building AI capabilities, fostering public-private partnerships, and promoting research and development in AI for cybersecurity. The strategy should also address the ethical implications of AI, ensuring that AI systems are transparent, accountable, and aligned with human rights by removing all the ambiguities, engulfing in the cyberspace.

Enhancing International Cooperation

No negation with this factor that Cyber terrorism is a global threat so in order to tackle, this thing requires international cooperation. Bharat should actively participate in global initiatives aimed at combating cyber terrorism and regulating AI. This includes engaging with international organizations, such as the United Nations and the International Telecommunication Union, to develop global standards and best practices for AI and cybersecurity.

Building Cybersecurity Infrastructure

To effectively combat AI-driven cyber terrorism, Bharat needs to invest in its cybersecurity infrastructure. This includes developing advanced AI-driven cybersecurity tools, training cybersecurity professionals, and establishing centers of excellence for AI and cybersecurity research. Additionally, the government should also work closely with the private sector to ensure that critical infrastructure is protected against AI-driven cyber threats.

Promoting Cybersecurity Awareness and Education

Public awareness and education are crucial for preventing cyber terrorism across all the corners of the world. Bharat should promote cybersecurity literacy among its citizens, emphasizing the risks associated with AI-driven cyber-attacks. At a global level many countries already have taken initiative regarding this, in such a case this thing recommend a very high time for Bharat as well to make some progressive programs with schemes to make everyone well aware in this context with all its core. Educational institutions should be encouraged to include cybersecurity and AI in their curriculum, preparing the next generation of professionals to handle these challenges.

AI-Driven Economic Growth

AI can contribute to economic growth of Bharat by fostering innovation and creating new opportunities in the cybersecurity sector and in lot of other fields. By investing in AI research and development, Bharat can station itself as a global leader in AI and cybersecurity, driving economic growth and creating high-skilled jobs. With the help of AI, today it is possible for numerous people to fulfill their dreams either it is in the field of business, IT sector, film making or any other sphere. It allows the democratization in all fields via this a common man is also able to live a life of his dream so far. For instance a musician would be able to make videos without spending a lot, an IT employee would be able to become a good film maker etc.

Strengthening National Security

A strong AI-driven cybersecurity strategy is essential for protecting national security of Bharat. With the help of AI, Bharat can enhance its ability to detect and respond to cyber threats easily, ensuring the security and resilience of its digital infrastructure. This is particularly important as Bharat increasingly relies on digital technology for governance, finance, and critical infrastructure.

Enhancing Governance and Public Trust

AI can also improve governance by enhancing the transparency and accountability of government operations. AI-driven tools can be used to monitor government systems, detect incongruity, and ensure compliance with regulations. This can help build public trust in government institutions, which is essential for achieving the vision of Viksit Bharat.

Vision for Viksit Bharat: Legal and Strategic Considerations

The vision for a "Viksit Bharat" entails not only economic and technological development but also the establishment of a secure and just society. In this context, the legal regulation of AI and its role in fighting against cyber terrorism must be aligned with the developmental aims of Bharat. According to the NITI Aayog's National Strategy for Artificial Intelligence, AI should be used to enhance governance, improve public services, and ensure national security (NITI Aayog, 2018). Though, this vision also requires the establishment of legal frameworks that can adapt to the evolving nature of AI and cybersecurity threats.

Analysis and Discussion

1. Current Legal Frameworks and Their Limitations

Contemporary legal framework of Bharat for cybersecurity, primarily based on the Information Technology Act (2000), and its amendments, provides a foundation for addressing cyber threats. However, this framework is not adequately equipped to handle the complexities introduced by AI in cyber terrorism. The lack of specific regulations addressing AI's dual-use nature, where AI can be used for both security and malicious purposes, put a significant challenge. Furthermore, the rapid evolution of AI technologies outpaces the legislative process, leading to potential gaps in the law. These gaps can be exploited by cyber terrorists, who may use advanced AI techniques to evade detection and perpetrate attacks. Therefore, there is a pressing need for dynamic legal frameworks that can adapt to technological advancements.

2.Proposed Legal and Regulatory Frameworks

To address the challenges identified, this paper proposes several key elements for a legal and regulatory framework that aligns with the vision of Viksit Bharat: a). AI-Specific Legislation: Bharat should develop AI-specific legislation that addresses the unique challenges posed by AI in cybersecurity. This legislation should include provisions for the regulation of AI development and deployment, with a focus on preventing its misuse by cyber terrorists.

b). International Collaboration: Cyber terrorism is a global threat that requires international cooperation. Bharat should actively participate in international efforts to develop global standards for AI and cybersecurity, ensuring that its legal frameworks are aligned with international best practices.

c). Ethical Guidelines and Oversight: Any legal framework for AI in cybersecurity must include ethical guidelines to protect individual rights and freedoms. An independent oversight body should be established to monitor the use of AI in national security and ensure compliance with ethical standards.

d). Capacity Building and Public Awareness: To effectively combat cyber terrorism, there is a need for capacity building within law enforcement and the judiciary. Additionally, public awareness campaigns should be launched to educate citizens about the potential risks and benefits of AI in cybersecurity.

3.Vision for Viksit Bharat: Integrating AI into National Security

The integration of AI into national security efforts is essential for realizing the vision of Viksit Bharat. AI can enhance the detection and prevention of cyber threats, improve the efficiency of law enforcement, and contribute to the overall security of the nation. However, this integration must be guided by an imperative legal framework that balances national security with the protection of civil liberties. In line with the vision of Viksit Bharat, Bharat should aim to become a global leader in AI-driven cybersecurity. This will require significant investment in research and development, as well as the establishment of partnerships with other nations and international organizations. By proactively addressing the legal challenges associated with AI and cyber terrorism, Bharat can position itself at the forefront of global efforts to secure cyberspace effectively.

Conclusion

The aim of this research paper is to focus on the integration of artificial intelligence (AI) into the legal framework to battle against cyber terrorism is not only a necessity but also an opportunity for Bharat to position itself as a global leader in the digital age. The vision for "Viksit Bharat" envisions a nation that is technologically advanced, economically powerful, and secure from emerging threats. To realize this vision, Bharat must proactively address the legal and ethical challenges posed by AI in cybersecurity, ensuring that these technologies are utilize responsibly and effectively. The current legal frameworks, while foundational, require significant enhancements to keep pace with AI's rapid development. By enacting AI-specific legislation, Bharat can close existing regulatory gaps, ensuring that AI is used to protect the nation without infringing on individual rights. As international collaboration and alignment with global standards will be crucial in developing a resilient and forward-looking legal framework that anticipates future challenges. On a positive note, AI holds an immense potential to transform the national security landscape of Bharat, by using AI's capabilities in data analysis, threat detection, and predictive modeling. To strengthen national security, economic stability and social progress are the key pillars of the vision for Viksit Bharat. Moreover, the ethical integration of AI into national security can serve as a model for other nations, positioning Bharat as a leader in the global discourse on AI and cybersecurity. By embedding ethical considerations into the legal framework and establishing robust oversight mechanisms, Bharat can ensure that its pursuit of technological advancement does not come at the cost of civil liberties. Ultimately, the careful and strategic integration of AI into the national security of Bharat apparatus, supported by a vigorous legal framework, will be instrumental in achieving the vision of Viksit Bharat, a developed, secure, and just society where technology serves for wellbeing of mankind.

Works Cited

Boulanin, Vincent, and Maaike Verbruggen. *Mapping the Development of Autonomy in Weapon Systems*. SIPRI, 2017.

Calo, Ryan. "Artificial Intelligence Policy: A Primer and Roadmap." *SSRN*, 2015.

Chakravarti, A. "The Ethics of AI in Law Enforcement." *Journal of Indian Law and Society*, vol. 8, no. 2, 2021, pp. 145–165.

Chinese Government. AI and National Security: A Strategic Approach. 2022.

European Commission. AI Regulation and Cybersecurity: A European Perspective. 2021.

Floridi, Luciano. *The Ethics of Artificial Intelligence*. Oxford UP, 2019.

Indian Government. Information Technology Act, 2000.

Indian Government. Personal Data Protection Bill, 2019.

Johnson, Mary A. "Blockchain Technology and Its Impact on Digital Transactions: A Legal Perspective." *International Journal of Law and Technology*, vol. 15, no. 4, 2018, pp. 321–340.

Ministry of Electronics and Information Technology. Artificial Intelligence for National Security. Government of India, 2022.

Ministry of Electronics and Information Technology. National Cyber Security Policy, 2013. Government of India, 2013.

NITI Aayog. National Strategy for Artificial Intelligence. Government of India, 2018.

Paliwal, Aseem, and Ahmad. "Emerging Technologies and Future Challenges in Indian Cyber Law." 2024.

Patel, Rakesh. "Privacy Challenges in the Internet of Things Era." *Cybersecurity Review*, vol. 12, no. 3, 2019, pp. 87–102.

Smith, John. "Legal Implications of Artificial Intelligence: A Comparative Analysis." *Journal of Cyber Law*, vol. 25, no. 2, 2020, pp. 45–63.

Tripathi, A. "Cybersecurity Laws in India: An Analysis." *Indian Journal of Law and Technology*, vol. 16, no. 1, 2020, pp. 24–42.

U.S. Department of Defense. AI in Cyber Defense: The Role of the Joint Artificial Intelligence Center (JAIC). 2020.