Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

Ai-Enhanced Cyber Terrorism: Legal Preparedness And Response In India

Asha
Ph.D. Scholar, Department of Law,
Gurugram University

Submission date 12.04.2026 | Acceptance date: 25.04.2026 | Publication: 29.05.2026

ABSTRACT:

The rapid advancement of Artificial Intelligence (AI) has transformed the landscape of cyber terrorism, introducing sophisticated threats that challenge existing legal frameworks. This research paper examines the preparedness of India's legal system to address AI-enhanced cyber terrorism, highlighting the gaps and challenges within the current legislative structure. While the Information Technology Act, 2000, and its 2008 amendment provide a foundation, they fall short of addressing the unique complexities posed by AI-driven threats, such as autonomous cyber-attacks, deep fakes, and AI-generated misinformation. The difficulties in attributing and assigning accountability for AI-based cyber-attacks further complicate the legal response, revealing a critical need for updated legislation and AI-specific regulations.

The paper also explores the privacy-security dilemma, emphasizing the tension between broad surveillance powers and individual privacy rights in the context of AI. Additionally, it discusses the challenges of international collaboration in combating cross-border AI-enhanced cyber terrorism. To strengthen India's preparedness, the paper recommends updating existing laws, developing AI-specific cybersecurity regulations, enhancing attribution mechanisms, and promoting international cooperation. These steps are essential for creating a more resilient legal framework capable of effectively responding to the evolving threats of AI-enhanced cyber terrorism, ensuring both national security and the protection of civil liberties.

Keywords : Artificial Intelligence (AI), AI-Enhanced Cyber Terrorism

INTRODUCTION

The rapid evolution of Artificial Intelligence (AI) has brought about transformative changes across various sectors, including cybersecurity. While AI offers immense potential to enhance security measures, it also presents new challenges, particularly in the context of cyber terrorism. Cyber terrorism, defined as the convergence of terrorism and cyberspace, involves the use of digital technologies to conduct attacks that cause significant harm or create widespread fear. Oxford defines cyberterrorism as the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society. When AI is integrated into these cyber threats, the scale, sophistication, and impact of such attacks can be unprecedented.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

This phenomenon, termed AI-enhanced cyber terrorism, represents a growing concern for nations worldwide, including India. Hostile actors use generative AI tools to create manipulated variants of content, evade detection mechanisms, and produce synthetic propaganda. Cybercriminals exploit AI's ability to learn and adapt, creating highly customized attacks that can mutate and compromise systems with minimal detection.[1]

India, being one of the largest digital economies, is particularly vulnerable to cyber terrorism. With its increasing reliance on digital infrastructure, from financial services to critical national infrastructure, the potential for AI-driven cyber-attacks poses a significant threat to national security. AI-enhanced cyber terrorism involves the use of machine learning algorithms, deep learning, and other AI technologies to automate and amplify cyber-attacks. These attacks could range from sophisticated phishing schemes and deep fake propaganda to automated denial-of-service attacks and the manipulation of AI systems in critical sectors such as healthcare, finance, and defense.

The Indian legal framework, primarily governed by the Information Technology (IT) Act of 2000, has been the cornerstone of cybersecurity regulation in the country. However, this legislation, which was enacted at the dawn of the digital age, does not fully address the complexities introduced by AI in the realm of cyber threats. While amendments, such as the IT (Amendment) Act of 2008, have sought to enhance the legal infrastructure, they fall short in addressing the unique challenges posed by AI-enhanced cyber terrorism. For instance, issues related to the attribution of cyber-attacks, the regulation of AI technologies, and the ethical implications of using AI in counter-terrorism efforts are not adequately covered by the current legal provisions.

The inadequacy of existing laws is further exacerbated by the lack of a comprehensive national cybersecurity policy that incorporates AI-specific threats. The National Cyber Security Policy of 2013, while a step in the right direction, is outdated and does not reflect the advancements in AI and the corresponding risks. As AI technologies continue to evolve, the legal and policy frameworks must also adapt to effectively mitigate the risks associated with AI-enhanced cyber terrorism.

In conclusion, AI-enhanced cyber terrorism presents a complex and evolving challenge for India. While the country's digital landscape continues to grow, so too does its vulnerability to sophisticated cyber threats powered by AI. Addressing this threat requires a multifaceted approach, encompassing legal reform, policy updates, capacity building, and international collaboration. This paper aims to explore the current state of India's legal preparedness and response to AI-enhanced cyber terrorism, identifying gaps and proposing recommendations for strengthening the nation's cybersecurity framework.

MAJOR CASE STUDIES OF AI-DRIVEN CYBER TERRORISM

[1] Supra note 2.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

1. Deep Locker: AI-Powered Malware[2]

Deep Locker, a proof-of-concept malware developed by IBM Research in 2018, is an example of how AI can be used to enhance cyber-attacks. Unlike traditional malware, Deep Locker used AI to hide its malicious payload within a legitimate application, only activating when it identified its specific target using AI-driven facial recognition, geolocation, and voice recognition. Although Deep Locker was not deployed in real-world attacks, it highlighted the potential for AI to create highly targeted and stealthy cyber threats. Such malware could be used in cyber terrorism to launch attacks against high-profile targets with minimal risk of detection, increasing the effectiveness of cyber terrorist activities.

This case demonstrates how AI can be weaponized to create sophisticated malware that is difficult to detect and counter, posing significant challenges for cybersecurity defenses globally.

2. Project Raven: UAE's AI-Driven Surveillance and Cyber Espionage[3]

Project Raven was an initiative reportedly conducted by the United Arab Emirates, where former U.S. intelligence operatives helped the UAE government build an AI-driven cyber espionage and surveillance system. This system used AI to analyze vast amounts of data to monitor dissidents, journalists, and foreign governments.

The project demonstrated how AI can be used in state-sponsored cyber operations that border on cyber terrorism, as the tools developed could be repurposed for offensive cyber terrorism operations. The ability to conduct mass surveillance and cyber espionage on a global scale using AI poses significant threats to national and international security. This case highlights the dual-use nature of AI in cyber activities, where tools developed for surveillance can easily be adapted for cyber terrorism, threatening both civil liberties and state security.

3. AI-Powered Deep fake Attacks

Deep fakes, which use AI to create hyper-realistic but fake videos, have been increasingly weaponized for cyber terrorism. In 2019, a deep fake video was used to manipulate the stock market by falsely portraying a CEO, Ashish kumar Chauhan, making damaging statements about his company.[4] This demonstrates the potential for AI to be used in economic disruption as a form of cyber terrorism. Following such incidents, National Stock Exchange of India (NSE) has been issuing warnings to investors about deep fakes.[5]

---

[2] Editorial, Security Intelligence, Deep locker: How AI Can Power A Stealthy New Breed Of Malware, August 8, 2018.
[3] Editorial, Reuters, Inside the UAE's secret hacking team of American mercenaries, January 30, 2019.
[4] Editorial, Business Standard, NSE raises the raid flag on deep fakes: Here is how you can fall prey to such scams, April 10, 2024
[5] Ibid

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

Deep fake technology has the potential to create significant socio-political unrest by fabricating events or statements from key figures, leading to public panic, financial loss, or even inciting violence. Malicious actors can exploit AI's ability to mimic human behavior and deceive users.[6] The ability of AI to create convincing fake content poses a serious threat to trust in digital communications, with the potential to be exploited by cyber terrorists to destabilize societies.

POTENTIAL THREATS OF AI-ENHANCED CYBER TERRORISM IN INDIA

1. Automated Cyber Attacks

AI can be used to automate cyber-attacks, making them faster, more efficient, and scalable. For instance, AI can enhance Distributed Denial of Service (DDoS) attacks by automating the process of finding vulnerable devices and using them to launch large-scale attacks.[7] This increases the risk of critical infrastructure being targeted, including power grids, financial systems, and healthcare networks.

The accessibility and affordability of AI contribute to a surge in cyber threats globally. Countries with advanced digital infrastructures are particularly vulnerable. India's growing digital economy and reliance on technology in critical sectors make it a prime target for such attacks. Weekly attacks on Indian organizations increased by 18 percent in early 2023, with a 48 percent rise in bot attacks.[8] The potential disruption of services like banking, healthcare, and transportation could have severe consequences for national security and public safety.

2. AI-Driven Social Engineering Attacks

AI can enhance social engineering attacks by analyzing vast amounts of data to create highly personalized phishing schemes. AI algorithms can predict user behavior, crafting messages that are almost indistinguishable from legitimate communications, making it easier to deceive targets into divulging sensitive information.[9]

On a global scale, AI-driven social engineering could lead to large-scale data breaches, compromising the security of millions of individuals and organizations. With India's rapid digital adoption, a significant portion of the population is still unfamiliar with advanced cyber

[6] Milin Stanly, India AI, AI in cybersecurity: How is India grappling with the risks of cyber-attack, October 13, 2023.
[7] A. Ünver, "Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights," Eur. Parliam. Subcomm. Hum. Rights, no. May, 2024.
[8] Editorial, The Diplomat, Securing India's Digital Future: Cybersecurity Urgency and Opportunities, January 20, 2024.
[9] S. R. Sindiramutty, "Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence," Taylors Univ. Subang Jaya Malaysia, 2023.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

threats, making them vulnerable to AI-enhanced social engineering.[10] Such attacks could undermine trust in digital platforms, hindering India's digital growth.

3. AI-Powered Propaganda and Misinformation

AI can be used to generate and spread propaganda and misinformation at an unprecedented scale and speed. AI-driven bots can amplify divisive content on social media, while deep fakes can be used to manipulate public opinion by creating fake but believable news. Researchers have investigated how large language models (LLMs), such as ChatGPT, could be exploited by terrorists and violent extremists.[11] These LLMs can be "jailbroken," allowing them to bypass standards and policies that prevent them from generating extremist, illegal, or unethical content. Extremists could potentially use LLMs for training, operational planning, and propaganda.[12]

This threat has the potential to influence elections, incite violence, and destabilize societies by eroding trust in institutions and media. India, with its diverse and complex socio-political landscape, is particularly susceptible to AI-driven misinformation. The spread of fake news or inflammatory content could lead to communal unrest, political instability, and even violent conflict.

4. Targeted AI-Driven Attacks on Critical Infrastructure

AI can be used to identify vulnerabilities in critical infrastructure, such as power grids, water supply systems, and transportation networks. AI-enhanced cyber-attacks on these systems could lead to catastrophic failures, disrupting essential services and endangering lives. Experimental studies have explored how criminals might use generative AI for planning and implementing ransomware attacks.[13] AI-driven techniques could enhance the sophistication and impact of ransomware campaigns.

India's critical infrastructure, much of which is outdated and vulnerable, could be a prime target for such attacks. The National Critical Information Infrastructure Protection Centre (NCIPC) and National Cyber Coordination Centre (NCCC) remain underutilized.[14] India ranks third globally in cyber-attacks, accounting for 8 percent of ransomware detections.[15] A successful AI-driven attack on India's power grid or transportation system could cripple the economy and cause widespread panic and chaos.

LEGAL FRAMEWORK FOR COMBATING CYBER TERRORISM IN INDIA

[10] Supra note 8.
[11] Supra note 10.
[12] Supra note 10.
[13] F. Teichmann, "Ransomware attacks in the context of generative artificial intelligence—an experimental study," Int. Cybersecurity Law Rev., vol. 4, no. 4, pp. 399–414, 2023.
[14] Supra note 10.
[15] Supra note 10.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

India's legal framework for combating cyber terrorism is built upon a combination of national legislation, regulations, and policy initiatives. These laws aim to address the various aspects of cyber terrorism, ranging from prevention and detection to prosecution and punishment. However, the rapid evolution of cyber threats, especially with the advent of AI-enhanced cyber terrorism, poses significant challenges to this legal framework.

1. **The Information Technology Act, 2000**

"The Information Technology Act (ITA) is the primary legislation in India that addresses various cybercrimes, including hacking, identity theft, and online fraud. It provides legal provisions to deal with offenses related to unauthorized access, data theft, identity theft, and financial fraud committed through electronic means."[16] Key provisions relevant to cyber terrorism include:

- **Section 66F: Punishment for Cyber Terrorism**

This section specifically addresses cyber terrorism, defining it as any act done with intent to threaten the unity, integrity, security, or sovereignty of India, or to strike terror among people by disrupting or attempting to disrupt essential services, causing or likely to cause death, injury, or extensive damage.

Penalties: Offenses under Section 66F are punishable with life imprisonment, reflecting the seriousness with which India views cyber terrorism.

- **Section 69: Power to Issue Directions for Interception or Monitoring of Information**

This section grants the government the authority to monitor and intercept communications to safeguard national security. It is a crucial tool in detecting and preventing cyber terrorism. However, the broad powers granted under this section have raised concerns about privacy and potential misuse.

- **Section 70: Protected Systems**

Section 70 designates critical information infrastructure (CII) as "protected systems." Unauthorized access to these systems is punishable with imprisonment and fines. This provision aims to safeguard vital national infrastructure from cyber terrorist attacks.

2. **The Indian Penal Code (IPC), 1860**

The IPC, though not specifically designed to address cyber terrorism, contains provisions that can be applied to cyber terrorist activities:

[16] The Information Technology Act, 2000 (Act No. 21 of 2000).

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

- **Section 121: Waging, Attempting to Wage War, or Abetting Waging of War Against the Government of India**

This section criminalizes acts of war against the state, which can include acts of cyber terrorism intended to destabilize the government.

- **Section 124A: Sedition**

Although controversial, this section could be invoked in cases where cyber terrorism involves incitement against the government through online platforms.

Sections such as 419[17], 420[18] and 468[19] are also commonly used to prosecute cases involving online fraud and identity theft.

3. Information Technology (Amendment) Act, 2008

The Information Technology (Amendment) Act, 2008[20] is a significant piece of legislation in India's legal framework aimed at addressing the evolving challenges in the digital and cyber domains. This amendment to the original Information Technology Act, 2000, was introduced to strengthen the legal provisions related to cybersecurity, data protection, and cybercrime, in response to the rapid technological advancements and the growing incidence of cybercrimes.

Key Provisions of the IT (Amendment) Act, 2008

a. Introduction of New Cyber Crimes

The amendment introduced several new cybercrimes that were not adequately covered under the original IT Act, 2000. These include:

- **Cyber Terrorism (Section 66F):** The amendment defined and criminalized cyber terrorism, which involves using computer systems, networks, or resources to commit acts that threaten the sovereignty, integrity, or security of India or cause fear among the public.[21]
- **Identity Theft (Section 66C):** The unauthorized use of another person's identity, such as passwords or other unique identification features, is criminalized under this section.[22]
- **Phishing and Fraud (Section 66D):** The Act addresses cheating and fraud by impersonation using computer resources, commonly referred to as phishing.[23]

[17] Indian Penal Code, 1860, Section 419 Cheating by personation.
[18] Indian Penal Code, 1860, Section 420 Cheating and dishonestly inducing delivery of property.
[19] Indian Penal Code, 1860, Section 468 Forgery for the purpose of cheating.
[20] The Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009).
[21] NAGARATHNA. A, CYBER-CRIMES AND INDIAN LEGAL REGULATORY FRAMEWORK – A REVIEW, Rostrum's Law Review, Volume VI Issue I
[22] Ibid

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

- **Child Pornography (Section 67B):** The distribution, transmission, or publishing of child pornography or sexually explicit material depicting children is specifically criminalized.[24]

b. Data Protection and Privacy

Section 43A: The amendment introduced this section to address issues related to data protection. It mandates that companies handling sensitive personal data implement reasonable security practices to protect such data. If a company fails to do so and causes wrongful loss or gain to any person, it is liable to pay compensation.[25]

Section 72A: This section deals with the breach of confidentiality and privacy. It penalizes the disclosure of personal information by any service provider without the consent of the person concerned, especially when the information is obtained under a lawful contract.[26]

c. Intermediary[27] Liability

Section 79: The amendment redefined the liability of intermediaries, such as internet service providers, social media platforms, and other entities that facilitate online communication. Under this section, intermediaries are generally exempt from liability for third-party content hosted on their platforms, provided they follow due diligence guidelines and remove any offending content upon receiving actual knowledge of its illegality.

d. Digital Signatures and Authentication

The amendment replaced the term "digital signature" with "electronic signature" to broaden the scope of electronic authentication methods recognized under the law. This change aimed to accommodate the evolving technologies in electronic authentication and validation.

Section 10A: This section was introduced to grant legal recognition to electronic contracts. It ensures that contracts formed through electronic means are legally valid and enforceable.[28]

e. E-Governance and E-Commerce

The amendment also made provisions to promote e-governance and e-commerce by recognizing electronic records and digital signatures in governmental and commercial transactions.

f. Establishment of Adjudicating Officers and Cyber Appellate Tribunal

[23] Ibid
[24] Ibid
[25] Ibid
[26] Ibid
[27] Ibid
[28] Supra note 23.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

The IT (Amendment) Act, 2008, strengthened the legal infrastructure for adjudicating cybercrimes by establishing adjudicating officers who have the authority to handle cases related to contraventions of the Act. It also reinforced the role of the Cyber Appellate Tribunal, which was set up to handle appeals against decisions of the adjudicating officers.[29]

g. Strengthening of Law Enforcement Powers

The amendment granted additional powers to law enforcement agencies, allowing them to intercept, monitor, and decrypt information in the interest of national security, public order, or to prevent incitement to an offense. These powers, however, are subject to procedural safeguards to prevent misuse.[30]

In addition to enacting specialized legislation to address cyber-crimes, the Government of India and various State Governments have implemented several additional measures to combat this issue. Dedicated cyber-crime units and police stations have been established to specifically investigate cyber-related offenses. Furthermore, the Central Bureau of Investigation (CBI) has created a specialized framework to oversee cyber-crimes, which includes the establishment of the Cyber Crime Investigation Cell and the Cyber Forensics Laboratory.[31]

4. National Cyber Security Policy, 2013

The National Cyber Security Policy, 2013[32], was introduced to create a framework for securing cyberspace in India. The policy aims to protect information, information infrastructure, and devices from cyber threats and attacks, including cyber terrorism.

Objectives:

- Strengthening the legal and regulatory framework for cybersecurity.
- Promoting public-private partnerships for enhancing cyber resilience.
- Developing indigenous technologies for cybersecurity.

Limitations:

- The policy is considered outdated and does not adequately address the rapid advancements in cyber threats, particularly AI-enhanced cyber terrorism.
- There is a need for an updated policy that incorporates current technologies and evolving threats.

5. Cybersecurity Guidelines by CERT-In[33]

[29] Supra note 22.
[30] Supra note 22.
[31] Supra note 23.
[32] The National Cyber Security Policy, 2013

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

The Indian Computer Emergency Response Team (CERT-In) issues guidelines and advisories to enhance cybersecurity across sectors. While these guidelines are not legally binding, they play a crucial role in mitigating cyber threats.

Role in Combating Cyber Terrorism:

- CERT-In's advisories often include specific measures to counteract cyber terrorism, such as securing critical infrastructure and responding to cyber incidents.
- CERT-In also coordinates incident responses at the national level, making it a key player in India's cybersecurity landscape.

6. The Unlawful Activities (Prevention) Act (UAPA), 1967

The UAPA is India's primary anti-terrorism law and has been amended to include cyber terrorism within its ambit:

Section 15: Terrorist Act

The definition of a "terrorist act" under UAPA is broad and can include acts of cyber terrorism, such as disrupting critical infrastructure or spreading terror through digital means.[34] The UAPA's provisions can be used to prosecute individuals or groups involved in cyber terrorist activities, enhancing the legal framework's capacity to address such threats.

7. Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime, also known as the Convention on Cybercrime, is the first international treaty aimed at addressing internet and computer crime by enhancing cooperation among nations. It was opened for signature on November 23, 2001, in Budapest and serves as a legal framework allowing practitioners from different countries to share experiences and cooperate effectively in combating cybercrime.

"India is not a signatory to the Budapest Convention on Cybercrime. However, the convention serves as a global legal framework for cybercrime cooperation, promoting international cooperation, harmonization of laws, and mutual legal assistance in investigating and prosecuting cybercrimes."[35]

CHALLENGES IN INDIA'S LEGAL FRAMEWORK

[33] Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India
[34] The Unlawful Activities (Prevention) Act (UAPA), 1967
[35] Council of Europe, Convention on Cybercrime, ETS No. 185.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

The integration of AI into cyber terrorism introduces complex challenges that expose significant gaps in India's legal framework. While existing laws like the Information Technology Act, 2000, provide a foundation, they are not fully equipped to handle the nuances of AI-driven threats.

i. **Outdated Legislation:** The IT Act and related laws were designed for traditional cyber threats and do not address AI-specific issues such as autonomous attacks or deep fakes. The rapid evolution of AI outpaces legislative updates, creating vulnerabilities that cyber terrorists can exploit.
ii. **Attribution and Accountability:** AI-enhanced attacks are difficult to trace, complicating the process of assigning liability. Existing laws do not clearly define how to attribute AI-driven attacks, making prosecution challenging.
iii. **Lack of AI-Specific Regulations:** India lacks comprehensive regulations for the ethical and secure use of AI, particularly in the context of cybersecurity. Without clear guidelines, the potential misuse of AI in cyber terrorism remains unaddressed, leaving a regulatory vacuum.
iv. **Intermediary Liability and Content Regulation:** Current laws do not fully cover the regulation of AI-generated content like deep fakes, which can be used for misinformation. The rapid creation and dissemination of harmful AI-generated content are difficult to control under existing regulations.
v. **Privacy vs. Security Dilemma:** The broad surveillance powers granted under current laws often conflict with privacy rights, especially when AI is used in surveillance. Balancing national security with privacy concerns becomes more complex as AI capabilities grow.
vi. **International Collaboration and Jurisdictional Issues:** India's legal framework is primarily national, with limited provisions for international cooperation in AI-related cyber terrorism cases. Jurisdictional issues complicate the investigation and prosecution of cross-border AI-enhanced cyber-attacks.

RECOMMENDATIONS FOR STRENGTHENING RESPONSE AGAINST AI-ENHANCED CYBER TERRORISM

i. **Update and Expand Legislation:** Amend the IT Act to include AI-specific provisions, addressing issues like AI-driven attacks and autonomous systems. A more adaptive legal framework that can better handle AI-enhanced cyber threats.
ii. **Develop AI-Specific Cybersecurity Regulations:** Establish clear guidelines for AI use in cybersecurity, focusing on ethical development, accountability, and risk management. Responsible AI innovation with mitigated risks in cybersecurity.
iii. **Enhance Attribution Mechanisms:** Invest in technologies and international cooperation to improve attribution of AI-driven attacks. More effective prosecution and deterrence of AI-enhanced cyber terrorism.
iv. **Strengthen Intermediary Liability:** Update laws to ensure intermediaries manage AI-generated content effectively, reducing the spread of harmful material. A more robust digital ecosystem with better control over AI-driven threats.

v. **Balance Privacy and Security:** Create legal guidelines for AI surveillance, ensuring security measures do not infringe on privacy. A balanced approach that protects both security and civil liberties.

vi. **Promote International Collaboration:** Engage in international agreements focused on AI and cyber terrorism to address jurisdictional challenges. Enhanced global cooperation in combating AI-enhanced cyber terrorism.

CONCLUSION

AI-enhanced cyber terrorism represents a significant and evolving threat that challenges India's current legal framework. While existing laws such as the Information Technology Act provide a foundation, they are insufficient to address the complexities introduced by AI-driven cyber threats. The gaps in legislation, particularly concerning AI-specific regulations, attribution challenges, and the balance between privacy and security, highlight the urgent need for reform.To effectively combat AI-enhanced cyber terrorism, India must proactively update its legal framework, incorporating AI-specific provisions and strengthening cybersecurity regulations. Enhancing attribution mechanisms and ensuring that intermediary liability laws account for AI-generated content are also crucial steps. Additionally, fostering international collaboration is essential to address the cross-border nature of these threats. By addressing these gaps and implementing the recommended reforms, India can better safeguard its national security while protecting individual rights. A comprehensive and adaptive legal approach will not only enhance India’s preparedness against AI-enhanced cyber terrorism but also set a global example in managing the emerging risks associated with AI in cyberspace.

References

[1] S. R. Sindiramutty, “Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence,” *Taylors Univ. Subang Jaya Malaysia*, 2023, [Online]. Available: http://arxiv.org/abs/2401.00286

[2] R. Debbarma, “The Legal Framework And Challenges In Prosecuting Cybercrimes Including Hacking , Identity Theft , And Online Fraud,” *Res Mil.*, vol. 13, 2023.

[3] M. Nadji, “The role of artificial intelligence in combating cyber terrorism.,” *Ius Sci.*, vol. 2, no. 9, pp. 211–227, 2023, doi: 10.12795/iestscientia.2023.i02.10.

[4] A. Ünver, “Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights,” *Eur. Parliam. Subcomm. Hum. Rights*, no. May, 2024, doi: 10.2861/907329.

[5] F. Teichmann, “Ransomware attacks in the context of generative artificial intelligence—an experimental study,” *Int. Cybersecurity Law Rev.*, vol. 4, no. 4, pp. 399–414, 2023, doi: 10.1365/s43439-023-00094-x.

[6] A. Kawoosa, "Strengthening India's Defense: Assessing Legal Frameworks for Cyber Warfare Preparedness and Overcoming Challenges," *burnishedlawjournal.in*, vol. 5, no. 2, 2024.

[7] R. Supraja, "THE EMERGING CONCEPT OF CYBER TERRORISM IN INDIA: A DIVE INTO THE LEGAL FRAMEWORKe No Title," *Leg. Upanishad J.*, vol. 1, no. 1, pp. 13–9, 2023.