SUPREMO AMICUS

VOLUME 40 | February, 2026 ISSN 2456-9704

USE OF ARTIFICIAL INTELLIGENCE BY TERRORIST ORGANISATIONS: EMERGING THREATS TO INDIAN CYBERSECURITY AND NATIONAL SECURITY

By *Dr. Ruchi Pathak*
From *B.J.R Institute of Law, Bundelkhand University, Jhansi*

ABSTRACT

The increasing convergence of Artificial Intelligence (AI) with terrorism presents a multidimensional threat to India's national security and cybersecurity frameworks. AI's dual-use character enables terrorist organizations to exploit intelligent systems for surveillance evasion, radicalization, cyberattacks, and misinformation campaigns. This paper critically examines the emerging applications of AI by non-state actors and explores how these capabilities are transforming the nature, scale, and anonymity of terrorist operations in the Indian context. It assesses key incidents, including the use of deepfakes, AI-powered drones, and AI-enhanced malware targeting Indian critical infrastructure. The paper further identifies existing legal and institutional gaps, including the limitations of the Information Technology Act, 2000, and the absence of AI-specific legislative mechanisms. While India has initiated several policy frameworks through CERT-In, NITI Aayog, and the Digital Personal Data Protection Act, the paper argues for the urgent need to adopt a robust, anticipatory, and ethical legal architecture to govern AI deployment and mitigate its weaponization by terrorist entities. Comparative insights from jurisdictions such as the USA, Israel, and the EU highlight the importance of coordinated intelligence, legal innovation, and international cooperation in countering AI-enabled terrorism.

Keywords: Artificial Intelligence; Cybersecurity; Terrorism; National Security; Deepfakes; India; Facial Recognition; Autonomous Weapons; IT Act; AI Governance.

I. INTRODUCTION

Artificial Intelligence (AI) has emerged as one of the most transformative technologies of the 21st century, revolutionizing sectors ranging from healthcare to defence. However, the dual-use nature of AI makes it susceptible to malicious exploitation, including by non-state actors such as terrorist organizations. With the proliferation of autonomous systems, intelligent surveillance tools, and machine learning-driven malware, AI has opened a new frontier in the domain of asymmetric warfare and cyberterrorism. The sophistication and scalability enabled by AI have significantly enhanced the capacity of terrorist networks to plan, coordinate, and execute operations while remaining undetected by conventional counterterrorism frameworks.[1]

India, with its vast digital ecosystem, strategic geopolitical location, and ongoing regional security challenges, faces a heightened vulnerability to AI-assisted terrorism. The integration of AI in national security infrastructure remains at a nascent stage, and the legal regime surrounding it is underdeveloped. While India's cybersecurity strategies and national security doctrines have evolved over the years, they often fall short of addressing the complexities posed by AI-powered threats.[2]

Recent instances—such as the use of AI-enhanced drones by insurgents[3], deepfake-based propaganda

[1] I. Syllaidopoulos, K. Ntalianis & I. Salmon, "A Comprehensive Survey on AI in Counter-Terrorism and Cybersecurity: Challenges and Ethical Dimensions", *IEEE Access*, Vol. 13, 2025, pp. 112201–112222.

[2] S. Nigam, "Exploring the Impact of Artificial Intelligence on Indian National Security Dynamics", *Int'l JL Mgmt. & Human.*, Vol. 31, 2024, p. 265

[3] N. Vashishtha, "Artificial Intelligence-Assisted Terrorism: A New Era of Conflict", *Vivekananda International Foundation*, August 29, 2023, available

aimed at inciting communal tensions[4], and targeted AI-driven cyberattacks on government servers[5]—signal a shift from traditional terrorism to technologically augmented warfare. These developments call for a critical assessment of India's legal preparedness, technological resilience, and policy foresight to combat emerging threats.

This paper aims to explore the evolving use of AI by terrorist organizations and critically assess the vulnerabilities it creates for India's national security and cybersecurity framework. It further identifies legislative gaps, proposes legal and policy reforms, and evaluates international best practices that can inform India's response to this new generation of terrorism.

II. UNDERSTANDING AI & ITS MALICIOUS POTENTIAL

Artificial Intelligence (AI) refers to the ability of machines and algorithms to perform tasks that typically require human intelligence, such as decision-making, learning, problem-solving, and pattern recognition.[6] It is a broad domain encompassing technologies like machine learning (ML), natural language processing (NLP), computer vision, and robotics. While AI holds vast potential for economic development and technological advancement, its dual-use nature raises significant security and ethical concerns, especially when exploited by malicious actors.

One of the most critical features of AI is its *autonomy*—the ability to act independently without direct human input. In the context of cybersecurity and terrorism, this autonomy can be manipulated for automation of attacks, adaptive evasion from surveillance systems, and self-learning malware that evolves with its environment.[7] Terrorist groups and extremist networks are now exploring AI to improve target selection, camouflage operations, and disseminate ideologies at scale.

The malicious applications of AI are numerous and evolving. These include:

- AI-driven disinformation campaigns: Through tools such as deepfakes, AI can produce hyper-realistic but fake video or audio content, which may be used to incite communal violence, mislead authorities, or manipulate elections.[8]
- Autonomous weapon systems: Drones or robotic devices powered by AI can be programmed to carry explosives or monitor high-value targets without human oversight.[9]

at https://www.vifindia.org/article/2023/august/29/Artificial-Intelligence-assisted-Terrorism-A-New-Era-of-Conflict (last visited on Sept. 28, 2025).

[4] A. Gupta & A. Guglani, "Scenario Analysis of Malicious Use of Artificial Intelligence and Challenges to Psychological Security in India", in *Proceedings of the Malicious Use of AI and Psychological Security Conference*, Springer, 2023, pp. 195–208.

[5] MA Goffer, MS Uddin & SN Hasan, "AI-Enhanced Cyber Threat Detection and Response: Advancing National Security in Critical Infrastructure", *Journal of Cybersecurity and Critical Infrastructure*, 2025, available at https://www.researchgate.net/publication/390898054 (last visited on Sept. 28, 2025).

[6] I. Syllaidopoulos, K. Ntalianis & I. Salmon, "A Comprehensive Survey on AI in Counter-Terrorism and Cybersecurity: Challenges and Ethical Dimensions", *IEEE Access*, Vol. 13, 2025, pp. 112201–112222.

[7] PK Srivastava, BS Roohani, R Aggarwal et al., "Implementation Challenges Faced by Artificial Intelligence for National Security", in *Cyber Security*, Taylor & Francis, 2024, pp. 225–239.

[8] A. Gupta & A. Guglani, "Scenario Analysis of Malicious Use of Artificial Intelligence and Challenges to Psychological Security in India", in *Proceedings of the Malicious Use of AI and Psychological Security Conference*, Springer, 2023, pp. 195–208.

[9] N. Chitadze, "Artificial Intelligence, Terrorism, and Cyber Security: Challenges and Opportunities", in *Machine Intelligence Applications in Cyber-Risk Management*, IGI Global, 2025, pp. 161–178.

- AI-enhanced cyberattacks: Intelligent malware, phishing bots, and denial-of-service attacks can exploit vulnerabilities at faster and more devastating scales than traditional hacking.[10]
- Facial recognition spoofing: Terrorist actors may use AI to defeat biometric systems and surveillance infrastructure.[11]
- Recruitment and radicalization: AI tools are being deployed to personalize extremist content using NLP algorithms, enabling deeper psychological manipulation.[12]

As India rapidly digitizes its infrastructure under initiatives such as *Digital India* and *Smart Cities Mission*, its exposure to AI-driven threats increases. Yet, the national security and legal architecture remains under-equipped to pre-empt or mitigate such threats. In the absence of tailored legal safeguards, the proliferation of malicious AI could destabilize India's internal security and pose transnational risks.

Understanding the technological underpinnings and potential misuse of AI is therefore essential—not only for law enforcement and intelligence agencies—but also for lawmakers and civil society. A nuanced legal and policy discourse must evolve in parallel with technological advancements to ensure India's sovereignty and public safety are not compromised.

III. EMERGING TERRORIST USES OF AI

The evolving landscape of terrorism in the 21st century reflects an increasing dependence on cutting-edge technologies, with Artificial Intelligence (AI) at the core of these disruptive changes. Traditionally, terrorist groups relied on rudimentary means for communication, surveillance, and propaganda. However, the digitization of warfare and the democratization of AI tools have drastically transformed the operational capabilities of non-state actors. AI now offers them the capacity to operate with precision, anonymity, and psychological influence—characteristics that challenge conventional national security frameworks and render traditional counter-terrorism mechanisms inadequate. Terrorist organizations across the globe, including those operating in South Asia, have begun leveraging AI across various stages of the terrorist value chain: from recruitment and financing to surveillance evasion, operational coordination, and attack execution. The convergence of AI with cyber capabilities has created what experts call "intelligent terrorism"—a paradigm shift that blends algorithmic learning with human malice.[13]

Terrorist Applications of AI

1. AI-Enhanced Surveillance Evasion

AI-powered encryption and anti-surveillance tools are increasingly being used by terrorist organizations to obscure their digital footprints. By integrating machine learning algorithms into their communication channels, terrorists can identify surveillance patterns and modify their behavior in real-time. These systems may even employ adversarial AI techniques to confuse and mislead national surveillance systems.[14] Such applications

[10] MA Goffer, MS Uddin & SN Hasan, "AI-Enhanced Cyber Threat Detection and Response: Advancing National Security in Critical Infrastructure", *Journal of Cybersecurity and Critical Infrastructure*, 2025, available at https://www.researchgate.net/publication/390898054 (last visited on Sept. 29, 2025).

[11] A. Verma, "Growth of Artificial Intelligence in the Indian Legal System and Its Impact on Cyber Terrorism in India", *LawFoyer Int'l J. Doctrinal Legal Research*, Vol. 2, 2024, pp. 132–147.

[12] SF Abiade, "AI Sovereignty and Security: Governing AI-Enabled Counterterrorism in Telecom Networks in the Global South", *Journal of Engineering Technology Research and Ethics*, 2024, pp. 53–68.

[13] R. Montasari, *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*, Springer, 2023, pp. 18–27.

[14] A. Verma, "Growth of Artificial Intelligence in the Indian Legal System and Its Impact on Cyber

drastically reduce the efficacy of state-sponsored monitoring efforts, particularly in urban areas saturated with CCTV and internet traffic surveillance.

2. Facial Recognition Spoofing

Facial recognition systems—deployed in airports, border security, and urban security infrastructures—are widely used in India and globally for counter-terrorism and crime detection. However, terrorists are exploiting Generative Adversarial Networks (GANs) to create realistic facial masks or manipulate facial data to deceive these systems. This technique, known as "face morphing," has allowed operatives to cross borders or remain undetected in areas under high scrutiny.[15] The threat is compounded by the fact that open-source software required for such spoofing is freely available online, democratizing access to this powerful capability.

3. Deepfake Propaganda for Recruitment

Deepfakes represent one of the most alarming manifestations of malicious AI. Using neural networks, terrorists create fabricated video and audio content that appears authentic. These can show fake atrocities, impersonate political or religious leaders, or spread fabricated hate content designed to recruit individuals and provoke communal violence. In 2023, a fake video allegedly showing Indian security forces committing atrocities against a minority group went viral on encrypted messaging platforms and was later found to be AI-generated.[16] Such incidents highlight how deepfakes can be weaponized to destabilize societies and escalate radicalization.

4. AI-Generated Disinformation

Beyond deepfakes, terrorists are using large language models and NLP tools to produce vast amounts of believable yet false narratives, often tailored to vulnerable demographics. AI-generated fake news is pushed through botnets on social media, which learn and optimize engagement patterns to spread misinformation effectively. These campaigns are often geo-targeted to exploit ethnic, religious, or political divides in India's sensitive regions such as Jammu & Kashmir, Manipur, and the Northeast.[17] Disinformation warfare is now a low-cost, high-impact strategy in the arsenal of ideological extremists.

5. Autonomous Drones for Tactical Attacks

AI-powered unmanned aerial vehicles (UAVs), often referred to as "killer drones", are now within reach of well-funded terrorist networks. These drones can be programmed to follow, identify, and strike targets using image recognition and GPS tracking. The 2021 drone attack on the Indian Air Force base in Jammu was the first instance of drones being used by non-state actors for direct kinetic attack on Indian soil.[18] Though AI's role was not confirmed in that case, security analysts have since raised concerns about autonomous swarm drones, which can coordinate without human input using AI protocols.

Case Study: Islamic State's Use of AI Bots for Encrypted Messaging and Recruitment

Terrorism in India", *LawFoyer Int'l J. Doctrinal Legal Research*, Vol. 2, 2024, p. 139.

[15] S. Yu & F. Carroll, "Implications of AI in National Security: Understanding the Security Issues and Ethical Challenges", in *Artificial Intelligence in Cybersecurity*, Springer, 2022, pp. 115–119.

[16] A. Gupta & A. Guglani, "Scenario Analysis of Malicious Use of Artificial Intelligence and Challenges to Psychological Security in India", Springer, 2023, pp. 200–202.

[17] MA Goffer, MS Uddin & SN Hasan, "AI-Enhanced Cyber Threat Detection and Response: Advancing National Security in Critical Infrastructure", *Journal of Cybersecurity and Critical Infrastructure*, 2025, available at https://www.researchgate.net/publication/390898054 (last visited on Sept. 29, 2025).

[18] PK Srivastava, BS Roohani, R Aggarwal et al., "Implementation Challenges Faced by Artificial Intelligence for National Security", in *Cyber Security*, Taylor & Francis, 2024, p. 233.

The Islamic State (ISIS) has been a pioneer among terrorist groups in adopting digital technologies, and its ventures into AI have amplified its global threat. The group has leveraged AI-driven bots to operate autonomously on encrypted messaging platforms such as Telegram, Discord, and WhatsApp. These bots can converse in multiple languages, identify potential recruits based on behavioral profiling, and direct them to deeper layers of radicalization networks on the dark web.[19]

A 2023 report by the **International Centre for the Study of Radicalisation** documented how ISIS deployed an AI chatbot named *"Khurasani"* which engaged users in religious dialogue, answered doctrinal questions, and recommended materials based on user interest levels. The bot adjusted its tone and content dynamically, based on interaction metrics—a clear application of machine learning principles in psychological warfare.[20]

More alarmingly, these bots were integrated into broader AI-based recommendation engines that analyzed social media activity to locate vulnerable individuals. Once identified, these targets were contacted via fake profiles and drawn into radicalization pipelines. The sophistication of this system allowed ISIS to scale its reach with minimal human intervention, evading detection even on platforms with active content moderation policies.

IV. IMPACT ON INDIAN CYBERSECURITY

India's strategic ambition of becoming a digitally empowered society—through flagship programmes like *Digital India*, *Smart Cities Mission*, and *Aadhaar*—has exponentially expanded its digital surface area. While this digital transformation has enabled economic and governance gains, it has also rendered India vulnerable to cyber threats, particularly those powered by artificial intelligence (AI). The application of AI by terrorist organizations introduces complex risks to India's cybersecurity landscape.

One of the most serious threats is the use of AI-enabled tools for cyber intrusions into critical infrastructure such as power grids, hospitals, defence communication systems, and financial networks. The ransomware attack on the All India Institute of Medical Sciences (AIIMS) in 2022, which paralyzed its servers for weeks, demonstrated how India's health systems remain unprepared for sophisticated cyber threats[21]. Although attribution remained unclear, security experts suggested possible use of self-propagating malware with learning capabilities, indicating AI involvement[22].

AI also enables advanced phishing attacks and data breaches that adapt to users' behavioural patterns. Machine learning algorithms can profile targets based on social media activity and tailor malicious payloads, making attacks more effective and harder to detect[23]. Government departments—particularly those involved in defence and nuclear operations—have been frequently targeted by such AI-enhanced intrusions.

Disinformation is another major vector of concern. AI-generated fake news and deepfakes have been used to incite communal violence, particularly in volatile

[19] S. Nigam, "Exploring the Impact of Artificial Intelligence on Indian National Security Dynamics", *Int'l JL Mgmt. & Human.*, Vol. 31, 2024, p. 269.

[20] International Centre for the Study of Radicalisation, *AI and Terrorism: The Rise of Autonomous Radicalisation Tools*, ICSR Report Series, King's College London, 2023, pp. 6–12.

[21] "AIIMS Delhi servers hit by major cyberattack, 4 days of disruption", *The Hindu*, Nov. 28, 2022, available at https://www.thehindu.com/news/national/aiims-delhi-servers-hit-by-major-cyberattack/article66186033.ece (last visited Sept. 29, 2025).

[22] MA Goffer, MS Uddin & SN Hasan, "AI-Enhanced Cyber Threat Detection and Response", *Journal of Cybersecurity and Critical Infrastructure*, 2025, p. 21.

[23] I. Syllaidopoulos, K. Ntalianis & I. Salmon, "A Comprehensive Survey on AI in Counter-Terrorism and Cybersecurity", *IEEE Access*, Vol. 13, 2025, pp. 112201–112222.

regions like Kashmir and parts of Northeast India[24]. In 2023, a deepfake video purportedly showing Indian Army personnel desecrating religious symbols circulated widely on encrypted platforms before being debunked by fact-checkers[25].

AI also enables *cyber-physical attacks*, where physical infrastructure is targeted via digital means. For instance, India's railway signalling systems or air traffic control mechanisms—if infiltrated using AI-enhanced code—could be disrupted to devastating effect.

Cybersecurity threats posed by AI do not remain confined to the digital domain. They spill over into national security, diplomatic relations, and civil order. India's adversaries—both state and non-state—can exploit these vulnerabilities to erode trust in governance, sabotage military preparedness, and trigger social unrest.

V. LEGAL & POLICY RESPONSES IN INDIA

Despite growing threats, India's legal framework to regulate the malicious use of AI—especially by terrorist organizations—remains fragmented and underdeveloped. Current legal responses are reactive rather than anticipatory, and there is a notable absence of AI-specific legislation or regulatory institutions.

1. Information Technology Act, 2000

India's principal cyber law, the *Information Technology Act, 2000* (IT Act), criminalizes hacking, identity theft, and cyberterrorism under Sections 66 and 66F[26]. While these provisions provide a basic deterrent framework, they are inadequate to address advanced AI threats such as deepfakes, autonomous bots, and generative malware.

2. National Cyber Security Policy, 2013

The *National Cyber Security Policy (NCSP) 2013* recognizes the need to protect critical information infrastructure and calls for coordinated responses. However, it is outdated in its approach and does not account for AI's evolving threat matrix[27]. It lacks provisions for algorithmic accountability, ethical AI deployment, or state oversight of AI R&D.

A revised policy was proposed in 2021 but has not yet been formally enacted[28].

3. CERT-In Guidelines

The *Indian Computer Emergency Response Team* (CERT-In), under the Ministry of Electronics and Information Technology (MeitY), issues security advisories and handles cyber incident response. Its 2022 directive mandates data sharing on cyber incidents within 6 hours[29]. While this improves visibility, CERT-In has no powers to preemptively regulate AI-based technologies or enforce standards on developers.

4. Data Protection Regime

India's *Digital Personal Data Protection Act, 2023* introduces data fiduciaries and user consent norms, marking progress in privacy protection[30]. However, the Act focuses on personal data processing and does

[24] N. Vashishtha, "Artificial Intelligence-Assisted Terrorism: A New Era of Conflict", *Vivekananda International Foundation*, Aug. 29, 2023.
[25] A. Gupta & A. Guglani, "Malicious Use of Artificial Intelligence and Psychological Security in India", *Springer*, 2023, pp. 201–203.
[26] Information Technology Act, 2000, §§ 66, 66F.
[27] National Cyber Security Policy, 2013, Ministry of Electronics & IT, Government of India.
[28] Debashis Panda, "Revised Cyber Security Policy Drafted: Awaiting Approval", *The Economic Times*, Dec. 18, 2021.
[29] CERT-In Directions on Cybersecurity Incidents, 28 April 2022, available at https://www.cert-in.org.in (last visited Sept. 29, 2025).
[30] Digital Personal Data Protection Act, 2023, Gazette Notification, Government of India.

not address non-personal data, AI decision-making transparency, or deepfake criminalization.

The Supreme Court's judgment in *Justice K.S. Puttaswamy v. Union of India* recognized privacy as a fundamental right, reinforcing the need for strong surveillance safeguards[31]. Yet, the judgment did not provide operational guidance for AI governance.

5. Institutional Gaps

India lacks:

- An AI regulatory body akin to the EU's AI Office or U.S. NIST AI Framework.
- AI-specific guidelines for counterterrorism agencies.
- Coordination protocols between intelligence, judiciary, and technology regulators.

While NITI Aayog's *National Strategy on AI (AIM)* addresses innovation and ethics, it is non-binding and policy-driven, not legislative[32].

6. International Cooperation

India is a member of several global forums on cybercrime and AI ethics, such as the Global Partnership on AI (GPAI). However, its counterterrorism agreements with neighboring countries rarely incorporate AI-specific clauses[33].

VI. CONCLUSION

The integration of Artificial Intelligence into terrorist operations presents a formidable challenge to India's cybersecurity and national security architecture. From AI-driven surveillance evasion and deepfake propaganda to autonomous drones and disinformation warfare, terrorist groups are increasingly leveraging sophisticated technologies to amplify their impact. India's existing legal and policy frameworks, while evolving, remain insufficient to address the rapidly changing threat landscape. A proactive, multi-stakeholder approach—combining legislative reform, institutional strengthening, international cooperation, and ethical AI governance—is essential to safeguard national interests and ensure resilient digital sovereignty in the face of AI-augmented terrorism.

REFERENCES

1. I. Syllaidopoulos, K. Ntalianis & I. Salmon, "A Comprehensive Survey on AI in Counter-Terrorism and Cybersecurity: Challenges and Ethical Dimensions", *IEEE Access*, Vol. 13, 2025, pp. 112201–112222.
2. MA Goffer, MS Uddin & SN Hasan, "AI-Enhanced Cyber Threat Detection and Response: Advancing National Security in Critical Infrastructure", *Journal of Cybersecurity and Critical Infrastructure*, 2025, available at https://www.researchgate.net/publication/390898054 (last visited on Sept. 29, 2025).
3. A. Gupta & A. Guglani, "Scenario Analysis of Malicious Use of Artificial Intelligence and Challenges to Psychological Security in India", in *Proceedings of the Malicious Use of AI and Psychological Security Conference*, Springer, 2023, pp. 195–208.
4. N. Vashishtha, "Artificial Intelligence-Assisted Terrorism: A New Era of Conflict", *Vivekananda International Foundation*, 29 August 2023, available at https://www.vifindia.org/article/2023/august/29/Artificial-Intelligence-assisted-Terrorism-A-New-Era-of-Conflict (last visited on Sept. 29, 2025).
5. A. Verma, "Growth of Artificial Intelligence in the Indian Legal System and Its Impact on Cyber Terrorism in India", *LawFoyer Int'l J. Doctrinal Legal Research*, Vol. 2, 2024, pp. 132–147.

[31] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

[32] NITI Aayog, "National Strategy for Artificial Intelligence – #AIForAll", 2018, available at https://www.niti.gov.in (last visited Sept. 29, 2025).

[33] K. Srivastava, "Artificial Intelligence and National Security: Perspective from the Global South", *Int'l JL Changing World*, Vol. 2, 2023, pp. 175–182.

6. PK Srivastava, BS Roohani, R. Aggarwal et al., "Implementation Challenges Faced by Artificial Intelligence for National Security", in *Cyber Security*, Taylor & Francis, 2024, pp. 225–239.
7. S. Yu & F. Carroll, "Implications of AI in National Security: Understanding the Security Issues and Ethical Challenges", in *Artificial Intelligence in Cybersecurity*, Springer, 2022, pp. 110–121.
8. S. Nigam, "Exploring the Impact of Artificial Intelligence on Indian National Security Dynamics", *Int'l JL Mgmt. & Human.*, Vol. 31, 2024, pp. 265–272.
9. K. Srivastava, "Artificial Intelligence and National Security: Perspective from the Global South", *Int'l JL Changing World*, Vol. 2, 2023, pp. 175–182.
10. R. Montasari, *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*, Springer, 2023, pp. 18–27.
11. CERT-In, "Directions on Cybersecurity Incident Reporting", Ministry of Electronics & IT, 28 April 2022, available at https://www.cert-in.org.in (last visited on Sept. 29, 2025).
12. Ministry of Electronics & Information Technology (MeitY), *National Cyber Security Policy*, Government of India, 2013.
13. Debashis Panda, "Revised Cyber Security Policy Drafted: Awaiting Approval", *The Economic Times*, 18 December 2021.
14. Government of India, *Digital Personal Data Protection Act*, 2023, Gazette Notification.
15. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
16. NITI Aayog, "National Strategy for Artificial Intelligence – #AIForAll", Government of India, 2018, available at https://www.niti.gov.in (last visited on Sept. 29, 2025).
17. International Centre for the Study of Radicalisation, *AI and Terrorism: The Rise of Autonomous Radicalisation Tools*, King's College London, ICSR Report, 2023, pp. 6–12.
18. "AIIMS Delhi Servers Hit by Major Cyberattack, 4 Days of Disruption", *The Hindu*, 28 November 2022, available at https://www.thehindu.com/news/national/aiims-delhi-servers-hit-by-major-cyberattack/article66186033.ece (last visited on Sept. 29, 2025).

*****