Page 1764 - 1778 **DOI:** *https://doij.org/10.10000/IJLMH.119792*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Artificial Intelligence in the Cyber Battlefield: Legal Challenges in Liability, Attribution, and Forensic Evidence

PRAVEEN ARYA[1]

ABSTRACT

Artificial Intelligence (AI) is rapidly reshaping the nature and intensity of cyber threats, enabling attackers to launch autonomous, adaptive, and anonymised digital assaults across jurisdictions. The rise of intelligent malware, algorithmic disinformation, and self-evolving cyber intrusions has introduced unprecedented complexity into legal doctrines of attribution, liability, and evidence. This paper critically examines the legal challenges emerging from the use of AI in cyberwarfare, particularly in the Indian context. It explores whether traditional principles of tort law and statutory cyber regulation are equipped to handle scenarios where harm is caused by autonomous systems rather than human actors. The evidentiary and forensic difficulties in identifying perpetrators, preserving digital integrity, and establishing intent in such cases are analysed in light of existing laws such as the Information Technology Act, 2000 and the Indian Evidence Act, 1872. Through doctrinal study, real-world illustrations, and comparative analysis with international frameworks including the Tallinn Manual, the EU AI Act, and United States cybersecurity policy, this research proposes reforms in legal structure, evidentiary standards, and institutional architecture. It concludes that India's preparedness for AI-enabled cyber warfare remains doctrinally underdeveloped and institutionally fragmented, necessitating urgent legal innovation and forensic modernisation to uphold digital sovereignty and the rule of law in the algorithmic era.

I. INTRODUCTION

Artificial Intelligence (AI) is no longer a futuristic abstraction but a present-day reality with profound implications across legal, economic, and security domains. In the digital age, AI has transcended its foundational role as a tool of optimisation or automation and has emerged as a potent instrument in the conduct of cyber operations, including cybercrime, cyber espionage, and even cyberwarfare. Its integration into offensive digital capabilities has significantly altered the nature, scale, and attribution of cyberattacks, enabling acts that are autonomous, evasive, and often legally untraceable. These developments have created a new dimension of

[1] Author is a LL.M. Student at IILM University, Greater Noida, India.

 [ISSN 2581-5369]

technological threat—one that disrupts not only data systems but also the foundations of existing legal doctrine.

AI's ability to learn, adapt, and self-execute commands allows malicious actors to deploy sophisticated digital assaults without requiring continuous human intervention. Unlike conventional cybercrimes which can often be traced back to a user's intent or command, AI-driven attacks may be carried out by systems that have been trained to evolve and act based on environmental data or self-generated outputs. This complicates the application of traditional legal concepts such as intent, foreseeability, and direct causation. The growing reliance on AI in cyberattacks also introduces novel questions about attribution in international law, particularly when the source of an attack is obscured by proxy systems or distributed networks that operate across multiple jurisdictions. In this environment, the legal response cannot rely on static norms or procedural templates developed for an earlier technological age[2].

The Indian legal framework, while progressive in certain areas of cyber regulation, remains predominantly grounded in the Information Technology Act, 2000, which does not envisage the legal complexities introduced by autonomous or semi-autonomous AI systems[3]. Issues of liability for AI-driven harm, whether in civil or criminal contexts, remain unresolved. Similarly, the Indian Evidence Act, 1872, though amended in part to accommodate digital records, lacks specificity in addressing the evidentiary challenges posed by self-altering or opaque AI-generated data[4]. These statutory limitations, coupled with institutional fragmentation among enforcement agencies, have resulted in an underprepared legal infrastructure to deal with the realities of AI-enabled cyber threats.

From a forensic standpoint, the use of AI in cyberattacks presents acute challenges in evidence preservation, admissibility, and chain of custody. Forensic tools and protocols developed to track traditional cyber intrusions often fall short when dealing with algorithmically generated attacks that leave no static logs, use generative adversarial networks to simulate legitimate behaviour, or autonomously delete traces of intrusion[5]. The problem is further exacerbated in the context of cross-border data flows, where legal and procedural cooperation between states is often slow, incomplete, or non-existent.

This paper seeks to examine these emerging challenges through a doctrinal and comparative

[2] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 4–8 (Michael N. Schmitt ed., Cambridge Univ. Press 2017).
[3] Information Technology Act, No. 21 of 2000, § 66, India Code (2000).
[4] Indian Evidence Act, No. 1 of 1872, § 65B, India Code (1872).
[5] See Nat'l Inst. of Standards & Tech., AI Risk Management Framework 1.0 (2023), https://www.nist.gov/itl/ai-risk-management-framework.

 [ISSN 2581-5369]

analysis of liability, attribution, and forensic norms applicable to AI-induced cyber threats. It evaluates the extent to which Indian legal systems are equipped to address the disruptive convergence of AI and cyber operations. The study draws upon international developments such as the Tallinn Manual on the International Law Applicable to Cyber Operations[6], the European Union's Artificial Intelligence Act[7], and institutional practices in the United States, to suggest reformative strategies for Indian law. Rather than treat AI merely as a technological upgrade to existing systems, the research recognises it as a paradigm shift in the nature of cyber conflict, requiring a recalibration of legal assumptions, investigative tools, and institutional priorities.

In doing so, the paper contributes to the urgent discourse on digital sovereignty, the rule of law in cyberspace, and the future of AI governance within the legal and constitutional framework of India.

II. ARTIFICIAL INTELLIGENCE AND THE EVOLUTION OF CYBER THREATS

The application of Artificial Intelligence to cyber operations has fundamentally altered the strategic and technical landscape of digital threats. Traditional cyberattacks typically require continuous human direction, rely on known exploit patterns, and are limited by the attacker's operational knowledge. In contrast, AI-driven attacks leverage machine learning, pattern recognition, and autonomous decision-making to launch adaptive, unpredictable, and self-modifying assaults[8]. These systems are capable of learning from target behaviours, bypassing conventional security measures, and reconfiguring themselves in real time. This significantly challenges detection, defence, and legal classification.

AI is not a monolithic tool but a spectrum of technologies that include natural language processing, neural networks, computer vision, and generative models. Each of these has found deployment in the cyber battlefield. For instance, deep learning algorithms can be used to craft spear-phishing messages that mimic legitimate communication styles, making them harder to detect. Generative adversarial networks (GANs) can create convincing deepfakes that undermine trust in digital evidence or public discourse. Reinforcement learning models have been used to train malware to avoid endpoint detection systems by simulating environments and adapting to defensive triggers.

The use of such technologies raises serious concerns about attribution and traceability. In

[6] *Tallinn Manual 2.0*, supra note 1.
[7] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final.
[8] Nat'l Inst. of Standards & Tech., *AI Risk Management Framework 1.0* (2023), https://www.nist.gov/itl/ai-risk-management-framework [hereinafter NIST AI RMF].

several cases, AI-based intrusions have been routed through decentralised botnets, anonymised via blockchain-based infrastructure, or embedded within commonly used digital tools. This makes the identification of the originator of the attack legally uncertain, whether it is a state, a non-state actor, or an autonomous agent. Without a clear attribution, the invocation of legal remedies, both at the domestic and international level, becomes nearly impossible. The Tallinn Manual has attempted to codify principles of state responsibility and attribution in cyber operations. However, even it acknowledges the inadequacy of current international law in addressing AI-based attacks where no identifiable human actor or sovereign directive exists.

A further complication arises from the increasing availability of AI tools in the open-source domain. Threat actors no longer need to develop proprietary algorithms or invest in advanced computing infrastructure. Publicly available AI models, repurposed generative software, and dark web marketplaces now enable low-cost, high-impact cyber offensives that can be scaled and deployed with little traceability. This democratisation of AI-powered cyber weaponry broadens the threat landscape, making it more volatile, asymmetrical, and legally ambiguous.

India, like many jurisdictions, remains vulnerable to these developments. Incidents such as the "Dance of the Hillary"[9] malware campaign, which reportedly used a malicious AI-enhanced payload disguised as a media file, illustrate how easily digital users can be manipulated and compromised. Although such examples serve as warnings, the broader lesson lies in recognising that the very nature of digital warfare is undergoing transformation. It is not merely the tools of attack that are changing, but also the actors, objectives, and modes of execution. The intersection of AI and cyber operations represents a shift from manual intrusion to algorithmic dominance. The rules of engagement and principles of legal accountability, however, remain largely undefined.

This transformation necessitates not only technological countermeasures, but legal reform that is equally sophisticated. A reactive approach rooted in static legislation cannot suffice. The law must anticipate and respond to the evolving contours of digital threats driven by AI capabilities. If it fails to do so, it risks becoming irrelevant in the face of dynamic, decentralised, and intelligent systems.

[9] Bhavya Bagga, 'Dance of the Hillary' Malware Targets Indian Users via Messaging Apps, APAC News Network (May 9, 2025), https://apacnewsnetwork.com/2025/05/dance-of-the-hillary-malware-targets-indian-users-via-messaging-apps/.

 [ISSN 2581-5369]

III. LEGAL ATTRIBUTION AND RESPONSIBILITY IN AI-BASED CYBER OPERATIONS

A. Challenges of Attribution in International Law

One of the most pressing challenges in the legal analysis of AI-enabled cyber operations is the issue of attribution. In conventional cybercrime, investigators often rely on digital footprints, IP tracking, or behavioural analysis to link an act to an individual or a group. However, when artificial intelligence is deployed to execute or even initiate the attack, the question of agency becomes significantly more complex. Unlike human-led offences, where culpability can be established through intent, knowledge, and participation, AI systems may act independently based on pre-set parameters, self-learning inputs, or environmental triggers. This detachment from direct human command presents a substantial obstacle to both civil and criminal attribution.

In the context of international law, attribution is primarily governed by customary norms, including those encapsulated in the Articles on Responsibility of States for Internationally Wrongful Acts, and increasingly referenced in the Tallinn Manual[10]. These principles require that a wrongful act must be committed by an organ of the state or by persons or groups acting under its direction or control. However, when the offensive act is committed by an AI agent operating with a degree of autonomy, it may fall outside the traditional definitions of state control, particularly if the origin is anonymised through decentralised networks or if the AI evolves in ways unintended by its initial programmers.

B. Doctrinal Gaps in Domestic Cyber Legislation

In domestic legal systems, including India, the difficulty is compounded by the absence of legislation that clearly addresses responsibility for harm caused by intelligent systems. The Information Technology Act, 2000 focuses on offences committed by "persons" using computer resources, but does not define whether liability can be extended to those who develop or deploy autonomous systems that later commit harmful acts[11]. The lack of clarity around whether such systems should be treated as tools, co-agents, or independent legal entities has generated substantial theoretical debate but little legislative guidance.

C. Tortious and Vicarious Liability for AI-Induced Harm

Tort law, while historically adaptable, is also tested by the rise of autonomous systems. In negligence claims, the standard of care and foreseeability of harm are critical components. However, with AI, the notion of foreseeability becomes fluid. A developer may not have

[10] *Tallinn Manual*, supra note 1
[11] Information Technology Act, supra note 2

 [ISSN 2581-5369]

anticipated specific outcomes generated by an evolving algorithm, especially where reinforcement learning or unsupervised data modelling is involved[12]. This raises the question of whether strict liability principles should be invoked, placing responsibility on those in control of the system, regardless of fault. Alternatively, courts may explore product liability doctrines, particularly in scenarios where AI systems are embedded in commercial goods or services. Yet such analogies may not apply cleanly to software-only models or decentralised deployments.

In Indian jurisprudence, where the concept of vicarious liability is well-established, an argument could be made for extending liability to those who operate or benefit from AI systems, even if they are not the direct perpetrators of the cyber offence. However, this would require judicial innovation or statutory amendment, as current frameworks do not account for scenarios where the actus reus is committed by a non-human, autonomous agent. Furthermore, establishing mens rea in such cases becomes problematic, as the mental element necessary for criminal liability is absent in machines, and attributing it to a human actor may require a degree of proximity or foreseeability that is not always present.

D. Comparative Legal Developments and Indian Scope for Reform

Comparative legal systems offer useful illustrations. In the United States, some courts have begun to grapple with the notion of algorithmic accountability, particularly in the context of discrimination or automated decision-making[13]. The European Union's draft Artificial Intelligence Act, although regulatory in nature, recognises the layered responsibility of developers, deployers, and users in AI-based harms[14]. It further categorises certain applications of AI as "high-risk," mandating strict compliance and transparency protocols.

These unresolved issues suggest that existing legal tools in India are inadequate to address the unique nature of AI-driven cyber threats. Attribution, both for state and individual responsibility, must evolve beyond human-centric models and recognise the complex interplay between coding intent, autonomous operation, and downstream harm. Failure to reform these frameworks risks leaving victims without remedy and enabling malicious actors to exploit the legal ambiguity surrounding AI deployment in cyberspace.

[12] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 143–45 (Harv. Univ. Press 2018)
[13] See Andrew D. Selbst, Disparate Impact in Big Data Policing, 52 Ga. L. Rev. 109 (2017)
[14] European Commission, *Proposal for a Regulation on Artificial Intelligence*, COM (2021) 206 final, at 6–7

 [ISSN 2581-5369]

IV. FORENSIC CHALLENGES IN AI-POWERED CYBER INCIDENTS

A. Chain of Custody and Evidentiary Integrity

The integration of artificial intelligence into cyberattacks has created complex challenges in the domain of digital forensics. Unlike conventional cyber intrusions, which typically involve traceable activity by identifiable users, AI-powered attacks often leave behind fragmented or deliberately obfuscated trails. These challenges are not merely technical but also legal, as they directly impact the ability of enforcement agencies to collect, preserve, authenticate, and present evidence in a manner that is admissible in court.

At the core of digital forensics lies the principle of the chain of custody, which ensures that evidence collected from a digital environment remains untampered from the point of seizure to presentation in court. In AI-enabled intrusions, however, the source code, command instructions, and attack patterns may be generated dynamically by the system itself, without a pre-coded signature or predictable behaviour. Some AI-driven malwares are designed to self-destruct or erase logs once a task is executed. Others may modify timestamps, inject false entries, or mimic legitimate user activity to confuse forensic tools. These features severely limit the reliability of evidence retrieved after the incident and raise doubts about its authenticity.

B. Admissibility Issues under the Indian Evidence Act

The Indian Evidence Act, 1872, as amended to accommodate electronic records, requires that digital evidence be accompanied by proper certification under Section 65B. While this provision addresses the procedural aspect of admissibility, it does not deal with the more foundational question of evidentiary integrity in an AI context. When AI systems can autonomously generate, manipulate, or erase information, the traditional methods of hash verification, log correlation, and metadata analysis become unreliable. This creates a risk of evidence being challenged not only on technical grounds but also on legal presumptions regarding its source, continuity, and reliability.

C. Institutional Limitations in Digital Forensics

Moreover, the scale and complexity of AI-generated data complicate forensic analysis. A single AI agent may interact with multiple systems, extract massive datasets, and execute parallel operations, each leaving behind a unique trace. In such cases, forensic investigators must differentiate between primary and secondary artefacts, establish causation chains, and link activities to specific outcomes. These requirements are difficult to meet in high-velocity

 [ISSN 2581-5369]

environments where logs are overwritten, systems rebooted, or external nodes involved in the attack are located in foreign jurisdictions. The volatility of evidence in such scenarios makes it vulnerable to contamination, inadvertent deletion, or legal inadmissibility.

Institutional limitations further aggravate the situation. While central agencies such as the Computer Emergency Response Team (CERT-In), the National Critical Information Infrastructure Protection Centre (NCIIPC), and the cyber forensics units of the Central Bureau of Investigation and Enforcement Directorate possess baseline capabilities, these are often inadequate for real-time AI attribution and analysis[15]. State-level agencies, which are frequently the first responders in cyber incidents, lack the expertise, equipment, or legal clarity to preserve evidence from sophisticated AI-driven threats. The absence of standardised protocols for handling AI-generated logs or models during seizure further increases the margin for procedural error.

D. Global Trends in AI Forensic Readiness

International developments highlight the urgency of reform. For example, the European Union's Cybersecurity Act[16] and the United States National Institute of Standards and Technology (NIST) have begun drafting technical frameworks for AI-related forensic readiness. These include standards for the logging of machine decisions, the forensic auditability of algorithmic processes, and the creation of immutable logs that cannot be altered by the AI system itself. Such measures are designed to enhance both traceability and evidentiary validity in digital environments influenced by artificial intelligence.

India has yet to adopt a comparable framework. Although amendments to the Information Technology Act and procedural codes have addressed certain aspects of electronic evidence, there remains a vacuum in the context of AI-specific forensics. Without clear legal provisions, investigators, prosecutors, and courts must rely on generalised assumptions about the integrity and reliability of digital traces. This is an increasingly untenable position as AI becomes more sophisticated and capable of outmanoeuvring legacy forensic techniques.

To ensure the rule of law in the digital domain, India must prioritise the development of AI-aware forensic protocols, backed by statutory recognition and institutional support. These should include legal guidelines for the seizure and preservation of AI-generated data, expert certification for the auditability of algorithmic decisions, and the admissibility of advanced

[15] CERT-In, *Annual Report on Cyber Incident Trends*, Government of India (2023), https://www.cert-in.org.in.
[16] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on Information and Communications Technology Cybersecurity Certification (Cybersecurity Act), 2019 O.J. (L 151) 15.

 [ISSN 2581-5369]

forensic tools capable of interpreting machine-originated activity. Only then can the legal system keep pace with the shifting dynamics of cyber conflict shaped by intelligent, adaptive, and opaque technologies.

V. INSTITUTIONAL AND LEGAL GAPS IN THE INDIAN FRAMEWORK

A. Outdated Statutory Foundations and Doctrinal Ambiguities

Despite the increasing frequency and sophistication of AI-driven cyber threats, India's legal and institutional framework remains poorly equipped to deal with the complexities they present. While the Information Technology Act, 2000 was a pioneering piece of legislation at the time of its enactment, it was never intended to regulate autonomous systems or algorithmic agents capable of executing cyberattacks without direct human instruction. Similarly, existing institutional mechanisms such as CERT-In and the NCIIPC function with limited mandates and operate in a fragmented environment that lacks cohesive oversight or coordination in dealing with AI-generated incidents.

The absence of explicit legal recognition of AI as a source of autonomous harm constitutes a fundamental gap in Indian law. Neither the IT Act nor the Indian Penal Code, now succeeded by the Bharatiya Nyaya Sanhita, defines AI-generated acts as legally attributable. This omission leaves courts and law enforcement without a statutory basis for determining liability, initiating prosecutions, or providing remedies in cases where harm is caused by self-directed systems.

B. Enforcement Limitations and Resource Constraints

In such scenarios, investigators are forced to treat the AI tool either as a weapon used by a human actor or as an unforeseeable anomaly, both of which restrict the scope of legal intervention. The challenge is compounded by the lack of institutional expertise and resource allocation. Most Indian cybercrime cells are structured to handle cases of phishing, unauthorised access, identity theft, or social media abuse. These teams, while effective in handling conventional digital crimes, are not trained or resourced to investigate algorithmic intrusions, forensic anomalies created by AI, or transnational attacks involving self-deploying malware.

Furthermore, jurisdictional overlaps between central and state agencies create procedural bottlenecks that delay investigation and reduce the likelihood of timely enforcement. The absence of a coordinated command or case allocation system means that AI-linked cybercrimes may fall between institutional cracks.

C. Judicial Gaps and Absence of Jurisprudence

In terms of adjudication, the Indian judicial system has not yet evolved a consistent jurisprudence on AI liability. While courts have recognised the admissibility of electronic evidence and the importance of digital traceability in several high-profile cases, there has been no judicial articulation of standards for AI-generated activity, particularly in matters involving intent, causation, or foreseeability. In the absence of such guidance, lower courts remain constrained in their capacity to evaluate AI-related evidence, assign responsibility, or enforce remedial action.

Without binding precedent or clear doctrinal innovation, courts are likely to treat AI systems as technological intermediaries rather than potential sources of legal harm, thereby limiting the development of a coherent legal position on AI-induced damage.

D. Lack of Binding Oversight and Compliance Mechanisms

The regulatory vacuum also extends to oversight and compliance. There is currently no legal requirement for AI developers, vendors, or deployers to ensure auditability, traceability, or ethical conformity in the tools they produce. The guidelines issued by NITI Aayog[17], while important from a policy perspective, are voluntary in nature and lack the binding force necessary to enforce compliance or penalise violations.

This regulatory laxity enables the unchecked deployment of AI systems with potentially harmful capabilities, without consequence for their designers or operators. In the absence of mandatory standards, businesses have little incentive to invest in safety-by-design practices or third-party risk assessments.

E. Fragmentation in Policy-Making and Siloed Regulation

India continues to address AI and cyber regulation in silos. Policies on data protection, cyber sovereignty, and AI governance are being developed in isolation, with minimal inter-agency collaboration or legislative integration. The result is a fragmented regulatory landscape that lacks both preventive and corrective capacity. Without a central statutory authority or legal doctrine to consolidate AI-related oversight, Indian agencies remain vulnerable to disjointed responses, jurisdictional confusion, and procedural inefficiencies.

Internationally, the regulatory discourse has already begun to evolve. The European Union's draft Artificial Intelligence Act classifies high-risk AI systems and mandates extensive documentation, risk assessment, and human oversight. Similarly, the United States has issued

[17] NITI Aayog, *National Strategy for Artificial Intelligence* (2018), https://niti.gov.in/national-strategy-artificial-intelligence.

executive guidance on AI system accountability in federal cybersecurity practices. These frameworks do not merely aim to regulate the private use of AI, but also to build the institutional capacity necessary to respond to AI-generated harm in the public interest.

F. Need for Comprehensive Reform and Institutional Realignment

To move beyond these limitations, India must consider enacting comprehensive legislation that addresses AI use in critical sectors, defines liability standards for autonomous agents, and mandates forensic auditability for high-risk AI systems. Such legislation should be accompanied by institutional reforms, including the creation of AI-focused cyber response units, specialised judicial benches for digital evidence cases, and regulatory bodies equipped to monitor algorithmic activity in real time.

These reforms would not only enhance enforcement capability but also align India with international best practices and reinforce the constitutional commitment to accountability, due process, and the rule of law in the digital age.

VI. RECOMMENDATIONS AND THE WAY FORWARD

A. Legislative Reform for AI-Specific Liability

A foundational step in addressing AI-driven cyber threats is the legal recognition of AI-specific liability within India's statutory framework. The Information Technology Act, 2000 must be amended to define the legal status of autonomous digital systems and clarify the scope of liability for developers, operators, and end-users. The law should accommodate principles of strict and vicarious liability where human intent cannot be directly established but control or foreseeability is evident.

Statutory provisions should also account for high-risk AI deployments and establish legal duties of care for those who introduce such technologies into sensitive environments, including finance, health, infrastructure, and defence.

B. Institutional Strengthening and Specialised Enforcement

India must invest in building institutional capacity to investigate and respond to AI-enabled cyber threats. The establishment of specialised AI-Cyber Cells under CERT-In, NCIIPC, and state cybercrime units is essential. These units must be staffed with experts trained in algorithmic forensics, neural network audits, and adversarial testing.

Further, enforcement agencies should be empowered with real-time data access tools and cross-jurisdictional coordination protocols to respond swiftly to sophisticated and distributed cyberattacks. The establishment of a central AI regulatory authority may also be considered to

 [ISSN 2581-5369]

streamline oversight and compliance.

C. Judicial Modernisation and Procedural Adaptation

To ensure fair adjudication in AI-linked offences, judicial infrastructure must adapt to the evolving nature of digital evidence. Dedicated benches for cyber law and technology-related disputes should be constituted in higher courts, supported by technical experts to interpret AI-generated records and system logs.

Procedural reforms must also include updated evidentiary standards for admissibility of algorithmic evidence, guidelines for auditability, and safeguards for the rights of accused persons when machine-generated data forms the basis of prosecution.

D. Comprehensive Regulation and Risk Classification Framework

India must adopt a centralised risk-based regulatory model for AI, similar to the European Union's draft Artificial Intelligence Act. This framework should classify AI systems based on potential societal harm and impose escalating compliance requirements accordingly.

High-risk systems should be subject to mandatory registration, independent auditing, and legal oversight. Developers and deployers must be required to implement explainability features, ethical guardrails, and data governance mechanisms to ensure lawful and accountable use of AI.

E. Strengthening AI Forensics and Evidentiary Protocols

A national AI forensics policy must be developed to guide law enforcement and forensic laboratories in handling algorithmically generated or manipulated evidence. This includes tools for reverse engineering neural networks, verifying model outputs, and maintaining an auditable trail of system behaviour.

Standards for forensic integrity, expert certification, and admissibility of algorithmic logs should be enacted through rules framed under the IT Act and the Evidence Act, in consultation with technical experts and judicial stakeholders.

F. International Cooperation and Cyber Diplomacy

Given the cross-border nature of AI-enabled cyberattacks, India must intensify its participation in international cyber law discussions and multilateral forums. Treaties and mutual legal assistance agreements should be updated to include provisions for AI-based evidence sharing, jurisdictional recognition of AI forensics, and coordination in cyber attribution cases.

 [ISSN 2581-5369]

India may also benefit from contributing to the development of global norms on autonomous cyber operations, drawing from the Tallinn Manual, Budapest Convention, and FATF digital asset standards.

G. Capacity Building, Awareness, and Legal Education

To sustain legal preparedness, AI law and forensic cybercrime must be included in law school curricula, judicial training academies, and regulatory workshops[18]. Public prosecutors, judicial officers, and enforcement personnel must receive ongoing training in legal standards surrounding AI, machine learning systems, and digital evidence analysis.

Raising public awareness on risks such as deepfakes, algorithmic manipulation, and intelligent malware will also be essential in fostering a culture of legal literacy and digital vigilance.

VII. CONCLUSION

The integration of artificial intelligence into the cyber domain has fundamentally challenged traditional legal conceptions of agency, liability, evidence, and sovereignty. AI systems, capable of acting autonomously and adapting in real time, expose critical vulnerabilities in India's cyber laws, enforcement mechanisms, and adjudicatory processes. As cyberwarfare evolves from human-executed scripts to algorithmically orchestrated attacks, the legal infrastructure must evolve in parallel.

India's existing statutory and institutional frameworks, though moderately equipped for conventional cyber threats, are doctrinally ill-prepared for the complex and decentralised nature of AI-induced harm. A piecemeal response is no longer tenable. Urgent reforms are needed across legislation, enforcement, forensics, judicial interpretation, and global cooperation.

This paper has attempted to highlight these challenges and propose a roadmap for legal and institutional renewal. The objective is not merely to modernise cyber regulation but to uphold constitutional principles of justice, accountability, and digital sovereignty in an era increasingly defined by artificial intelligence. It is only through such holistic reform that India can assert leadership in the governance of AI and maintain the rule of law in the digital battlefield.

*****

[18] Roger Brownsword, *Law, Technology and Society: Reimagining the Regulatory Environment* 289 (Routledge 2020).

 [ISSN 2581-5369]

VIII. REFERENCES AND SUPPORTING MATERIAL

Statutes and Legal Instruments

- *Information Technology Act, 2000*
- *Indian Evidence Act, 1872*
- *Bharatiya Nyaya Sanhita, 2023*
- *Articles on Responsibility of States for Internationally Wrongful Acts, 2001*
- *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*
- *European Union Artificial Intelligence Act (Proposed Regulation, 2021)*
- *Executive Order 14028 on Improving the Nation's Cybersecurity, United States*
- *Cybersecurity Act of the European Union, Regulation (EU) 2019/881*

Case Law

- *Vijay Madanlal Choudhary v. Union of India, (2022) SCC OnLine SC 929*
- *Pankaj Bansal v. Union of India, (2023) SCC OnLine SC 1240*
- *Google LLC v. CNIL, Case C-507/17, European Court of Justice (2019)*

Books and Commentaries

- Schmitt, Michael N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017
- Murray, Andrew, *Information Technology Law: The Law and Society*, Oxford University Press, 2023
- Brownsword, Roger, *Law, Technology and Society: Reimagining the Regulatory Environment*, Routledge, 2020
- Hartzog, Woodrow, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Harvard University Press, 2018
- Garner, Bryan A. (ed.), *Black's Law Dictionary*, 11th ed., Thomson Reuters, 2019

Reports and Articles

- NATO CCDCOE, *Tallinn Manual 2.0 – Highlights and Commentary*, 2017
- European Commission, *Proposal for a Regulation on Artificial Intelligence*, COM(2021) 206 final

 [ISSN 2581-5369]

- National Institute of Standards and Technology (NIST), *AI Risk Management Framework 1.0*, 2023
- NITI Aayog, *National Strategy for Artificial Intelligence*, Government of India, 2018
- CERT-In, *Advisories and Guidelines on Cyber Threats and Critical Infrastructure Protection*, 2022
- Ministry of Electronics and Information Technology (MeitY), *IndiaAI Mission – Policy Draft*, 2023

Web Sources

- NATO CCDCOE, Tallinn Manual Project: https://ccdcoe.org/research/tallinn-manual
- EU Artificial Intelligence Act Portal: https://artificialintelligenceact.eu
- NIST AI RMF Overview: https://www.nist.gov/itl/ai-risk-management-framework
- NITI Aayog – National AI Strategy: https://niti.gov.in/national-strategy-artificial-intelligence
- CERT-In Official Portal: https://www.cert-in.org.in
- Ministry of Electronics and IT (India): https://www.meity.gov.in

*****