ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

ARTIFICIAL INTELLIGENCE (AI) AND CYBERSECURITY LAW: LEGAL ISSUES IN AI-DRIVEN CYBER DEFENSE AND OFFENSE

R. Arjuna Rao[1], Dr. O.P Gupta[2], Dr. Akash Saxena[3]
[1]Research Scholar, [2]Pro-Vice Chancellor, [3]Professor
Shridhar University, Pilani 333031

ABSTRACT

The integration of Artificial Intelligence (AI) into cyber security has transformed both defensive and offensive strategies in cyberspace. While AI offers enhanced threat detection, rapid response capabilities, and predictive analytics, it also poses novel risks and legal challenges when used for cyber offenses. This paper explores the evolving landscape of AI in cyber security, focusing on the legal issues surrounding its deployment for both protection and attack. It highlights existing national and international legal frameworks, identifies regulatory gaps, and provides recommendations for future governance.

KEYWORDS: *Artificial Intelligence (AI), cyber security, Transparency, Legal Implications*

1. INTRODUCTION

AI technologies are increasingly being used to automate cyber security operations, detect anomalies, and mitigate threats. Simultaneously, malicious actors are leveraging AI to conduct sophisticated cyber attacks. The dual-use nature of AI raises critical legal and ethical concerns. This paper aims to examine these concerns and assess the adequacy of current legal frameworks in addressing them.

2. AI IN CYBER DEFENCE: PROMISE AND PERILS

2.1 Applications

1. AI-powered Intrusion Detection and Prevention Systems (IDPS)

AI-enhanced IDPS utilize machine learning algorithms to detect anomalies in network traffic and system behavior. These systems can identify threats in real time, adapt to new attack patterns, and prevent potential intrusions automatically.

Legal Implications:

- **Privacy Concerns:** Continuous monitoring may infringe on employee or user privacy.
- **Transparency:** Decision-making by black-box AI models may not be explainable in court.
- **Compliance:** Must align with data protection laws like GDPR, especially when processing personal data.

2. Machine Learning Models for Predictive Threat Intelligence

These models analyze vast datasets to predict future cyber threats by identifying patterns, trends, and behaviors of known attack vectors. They support proactive security postures.

Legal Implications:

- **Data Sourcing Legality:** Use of scraped, unverified, or cross-jurisdictional data may breach data handling laws.
- **Bias and Reliability:** False positives could lead to unjust disciplinary or legal action.
- **Accountability:** Errors in prediction could cause significant financial or reputational harm—raising questions of liability.

3. Automated Incident Response and Forensic Analysis

AI systems automate detection, classification, and response to cyber incidents. In forensic contexts, AI can rapidly parse logs, trace attack origins, and identify compromised assets.

Legal Implications:

- **Chain of Custody:** Use of AI in evidence collection must ensure legal admissibility.
- **Due Process:** Automated actions (e.g., terminating user sessions) must respect organizational and legal protocols.
- **Auditability:** AI-driven forensic tools must provide clear logs and documentation for use in investigations or court.

4. Behavioral Analytics for Identifying Insider Threats

These systems use AI to profile normal user behavior and flag deviations that may indicate malicious intent, such as data exfiltration or policy violations.

Legal Implications of Behavioral Analytics in Insider Threat Detection

1. **Workplace Surveillance**
   - **Issue:** AI-driven monitoring of employee behavior may be perceived as invasive surveillance.
   - **Legal Concern:** In many jurisdictions, constant tracking of employee actions without proper justification or safeguards may violate privacy laws and labor rights.
   - **Example:** The European Court of Human Rights (ECHR) has ruled against excessive employer surveillance without informed consent.
2. **Consent and Notification**
   - **Issue:** Employees or users must be informed if their behavior is being monitored by AI tools.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

- **Legal Concern:** Failure to notify or obtain consent can breach data protection laws like the **GDPR** (Article 13) or **India's Digital Personal Data Protection Act, 2023**.
- **Best Practice:** Implement clear user policies and privacy notices outlining the scope, purpose, and technology used.

3. **Discrimination Risks**
   - **Issue:** AI models trained on biased or unbalanced data may disproportionately target specific groups (e.g., by gender, ethnicity, or role).
   - **Legal Concern:** Discriminatory profiling could lead to violations of **equal opportunity laws**, civil rights statutes, and trigger organizational liability.
   - **Mitigation:** Regular audits of AI algorithms for fairness, bias correction, and transparency.

2.2 Legal and Ethical Issues in AI-Based Cyber Defense in India

India, as a rapidly digitizing economy and a hub for IT services, is increasingly integrating Artificial Intelligence into its cybersecurity infrastructure. While AI-based defenses promise efficiency and scalability, they raise significant legal and ethical challenges within the Indian legal framework.

1. Data Privacy
   - **Legal Context:** India's **Digital Personal Data Protection Act, 2023 (DPDP Act)** governs the processing of personal data by both government and private entities.
   - **Implications for AI:**
     - AI models must adhere to principles of **purpose limitation**, **data minimization**, and **consent-based processing**.
     - **AI-based threat detection tools** often process personal logs and behavioral data, raising compliance issues if such data is collected or used without consent.
   - **Challenge:** The lack of clarity on **automated decision-making** in the DPDP Act creates regulatory uncertainty for AI deployments.

2. Liability

- **Legal Framework:** The **Information Technology Act, 2000**, as amended, and associated rules (e.g., Intermediary Guidelines, CERT-In Directions) address cyber incidents but are silent on AI-specific liability.
- **Implications:**
  - There is **no statutory clarity** on who is liable if AI-based systems fail—developers, service providers, or deploying organizations.
  - In sectors like banking and telecom, **sectoral regulators (e.g., RBI, TRAI)** may impose additional cybersecurity obligations, indirectly influencing AI accountability.

3. Transparency and Explain ability

- **Issue:** Many AI-based systems used in cybersecurity (e.g., anomaly detection) function as black boxes.
- **Ethical Concern:** Lack of transparency in decision-making could:
  - Undermine trust in automated incident response tools.
  - Prevent effective **judicial or administrative scrutiny** in cases involving breaches or disputes.
- **Legal Gap:** Indian law does not currently mandate **algorithmic transparency** or **right to explanation** in AI-related decisions, unlike the EU's GDPR.

4. Due Diligence Obligations

- **Under the IT Act:** Organizations must implement "reasonable security practices" under **Section 43A** and comply with the **SPDI Rules (2011)**.
- **CERT-In Guidelines (2022):**
  - Mandate logging, breach reporting, and specific security practices that may apply to AI systems.
  - These obligations place a **compliance burden** on entities using AI, particularly when AI systems are involved in critical infrastructure.
- **Concern:** The **lack of AI-specific cybersecurity standards** makes it difficult for organizations to evaluate whether their AI defenses meet legal expectations.

5. Ethical Concerns

- **Surveillance and Privacy:** AI-based monitoring tools (like behavior analytics) could lead to unethical surveillance of employees or citizens.
- **Bias and Discrimination:** Without proper auditing, AI models may reinforce bias, leading to unfair treatment in security-related decisions.
- **Need for Ethical AI Framework:** While **NITI Aayog** has proposed ethical AI principles, they remain **non-binding** and lack legal enforceability.

3. AI IN CYBER OFFENSE: EMERGING THREATS

While AI has enhanced cybersecurity defenses, it also introduces unprecedented capabilities for conducting cyber offenses. Malicious actors, including state and non-state entities, are now employing AI to execute more effective, scalable, and evasive cyberattacks. This section examines various AI-driven offensive techniques and the legal challenges they pose under national and international law.

3.1 Examples of AI-Driven Attacks

1. **AI-Generated Phishing and Deepfakes**
   - AI tools such as GPT-based models can craft highly convincing phishing emails tailored to specific targets (spear phishing).
   - Deepfake technology enables the creation of fake audio/video to impersonate executives, spread misinformation, or manipulate public opinion.
   - **Real-world Incident:** A CEO was tricked by a deepfake voice scam into transferring $243,000 (reported by *Wall Street Journal*).
2. **Intelligent Malware and Adaptive Bots**
   - AI is used to develop self-learning malware that adapts to defenses, evades detection, and optimizes its payload deployment.
   - Botnets enhanced with reinforcement learning can dynamically switch targets or attack vectors.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

3. **AI-Enhanced Social Engineering**
   - Natural Language Processing (NLP) models enable real-time, context-aware chatbots to impersonate human agents or deceive users.
   - AI can analyze social media data to identify psychological vulnerabilities for targeted manipulation.
4. **Autonomous Offensive Cyber Tools**
   - AI-driven systems can autonomously identify vulnerabilities, exploit them, and carry out coordinated attacks with minimal human oversight.
   - These systems blur the line between conventional hacking and autonomous cyber warfare.

3.2 Legal Challenges

1. **Attribution**
   - **Problem:** AI-generated attacks may originate from distributed networks and use anonymization techniques, complicating attribution.
   - **Legal Concern:** Under international law (e.g., **Tallinn Manual 2.0**), attributing cyberattacks to a state is essential for invoking countermeasures—but AI obfuscates this process.
   - **India's Position:** Attribution is not formalized in Indian law, creating evidentiary challenges for prosecution or retaliation.
2. **Sovereignty Violations**
   - AI-enabled cross-border attacks may infringe on a nation's digital sovereignty or violate the principle of non-intervention.
   - **Legal Gap:** There is no global consensus on how international humanitarian law (IHL) applies to autonomous cyber operations.
3. **Accountability**
   - **Issue:** If an autonomous AI tool executes an unlawful act (e.g., data theft, sabotage), assigning responsibility becomes complex.
   - **Legal Dilemma:** Should liability rest with the developer, the user, or the AI itself? This is particularly relevant under criminal and civil liability doctrines.
4. **Breach of International Norms**
   - **Tallinn Manual:** Addresses the use of cyber means in armed conflict, but it does not yet fully cover AI-driven cyberwarfare.
   - **Geneva Conventions and IHL:** There is ambiguity on how these apply to AI-based cyber tools used in conflict.
   - **Budapest Convention on Cybercrime:** Focuses on prosecuting cybercrime but lacks AI-specific provisions.
5. **Dual-Use Technology Regulation**
   - AI tools can serve both civilian and military purposes (e.g., NLP for education vs. phishing). Export controls and technology governance are still in nascent stages.
   - **Concern:** The misuse of dual-use AI for cyber offenses remains under-regulated globally.

3.1 Examples of AI-Driven Attacks

- AI-generated phishing campaigns and deepfakes.
- Intelligent malware capable of adaptive behavior.
- AI-enhanced social engineering and reconnaissance.

3.2 Legal Challenges

- **Attribution:** Difficulties in tracing AI-generated attacks to specific actors.
- **Sovereignty Violations:** Cross-border attacks challenge traditional jurisdictional norms.
- **Accountability:** Complexities in assigning legal responsibility for autonomous actions.
- **International Law Violations:** Issues under the Tallinn Manual and International Humanitarian Law (IHL).

4.LEGAL AND REGULATORY FRAMEWORKS IN INDIA

India's legal and regulatory environment for cybersecurity is evolving to accommodate emerging technologies, including Artificial Intelligence (AI). While India lacks a unified legal framework explicitly governing AI in cybersecurity, several existing laws, sectoral guidelines, and policy initiatives touch upon key aspects such as data protection, digital infrastructure security, AI governance, and ethical use. This section provides a structured overview of the major legal instruments and regulatory bodies relevant to AI in cyber defense and offense.

4.1 Information Technology Act, 2000 (IT Act)

- **Primary Cyber Law in India:** Governs electronic records, cybercrime, and data protection.
- **Key Provisions:**
  - **Section 43A:** Imposes liability for failure to protect sensitive personal data.
  - **Section 66:** Covers hacking and identity theft, applicable to AI-generated offenses.
  - **Section 70B:** Empowers **CERT-In** (Computer Emergency Response Team – India) to coordinate responses to cybersecurity incidents.
- **Limitations:** The Act does not address AI-specific concerns such as algorithmic accountability, autonomous decision-making, or AI-based cyber warfare.

4.2 Digital Personal Data Protection Act, 2023 (DPDP Act)

- **Applies to:** All entities processing personal data digitally within India or of Indian citizens abroad.
- **Relevance to AI:**
  - Requires consent-based processing, purpose limitation, and data minimization—principles directly affecting AI training and deployment.
  - Establishes a **Data Protection Board** to enforce compliance and handle grievances.
- **Gap:** The Act does not specifically regulate automated decision-making or AI profiling, though

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

such practices may affect individual rights and freedoms.

4.3 Indian Penal Code (IPC), 1860

- **Applicability:** Sections related to fraud (Section 420), identity theft, defamation, and criminal conspiracy may apply to AI-assisted cyber offenses.
- **Challenge:** Traditional legal doctrines may not fully capture the autonomous and evolving nature of AI-generated attacks.

4.4 Sectoral Guidelines and Regulatory Authorities

- **CERT-In Guidelines (April 2022):**
  - Mandate logging, reporting of cyber incidents, and time-bound response.
  - Relevant for AI-based defense systems that detect or respond to incidents autonomously.
- **Reserve Bank of India (RBI):**
  - Mandates cybersecurity controls for financial institutions; AI tools in fraud detection must comply with these standards.
- **SEBI, IRDAI, and TRAI:**
  - Issue sector-specific norms that may intersect with AI-based cybersecurity tools in finance, insurance, and telecom sectors.

4.5 NITI Aayog's Responsible AI Guidelines

- **Non-Binding Principles:** Focus on safety, accountability, inclusivity, transparency, and privacy in AI use.
- **Impact:** While not legally enforceable, these guidelines influence policy discourse on ethical AI deployment, including in cybersecurity.
- **Need for Legislation:** A dedicated **AI regulation law** is under discussion but yet to be introduced.

4.6 Cybersecurity Policy Initiatives

- **National Cyber Security Policy, 2013:**
  - Provides a broad framework for protecting cyberspace, but is outdated for AI-era threats.
- **National Cybersecurity Strategy (Draft – 2020):**
  - Proposes an AI-integrated cyber defense approach, capacity-building, and legal reforms.
  - Yet to be officially adopted.

4.7 Challenges and Gaps

- **Lack of AI-Specific Regulation:** No statutory definition of AI, accountability framework, or licensing model for high-risk AI.
- **Attribution and Liability:** Indian law lacks mechanisms for attributing AI-generated attacks or assigning responsibility in case of failure or misuse.
- **Judicial Readiness:** Courts are still developing jurisprudence on digital evidence and AI explainability, raising admissibility and fairness issues.
- **Need for Harmonization:** Sectoral silos, outdated policies, and the absence of unified AI-cybersecurity norms lead to fragmented compliance obligations.

CONCLUSION

India's current legal and regulatory frameworks provide a foundational base for AI and cybersecurity governance but fall short in addressing the nuanced challenges posed by AI-driven cyber threats. A forward-looking, technology-neutral, and risk-based regulatory regime—backed by cross-sectoral cooperation and international alignment—is essential to effectively govern AI in cybersecurity.

REFERENCES

1. *Information Technology Act, 2000 (as amended) Government of India. https://www.indiacode.nic.in/handle/123456789/1999.*
2. *Digital Personal Data Protection Act, 2023 Ministry of Electronics and Information Technology (MeitY), Government of India.https://www.meity.gov.in/digital-personal-data-protection-act-2023*
3. *CERT-In Directions under Section 70B of the IT Act (April 2022) Computer Emergency Response Team – India (CERT-In), MeitY.https://www.cert-in.org.in/*
4. *NITI Aayog. (2021). Responsible AI for All: Strategy Document https://www.niti.gov.in/responsible-ai*
5. *National Cyber Security Policy, 2013 Department of Electronics and Information Technology (DeitY), Government of India. https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013%281%29.pdf*
6. *Draft National Cybersecurity Strategy (2020) Data Security Council of India (DSCI). https://www.dsci.in/content/national-cyber-security-strategy-2020*
7. *Indian Penal Code, 1860, Government of India. https://www.indiacode.nic.in/handle/123456789/2263*
8. *Reserve Bank of India – Cybersecurity Frameworks for Banks and NBFCs RBI Circulars. https://www.rbi.org.in*
9. *Budapest Convention on Cybercrime (2001) Council of Europe. India is not a signatory but the convention serves as an international benchmark. https://www.coe.int/en/web/cybercrime/the-budapest-convention*
10. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Schmitt, M. N. (Ed.). (2017). Cambridge University Press.*