IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

CYBERCRIME IN INDIA: LEGAL FRAMEWORKS, EMERGING THREATS, AND THE ROLE OF AI IN DETECTION AND DEFENCE

[1]Rahul Karne, [2]Akhil Dudhipala [3]Pavan Kumar Pativada
[123]Independent Researcher
[1]rahulreddy.karne@gmail.com, [2]dudhipalaakhil@gmail.com, [3]pkpativada@gmail.com

Abstract: *India's swift digitisation—mobile payments, e-governance, and wider Internet access to over 800 million—has simultaneously led to greater cybercrime threats. The National Crime Records Bureau (NCRB) reported that cybercrime cases increased from 50,035 in 2020 to 65,893 in 2022, a 24.4% increase in the two-year period (Ministry of Home Affairs, 2024). Most cybercrime (64 %+) consists of financial fraud, particularly phishing scams, Unified Payments Interface (UPI) payment fraud, and credit/debit card scams. Their UPI fraud increased by 85% from 2022 to 23, with 2.7 million complaints levied, resulting in losses of over ₹2,145 crore (Gupta, 2024; ETBFSI Research, 2024). Other non-trivial cyber crimes can include online harassment and cyberbullying (Das, 2024), cyberterrorism and misinformation (Raina, 2024), massive hacking breaches of data by institutions (Kalra, 2024; Safi, 2018), child sexual abuse and online grooming (Das, 2024; Sur, 2023), and intellectual property infringements, such as piracy—which cost the Indian film and entertainment industry, as an example, an estimated ₹22,400 crores in 2023 (PTI, 2024). This paper categorises and analyses these threats and expands professionally the use of Artificial Intelligence (AI) technology to deal with the defence and offence of cyber crimes. On the defensive end of the spectrum, AI is being used to identify banking fraud, phishing detection, image-based child safeguarding, and deepfakes (Gregoire, 2024; Shankari, 2024). On the offensive side of the spectrum, the threat actors are using AI-based technologies (especially large language models and generative media) to assist with phishing, impersonation fraud, and social engineering (CyberPeace Foundation, 2024). This research also looks at how India's regulatory framework is evolving, including their Information Technology Act (2000, amended 2008), Indian Penal Code, POCSO Act and proposed Digital Personal Data Protection Act (2023) (Lawton, 2023), in comparison to other country frameworks like the EU's General Data Protection Regulation (GDPR) and the future AI Act (Ministry of Information & Broadcasting, 2023). The research ends with the systemic issues that challenge work, like fragmented enforcement, jurisdictional limits, data privacy, AI bias, and the national cybersecurity workforce shortage. There is a value in an interdisciplinary, multi-layered approach of flexible legislation, AI-based threat monitoring, and international partnership in the complicated nature of issues that weaken India's ability to respond to these rising threats.*

IndexTerms **– Cybercrime In India, AI, Artificial Intelligence, Financial Fraud, Deepfakes, Child Exploitation Detection, Cyberbullying, Data Breaches, Digital Piracy, POSCO, GDPR, Indian Cyber Law, Information Technology Act, Digital Personal Data Protection Act (DPDPA).**

I. INTRODUCTION

While India's digital revolution has created immense potential for socio-economic growth, it has also created a huge and increasingly targeted cyber-attack surface. With over 800 million active internet users and a rapidly developing ecosystem of mobile-based digital solutions, including e-governance, online education, and financial technology, India has entered a period of unprecedented cybercrime growth. According to the National Crime Records Bureau (NCRB) data reported, the number of reported cybercrime incidents has jumped from 50,035 in 2020 to 52,974 in 2021, up to 65,893 in 2022 – a growth rate of 24% annually (Ministry of Home Affairs, 2024). This growth in cybercrime is not only the result of expanding digital use but also the emergence of new criminal modalities in cyberspace.

The vast majority of cybercrime amplifies research and data on forms and types of cyber fraud. Financially motivated cybercrime in 2022 totalled 64.8%, accounting for 42,710 cases, which comprises scams of phishing attacks, UPI payment fraud, and card fraud (Manral & Sinha, 2023). In FY2023–24, UPI fraud alone increased by 85%, from a FY2023–24 count of 0.725 million cases to 1.342 million cases, with average financial loss totals reported to Rs 2,145 crore from 2.7 million reported incidents (Gupta, 2024; ETBFSI Research, 2024). Beyond financial crimes, cybercriminals are increasingly exploiting digital platforms to

engage in online harassment, hate speech, and radicalization; misinformation dissemination, including new uses of deepfake video for political manipulation; breaches of institutions/systems; and engagement in grooming and child exploitation, including illegal distribution of content (Das, 2024; Sur, 2023). The entertainment sector has also seen large-scale losses, with an estimated ₹22,400 crore lost to digital piracy, as noted in the EY-IAMAI Report, in the year 2023 alone (PTI, 2024).

A multitude of issues have contributed to this upsurge. The pandemic resulted in a massive shift to remote work that made the country more vulnerable, combined with the rapid adoption of digital payment systems and the move to online services. Meanwhile, cybercriminals have exploited social media and encrypted messaging systems to promote threats and trick victims more rapidly and with far more anonymity than before. India's regulatory response is evolving but still characterised by disorder and uncertainty. The Information Technology Act of 2000 (and its amendments in 2008) is an initial legal framework for punishing cyber offences. In addition, there are other provisions in the Indian Penal Code (IPC), the POCSO Act, and sector-based guidelines to address the larger concept of cybercrime. The larger Digital Personal Data Protection Act (2023) represents a leap toward having its own regulations for data and privacy (Lawton, 2023). These domestic initiatives also rely on international benchmarks such as the EU's General Data Protection Regulation (GDPR) and the soon-to-be-enacted EU AI Act (Ministry of Information & Broadcasting, 2023).

In this landscape, Artificial Intelligence (AI) plays a somewhat counterintuitive role as both, a facilitator of security with advances in anomaly detection, natural language processing and computer vision enabling fraud detection, content moderation and identification of abuse on one hand; while on the other, it enables our adversaries to centrally use AI tools to scale of attacks in order to automate threats; including sourcing high fidelity phishing material and manipulated media. For example, a 2024 research report discussed a real-life phishing incident against a financial institution in India perpetrated by AI. Our adversary applied AI to create the phishing event (CyberPeace Foundation, 2024).

This report aims to classify the main types of cybercrime in India with respect to their types of financial fraud, cyberbullying and harassment, cyberterrorism and misinformation, data breaches and hacking, child sexual exploitation and abuse, and intellectual property theft. It will consider the origins of each with case studies and the application of AI tools for detection and remediation. The report will also explore the strengths and weaknesses of India's national legal framework to provide high-level recommendations on policy gaps for enforcement, ethics, and tie into best practices globally. The report represents an effort to assess the interplay among AI, law, and governance in shaping a secure digital future for India.

II. RELATED WORK

There is an extensive body of literature related to cybercrime and cybersecurity studies, and relatively few works specifically examine India with an AI perspective. Cybercrime surveys globally categorise threats, including (but not limited to) fraud, malware, hacking, and online abuse (Jiaxin et al., 2022). Jiaxin et. al (2022) and others reviewed deep fake detection techniques globally (Jiaxin et al., 2022). Cyberbullying and online harassment of children and youth, are documented in recent social science works, where inter alia they map the particularly high rates of online victimization in India (for example, one study suggests over 33% of children report experiencing one or more types of online harassment) (Das, 2024; Sur, 2023). In the area of law, there is discussion on India (and broader concerns globally) in analyses of the IT Act and India's new data privacy law (Lawton, 2023; Ministry of Home Affairs, 2024). Prior works also discuss AI in the context of security: machine learning for intrusion detection and fraud detection survey articles (for example, supervised and unsupervised methods to detect network intrusion) (CyberPeace Foundation, 2024; Gregoire, 2024). New reports in the industry demonstrate the use of AI in enterprise security and the AI-fueled evolution of threats (Gupta, 2024; CyberPeace Foundation, 2024). However, comparative studies aligning cybercrime trends in India, enabling statutes, and AI-based threat mitigation are few and far between.

This work seeks to address that void by enhancing existing information in the context of published government crime data, news articles, and recent academic/industry studies. This includes government data (Ministry of Home Affairs, 2024; CERT-In, 2023) and media data in addition to over 26 other recently published highly referenced studies (2022–2024), including world affairs forums and technology policy repositories (Raina, 2024; PTI, 2024). This paper simultaneously focuses on technical and research applications (for example, a survey of increasing UPI fraud, cyber-attack vectors, and relevant statutes) (Gupta, 2024; ETBFSI Research, 2024). While our methodology is similar to existing comprehensive reviews (e.g., reviews for synthetic media), it is designed to reflect the Indian context and treat AI as the threat actor and mitigator, an aspect practitioners particularly emphasise. As such, this study's approach adds to the existing domain-specific surveys a coherent, up-to-date synopsis of cybercrime in India, issues with legal status, and the frontier of current AI-based threat mitigations and challenges.

III. METHODS AND BACKGROUND

We undertook a systematic literature review and data analysis. Our primary data source was the official reports with statistics (NCRB, CERT-In annual reports) (Ministry of Home Affairs, 2024; CERT-In, 2023), government press releases, and respected media sources (e.g., The Indian Express, Times of India, Reuters) for the latest incidents and quotes (Manral & Sinha, 2023; Das, 2024; Kalra, 2024). We also investigated technology-oriented publications on AI techniques (particularly those dealing with fraud, intrusion, and deepfake detection), but our approach was not specifically experimental but analytic. We segmented cybercrime by transgressor commonality of motive and means (profit-motivated, ideologically/motivated, exploitative, etc.), and established characteristics and countermeasures for each category. Where possible, we leverage quantitative trends (e.g., counts of serious crime [Ministry of Home Affairs, 2024; CERT-In, 2023], or a survey of losses from piracy in the Indian entertainment industry, ₹22,400 crore in 2023: EY-IAMAI Report - Times of India) (PTI, 2024) and qualitative case studies.

For legal context, we present relevant provisions of Indian law. The primary cyber law is the Information Technology Act, 2000 (Amended 2008), which establishes offences such as unauthorized access, hacking, data theft, identity theft, and cyber terrorism (s. 66F). For example, IT Act §66D denounces online cheating consisting of impersonation, §67/67A creates a criminal offence for obscene material, and §69 provides for authority interception. (Not to be overlooked, the Supreme Court declared Section 66a – criminalising offence of "sending offensive messages" online – unconstitutional in 2015) (Ministry of Home Affairs, 2024). Other statutes explore analogous crimes: Indian Penal Code, 1860 which is the root of traditional law offences (murder, kidnapping, defamation, etc.) that can take place either online or offline; and specialized acts like the Protection of Children from Sexual Offences (POCSO) Act, 2012 which covers online child abuse (Das, 2024). The Digital Personal Data Protection Act, 2023, represents India's first major privacy law and includes GDPR-type stipulations for consent and fiduciary responsibilities (Lawton, 2023) (also with notable exceptions for interests in security and law enforcement) (Lawton, 2023). The Cinematograph (Amendment) Act, 2023 (still awaiting notification), seeks to address digital piracy. It prohibits unauthorised recording in cinemas while also requiring online platforms to monitor possible anti-piracy engagement (Ministry of Information & Broadcasting, 2023).

We would now discuss relevant international frameworks. The General Data Protection Regulation (GDPR) and forthcoming AI Act from the EU provide reference points for standards in privacy and AI accountability. For example, while India's DPDP Act has borrowed principles from the GDPR, aspects like weak data localisation from previous drafts of the act leave something to be desired (Lawton, 2023). Although India has not yet fashioned a dedicated law on AI, several global references, such as the GDPR's risk-based approach and transparency obligations, will undoubtedly continue to influence how this regulation is developed. These reference points at the international and regional levels provide comparisons for India's own approach to regulating AI and cybercrime.

To summarise, our methodological approach has consisted of categorising threats, collecting relevant data and anecdotes, and analysing that data in relation to legal texts and AI security literature. The previous background section provides the foundation for discussing each of the categories of cybercrime and their inter-relationship with AI and law.

IV. CASE STUDIES AND APPLICATIONS

We will now address the six significant categories of cybercrime impacting India today, and for each, if available, present statistics, examples, and AI/defensive applications.

4.1 Financial Frauds - Phishing, UPI Scams, and Card Schemes

Financial fraud is the most common type of cybercrime in India, propelled by the rapid adoption of digital payments. In 2022, 64.8% of cybercrimes were financially motivated (Manral & Sinha, 2023). Financial scams include phishing (email/SMS scams impersonating banks), vishing (voice scams), SIM swaps to take over OTP messages, malware/key loggers, and fraudulent UPI requests, often by way of deceptive QR codes. While the UPI system is the prevailing digital payment system in India, reported scams sharply increased, with 85% reported fraud cases in FY2023- 24 (1.342 million). Reported fraud losses were ₹2,145 crore (Gupta, 2024; ETBFSI Research, 2024). Cyber-attack numbers may further exaggerate the threat because phishing scams increasingly rely on social-engineering techniques like impersonating bank and financial institution staff, fake alerts of urgency, and fake apps designed to work or take over apps installed on users' electronic devices. For example, a UPI "collect" scam deceptively collected payment authorisations by disguising fraud schemes as legitimate micro-transactions. SMS phishing has also taken off, especially exploiting schemes related to COVID-19 vaccines and fake banking operational updates. Job scams have also increased in recent years due to the changes in remote work, and fake-portal job scams have been launched.

4.1.1 AI in Defence:

The financial sector, including banks and payment platforms, currently deploys AI and machine learning models to detect fraud when payment transactions become anomalous against the detected behaviour of the user, including behaviours like authentication attempts made from a new device or unexpected large transfers. While CPFIR shows promise to create donor anonymity while maintaining registries of fraud, the National Payments Corporation of India (NPCI), which deals with payments via UPI, has recently begun to triage alert notifications using AI (Gupta, 2024). The Government of India's Department of Financial Services made a regulation requiring AI and machine learning-based fraud prevention tools to be used. Some well-known techniques used for transaction inspection use neural networks or ensemble models to discover phishing attempts and shut down fake sites. Other tools like behavioural biometrics (detecting activity patterns like typing and mouse movements) are enhancing current access control techniques, but warrant caution. Cybercriminals have also begun to utilise AI when conducting attacks, including in a case study completed in 2024 that used AI-generated spear-phishing emails that closely mimicked the writing style of the purchasing bank's CEO (CyberPeace Foundation, 2024). From this perspective, both sides of this battle can be seen to be engaging in an "arms race" using their newly discovered cyber capabilities.

4.1.2 Legal Framework:

Section 66D of the IT Act deals with cheating and impersonation, while Section 66C of the IT Act deals with impersonation or representation, and the relevant IPC offences include cheating and forgery. Regulation also plays a significant role in the banking sector, where regulators like the Reserve Bank of India (RBI) require banks under their License to report on incidents of cybersecurity. In the case of aggregate beneficiary data incorporated from financial companies, data published from the RBI for the period from January 1, 2023, to October 31, 2023, suggested 13 lakh or 1.3 million cyberattacks may occur (averaging approximately 40,000 per day) (Sharma, 2023). In August 2024, a ransomware attack stopped the operations of 300 small banks (Kalra, 2024). In addition, additional regulatory steps aimed at establishing strong government KYC rules in UPI and requiring the reporting of fraud in UPI and bank systems have not kept pace with cyber criminals' constantly evolving digital repertoire.

4.2 Cyberbullying and Online Harassment

Online harassment is on the rise in India—hate speech, cyber-stalking, and extortion that heavily impact the youth. It is estimated that over 33% of children in India are victims of cyberbullying (a behaviour that manifests in many forms) (Das, 2024; Sur, 2023). In 2020, the NCRB reported 1,614 cyberstalking cases, 762 cases of blackmail, and 84 cases of online defamation (Ministry of Home Affairs, 2024). The COVID-19 pandemic increased this type of online abuse: when children are online without supervision, reports show that even in 2020, there were increases (by 32%) in children being victims of cybercrime (Das, 2024). The mental health effects of online abuse on victims are particularly devastating for children, who are often plagued with depression, anxiety, and suicidal thoughts. For other crimes, reports indicated online pornography dissemination crimes have increased and are three times what they were, and evidence of children as victims of bullying has also increased threefold.

4.2.1 AI in Defence:

Many social media companies have shifted to AI-enabled moderation on their platforms, especially Natural Language Processing (NLP) engineering, to flag hate speech, abusive comments, and bullying behaviours. Platforms often employ deep learning models to analyse millions of messages at once and computer vision systems to pull out offensive images or memes. Additional help and support for victims came in the form of AI-enabled chatbots and help-desk support. In the governmental space, AI has provided some capacity to trace anonymous abusers through their usernames and IP addresses and correlate the patterns of their abuse, among other enforcement options. Challenges still exist in the AI space—AI-based moderation can produce false positives, confuse cultural context, and censor permissible content. Current research activity is focused on sentiment analysis to be conducted with many diverse Indian languages, dialects, and slang (Gregoire, 2024).

4.2.2 Legal Framework:

While the IT Act (punishing the sending of "offensive" messages) initial enabling provision 66A was struck down in 2015, several other government provisions related to online abuse remain intact (Ministry of Home Affairs, 2024). The prohibition of obscene content is covered by Section 67 of the IT Act, Section 67A and 67B prohibit child pornography. Hate speech is addressed in many ways in the IPC—Section 503 (criminal intimidation; incitement), and 153A and 505. Reforms made by the government, particularly with the introduction of the Justice Verma Committee and the Criminal (Amendment) Act 2013, recognised a suite of cyber offences (Section 66e spans broadly to privacy and Section 67d outlines and proposes punishments for harassment of women). Acknowledging changes in online harassment, multiple provisions were added to act as a deterrent. However, despite laws still being present in penal codes, enforcement remains weak. Victims often choose not to report or report to police who have no experience in cyber-forensics, while NGOS are working to expand helplines and make legal proceedings faster.

4.3 Cyberterrorism and Online Misinformation

This subsection discusses cyberattacks targeting ideologies or politics (cyberterrorism), as well as misinformation or propaganda. While cyberterrorism is merely intimidation or disruption in the digital space, it is also very rare (usually at the high-end of risk to critical infrastructure and public order), and is deemed low risk to public order, as we have previously discussed. In India, there is a higher prevalence of state-sponsored hacking or propaganda from extremist groups, including multiple high-profile data breaches that were detrimental to journalists and researchers (Safi, 2018; Kalra, 2024).

The most pervasive threat to collective action is online misinformation, especially fake news, especially through social media and messaging applications. For example, AI tools to generate deepfakes during the 2024 Indian general elections targeting candidates and public sentiment, were a concern (Raina, 2024). As India anticipated this threat, it also launched a Deepfakes Analysis Unit (DAU) in partnership with other agencies as part of the Misinformation Combat Alliance. This included a WhatsApp tipline for the public to flag when they encounter questionable or fake media. DAU has since March 2024 analysed hundreds of media files, corroborating the widespread use of synthetic media generally (Raina, 2024), and the Global Risk Report lists AI-aided misinformation as one of the greatest short-term global risks identified by the World Economic Forum.

4.3.1 AI in Defence:

Generative AI will play a significant role in countering cyberterrorism, misinformation, or disinformation. Machine learning can detect not just botnets and fake accounts but also coordinated misinformation campaigns using graph-based ML. News authenticity can be classified by NLP models, specifically transformer models. For a deepfake, machine vision and audio signal processing can identify visual/audio discrepancies by using convolutional neural networks (CNNS) and autoencoders (Jiaxin et al., 2022). Some nations have systems that can verify the associated digital signatures of valid content. Like in cyberterrorism, adversaries also utilise generative AI (i.e., to fake an unrealistic speech or video). I think the most feasible approach is DAU's hybrid model—AI with a human review process provided as a model—and there is discussion from researchers starting to explore explainable AI explicitly on the rationale to flag content as false to increase user trust in the process (Gregoire, 2024; Raina, 2024).

4.3.2 Legal Framework:

Cyberterrorism can be prosecuted under Section 66F of the IT Act for threats to national sovereignty in combination with the Unlawful Activities (Prevention) Act (UAPA) for activity that is traceable back to prohibited or banned organisations. It is very rare that anybody gets prosecuted for cyberterrorism, but the problem of attribution for the enforcement of the law often takes a long time to trace. Legally, misinformation rather than disinformation can be prosecuted under IT Rules 2021, where deepfakes are a criminal offence, and criminalised false news that likely disturbs public order (Ministry of Home Affairs, 2024). India has also been vaguely aware of trends regarding global standards for AI regulation, like the EU AI Act, and it seems they are toying with similar mandates for transparency in AI use. In addition, the amended 2023 Cinematograph Act allows for oversight on the new use of AI, by including penalties for the use of media content in an improper or unethical way in an electoral setting (Ministry of Information & Broadcasting, 2023).

4.4 Data Breaches and Hacking

This subsection discusses cyberattacks targeting ideologies or politics (cyberterrorism), as well as misinformation or propaganda. While cyberterrorism is merely intimidation or disruption in the digital space, it is also very rare (usually at the high end of risk to critical infrastructure and public order), and is deemed low risk to public order, as we have previously discussed. In India, there is a higher prevalence of state-sponsored hacking or propaganda from extremist groups, including multiple high-profile data breaches that were detrimental to journalists and researchers.

The most pervasive threat to collective action is online misinformation, especially fake news, which often spreads through social media and messaging applications. For example, AI tools were used to generate deepfakes during the 2024 Indian general elections, targeting candidates and public sentiment. As India anticipated this threat, it also launched a Deepfakes Analysis Unit (DAU) in partnership with other agencies as part of the Misinformation Combat Alliance. This included a WhatsApp tipline for the public to flag questionable or fake media. DAU has, since March 2024, analysed hundreds of media files, corroborating the widespread use of synthetic media generally, and the Global Risk Report lists AI-aided misinformation as one of the greatest short-term global risks identified by the World Economic Forum (Raina, 2024).

4.4.1 AI in Defence:

Generative AI will play a significant role in countering cyberterrorism, misinformation, or disinformation. Machine learning can detect not just botnets and fake accounts but also coordinated misinformation campaigns using graph-based ML. News authenticity can be classified by NLP models, especially transformer models. For deepfakes, machine vision and audio signal processing can identify visual/audio discrepancies by using convolutional neural networks (CNNS) and autoencoders. Some nations have systems that can verify the associated digital signatures of valid content. Like in cyberterrorism, adversaries also utilise generative AI (e.g., to fake a speech or video). The most feasible approach appears to be DAU's hybrid model—AI with a human review process—and researchers are beginning to explore explainable AI (XAI) explicitly to justify why flagged content is false and to build user trust.

4.4.2 Legal Framework:

Cyberterrorism can be prosecuted under Section 66f of the IT Act for threats to national sovereignty, in combination with the Unlawful Activities (Prevention) Act (UAPA) for activity traceable to prohibited or banned organisations. Prosecutions are rare due to the challenge of attribution. Misinformation (rather than disinformation) can be prosecuted under the IT Rules, 2021, where deepfakes are criminalised, and false news likely to disturb public order is penalised. India has been monitoring global trends such as the EU AI Act and seems poised to adopt similar mandates for transparency and explainability in AI systems. Additionally, the amended Cinematograph Act of 2023 allows oversight of AI/automated content in media and penalises its unethical use during elections (Ministry of Information & Broadcasting, 2023).

4.5 Child Pornography and Online Grooming

The issue of child online sexual exploitation is a rising and serious concern in India. Evidence shows that, despite a decrease in other reported cybercrimes, the National Crime Records Bureau (NCRB) Cyber Crime Circular documented a staggering 32% increase in crimes against children in 2022, with 1,823 reports—up from 1,376 in 2021 (Das, 2024). Of these, 1,171 were related to child pornography, while 158 were identified as cases of cyberstalking or cyberbullying. The pandemic significantly heightened children's exposure to online predators, as they were often unsupervised while engaging with digital platforms. Groomers increasingly use gaming and social media platforms, adopting fake identities to initiate contact and groom children on personal devices. Additionally, incidents of abuse on live-streaming platforms have given predators real-time access to minors, further complicating detection and prevention efforts.

4.5.1 AI in Defence:

AI plays a key role in child protection, especially in detecting child sexual abuse material (CSAM). Tools such as Microsoft PhotoDNA use image hashing to match and identify known CSAM across platforms (Gregoire, 2024). Globally, deep learning image recognition systems are being trained to detect new or altered abusive content based on visual features. On messaging platforms, Natural Language Processing (NLP) and network behaviour analysis are helping flag suspicious behaviour, such as repeat contact attempts by groomers. Projects like Project Arachnid and global nonprofit efforts (e.g., NCMEC) are actively scanning and removing CSAM from the internet. While precision in CSAM detection continues to improve, ethical constraints remain, and predators continue to use new methods of spreading illicit material (Shankari, 2024).

4.5.2 Legal Framework:

India already has specific legislation to protect children from online sexual exploitation (COSE). The Protection of Children from Sexual Offences (POCSO) Act, 2012, criminalises all forms of child sexual abuse, explicitly recognising that minors cannot legally consent to any form of sexual activity. Additionally, the Information Technology Act includes Section 67A, which penalises child pornography, and the Indian Penal Code's Section 292 prohibits the distribution of obscene material. The Cinematograph (Amendment) Act, 2023, introduced jurisdictional oversight and restrictions for explicit content in cinema and OTT platforms. Enforcement primarily remains under the IT Act and the POCSO Act. While Fast Track Courts provide a mechanism for prosecution, most CSAM is hosted abroad, making cross-border cooperation essential. Government agencies like CERT-In and NGOS continue to raise public awareness and push for more comprehensive and technologically relevant protections.

4.6 Intellectual Property Theft and Digital Piracy

Rampant piracy is a battle that India's creative and software industries are wrestling with, especially in the media and entertainment sector. By way of context, the estimated losses to the media and entertainment sector through piracy, related to doing

illegitimate things with the online distribution of film, music, and streaming, is approximately ₹22,400 crore (~$2.7 billion), according to the EY-IAMAI 2023 report (PTI, 2024). More than 50% of Indian internet users confessed to consuming pirated media, and those who did report piracy did so due to high subscription fees and/or unavailability of content. Piracy creates a parallel economy that robs the media of revenue.

4.6.1 AI in Defence:

AI is being deployed to tackle digital piracy. With ACR or Automated Content Recognition, platforms can scan and find copyrighted content on P2P (peer-to-peer) networks. AI-powered digital watermarking and fingerprinting can embed invisible identifiers that are used to specify ownership in content items to assist in importing from abroad and provide evidence of an infringement. For platforms like YouTube and Meta, AI can also help identify copyright violations by flagging items posted by users that appear similar to or identical in content, style, and sequence, and copyright-protected materials. In the software industry, machine learning is being used for binary similarity detection to determine pirated software. There are also experiments using blockchain that can record or verify original works from original creators via a distributed ledger that enables some level of IP protection.

4.6.2 Legal framework:

As for the existing legal framework, India's Copyright Act, 1957 includes civil and criminal penalties for copyright owners, and the Cinematograph (Amendment) Bill, 2023 criminalises the unauthorised recording of movies in theatres, but also the platforms that host pirated content (Ministry of Information & Broadcasting, 2023). The enforcement mechanisms of blocking websites, raiding streaming services, or finding the service and shutting it down are done through the work of Anti-Piracy Cells. However, enforcement of piracy using copyright law remains fraught with obstacles such as jurisdictional issues for piracy across borders, the anonymity of infringers, and consumer/user reluctance to engage with enforcement mechanisms. On the positive side, the industry and government are aware of the demand for piracy and cognizant of its implications. The SIGN conference and many other initiatives are working to provide information on legitimate streaming. The EY report also highlighted the importance of collaboration and that copyright law should be amended to reflect a balance between stakeholders in the art space, artists, content creators, film, music, and streaming platforms, and protect vulnerable stakeholders.

V. Challenges and Limitations

India has made advances in fighting cybercrime, stimulated by decreased inhibitions in policing and prosecution. However, the difficulties are significant, especially in terms of influencing balances and applying AI responsibly and in ways we accept. Below are the highlighted issues:

5.1 Legal and Enforcement Gaps

India's Information Technology Act and the Indian Penal Code have, at times, been described as been constructed and up to date, as vague legislation. For example, the IT Act is outdated and does not create clear pathways for new technologies (AI, cryptocurrencies). Relevant policing capacities are limited in trained cyber-police and forensic officers. Jurisdictional problems arise when crime is multi-jurisdictional. Privacy versus surveillance creates a dilemma, where strong encryption can protect the user but hinder investigations. The new DPDP Act allows government agencies to avoid certain requirements of privacy (Lawton, 2023) and presents trade-offs between security and privacy.

5.2 Technological Arms Race

As defenders assess AI, so do attackers. Generative AI allows the creation of new threats (phishing, deepfakes, etc.), which means we will have to constantly evolve defensive, adaptive, and detection methods. AI systems can also be biased or duped by adversarial examples (small perturbations that confuse classifiers). For instance, an image detection AI may pass an image on CSAM just because it was slightly perturbed. It is difficult to ensure that AI models are trained and updated with realistic training data that represents threats properly.

5.3 Data and Awareness

AI is only as effective as good data. In India, the absence of datasets that have been labelled for the local languages and contexts (e.g., hate speech in Hindi, Tamil, etc.) makes it extremely difficult to train models. The awareness regarding cyber risks is not equal, and the fact that most citizens have fallen for even basic social engineering scams due to a lack of digital literacy. If agents have weak awareness, they will not report something in a timely manner, which reduces the potential for prevention.

5.4 Infrastructure and Scale

India is too large (hundreds of millions of users), and therefore, cyber-defences need to be operated at scale. Other than large cities, smaller cities and even villages do not have cybersecurity infrastructure. The payment systems and telecom networks may be robust, but they may create single points of failure (as we saw with the C-Edge ransomware incident)(Kalra, 2024).

5.5 Ethics/Bias

An adherence to the rights of all individuals is complex if AI tools are used for surveillance and/or censorship. For example, automated content filters can over block free speech. Issues of bias persist in AI models: if there is bias in the training data, the model may unfairly flag certain communities (a known issue regarding hate-speech detection). Questions of adequate audits of AI tools could be complex, especially since India does not have a comprehensive set of AI governance frameworks (although whoever may propose an EU AI Act will likely influence regulation in India).

All in all, AI and digitisation are useful and powerful defenders. Nevertheless, they also introduce other vulnerabilities and ethical dilemmas. Importantly, the use of technology to shield and protect Indo-Pacific countries from violent extremism and other illicit activities must be deliberate and responsible. Successful navigation of these trade-offs will require robust interdisciplinary teams made up of technologists, legal experts, and civil society.

VI. FUTURE DIRECTIONS

In the future, there are multiple promising pathways we can explore for increasing India's cyber resilience, while also facilitating ethical AI use:

6.1 Artificially intelligent detection that evolves

Ongoing work on AI models that detect threats is needed; this can be associated with multimodal generative AI systems that consider images, text, and network data simultaneously, and advanced (what will be) unsupervised and continuous learning processes to help identify the unknown. Additionally, the researchers will have to build and keep up with explanations about AI-based systems (eXplainable AI (XAI)) in order to give human analysts context for understanding the rationale behind decisions made by a model. The researchers may additionally investigate federated learning processes to have models built collaboratively with banks and businesses (where protected information is not shared).

6.2 Legal and Policy Change

The development of new laws shifts as new technologies emerge; this is a key aspect of an evolving cybersecurity ecosystem. For example, there may be explicit criminal statutes that help hold people criminally responsible for misadventures with artificial intelligence, or for digital extortion and cryptocurrencies. New laws are being developed to define data privacy laws that attempt to juggle innovation and protection, along with lessons learnt from the existential muddle on GDPR (General Data Protection Regulation) that evolved. Countries collaborating together going forward (cyber diplomacy) is going to be increasingly more significant; India should do everything possible to work on forming global cyber behaviours (e.g., consensus agreements from the UN on cyber agreements and digital trade pacts).

6.3 Public-Private Partnerships

The majority of the infrastructure to date is in the hands of the private sector (ISPS, cloud service providers). Ongoing partnerships can be developed to maximise threat intelligence (the government facilitating shared threat intelligence) and industry-sponsored open databases (on open platforms / finding common interest fields such as 'libraries' of malware and hate speech corpus). An example is India's DAUS, which posts a public tipline on WhatsApp (Deepfakes: How India is tackling misinformation during elections | World Economic Forum) in maintaining a collaborative system and uses a public-private model. Future developments may include competitions to crowdsource and the building of new detection algorithms.

6.4 Capacity Building and Awareness

More training and education are needed for the professionals and workers who are engaged in the cybersecurity ecosystem (law enforcement, judiciary, IT professionals). As cybercrime grows in India, new educational and training initiatives can play a role in reducing vulnerability. Education in schools at a local level, along with public information campaigns (including media campaigns), creates a vulnerable society. Initiating cyber ranges and running simulation drills can prepare institutions for possible attacks.

6.5 Responsible AI Governance

India is at the beginning stages of its AI policy framework and should build regulations similar to the proposed EU AI Act — including risk assessment, transparency, and continued human accountability for previously identified high-risk AI systems (Deepfakes: How India is tackling misinformation during elections | World Economic Forum) While the regulatory terms will need to be modified for a local context, governments and companies will need guidelines for auditing and mitigating AI related bias, specific to security applications.

6.6 Technology Innovation

New technologies can also provide strength to security. As quantum computers are being built, we already need quantum-resistant cryptography. Blockchain-based identity systems may lessen fraud (make identity harder to manipulate). Researchers are also working on potential solutions, such as having AI-driven cyber patrol bots/personal assistant bots, and using honeypots/tokens to bait attackers. All of these initiatives can be transformed into tools in the fight against cybercrime, alongside India's growing pool of talented tech professionals. Ongoing research (including maintenance/quality meta-analyses and benchmarks located in India) can provide meaningful evidence-based policy directions.

VII. CONCLUSION

Cybercrime in India is a complex problem at the frontier of technology, law, and society. Our meta review finds that as India increases its digital footprint, the scale and sophistication of threats increase. From a legal framework, India has made strides, alongside sometimes daunting AI-based defences, but it is important to recognise shortcomings. Today, the main threat is around financial cyber frauds (Manral & Sinha, 2023) (BGandh, 2023), but there are myriad examples of emerging threats around the corner, such as deepfakes, ransomware (e.g., AIIMS), and online child exploitation (including child exploitation via gaming). As a dual-use technology, AI is a weapon for criminals and a shield for victims: while the vulnerability of advanced machine learning is essential for detecting phishing, malware, and unwanted content, criminals innovate through adversarial use of AI.

We place high importance on the technical innovations being matched with appropriate, strong policies. New schema building la ws to fortify the IT Act enforcement and encourage laws around cybersecurity education will need to be both resourced and maintained. Improving capabilities in cybersecurity is essential, as is collaboration across borders. Last but not least, responsible development and innovation for AI, with considerations to ethics and bias, will determine whether such technology can enhance security at all.

In conclusion, a moment of reckoning for India! With state-of-the-art AI and contingency planning in a framework that promotes protection, as well as advocacy/ awareness of the background context of digital crime, India can make strides in countering crime online. We provided details on current trends, rich case studies and/or programmes, and new research possibilities; now it is up to legislators, the private sector, civil society, and researchers to take action!

REFERENCES

[1] Ministry of Home Affairs (India), "Increase in Cyber Crimes" (Press Release), 7 Feb. 2024. Available: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505 (Press Release: Press Information Bureau).
[2] M. S. Manral and J. Sinha, "24% rise in cybercrime in 2022, 11% surge in economic offences: NCRB report," The Indian Express, 4 Dec. 2023.
[3] A. Sur, "CERT-In tackled over 1.39 million cybersecurity incidents in 2022: Annual report," Moneycontrol, 15 Nov. 2023.
[4] M. Das, "Child cyber crime surges 32% reveals NCRB data, underlining vulnerability to online risks," The Times of India, 26 Jan. 2024.
[5] M. M. Graham, "Deepfakes: Federal and state regulation aims to curb a growing threat," Thomson Reuters Institute (Legal Insight), 26 Jun. 2024.
[6] C. Gregoire, "Microsoft's Photodna: Leading the Fight Against Child Sexual Abuse Imagery," Thorn Blog (accessed Apr. 2024).
[7] I. Gupta, "UPI Fraud Up by 85% in FY2023- 24: Finance Ministry Data Reveals," Medianama, 26 Nov. 2024.
[8] G. Lawton, "What is the Digital Personal Data Protection Act, 2023?" TechTarget, 25 Aug. 2023.
[9] Ministry of Information & Broadcasting (India), "Parliament Passes Cinematograph (Amendment) Bill, 2023" (Press Release), Press Information Bureau, 31 Jul. 2023.
[10] S. Parasnis, "China Backed Hacker Group Behind 2022 AIIMS Attack: Report," Medianama, 27 Jun. 2024.
[11] M. Safi, "Reporter who exposed India data breach named in criminal complaint," The Guardian, 9 Jan. 2018.
[12] Economic Times, "Indian Railway Data Leak: 30 million Railway customers' data for sale on the dark web," 28 Dec. 2022.
[13] ETBFSI Research, "UPI frauds: Indians lose Rs 2,145 crore across 2.7 million reported incidents since 2022-23, says govt," The Economic Times (BFSI), 28 Nov. 2024.
[14] PTI, "Indian entertainment industry lost Rs 22,400 crore to piracy in 2023: EY-IAMAI report," The Times of India, 23 Oct. 2024.
[15] CERT-In Annual Report 2022, "CERT-In tackled 1,391,457 incidents" (Moneycontrol summary), 15 Nov. 2023.
[16] A. Sharma, "13 lakh cyber attacks hit Indian banks in 10 months; Who is behind them?" India Today, 29 Dec. 2023.
[17] J. Kalra, "Ransomware attack forces hundreds of small Indian banks offline," Reuters, 1 Aug. 2024.
[18] P. Raina, "Year of elections: Lessons from India's fight against AI-generated misinformation," World Economic Forum, 6 Aug. 2024.
[19] CyberPeace Foundation, "Research Report: AI-Driven Phishing Attack on a Financial Institution in India (2024)," 2024.
[20] E. Shankari, "Protecting children from online CSAM," Shankar IAS Review, 2024.