Cyber Crime in India

Mr.Vitthal B. Nesarikar[1], Dr. Piyush Maheshwari[2]
[1]*Research Scholar at Chhatrapati Shivaji Maharaj University, Navi Mumbai, Maharashtra, India*
[2]*Assistant Professor at KLE College of Law, Navi Mumbai, Maharashtra, India*
[2]*Assistant Professor at Chhatrapati Shivaji Maharaj University Navi Mumbai, Maharashtra, India*

***Abstract*—As India solidifies its position as a global digital economy, the landscape of cyber threats has transitioned from simple phishing to sophisticated, AI-driven psychological warfare. This paper examines the surge in cybercrime—recording a 24% spike in 2025—and analyzes the socio-legal response through the IT Amendment Rules, 2026. It explores the "industrialization" of cybercrime, specifically focusing on digital arrests, investment scams, and the weaponization of deep fakes.**

I. INTRODUCTION

With over 86% of Indian households connected to the internet by 2025, the "attack surface" has expanded beyond urban hubs into Tier-2 and Tier-3 cities. In 2025 alone, India recorded 28.15 lakh cybercrime cases, with financial losses totaling approximately ₹22,495 crore. The emergence of "Cyber-Slave" compounds in Southeast Asia has further globalized the threat to Indian citizens.

Cyber crime is one of the most common crimes worldwide, the criminals used advanced technology and the victims sometimes unaware of the loss caused to them. As compared to traditional crime committing of cyber crime is easier because face to face meeting with the victims are not necessary. Sometimes, when the victims find out the criminal activities happened to them many days has gone and it is burdensome to track the culprit as this type of crime does not have definite space or area. As crime is committed through computer or computer devices, it is difficult to catch the criminals red handed and the actual crime rate is difficult to record by the officials. The data provided by various agencies are only those reported by the victims and targeted person; it is undoubtedly true that the actual numbers of cyber crime incidents are much higher than the total reported case.

NATURE OF CYBER CRIME

There is no universal accepted definition of cyber crime. The term is used to describe criminal activity in which computers or computer networks are a tool, a target, or a place of cri minal activity and includes everything from electronic cracking to denial of service attack.7 One distinct nature of cyber crime is it could easily be committed from anywhere without physically reach the victim and no eyewitnesses is needed. Physical violence and physical harm are not required. It may also be committed without the knowledge of the victim, but leaving him totally incapacitated at the same time. In many cases the victim recognizes the crime only after a huge loss or continual commission of crimes by the criminals.

CLASSIFICATION OF CYBER CRIMES

On the basis of the nature and purpose of offence, cyber crime may be broadly classified into three categories:

1. Cyber crime against individuals
2. Cyber crime against property
3. Cyber crime against society at large

1.The first category relates to which the effect mainly caused onto individuals or persons, some examples are:

• Harassment via e-mail - This type of cyber crime does not physically harm the victim but it may cause psychological harm and mental torture. It may be committed by sending unwanted, offensive, or intimidating electronic mails to another person.

• Cyber stalking – This is also known as ‘cyber teasing’. It involves following a person through various applications by using internet connection. It is an online course of conduct of a person by which the targeted person is terrorized, embarrassed, ashamed, molested, outranged of frightened. The

most common platforms used by the criminals are – Facebook, Instagram, X (previously known as twitter).

• Cyber defamation – Cyber defamation occurs when defamation takes place with the help of computer or by using internet. It has a deep negative impact as compared to traditional type of defamation because the criminals may easily spread defamatory matters widely by using internet connection. The results not only hurt the victim but it may harm their reputation forever.

The second category which is called as cybercrime against property does not caused direct harm to the individuals, but it greatly affect the property of the victims which results in a great loss due to the criminal acts. Some examples are –

Chaubey, M.K. (2017). Cyber Crimes & Legal measures. Regal Publications.

II. CURRENT TRENDS AND STATISTICS (2025-2026)

Metric	2024 Statistics	2025 Statistics
Total Reported Cases	22.68 Lakh	28.15 Lakh
Total Financial Loss	₹22,845 Crore	₹22,495 Crore
Leading Threat	Phishing/UPI Fraud	Investment Scams (76% of loss)
New Major Vector	Malware	AI-Deepfakes & Digital Arrests

III. CASE STUDIES: THE NEW FACE OF FRAUD

Digital Arrest Scams: Fraudsters use AI-generated voices and "virtual police stations" to simulate law enforcement environments, coercing victims into transferring funds to avoid "immediate arrest."

Investment & Trading Scams: These accounted for over 75% of total financial losses in 2025, fueled by high-inflation environments and the promise of quick returns via unverified trading apps.

The Cambodia-Vietnam Corridor: A significant portion of 2025-2026 frauds originated from organized syndicates in Southeast Asia, where individuals are often trafficked to work in "scam factories."

IV. LEGAL FRAMEWORK & THE 2026 AMENDMENTS

The Indian government has responded with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026. Key features include:

Synthetic Media (Deep fakes): Platforms must remove non-consensual deep fakes within 2 hours of reporting.

Mandatory AI Labeling: Any AI-generated content that appears "indistinguishable from reality" must carry a prominent label.

Takedown Timelines: General illegal content must now be removed within 3 hours (down from 24-36 hours).

Loss of Safe Harbour: Intermediaries failing to act on "SGI" (Synthetically Generated Information) lose legal immunity under Section 79 of the IT Act.

V. CHALLENGES IN ENFORCEMENT

Despite the I4C (Indian Cyber Crime Coordination Centre) blocking over ₹8,031 crore in fraudulent transactions, challenges remain:

Low FIR Conversion: In 2025, while 28 lakh cases were reported, only ~55,000 resulted in formal FIRs due to jurisdictional complexities.

The Forensic Gap: A shortage of trained cyber-forensic experts at the local police station level leads to backlogs in digital evidence analysis.

Mule Account Networks: The rapid siphoning of funds through layers of "mule" bank accounts across different states makes recovery difficult.

Indian cyber laws are primarily governed by the Information Technology (IT) Act, 2000 (amended 2008) and the new DPDP Act 2023, targeting crimes like hacking, fraud, and data theft. Key reporting mechanisms include the National Cyber Crime Reporting Portal (cybercrime.gov.in) and the 1930 helpline for financial fraud.

Key Indian Cyber Laws & Regulations

Information Technology Act, 2000: The primary law dealing with cybercrimes (Sections 65-75), including tampering (65), identity theft (66C), cheating by impersonation (66D), and child pornography (67B).
Digital Personal Data Protection Act (DPDP), 2023: Regulates personal data processing, requiring organizations to report data breaches.
IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: Mandates social media accountability to remove unlawful content.
Bharatiya Nyaya Sanhita (BNS): Replaces IPC, covering traditional crimes enacted through digital means.

How to Report Cyber Crime in India

National Cyber Crime Reporting Portal: Visit cybercrime.gov.in to report any cybercrime, with a special focus on crimes against women and children.
Helpline Number: Call 1930 to report financial frauds to initiate quick action against fraudulent bank accounts.
Local Police Station: File an FIR at the nearest police station if a prompt response is needed. Social Media Platforms: Use the reporting mechanism on platforms (Facebook, X, Instagram) for taking down offensive content.

Key Reporting Provisions & Guidelines

Evidence Collection: Maintain records of emails, chats, screenshots, URLs, and banking transactions.
Responsibility: The Indian Cybercrime Coordination Centre (I4C) under the Ministry of Home Affairs coordinates these efforts.
Reporting Timelines: Organizations must report incidents swiftly to minimize damage and comply with regulatory requirements.

Commonly Reported Crimes

Financial Fraud: OTP scams, UPI fraud, and banking phishing.
Cyberstalking/Bullying: Harassment over digital platforms.
Identity Theft: Stealing personal data for fraudulent activities.
Sextortion: Blackmail using explicit photos/videos.

VI. CONCLUSION

The battle against cybercrime in India has moved beyond technical firewalls into the realm of public psychology and rapid regulatory intervention. While the 2026 IT Rules provide a robust framework against AI-driven threats, the "Way Ahead" must include mandatory e-FIR systems and international treaties to dismantle cross-border scam syndicates.
The third category is cyber crime against the society at large. In this type of crime the intention of the cyber criminals are threatening the Government or organizations as a result to fulfilling their demand.
Those crimes mainly affect not a single individual but the society as a whole.Cyber terrorism against the Government organization is the most common crime under this category. In cyber terrorism, a particular is not affected but it has its vicious impact on the community at large. This is a matter of global concern having both domestic as well as international implications. Distribution of pirated software from one computer to another with an intend to destroy the data and official records of the government and accessing important information of Government or Organizations are the common types of crime under this category.

CYBER CRIME AND INDIAN SOCIETY

India witnesses various developments in communication and Information Technology. This also brings enormous growth in economy and financial status of the country. However, this technologicalimprovements result in various criminal activities. India was placed on the 80th position in a report focusing on local threats in the year 2023.12 Judiciary in India plays a significant role by various judicial pronouncement and many culprits are serving their punishment according to the relevant laws.
State of Tamil Nadu v. Suhas Katti13 is the first case in India to set a benchmark on cyber harassment.
This case was filed by a woman on the grounds of being harassed and getting obscene messages on various groups with the intention of offending her, which was sent by the man who was very keen in marrying her but she rejected him for which that person then started sending these kinds of obscene
messages. The case involved questions of cyber chase/stalking and harassment of women. After taking all relevant evidences the Court convicted the accused under Sections 469 and 509 of Indian Penal Code,
1860 and Section 67 of the Information and Technology Act, 2000.
9 Paranjape, V. (2023). Cyber Crimes & Law. Central Law Agency.

10 Explanation (ii) to Section 43 of Information Technology Act, 2000.
11 Explanation (iv) to Section 43 of Information Technology Act, 2000.

GOVERNMENT INITIATIVES

Progress in technology in turn results to threats in cyber space. The rapid changes and digitization of various sectors paved ways for cyber criminals to commit crimes not only to individuals but also to exploit and steal valuable data of the Government and organizations. The Indian Government feels the urgency to take positive efforts to battle this serious crime by providing various steps to mitigate the rising trends of cyber threats. Brief analyses of different Government initiatives are discuss below:

Information Technology Act, 2000:

The Information Technology Act, 2000 is the first and only Act passed by the Indian parliament which deals with electronic commerce and different modes crimes committed by the cyber criminals. This Act aimed to provide legal recognition for transaction carried out by means of electronic data exchange and other means of electronic communication, commonly referred to as 'electronic commerce' which involve the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing documents with the Government agencies.17 The Act is comprises with 13chapters spread over 94 sections and 4 schedules. After enforcing the Information Technology Act, 2000 four related important Acts – The Indian Penal Code, the Indian Evidence Act, the Banker's Books Act and the Reserve Bank of India Act were amended.

14 Cyber Case No. 21 of 2021
15 CS(OS) No. 1340 of 2012
16 Crl. Rev. P. 124 of 2013
17 Mishra, J.P. (2014). An Introduction to Cyber Law. Central Law Publication.

International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com
IJFMR250665035 Volume 7, Issue 6, November-December 2025 6

Information Technology (Amendment Act) 2008:

When time comes new methods of cyber crimes were committed by the criminals and various new techniques becomes relevant in the information communication world so that some provisions of the Information Technology Act, 2000 becomes ineffective to the present conditions. Therefore, the Information Technology (Amendment) Bill was passed by Lok Sabha on 22nd December, 2008 and by Rajya Sabha on 23rd December, 2008. The amended Act has omitted several sections, substituted for some other sections, expands the definition of cyber crime and new penalties for some offenses were added. Establishment of the Indian Computer Emergency Response Team (Cert-In):

The Indian Computer Emergency Response Team (CERT-In) is the Indian Government's established nodal agency to response computer security incidents as and when they occur. This agency is situated inside the Department of Information and Communications Technology. The main objective of this agency is establishment of incident response as provided under Section 70B of the Information Technology Act, 2000. Operating a 24x7 incident response Help Desk, CERT-In ensures timely responses to reported cyber security incidents. The organization offers comprehensive Incident Prevention and Response services alongside Security Quality Management Services to enhance cyber security measures across the nation. The CERT-In plays an imperative role in safeguarding India's cyber landscape. According to the Information Technology Amendment Act, 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Co-ordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed.

The Indian Computer Emergency Response Team (CERT-In) since its operation in the year 2004 has registered several cyber crimes cases. The following table shows the cases registered by the agency during the last three years –

Table 1: Cases Registered by the Indian Computer Emergency Response Team between 2021 - 2023 Sl. No. Year Phishing Incidents Network scanning and probing Virus/Malware incidents Website hacking incidents cyber